**Chapter 3: Disasters, Emergencies and Infrastructure Protection**

This chapter covers a number of connected areas that can be treated together. In the broadest sense, we are concerned here with disasters, emergencies and risks that occur within the countries covered in our analysis. In contrast to the previous chapter, the nature of these threats and disasters tend to be of a natural character although they may be exacerbated by human action. In contrast to the next chapter, these are matters within a given territory, of a domestic or transborder character rather than international interventions seeking to provide assistance to poorer states. The chapter examines a range of strategy documents and policy papers to get a feel for the types of issues and actions being discussed by policy makers as well as considering what reasons, strategies or motives lie behind these approaches and whether different countries and organisations have different approaches or motivations.

The baseline is provided by the UK case which, while addressing technical issues like infrastructure provision, maintains the focus on individual and community resilience. The US approach is found to have a similar emphasis in contrast to France and Germany where discussion of resilience is emerging, but where the idea of community resilience is largely absent. The chapter also gives extensive coverage to EU discussions of resilience since this is a significant area of developing debate across Europe.

**The UK approach to critical infrastructure protection and emergency preparedness**

This time we start the chapter with the UK approach to resilience, drawing on the vast amount of material available on UK government websites. As mentioned in the introduction, the focus of this chapter is not on specific areas such as climate change, flooding or telecommunications policy, but on critical infrastructure protection and emergency response in a more general sense. In the UK’s case, and following on from the findings of the previous chapter, the intention is to link these to community resilience. The UK sections will proceed by setting out the British government’s approach to infrastructure protection and emergency response, to examine key ideas like preparedness, and to move to the promotion of community resilience in dealing with some of the issues raised.

The UK government defines critical infrastructure as ‘those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends’ (Cabinet Office 2010c: 8). It also talks of Critical National Infrastructure (CNI) as: ‘Those infrastructure assets (physical or electronic) that are vital to the continued delivery and integrity of the essential services upon which the UK relies, the loss or compromise of which would lead to severe economic or social consequences or to loss of life (Cabinet Office 2010c: 8.). CNI covers nine areas - energy, food, water, transportation, communications, emergency services, health care, financial services and government.

In response to flooding in 2007 and the subsequent Pitt Report, the UK government set about establishing a cross-sector programme to improve critical infrastructure resilience in the face of natural hazards. In particular, the government launched the Critical Infrastructure Resilience Programme aimed at encouraging a better co-ordinated and more systematic approach to critical infrastructure and essential services. This would clarify the roles of the government, public sector bodies and private service providers and businesses. Relevant government departments would work with the private sector infrastructure operators to build resilience into critical infrastructure assets and to encourage business continuity (Cabinet Office 2010c: 5-6).

The Pitt Recommendations were agreed as necessary for guaranteeing a minimum interim standard of protection from flooding for critical national infrastructure across all sectors with further consideration of matters of cost, practicality, scale of activity and impact on owners. Considerations require taking into account probability of occurrences, severity, vulnerability and impact. Focusing on the promotion of resilience, this is defined in the Pitt Report as ‘the ability of a system or organisation to withstand and recover from adversity’ but suggests that the importance of protection must be balanced against the need to reduce the impacts of failure. In other words, this should not be protection at all costs. The UK government’s response stresses the need to balance investment in critical infrastructure protection with the needs of emergency response and recovery capabilities. It stresses interdependencies within and between sectors ‘in an increasingly networked society’ (Cabinet Office 2010c: 7). The government’s role is to build resilience into infrastructure provision and to ensure continuity of supply through such things as better designed assets, building additional network connections, providing backup facilities to ensure continuity, moving key components out of harm’s way, better sharing of information on infrastructure network performance and standards and enhancing skills and capabilities to respond to emergencies (Cabinet Office 2010c: 7).

The Cabinet Office is responsible for developing a cross-sector resilience-building programme and for coordinating this across different government departments and the public and private sectors. Flooding is the first natural hazard to be considered by these plans based on its place as the highest identified risk in the government’s National Risk Register. Other natural hazards will be considered as the approach develops. Despite the focus on natural hazards, the programme will also seek to work with those dealing with other national security threats, particularly the CONTEST counterterrorism strategy that was discussed in the previous chapter. A wider strategic framework – CNI Protection in the UK: Framework and Guidance – seeks to provide the common basis for all those involved in national infrastructure protection ranging from natural hazards to counterterrorism. Shared procedures will be developed where possible in order to provide a coherent approach to resilience across all sectors. The Critical Infrastructure Resilience Programme will also coordinate its activities with the Adapting to Climate Change Programme to meet the longer-term obligations of the Climate Change Act, and will work with Infrastructure UK to enable long-term planning and investment in infrastructure and delivery.

The Critical Infrastructure Resilience Programme can be seen as an example of the UK government promoting better communication, cohesion and planning across different sectors of government, society and infrastructure. It aims to reduce the most substantial risks, assess vulnerability and minimise disruption, providing a shared framework for cross-sector activity. It seeks to enhance collective capacity to absorb shock and respond quickly and to improve engagement and information sharing to ensure effective emergency response (Cabinet Office 2010c: 9). It argues for a ‘joined-up’ approach involving other government programmes including protection against terrorist attacks and climate change. The emphasis on cohesion is also evident in the focus on the government’s relationship the infrastructure owners and the relevant regulator. Voluntary cooperation is the preferred means of achieving shared aims, but stricter legislative powers will be employed if necessary. Governance from a distance will also be supported by monitoring techniques including setting standards and timeframes, developing a programme of measures for achieving the defined level of ambition, mechanisms for reporting progress on the implementation of the programme and a process for benchmarking business continuity plans **(**Cabinet Office 2010c: 7).

Alongside the Critical Infrastructure Resilience Programme we find the National Resilience Capabilities Programme (NRCP). This broader programme covers most types of civil emergency including accidents, natural hazards and human-made threats. As the name suggests, the aim is to build capability to deal with such emergencies with the main focus on response. This means ensuring such things as proper training, right equipment and supplies, clear plans and so on. As with other UK approaches to resilience, there is a strong emphasis on monitoring and information gathering which will be fed back into government understanding of the UK’s ability to respond to civil emergencies. The programme consists of capability ‘workstreams’ dealing with central, regional and local response capabilities in areas of essential services such as food, water, fuel, transport, health and financial services. The programme tests for resilience in these areas based around a series of exercises and training, while identifying what central government might do to increase resilience capabilities.

The Programme concentrates on building public awareness. A well-informed public, it is argued, is better able to respond to emergencies and minimise the impact these have on the community. Informing the public is also important in building trust. In many cases it will be the government that will first provide warnings and information for the public, but the NRCP is designed to responsibilise other organisations and local actors who must help raise awareness about risks and emergencies, establish procedures for dealing with emergencies should they occur and undertake risk assessment. The latter aspect is supported by the National Risk Register (NRR), first published by the government in 2008 in response to the National Security Strategy. This helps to provide advice on how people and businesses can prepare for civil emergencies while the NRCP aims to ensure that organisations have in place the necessary arrangements to inform, advice and warn the public.

In these programmes and practices we see certain strong features of the UK’s resilience approach. These can be said to entail a coordinated approach that strives to provide an effective and cohesive response, an emphasis on communicating with the public, responsiblisation of local actors and organisations, the policy of subsidiarity whereby response should be coordinated at the lowest level where possible, and an emphasis on preparedness. In its guidelines on emergency response and recovery, the UK Cabinet Office talks of how ‘all organisations and individuals that might have a role to play in emergency response and recovery should be properly prepared and be clear about their roles and responsibilities’ (Cabinet Office 2013a). This is consistent with our arguments for governmentality, indicating how government policy is devolving responsibilities and the engaging a range of actors at different levels. Subsidiarity seeks to do this at the lowest appropriate level, supported by government coordination where necessary. The government’s role is to ensure that there is clarity of purpose and that supporting objectives that are agreed, understood and sustained by all involved. In the rest of this section we will set out in more detail, how the role of government, in securing integration, effective coordination, cooperation and continuity is to be achieved. Having set out the role of government and the process by which other actors are responsibilised (and governmentalised), the next section will concentrate on setting out the UK government’s attempts to build community resilience in this particular area of policy making.

For all the talk of community resilience, it is absolutely the case that central government continues to play the dominant role as we saw in the last chapter. The Home Office is the lead department for terrorist related emergencies while other government departments will offer support for the wider impacts. The Cabinet Office works to clarify responsibilities. If these are unclear, it will advise on the lead government department. The responsibilities of the Cabinet Office itself include working with local and regional partners in emergency planning and government coordination, maintaining continuity of central government, ensuring a Lead Government Department is in place and providing staff to run crisis facilities (Cabinet Office 2013b: 19-20). In turn, Lead government Departments must maintain a state of readiness for responding to emergencies, planning, training and exercising and engaging in other preparatory work, while identifying other departments and agencies whose assistance might be needed. They should identify the capabilities of local responders and maintain awareness of the risks, threats and vulnerabilities within each field of responsibility.

Within the Cabinet Office is the Civil Contingencies Secretariat (CCS). This takes the lead initially, before the responsible Lead Government Department takes over. The Cabinet Office will then continue to provide support to Lead Government Departments during the planning, response and recovery phases. It promotes resilience-building through engaging key players and promoting the aims of anticipation, assessment, preparation, prevention, response and recovery as part of an integrated response to emergencies (Cabinet Office 2004a:12). Anticipation and assessment requires the conducting of risk assessments covering both long-term and shorter-term challenges (horizon scanning). As a result of the assessment of the risks, prevention measures are adopted including strategies for reduction or redistribution of risk. Preparedness plans require flexibility towards risk and unforeseen events, identifying key personnel, assets and arrangements (Cabinet Office 2004a: 9). Following response, the recovery phase is rooted in the community and requires interaction among a variety of government departments and local agencies. Throughout this, the CSS plays a key role in the gathering of information including identifying risks based on stakeholder and local knowledge, identifying assets, resource requirements and procedures, identifying relevant legislation and regulations and promoting best practice and learning lessons from previous incidents. The CSS is responsible for the National Resilience Capabilities Programme discussed earlier (Cabinet Office 2004a:21).

Moving to other responders, the government classifies these as Category 1 organisations that form the core response to most emergencies and Category 2 organisations who are ‘cooperating bodies’. Category 1 organisations include the emergency services, local authorities and National Health Service bodies and are subject to the full set of civil protection duties. Their requirements are to:

* assess the risk of emergencies occurring and use this to inform contingency planning
* put in place emergency plans
* put in place business continuity management arrangements
* put in place arrangements to make information available to the public about civil protection matters and maintain arrangements to warn, inform and advise the public in the event of an emergency
* share information with other local responders to enhance co-ordination
* co-operate with other local responders to enhance co-ordination and efficiency
* provide advice and assistance to businesses and voluntary organisations about business continuity management (Cabinet Office 2013c).

Category 2 organisations include the Health and Safety Executive and transport and utility companies. These play a lesser role in planning work but have a (lesser) set of duties requiring cooperating and sharing relevant information with other Category 1 and 2 responders. Together, Category 1 and 2 organisations are required to form Local Resilience Forums to facilitate coordination and cooperation between responders at the local level. These in turn correspond to Local Resilience Areas based on the police area in which the responder’s functions are exercisable. These provisions are actually strongly enforced through the 2004 Civil Contingencies Act which places duties on local authorities and others to ensure they provide advice, assistance and measures to relating to business continuity management.

The UK’s approach to emergency planning requires these organisations to take into account the needs of different groups – victims, the vulnerable and responder personnel. Planning should aim at minimising the effects of an emergency and ensuring long term recovery (with government information provided in the National Recovery Guidance). Planning for the response phase requires crisis management to prevent or avert an emergency and address immediate effects while impact management deals with wider consequences. The government promotes the development of sub-national resilience capability based on a partnership with local responders and other organisations to ensure effective and coordinated planning and response. Subsidiarity places emphasis on local decision making, backed by government support where necessary. Plans for the recovery phase should deal with ‘rebuilding, restoring and rehabilitating the community following an emergency’ (Cabinet Office 3013b: 10). This phase is long-term and seeks to support affected communities in the reconstruction of physical infrastructure ‘and restoration of emotional, social, economic and physical well-being’ (Cabinet Office 3013b: 6-8). At this point we have arrived at UK government promotion of community resilience and the next section will look at the government approach to building this and business continuity.

**Building Community Resilience and Business Continuity**

The *Strategic National Framework on Community Resilience* has already been discussed in the previous chapter. It defines community resilience as ‘Communities and individuals harnessing local resources and expertise to help themselves in an emergency, in a way that complements the response of the emergency services (Cabinet Office 2011a: 11). The emphasis placed on getting people to help themselves is key to this strategy and indicates why this might be seen as a form of governmentality that encourages individual initiative and enterprising behaviour. The role of government, it seems, is to encourage people to take their own initiative. Indeed, it is argued that in many areas people are already taking responsibility for their own resilience and recovery, working with decision makers to determine the allocation of resources, making preparations and determining the recovery process (Cabinet Office 2011a: 7). As well as community resilience, there is a description of the resilient individual who is able to hold an informed understanding of the risks they face and their likely impacts. Resilient individuals need to be able to assess their vulnerability to risks, using this as motivation to act and be prepared (Cabinet Office 2011a: 11). The Pitt Report also argues the case for building community resilience, recommending that the government ‘establish a programme to support and encourage individuals and communities to be better prepared and more self-reliant during emergencies, allowing the authorities to focus on those areas and people in greatest need (Cabinet Office 2011a: 8).

To this end, the UK government is supporting a Community Resilience Programme that provides information in order to encourage communities and individuals to think about their vulnerabilities and, the infrastructure they rely on and the risks they face. People are told to consider this information and prepare themselves to be able to deal with the potential consequences of an emergency (Cabinet Office 2011a: 8). The stated aims of the Community Resilience Programme include increasing individual, family and community resilience, engaging existing approaches and successful initiatives, raising awareness of risk and local response capability, removing barriers that might inhibit or prevent participation in community resilience, encouraging dialogue between the community and relevant practitioners and providing tools to allow communities and individuals to address the wider community on the benefits of emergency preparedness (Cabinet Office 2011a: 5).

Recent guidance produced by the Cabinet Office captures most of the main themes present in the Anglo-Saxon approach to resilience and its relationship to society and business. The emphasis is on providing civil protection so people can go about their business freely and with confidence while the wider UK society – public and private sectors, community and business – are engaged in resilience building measures within their particular sectors. Advice is set out in various guides including *Resilience in Society: Infrastructure, Communities and Businesses.* Here it is argued that in order for communities to ‘help themselves’, people should ask themselves what they can do. They are asked the following three questions:

1. Are you aware of the risks you and your community might face, e.g. flooding?
2. How can you help yourself and those around you during an emergency?
3. What can you do to get involved in emergency planning in your community? (Cabinet Office 2014)

Communities will be better prepared if everyone uses their local knowledge and thinks about the potential impact particular emergencies like flooding or heatwaves could have on them, their family and their community. These arguments are repeated in guidelines to accompany the Civil Contingencies Act. Individuals and communities are better able to cope with emergencies if they have spent time planning and preparing and are aware of the resources, skills and expertise they possess. They will know their geographical area and the needs of members of their community and provide a link to existing local networks that response agencies can use (Cabinet Office 2004b: 46). The guidance promotes dialogue between the community, emergency practitioners and local authorities. Response agencies should take advantage of the community’s skills, resources, local knowledge and enthusiasm. Community resilience is rooted in the notion of the everyday based on the belief that everyday working practices and day-to-day functioning are the best foundations for developing effective plans (Cabinet Office 2004b: 23). Local authorities are understood in relation to the community they represent and their role in emergency response is seen as reflecting this (Cabinet Office 2004b: 33). Public health in particular is seen as important among a wide range of functions that local authorities carry out. The other important partner is the voluntary sector which can provide a diverse range of operational and support skills including psycho-social support (for example from faith groups), medial, clothing and feeding arrangements, information services, fundraising and equipment. Across all these bodies it is important to coordinate activities in such a way as to raise awareness and understanding, enhance capabilities and motivate and sustain self-resilience (Cabinet Office 2004b: 47).

The role of community is seen as particularly important in the recovery stage. As the guidance argues:

The management of recovery is best approached from a community development perspective. It is most effective when conducted at the local level with the active participation of the affected community and a strong reliance on local capacities and expertise. Recovery is not just a matter for the statutory agencies - the private sector, the voluntary sector and the wider community will play a crucial role. (Cabinet Office 2004b: 85)

Recovery, defined as rebuilding, restoring and rehabilitating the community is seen as a complex social and developmental process with four interlinked categories of impact that individuals and communities need to consider – humanitarian, economic, infrastructure and environmental. The best results are said to occur when the community can exercise a high degree of ‘self-determination’. Regeneration is also a significant theme that resonates with the more dynamic conceptions of resilience. Local communities can seize the opportunity to transform and revitalise their area through new commercial activities, improving skills, raising aspirations and improving the environment. Such transformation is seen as physical, social, and economic, but also psychological (Cabinet Office 2004b: 83).

Crises can at times, therefore, been seen as opportunities to regenerate and revitalise the community or area. There are, however, also more mundane interests present in the desire to maintain continuity and ‘keep things running’. An important part of the government’s ‘distant governance’ is to ensure good Business continuity management (BCM), ‘a process that helps manage risks to the smooth running of an organisation or delivery of a service, ensuring continuity of critical functions in the event of a disruption, and effective recovery afterwards’ (Cabinet Office 2014). The government role is to ensure that businesses and organisations have a clear understanding of BCM and can identify their key products and services and the threats they face.

Planning and exercising minimises the impact of potential disruption. It also aids in the prompt resumption of service helping to protect market share, reputation and brand. In order to be successful, BCM must be regarded as an integral part of an organisation’s normal ongoing management processes. To achieve this top-level buy-in is vital as it disseminates the importance of BCM throughout the organisation. Organisations are encouraged to carry out risk assessments and Business Impact Analysis. The guide *Keeping the Country Running: Natural Hazards and Infrastructure* provides advice on these as well as outlining standards of resilience. Governance from a distance operates through promoting best practice and information sharing rather than using additional regulation. As well as good BCM, regulated sectors should consider integrating resilience into annual reports, establishing monitoring and reporting systems for the most vulnerable sites, assessing and monitoring standards of infrastructure resilience, sharing information across sectors, improving resilience business cases and evaluating probability impact (Cabinet Office 2011b: 52).

Resilience is here understood as ‘the ability of assets, networks and systems to anticipate, absorb, adapt to and / or rapidly recover from a disruptive event’. A footnote goes on to state that ‘in its broader sense, it is more than an ability to bounce back and recover from adversity and extends to the broader adaptive capacity gained from an understanding of the risks and uncertainties in our environment. But for the purpose of this guidance, a narrower definition has been adopted (Cabinet Office 2011b: 14 – footnote 10). This recognises the wider socio-economic implications discussed above, but also accepts the need to concentrate on more technical aspects of infrastructure resilience. These are divided into four elements – resistance, reliability, redundancy and response. Resistance is focused on protection and the prevention of damage or disruption. In line with resilience thinking, the certainty of this and reliability of our knowledge is, however, questioned. Reliability is about ensuring that infrastructure components are designed in order to operate under a range of conditions. Again, resilience thinking warns of ‘insufficient awareness or preparation for events outside of the range’ that might produce significant wider and more prolonged impacts. (Cabinet Office 2011b: 15). The Redundancy component covers the design and capacity of the network or system. It includes things like backup installations, spare capacity and ability to switch to other parts of the network. For example, telecoms resilience works through the ability to re-route communications traffic. Finally, Response and Recovery concerns planning efforts and understanding of vulnerabilities as discussed above. In providing a summary understanding of infrastructure resilience the guidance combines the two elements of design and organisational ability:

resilience of infrastructure is provided through (a) good design of the network and systems to ensure it has the necessary resistance, reliability and redundancy (spare capacity), and (b) by establishing good organisational resilience to provide the ability, capacity and capability to respond and recover from disruptive events. The latter is gained through business operations and appropriate support for business continuity management. (Cabinet Office 2011b: 16)

At this point we have moved away from the focus on community towards more technical solutions to infrastructure problems. It is worth emphasising, therefore, that even in areas such as telecoms resilience there is some discussion of non-technical solutions, noting that no one technical solution is going to work all the time. In this particular area, focus can also be placed on the process used in communicating such as agreed protocols and the better organisation of responders (Cabinet Office 2013d).

**United States infrastructure resilience**

Presidential Policy Directive 21 (PPD-21) entitled *Critical Infrastructure Security and Resilience,* was introduced in February 2013 and calls for an update of the National Infrastructure Protection Plan (NIPP). This section looks at PPD-21 and the subsequent 2013 NIPP. These place their emphasis on security and resilience for critical infrastructure and emphasise changes to infrastructure risks, policies and operating environments and the increasing need to ‘integrate the cyber, physical, and human elements of critical infrastructure in managing risk’ (The White House 2013: 3). The motivations place strong emphasis on partnership efforts, innovation in managing risk and the need for an ‘enterprise approach to risk management’ (The White House 2013: 1). While this section looks at the NIPP and the Presidential Policy Directive, the following section will emphasise the forceful arguments for building community resilience in the National Plan.

The Presidential Policy Directive on infrastructure security and resilience makes a number of general arguments about the changing nature of security threats and challenges and the increasingly diverse and complex nature of critical infrastructure. This complexity derives from interdependence, multi-level authorities, diverse responsibilities and regulations, varied organisational structures and modes of operating and the mix of physical space and cyber space. Responsibility falls on infrastructure owners and operators to decide on effective strategies to make ensure security and resilience. However, this will also require integration into the national preparedness system with its emphasis on prevention, protection, mitigation, response, and recovery. PPD-21 therefore emphasises the importance of coordination and collaboration and shared responsibilities between different levels of government and the public and private owners and operators. The role of Federal government is to promote an integrated and holistic approach that reflects the infrastructure's interconnectedness and interdependency. The strategic imperatives of the Federal Government’s approach are:

1) Refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience;

2) Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government; and

3) Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure (The White House 2013)

The rest of the Policy Directive goes on to outline various roles and responsibilities of the Department (and Secretary) of Homeland Security in coordinating the Federal effort and carrying out the responsibilities assigned in the 2002 Homeland Security Act. The Secretary of Homeland Security will evaluate national capabilities, opportunities and challenges, analyse threats and vulnerabilities and identify security and resilience functions necessary for effective public-private coordination. Coordination efforts require the identification of key interdependencies among infrastructure sectors, monitoring the effectiveness of measures taken and providing strategic guidance for promoting a national unity of effort. Additional roles and responsibilities include maintaining national critical infrastructure centers to monitor emerging trends, threats and incidents, provide analysis, expertise, and other technical assistance and exchange of information and intelligence, conduct comprehensive assessments of vulnerabilities, coordinate Federal Government responses to cyber or physical incidents and report annually on the status of national critical infrastructure efforts as required by statute.

PPD-21 prepares the ground for the 2013 National Infrastructure Protection Plan. This defines critical infrastructure as ‘systems and assets, whether physical or virtual, so vital to the United States that the in­capacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters’ (Department of Homeland Security 2013: 7). To protect this infrastructure requires the collective identification of priorities, articulation of clear goals, mitigation of risk, measurement of progress and, crucially, adaptation based on feedback and the changing environment. Managing risk requires an ‘integrated approach’ across a diversity of actors. The 2013 NIPP is seen as distinctive in elevating security and resilience as the primary aim of infrastructure planning. It updates the risk management framework and aligns with the National Preparedness System in the mission areas of prevention, protection, mitigation, response, and recovery. Prevention activities are said to be most associated with addressing threats; protection efforts address vulnerabilities; response and recovery efforts minimize consequences while mitigation transcends the whole threat, vulner­ability, and consequence spectrum (Department of Homeland Security 2013: 19).

As with other strategies discussed in this chapter, the framing of the approach begins with the argument that we find growing interdependence across critical infra­structure systems and that this is particular so in relation to infor­mation and communications technologies. While offering greater opportunities, it also increases vulnerabilities: ‘In an increasingly inter­connected world, where critical infrastructure crosses national borders and global supply chains, the potential impacts increase with these interdependencies and the ability of a diverse set of threats to exploit them’ (Department of Homeland Security 2013: 8). The United States is also exposed to the effects of extreme weather which compounds the other risks and can have a significant impact on infrastructure operations. The policy and operating environment is also affected by vulnerabilities in the workforce such as a lack of skilled labour and maintenance expertise (Department of Homeland Security 2013: 8).

The NISS approach places such a high emphasis on risk that it might be described as an attempt to govern through risk. Security and resilience, it is argued, are best strengthened through appropriate risk management. Here risk management is taken to be the ‘process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost’ (Department of Homeland Security 2013: 7). Those responsible for critical infrastructure must develop strategies of risk mitigation and other ways to address risk including acceptance, avoidance, or transference. Addressing cross-sector dependencies and interdependencies requires information sharing and planning across the critical infrastructure community.

Therefore, risk management is most effectively achieved through partnerships based on trust, common interest and a shared vision. Risk needs to be identified and managed in a coordinated and comprehensive way across the critical infrastructure community to enable the effective allocation of security and resilience resources. Priorities should be determined jointly by the public and private sector, ‘integrating cyber and physical security and resilience efforts into an enterprise approach to risk management’ (Department of Homeland Security 2013: 14). Public-private partnerships are seen as central to maintaining security and resilience with the different levels of government and the public and private sectors each bringing unique experience, capabilities and core competences, the value of which helps bring distinct understanding of various challenges and solutions. Effective partnerships depend upon different attributes including clearly defined purpose and goals, frequent communication, flexibility, adaptability and measurable progress and outcomes to guide shared activities (Department of Homeland Security 2013: 14).

The other element of the NIPP that should be considered is the focus on levels of operation. There is first the recognition that the ‘United States benefits from and depends upon a global network of infrastructure that enables the Nation’s security and way of life’ (Department of Homeland Security 2013: 14). However, the National Plan is more focused on domestic efforts, while recognising the need to work with international partners. At the national level, the plan sets out a series of priorities and goals. These priorities and other risk management activities will be updated regularly. The plan also sets out a continuous cycle of evaluation. This involves the identification of outputs and outcomes associated with the national goals and priorities, the collection of performance data to assess progress in achieving these and evaluation of progress towards achievement of the national goals, priorities and vision (Department of Homeland Security 2013: 20). In addition to the National Plan, there will be evaluation of the achievement of the National Preparedness Goal at both the national and commu­nity levels and across different sector, considering their priorities and achievements in collaboration with different critical infrastructure partners (Department of Homeland Security 2013: 4)

The Plan’s ‘Call to Action’ uses the language of empowerment and capacity building to engage local and regional partners. Most risks and incidents are local in nature, or else have local consequences and it is necessary to develop initiatives on a regional scale in order to complement and operationalise the national effort. Local and regional partnerships are therefore seen as an essential part of the national effort and the aim of the Plan is to identify existing partnerships and encourage new ones that can enhance security and resilience. Locally based public, private, and non-profit organisations are encouraged to provide their perspective and assessment of risk and mitigation strategies with the state playing the role of facilitator and coordination of planning, resource allocation, and evaluation of progress (Department of Homeland Security 2013: 22).

This focus on coordination and facilitation and the empowerment of local actors is a good example of governance from a distance, albeit something that can be combined with decisive state action should the need arise. Another example of governance from a distance is the promotion of Sector Coordinating Councils (SCCs) which are self-organized, self-run, and self-governing bodies that enable owners, operators, trade associations, vendors, and others to interact across a range of policies, activi­ties, and issues. They represent the first point of contact for the Federal Government to engage with each sector’s critical infra­structure security and resilience activities. Their various functions include strategic communication and coordination between owners, operators, and suppliers and, if necessary, the government; supporting information-sharing; participating in planning efforts related to the revision of the National Plan and Sector-Specific Plans; coordinating exercises and training, public awareness, and associated implementation activities (Department of Homeland Security 2013: 35). By contrast, Government Coordinating Councils (GCCs) enable interagency, intergovernmental, and cross-jurisdictional coordina­tion within and across sectors. They bring together different representatives from government and each sector. The GCCs and SCCs are important in facilitating public-private coordination across different sectors and constituencies.

**Community resilience in PPD-8**

This section looks briefly at Presidential Policy Directive 8, National Preparedness since it is here that we find the strongest link with the more Anglo-Saxon notions of individual and community resilience. PPD-8. PPD-8 aims at an integrated ‘all-of-nation’ approach to preparedness, producing ‘a secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and haz­ards that pose the greatest risk’ (The White House 2015: iii). The National Plan is aligned with the National Preparedness Goal aimed at coordinating critical infrastructure risk management with national preparedness across different mission areas. PPD-8 is organized around several elements. The National Preparedness Goal states the ends to be achieved, the National Preparedness System describes the means to achieve these, the National Planning Frameworks explain delivery and an annual National Preparedness Report documents the progress being made. Various other guidance documents are aimed at the general public, businesses and non-profit organisations. PPD-8 argues that when everyone comes together the end result is more effective and that ‘involving the whole community in PPD-8 activities is what makes this effort unique… when it comes to national preparedness, all of us have a role to play’ (The White House 2015). At its core, therefore, is the requirement for everyone to be involved, that ‘preparedness is a shared responsibility’ and that government departments and agencies must work with the whole community to meet the objectives.

The 2015 National Preparedness Goal aims for a ‘secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to and recover from the threats and hazards that pose the greatest risk’. It emphasises the need for the whole community to work together and argues that individual and community preparedness is fundamental to success. The emphasis on individual and community resilience is clear: ‘Each community contributes to the Goal by individually preparing for the risks that are most relevant and urgent for them individually. By empowering individuals and communities with knowledge and skills they can contribute to achieving the National Preparedness Goal’ (FEMA 2015: 2).

The National Preparedness System document outlines the approach, resources and tools for achieving the National Preparedness Goal while national planning frameworks focus on each of the mission areas – prevention, protection, mitigation, response and recovery and defines how best to work together to meet the needs of individuals, families, communities and states in relation to these. Federal Interagency Operational Plans cover government activities to deliver on core capabilities in support of state and local plans across the five mission areas. Finally, the National Preparedness Report summarises progress towards the National Preparedness Goal. It provides a detailed analysis of the five mission areas including ranking their core capabilities. Throughout the reports, the government promotes a ‘whole community approach’ noting that while government ‘plays a critical role in coordinating national-level efforts, it is communities and individuals who lead efforts to implement preparedness initiatives throughout the Nation’ (Department of Homeland Security 2012: 1). The latest report notes, however, that while individual preparedness is key to community resilience, surveys continue to highlight the difficulties in successfully engaging the pubic (Department of Homeland Security 2016a: ii).

The community is central to mitigation activities and a resilience approach seeks to help community members make informed actions to reduce their risk (Department of Homeland Security 2016a: 17). It is argued that since communities can rarely avoid such risks completely, the Mitigation Framework encourages building Community Resilience before an occurrence through leadership, collaboration, partnership building, education, and skill building (Department of Homeland Security 2016a: 49).

The National Disaster Recovery Framework defines how Federal agencies promote effective recovery and examination of this framework shows the strongest influence of the idea of community resilience. It looks at the ability of a community to recover based on its pre-disaster preparedness, mitigation and capacity building. Hence resilient communities are understood as being those ‘with an improved ability to withstand, respond to and recover from disasters’, who are able to take timely decisions in response to the impact of disaster impact and who can engage in successful recovery planning and implementation (Department of Homeland Security 2016b: 5). Within these communities, successful recovery is based on the ability of individuals and families to ‘rebound from their losses in a manner that sustains their physical, emotional, social and economic well-being’ (Department of Homeland Security 2016b: 5). Individuals, families and households are said to have a key role to play in facilitating both their own recovery and that of the wider community (Department of Homeland Security 2016b: 11). In return, it is important that individuals can draw on community support while local government has primary responsibility for leading and managing community recovery. The Federal Government will act as a partner and facilitator, strengthening its role if this affects national security (Department of Homeland Security 2016b: 6).

All this again illustrates the Anglo-Saxon approach to resilience insofar as it promotes a more distant form of governance through facilitation, encouraging individuals, families and communities to better govern themselves. If this can be seen as a form of governmentality, then there are other elements of the community approach that indicate its more neoliberal character. As well as devolving responsibility downwards on to individuals and local actors, support for private sector solutions to local problems is a clear government priority. The private sector is seen as a crucial source of resilience through its provision of infrastructure services and other essential commodities and plays a key role in ensuring the ‘viability’ of a community. Recovery depends upon the private sector, working hand with the community and other local organisations (Department of Homeland Security 2016b: 14). However, a neoliberal approach is more than simply the promotion of the private sector. As a form of governance, it installs a sense of enterprise as well as responsibility among individual actors. A more transformative version of resilience is promoted whereby rather than simply returning to a previous condition, recovery offers ‘unique opportunities to reduce current and future risk and contribute to a more sustainable community’ (Department of Homeland Security 2016b: 8). It is argued that communities ‘can capitalize on opportunities’ during the rebuilding process, improving their sustainability and ‘livability’ goals, promoting future growth, improving economic competitiveness, enhancing the health and safety of the neighbourhood and making smart energy choices (Department of Homeland Security 2016b: 8). Moreover, while resilience involves the ability to withstand and recover, the key issue is the ability of people to prepare for and adapt to changing conditions. The responsibility for this ‘begins with the individual and integrates with the larger responsibility of the community’ (Department of Homeland Security 2016b: 26).

**Critical infrastructure protection in France**

This section looks at French infrastructure protection which had been undergoing a gradual transition from a strong form of state protection to a greater devolution of powers to the private sector and non-state actors. This has not, however, developed in a uniform manner and significant differences exist across areas of responsibility with the state continuing to play a decisive role in most cases.

Since 2004, civil protection has been subject to greater involvement from non-state actors. Law 2004-811 did two things – first to bring together different crisis management procedures into a unified approach; second, to give a greater role to municipalities who could now determine their own crisis management procedures at the local level. The law sought both greater coherence under the direction of the state, and greater local responsibility based on empowering municipal actors as well as seeking to promote a stronger understanding of risk culture among institutions, the private sector and civil society.

This started to challenge the traditional notion of civil protection as the sole responsibility of the state with little delegation to municipalities or private actors. For much of the twentieth century the state was, as elsewhere, the main owner and provider of critical infrastructure. Waves of privatisation have changed this situation with the state now required to secure specific obligations of service provision from various private operators. As Boucart argues (2015: 40), the state has definitely lost a significant part of its crisis intervention capacity as a result of these privatisations and the subsequent law 2015-811. As with the case in other countries, it now seeks to develop a role as coordinator for service provision, rather than direct provider. Civil defence and critical infrastructure protection has gradually shifted away from the idea of strong state protection towards issues like business continuity and preparedness, as discussed in the sections above. These developments are justified by the French authorities through the gradual introduction of resilience and the idea that the state must promote preparedness among private actors and the population, rather than trying to do everything itself.

In this context, resilience is introduced as the willingness and ability of a country, a society and its authorities to be able to withstand the consequences of an attack or catastrophe and quickly restore normal functioning, or at least a socially acceptable level of functioning. This concerns not only government but economic actors and the whole of civil society (Secrétariat général de la défense et de la sécurité nationale 2014a: 9).[[1]](#footnote-1) This statement from the General Secretary for Defence and National Security, giving instructions on vital activities, contains two things of note. Firstly, it supports the view that the French government is pushing for a whole of society approach that recognises that infrastructure is operated privately and that the cooperation of the private sector and civil society is necessary. Secondly, however, it remains wedded to the ‘conservative’ definition of resilience as restoring normal functioning, rather than the Anglo-Saxon view that crises present opportunities to adapt and reorganise rather than returning to the way that things were previously.

Critical infrastructure protection has, since 2006, been divided into twelve areas of vital importance. The state sector is comprised of civil activities, military activities, judicial activities and space and research. Citizen protection includes health, water management and food. Vital areas of the nation’s social and economic life are listed as energy, cyber security and electronic communication, transport, finances and industry. Each of these areas is given a coordinating minister.

Each area will Il revient à chaque opérateur d'identifier, dans son système de production, les composants névralgiques et de les proposer comme points d'importance vitale devant faire l'objet d'une protection particulière.identify its production system, critical components and needs for special protection with the government providing overall identification of threats and general vulnerabilities, defining the protection requirements and measures for implementation in line with France’s national security alert system – Vigipirate (Secrétariat général de la défense et de la sécurité nationale 2014b). The three levels of protection plans for operators of critical infrastructure are the Plan de sécurité d’opérateur (PSO) for large operators managing several vital infrastructures, the Plan particulier de protection (PPP) based on single operators in specific areas and the plan de protection externe (PPE) for accompanying measures in times of crisis in coordination with civil security forces and other sectors. Within this framework the operators of infrastructure have certain obligations to train their managers and security directors at central and local levels, carry out risk analyses, establish an operator security plan and identify the particular protection plan (PPP). The government, in turn, provides an external protection plan for operational support and will intervene if the operators are unable to cope with the crisis.

The overall legal and regulatory framework for these activities is provided through the Sécurité des Activités d’Importance Vitale (SAIV), the highest level of the system of protection against terrorism and serious risks. This defines security priorities and the procedures for implementation of necessary measures while facilitating relations with and between operators and public authorities and promoting prevention, preparedness and awareness. It is here that the reality of the French system becomes more evident. Rather than devolving significant power down to the twelve areas of vital importance the emphasis is on collective ownership of the defence strategy and the resilience of the nation. A hierarchical distribution of crisis responsibilities is preserved with the state playing the leading role in determining how implementation is to take place (Secrétariat général de la défense et de la sécurité nationale 2014a: 9). Bourcart (2015: 49) is correct, therefore to suggest that a paradox exists at the heart of the French approach to civil protection. The state declares its intention to devolve powers to civil society and the private sector, but at the same time implements top-down measures based on national laws, decrees and legally-binding ‘guidance’ to infrastructure operators that outlines exactly what plans they should develop.

SAIV provides the framework for defining and implementing security measures for the protection of vital points of importance (PIV). PIVs are understood as national establishments, facilities or structures which, if damaged or destroyed, would seriously weaken national economic, military or security capacity, or else seriously damage the health and wellbeing of the population (Secrétariat général de la défense et de la sécurité nationale 2014: 21).[[2]](#footnote-2) We see, therefore, a concern with both physical infrastructure including military and security apparatuses, and something more akin to governmentality in its concern with what is vital to society and the wellbeing of its citizens. On this point the French approach, like the German, is notably more pro-European than the UK approach, advocating a ‘social model’ understanding of what is vital to society rather than a neoliberal focus on individual self-reliance. Following the 2006 European Programme for Critical Infrastructure Protection of the critical infrastructure of the Member States, it is argued, is ‘indispensable to the maintenance of vital societal functions, health, the safety, security and economic or social well-being of citizens’ (Secrétariat général de la défense et de la sécurité nationale 2014: 49, my translation).[[3]](#footnote-3)

Another government body promoting resilience is the Ministry of the Environment and the General Commission for Sustainable Development. Launching the Integrated Assessment of Territorial Resilience initiative in 2012 it seeks to strengthen the capacity of local governments, communities and their infrastructure to respond to crises and disasters.

This is somewhat closer to the UK approach in looking at communities as well as infrastructure. Interestingly, it defines resilience, when applied to human societies, as maintaining a level of functioning, but also in the more dynamic sense of having the capacity to adapt in the face of hazards based on the capabilities and flexibility of the system (Commissariat Général au Développement Durable 2013: 2). A resilience strategy aims to encourage populations in vulnerable areas to take preventative measures, or to change their individual or collective behaviour. The project seeks to produce a guide that will help local actors – defined as local government and decentralised services, communities, the public sector, private companies, NGOs and associations – to analyse the causes of vulnerabilities, examine coping mechanisms and provide methodological assistance for shared solutions (Commissariat Général au Développement Durable 2013: 4).

Initiatives such as these suggest that away from official government policy, there is a more receptive attitude towards resilience thinking, particularly in relation to communities and civil society. Among research institutes, foundations and think-tanks we find positive promotion of the benefits of a resilience approach, perhaps most notably with the think-tank Haut Comité Francais pour la Défense Civile (HCFDC). Their position paper from 2010 promotes familiar themes such as business continuity management, coordination among stakeholders, public-private initiatives and the importance of local community involvement in resilience-building. It also notes how the idea of resilience is much stronger in the UK and that crisis management is carried out through local forums which enable essential actors to understand their requirements and to perform exercises in preparation. The legal framework and role of the state is ‘lighter’ with more responsibility falling on the actors themselves whereas in France crisis management is controlled by the state (Haut Comité Francais pour la Défense Civile 2010: 13). Yet, apparently, resilience is an unavoidable modern societal condition and it is a growing international trend that populations be more involved in comprehensive crisis management (Haut Comité Francais pour la Défense Civile 2010: 15).

The approach of the HCFDC is to promote better coordination between public and private actors, encourage mutual understanding and, through training and exercises, gain better knowledge of reciprocal crisis management tools. Communities can be encouraged to better understand how to cope with a crisis even if the state remains in charge of crisis management and emergency response. It is necessary to move away from the view that the state’s approach is the only possible understanding of a crisis. Different actors will have different perspectives and a comprehensive response requires a sharing of viewpoints. Communities too will often have a fuzzy understanding of the problems they face and will need better guidance and communication. The state cannot, indeed should not, plan everything. But it must manage priorities, plan for recovery of infrastructureand ensure restoration of essential services (Haut Comité Francais pour la Défense Civile 2010: 7).

Finally, the High Council for Strategic Education and Research, whose detailed report on resilience we shall discuss later, argues for the benefits of adopting a resilience strategy as part of a wider change paradigm. This advocates a vision of sustainable development leading to greater economic security, based on social and ecological durability, flexibility and resilience. Risks are increasingly unpredictable and environments are highly uncertain, but a clear strategy should be able to anticipate such uncertainty through better preparedness and clearer decision-making (Conseil Supérieur de la Formation et de la Recherche Stratégiques 2011: 55).

These discussions give some indication of the different approaches being advocated by various research institutes, think-tanks and foundations. Their promotion of resilience is certainly more enthusiastic than the official government position, and it is perhaps closer to the Anglo-Saxon point of view. Nonetheless, it is the introduction of resilience into government policy making that provides the opportunity for this further discussion and debate. This situation we will expect to continue, albeit with some of the reservations about the Anglo-Saxon understanding of resilience, as we shall outline later in the analysis section.

**German Infrastructure protection**

The German Federal Ministry of the Interior (BMI) set up the Critical Infrastructure Protection (CIP) Working Party of Federal Ministries in 1997 and the issue of infrastructure protection has developed since then through various campaigns and special commissions to raise awareness. Initiatives have begun to coordinate infrastructure protection with the private sector, particularly in areas such as IT security. Germany is, however, still somewhat behind the Anglo-Saxon countries in formulating policy and guidelines.

The purpose of this section is to indicate how critical infrastructure protection is developing in Germany, while lacking the conception of resilience found in Anglo-Saxon discourse. Partly, this is because the German approach gives a central role to government and the state, with little or no emphasis on building resilience within communities. However, this does not mean that there are not some similarities in policy and argument. The most important government document in this field is the *National Strategy for Critical Infrastructure Protection (CIP Strategy)*published in 2009. While the arguments are somewhat technical, the setting of the context contains familiar assumptions. The context, indeed, can be found in UK, US and EU arguments about the need for global competitiveness and infrastructure protection is justified on this basis:

Infrastructure in general and critical infrastructure in particular are the lifeblood of modern, efficient societies. Germany is among the leading industrial and technology-oriented nations. Germany's importance as a location for business and industry and ensuring the country’s competitiveness in a globalized economic and technological setting are crucially dependent, as preconditions for prosperity and progress, on the availability of high-performance and well-functioning infrastructure. Therefore, ensuring the protection of this infrastructure is a key function of security-related preparedness measures taken by industry and government agencies, and is a central issue of our country's security policy (Federal Ministry of the Interior 2009: 3)

While the importance of this infrastructure grows, so too does society’s vulnerability due to the extent to which ‘nearly all spheres of life are pervaded with, and dependent on, critical infrastructure’ (Federal Ministry of the Interior 2009: 5). These changed conditions are seen as necessitating greater trust and cooperation across different government departments, industry, business and civil society.

Critical infrastructure is defined as ‘*organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences*’(Federal Ministry of the Interior 2009: 4). While the UK approach emphasises business and communities, the German approach makes more reference to society as a whole. Infrastructure is considered critical ‘whenever it is of major importance to the functioning of modern societies and any failure or degradation would result in sustained disruptions in the overall system’ *(*Federal Ministry of the Interior 2009: *7)*. Protecting critical infrastructure ‘is a task of society as a whole, which calls for coordinated action supported by all players – government, business and industry, and the general public’ (Federal Ministry of the Interior 2009: 10). The attention of the state and of society should be directed at two threats in particular – the threat of terrorism, and the growing impact of natural hazards.

Infrastructure in Germany is divided into technical basic infrastructure and socio-economic services infrastructure. The technical side includes power supply, information and communications technology, transportation and water supply. The socio-economic services side includes public health, food, emergency and rescue services, disaster control and management, government, public administration, law enforcement agencies, finance, insurance business, media and cultural heritage objects (Federal Ministry of the Interior 2009: 7). Significant interdependency exists between these with socio-economic services largely dependent upon the technical basic infrastructure, but with the basic infrastructure dependent on socio-economic factors such as a stable legal system and functioning emergency service (Federal Ministry of the Interior 2009: 8).

The ownership and operation of this infrastructure, following most trends, is moving into the private sector. This is increasingly the case for public infrastructure services provided at local government level. With the private sector increasingly responsible for the security, reliability and availability of such infrastructure, the responsibilities and functions of the state or public authorities are mainly to ensure the safety and control of the supply of goods and services in times of crises when market mechanisms might not be reliable (Federal Ministry of the Interior 2009: 8). This approach takes privatisation policy for granted, deeming it an inevitable tendency, but does recognise that there are significant limits to what the market can do.

Thus, the German approach continues to emphasise the central role of the state, but notes the need for better cooperation, on a partnership basis, with other public and private actors. The state may do this as a moderator, or by rulemaking and regulating measures for safeguarding the ‘overall system’ and its procedures (Federal Ministry of the Interior 2009: 3). The guiding principles are ‘to build trusting co-operation between the state and business and industry’ (Federal Ministry of the Interior 2009: 12). The German approach is notable (and might be contrasted with the UK in this respect) in that this is backed up by a strong legal framework. It is noted that compared to other countries, Germany has a good record of security of supply because privately organized power supply companies are under a legal obligation to operate a secure, reliable and high-performance supply network (Federal Ministry of the Interior 2009: 4). As the guidance to companies and public authorities makes clear:

Public limited companies and limited liability companies (GmbH) are currently subject to overarching legal requirements for controlling risk and crises. The financial sector also has regulations which are obligatory in practice, such as minimum requirements for risk management (MaRisk). According to these regulations, the concept of enterprise security includes protecting persons and material goods such as buildings and facilities, maintaining operations through any kind of disruption up to a crisis, whether a stock market crisis, natural disaster or terrorist attack. (Federal Ministry of the Interior, 2008: 12)

The German approach to critical infrastructure protection is also affected by the federal structure of the German state. The Federation, the *Länder* and local governments are required to jointly act. And there is a structured implementation procedure across these three levels of government. Parallel work packages relate to definition of general protection targets; analysis of threats, vulnerabilities, and management capabilities; assessment of threats and identification of protection targets. Interestingly, it is emphasised that these work packages are implemented primarily by the public sector, while the Federal Ministry of the Interior coordinates at the federal level. Relevant companies and operators take responsibility for implementation of goal attainment measures, internal regulations, self-commitment agreements and risk assessment and communication (Federal Ministry of the Interior 2009: 16).

There is a neoliberal element that creeps into the argument that suggests the way forward is to govern through risk. It claims that: ‘No one-hundred percent protection of infrastructure and its operational effectiveness can be ensured by either the state or operators. The present security mentality must be converted into a new “risk culture”’ (Federal Ministry of the Interior 2009: 11). Creating a risk culture is the closest the CIP Strategy comes to the Anglo-Saxon approaches discussed above. This ‘novel risk culture’ will be based on cooperation among stakeholders, ‘risk communication among the state, companies, citizens and the general public’, more self-commitment from operators to manage and prevent incidents and ‘a greater and self-reliant self-protection and self-help capability of individuals or institutions affected by the disruption or compromise of critical infrastructure services’ (Federal Ministry of the Interior 2009: 11). This risk culture will help make society more robust and resistant in the face of vulnerabilities.

What is interesting here, however, is the mixed message that reflects the fact that the German approach is torn between two different ‘cultures’. The ‘novel risk culture’ promoted here is undoubtedly an Anglo-Saxon neoliberal one that seeks to promote private initiative, while responsibilising operators and individuals. It represents governance from a distance by governing through risk assessment and risk awareness. This suggests resilience insofar as it is accepted that we must give up on the idea of one hundred percent protection and accept that crises are inevitable. However, rather than drawing the obvious conclusions – that we must instead promote a culture of dynamic adaptability and reorganisation, the argument concludes with what might be considered the ‘conservative’ view of resilience; that is, that the aim of the strategy is to make society more robust and resistant. This is the ‘engineering view’ of resilience criticised by recent approaches – it seeks to protect things as they are and to resist rather than adapt. A similar ‘conservative’ view can be found in risk and crisis management guidelines for companies and government authorities: ‘The aim of crisis management for critical infrastructure organizations is to deal with a crisis while maintaining the greatest possible ability to function, and/or recovering critical functions as quickly as possible’ (Protecting Critical Infrastructures – Risk and Crisis Management: A guide for companies and government authorities, Federal Ministry of the Interior, 2008: 22). Indeed, these arguments advocate resistance, not resilience, and maintain the key role of the state as protector of society, rather than the Anglo-Saxon view of devolved governance through self-reliant individuals and communities.

To take this argument a little further, the strategy outlines three elements of risk management. First, Prevention – the identification of all existing and anticipated risks, critical elements and processes, so that severe disruption will be avoided. This will be done through ‘comprehensive proactive (preparedness) arrangements’ and ‘efficient risk and crisis management’. The Response element seeks to minimise the consequences of severe disruptions through effective emergency and crisis management and ‘effective self-help capabilities of the entities and establishments directly affected’ (Federal Ministry of the Interior 2009: 12). The Sustainability element seeks the establishment of protection standards to be developed jointly with the operators and in accordance with international standards. This again differs from Anglo-Saxon approaches to resilience which place less emphasis on prevention and protection. While there is the phrase ‘effective self-help capabilities’, it seems clear that the main direction for this strategy will come from the state and that the state maintains chief responsibility for protection.

There are other attempts at promoting risk management through vulnerability analysis and developing a methodology for analysing critical infrastructure sectors – in one case developing a ‘society-level criticality matrix’ to determine processes of significant and high criticality (Federal Office for Information Security 2004: 8). Vulnerability analysis looks at how risk elements in sub-processes determine how an organisation is affected. Dependence on these risk elements demands a combination of risk reduction, risk avoidance, risk shifting and risk acceptance (Federal Ministry of the Interior 2008: 22).

The Federal Office of Civil Protection and Disaster Assistance produces guidance and commissions academic work to promote better understanding and practices in this field. The best example of this work is the work on flooding – a natural hazard that has had a significant impact on Germany and central Europe in recent years. This is one issue – as noted also in the EU’s work – that has a cross-border impact requiring international cooperation. In one of the very few mentions of resilience in the German literature, it is suggested that:

The use of internationally applicable guidelines for assessing vulnerability at a community level can play a decisive role in achieving international cooperation in this area. Exchanging assessment data can lead to an improvement in flood management at a community and national level, as well as forming the basis for recommendations about resilience strategies. (Federal Office of Civil Protection and Disaster Assistance 2014: 24)

The 200 page guidance on flooding mentions resilience just this once, although the community focus is more central. This focus, however, is not on the role of community as understood in the UK documents, but as an object of measurement. The report’s main aim is to develop key vulnerability indicators covering such things as exposure, susceptibility, capability, evacuation time, coping capacity, insurance time, flood experience and flood protection measures in private households. Alongside the standardised core indicators are community-specific indicators listed as flood sensitivity, level of information on flood hazards, actual insurance cover and flood protection measures. These contain some of the issues discussed in the UK guidance. For example, the flood sensitivity indicator looks at how those people who are aware of their own flood risk are likely to be better prepared and better informed about the correct behaviour in event of an emergency (Federal Office of Civil Protection and Disaster Assistance 2014: 73). Such discussions are interesting, and are compatible with approaches that seek to measure levels of resilience. But they are largely technical accounts that construct the community as an object of analysis rather than as pro-active actor in flood prevention.

The conclusion to be drawn is that there as a much weaker sense of communities and individuals as actors. This can be seen positively or negatively depending on point of view. It could be claimed that the UK approach places the resilience of communities and individuals centre stage, or it could be claimed that this is a strategy of devolving responsibility away from the state by governmentalising the population. The lack of discussion of community resilience in the German literature might be seen as indicating lack of dynamism. Or it might be that this lack of emphasis on the role of communities occurs because German policy making retains its strong emphasis on the role of the state as the main responsible actor that people ultimately depend upon for protection and that the lesser emphasis on communities and individuals is due to a greater emphasis on society as a whole.

**Resilience in EU policy making**

This section looks at how the EU is dealing with a number of transborder challenges, particularly in relation to critical infrastructure, the civil protection Mechanism and climate change adaptation. These challenges arise in relation to basic societal functions and needs such as energy, transport and food distribution. The process of European integration, combined with the general trends towards interconnectedness and interdependence renders member states more vulnerable to transborder threats to such functions, exacerbated by the spread of communications and new technologies and by Europe-wide policies of market liberalisation. Hence threats to critical infrastructure are of particular importance in that they have an impact both on other member states, and the European economy as a whole. These impacts affect such areas as agriculture, economic growth and the competitiveness of EU regions (European Commission 2009a: 4). The Commission is particularly concerned to promote better coordination and cooperation across different countries and between different stakeholders – member states, the Commission, industry and business associations, standardisation bodies, owners, operators and users. Stakeholders are required to cooperate and contribute to the development and implementation of critical infrastructure protection according to their specific roles and responsibilities (European Commission 2005: 4). Developing an EU-wide framework is therefore necessary to maintain levels of infrastructure protection, but it is also noted that this should support the rules of competition within the internal market. The Commission will support this by assuming the role of facilitator, identifying, exchanging and disseminating best practices for transborder infrastructure protection which will provide the basis for a common framework (European Commission 2005: 5).

The protection of critical infrastructure is described under the subsidiarity principle as being first and foremost the responsibility of member states, the owners and operators. The EU’s role is to concentrate on those aspects of infrastructure protection that have transborder effects. This form of indirect governance emphasises the responsibility and accountability of owners and operators to make their own plans and decisions for protecting their assets (European Commission 2005: 4). However, there are accompanying principles of collective responsibility where member states set up measures for prevention and preparedness and the principle of solidarity (Morsut 2014: 147). The Solidarity Clause is aimed at getting member states to act together to assist in the event of a terrorist attack or natural or human-made disaster. It also encourages use of various EU instruments in areas of police and judicial cooperation and civil protection. However, despite being in place since the end of 2009, little use as been made of the Solidarity Clause and Member States have proved reluctant to activate binding procedures (Fuchs-Drapier 2011: 184).

Because of this, approaches to disaster prevention, for example, continue to emphasise that primary responsibility to protect citizens remains with member states but that the EU can, ‘in the spirit of solidarity’, be called upon to complement and support action taken at national, regional or local levels, while continuing to respect the principle of subsidiarity (European Council 2009: 1). Rather than strong compulsion, the Commission works through sharing and promoting various practices, lessons learnt and relevant data and information, raising awareness of the social, economic and environmental impacts of disasters and providing relevant information to policy makers. It encourages those involved in disaster prevention to work together and suggests developing a common legal framework if possible. However, it does not compel these things. Instead it seeks to make use of guidelines and methods to map risks, make assessments, raise public awareness, improve dissemination of forecasts, encourage exchange of policy makers and researchers and improve the links between existing early warning systems (European Council 2009: 7).

An important tool in the EU’s response to crises and disasters is the Union Civil Protection Mechanism. This offers assistance to any member state that is struggling to cope with the aftermath of a crisis or disaster. The Lisbon Treaty recognises civil protection as a formal policy area with competences shared between the EU and its member states based on the principles of complementarity and promotion. The main role of the Mechanism is to prevent or reduce the effects of crises through ‘fostering a culture of prevention’, improving cooperation, enhancing preparedness and facilitating rapid and efficient response as well as increase public awareness and preparedness for disasters (European Council 2013). The EU approach is to offer coordination and facilitation from a distance, encouraging member states and other actors to respond in the most appropriate ways, coordinate efforts, share information and encourage public awareness. The principle of subsidiarity is particularly relevant here as this determines the most appropriate level of intervention – either at European, national or local levels – with the EU only intervening if it can do so more effectively than member states and local actors.

In the area of environmental policy, we will look at the measures the EU is taking in response to the threats posed by climate change. The EU’s Adaptation Strategy for a more climate-resilient Europe focuses on how to respond to climate change at local, regional and EU levels through enhancing preparedness and capacity to respond. Again, most emphasis is placed on developing a coherent approach and improving coordination of actors. Of particular importance is the need to ensure coherence between national adaptation strategies and national risk management plans. It notes how many member states are developing such plans as cross sectoral planning instruments to better prevent and prepare for disasters on the basis of comprehensive national risk assessments (European Commission 2013a: 5). The first phase of the adaptation strategy seeks to establish knowledge of the consequences of climate change and to integrate adaptation into key EU policy areas. It argues for a combination of policy-based and market-based instruments, guidelines and public-private partnerships to deliver on adaptation (European Commission 2009b: 7). Vulnerability assessment should be carried out across member states to best determine various adaptation measures. The Commission will develop vulnerability indicators and means of monitoring both impacts and adaptation measures and to better understand the costs and benefits of adaptation (European Commission 2009b: 8).

Again, emphasis is placed on member states as having primary responsibility for protecting existing and future infrastructure from the impact of climate change. The EU’s role is to develop common standards and promote best practices, carry out risk assessments and assess the effectiveness of different adaptation measures while monitoring and evaluating past adaptation efforts (European Commission 2013a: 7). Looked at from the perspective of climate change, then the main aim of these approaches is to emphasise the need for adaptation. The main climate change paper, *Adapting to Climate Change: Towards a European Framework for Action*, is aimed at gettingpolicy-makersto understand climate change impacts with emphasis on policies with the optimal level of adaptation. The emphasis placed on climate change-resilient ecosystems means not simply trying to resist change, but working with nature’s ability to absorb or control impact. This is considered more effective and efficient than simply focusing on enhancing physical infrastructure (European Commission 2009b: 5).

The Commission is currently examining ways to improve the monitoring of impacts and adaptation measures so as to develop a set of vulnerability indicators. It is also seeking quantified information on the costs and benefits of adaptation while also analysing past efforts (European Commission 2009b: 8). The implementation of benchmarking is currently voluntary and non-binding, relying on self-assessments. It is intended, through current negotiations, to develop a framework with a set of standards and mechanisms that, while remaining non-binding, can be used to ensure that different actors can be held accountable for their actions. As a form of governance, it works by providing incentives for commitments to be met while ensuring ownership of the implementation process.

Standardisation is one technique by which the EU promotes a particular type of governance. The Commission began standardisation activities to better deal with adaptation considerations through European standardisation organisations (ESOs) to identify and map industry-relevant standards in the three designated priority areas – energy, transport and buildings. It also seeks to improve the market penetration of natural disaster insurance and insurance pricing and other financial products for risk-awareness prevention and mitigation which are seen as crucial for business and investment resilience (European Commission 2013a: 9). The ESOs will develop tools and guidance for standardisation, identify existing European standards and European standardisation deliverables most relevant for adaptation to climate change and draft new ones if necessary (European Commission 2014b: 3). The strategy sets out a framework and mechanisms for raising preparedness and resilience and does so by ”encouraging and supporting action by the EU Member States on adaptation”, providing the for better informed decision-making on adaptation and making key economic and policy sectors more resilient to the effects of climate change (European Commission 2013a: 11).

It is argued that standardisation efforts should also cover the overall actions relevant to risk management and that this should be supported by systematic actions to raise public awareness of risk and improve risk and crisis communication (education, involvement of media, networks). The main EU document on the Hyogo Framework for Action argues that:

The new framework should further contribute to enhance governance for disaster management at all levels and across all sectors, building effective coordination mechanisms and sustainable partnerships between different public authorities and relevant stakeholders (civil society, academia and research institutions, private sector). Involvement of relevant actors and communities in decision-making processes should be ensured through inclusive participatory mechanisms and the promotion of a right-based approach. Strong local structures and enhancement of local authorities' capacities are essential to improve planning and resilience of cities and ensure local political commitment and effective implementation of existing legal and policy frameworks. (European Commission 2014a: 8)

The need to involve communities and other relevant actors is a feature of EU strategy to shift emphasis away from reliance on physical infrastructure, particularly in relation to climate change. For example, coastal zone management strategy seeks a shift away from hard structures such as seawalls to protect coastlines and on to management policy to take into account adaptive local capacity. While engineering measures can improve the robustness and reliability of installations, more robust operational and maintenance procedures, demand management, forecasting and early-warning may prove more effective (European Commission 2013c). Perhaps the clearest statement of the promotion of the private sector comes in the Commission Communication *The post 2015 Hyogo Framework for Action: Managing risks to achieve resilience.* Here it is argued that the Hyogo Framework must be developed and implemented in close partnership with the private sector, international financial institutions and major investors. It argues for new initiatives to engage businesses and build partnerships across public, private and other stakeholders. It also places strong emphasis on the role of insurance and suggests that market-based instruments should be used to help those vulnerable disasters create effective financial contingency mechanisms (European Commission 2014a: 10). Similar suggestions for cooperation are contained in the EU’s response to the Sendai framework (European Commission 2016).

However, use of private insurance against risks is unevenly distributed across the EU with risk transfer varying by country. Most states are hesitant to outsource core tasks in crisis management to private companies although they do increasingly establish informal coordination mechanisms with private companies in areas like cyber-security and critical infrastructures (ANVIL 2014: 13). Primary emphasis on the private sector remains an Anglo-Saxon rather than European concern even if this is now increasingly promoted by EU bodies, particularly with ENISA, the body responsibly for information technology and cyber security. In other areas, to take a strong neoliberal approach would be to create significant political and ideological tensions and thus undermine the EU’s stated objective of better coordinating activities among Member States.

**Analysis: Infrastructure, disasters and governmentality**

Resilience features among all countries and organisations as a way of providing a more coherent approach to critical infrastructure. A good example of this is the UK’s Critical Infrastructure Resilience Programme which is concerned with promoting better communication, cohesion and planning across different sectors of government, society and infrastructure. In Germany and the US promoting a more integrated approach also reflects the federal political structure while in the EU such coordination must occur across member states.

Additionally, the Anglo-Saxon approach is marked by a concern with the role of individuals and communities. UK guidelines on emergency response and recovery invoke ‘all individuals and organisations’ as having a role to play and a responsibility to act (Cabinet Office 2013a). In the US responsibility of preparing for recovery ‘starts with the individual’ and integrates with the wider responsibilities of the community and local government. The National Preparedness Goal argues the need for the whole community to work together. Government therefore plays a supporting role, encouraging local initiative and installing a sense of responsibility among various actors. In the recovery phase, the best results are said to occur when communities can exercise a significant degree of self-determination. In the UK and US local communities are said to have opportunities for revitalising their environment through improving skills and knowledge and developing new commercial opportunities. This presents a more dynamic conception of resilience as transformative rather than simply reactive to crises.

One aspect of dynamism relates to the ability to embrace risk – indeed, it might be called governing though risk. UK guidelines describe this as ‘identifying, understanding, managing, controlling, monitoring and communicating risk’ with effective risk management the key to building resilience. This is particularly important in relation to investments and business continuity, promoting ‘organisational resilience’ in relation to uncertainties and disruptions to operation

(Cabinet Office 2011b: 14). A similar language is used in the United States (Department of Homeland Security 2013: 7) where the NISS approach emphasises risk acceptance, avoidance and transfer across various sectors of infrastructure. Risk is seen as a way of bringing together local and regional actors including public, private and non-profit organisations in order to develop various initiatives to support local resilience (Department of Homeland Security 2013: 22).

In Germany we saw that a risk-based strategy is also developing and that the Federal Ministry of the Interior (2009) calls this a ‘novel risk culture’. Indeed some of the conceptual arguments for resilience in Germany might actually better be understood as a more conventional argument for the development of a risk culture (Baban 2014). As with the US, there is also promotion of the private sector and private initiative. It is accepted that ownership and operation of critical infrastructure is passing into the private sector and that state responsibilities must be reformulated accordingly.

However, Germany differs from the Anglo-Saxon approaches by advocating strong state responsibility and legal protection. It is caught between the Anglo-Saxon promotion of private initiative and individual responsibility and a ‘whole of society’ approach emphasising robustness and resistance. The government’s research framework for civil security contains the following passage:

Civil security can only be guaranteed in the long term if the resilience of society is strengthened. For example, this would include improving the robustness and security of critical infrastructures and increasing the ability of the population to overcome crisis situations (Federal Ministry for Education and Research 2016: 13).

From a governmentality perspective, this places emphasis on enhancing the resilience of populations, but it invokes all of society and it emphasises robustness in relation to security strategy, something at odds with a neoliberal approach.

The introduction of resilience into discussions of French infrastructure protection follows a similar path. Following Bourcart (2015), we can say that significant privatisation of infrastructure provision means that the state and central government needs to justify the new situation. In particular, it works to legitimate public-private partnerships, business continuity planning and a certain amount of stepping back by the state through better involvement of local governments, individuals and infrastructure providers.

However, this is not really governance from a distance as understood by the governmentality account. Perhaps even more than in Germany, the French state remains the central actor with private companies and local actors having either little ability, or showing little interest in decision-making. As the main documents illustrate, the state has devolved some powers, but it continues to operate through decrees and legally-binding guidelines with the state showing little inclination towards promoting greater local autonomy (Bourcart 2015: 42). For their part, the private sector and municipalities show only partial engagement in the process with only 15 per cent of municipalities developing local emergency plans (Bourcart 2015: 49).

There are some similarities to the UK situation insofar as the UK’s Civil Contingencies Act also operates in a top-down prescriptive way, albeit with more interaction from those required to implement resilience plans. By contrast, the French private sector plays a largely passive role, encouraged by the belief that the state will continue to decide what is to be done. Most of all, while there is some devolution to the private companies and local government, there is not the same discourse of community and individual resilience present in Anglo-Saxon approaches to infrastructure protection.

Such differences are well illustrated in a scientific report by the High Council for Strategic Education and Research. In a section headed ‘Nothing is possible without genuine decentralisation’, it argues for a properly decentralised approach based on networks and locally situated and engaged actors. It goes on to note that France is the most centralised European country at a time when most problems require ever more localised solutions. Decentralisation is promoted as a more realistic way to harness the proliferation of social assets and French societal capacities. Indeed, the most important social dynamics run on complexities that are often ignored because of their informal, human character (Conseil Supérieur de la Formation et de la Recherche Stratégiques 2011: 29). In a later section of the report it is suggested that the resilience of a technical system, whether human or social, lies not in any simple capacity for robustness or ‘resistance’ to the threatening element, but in its agility, both human and systemic, in order to initiate the necessary changes (Conseil Supérieur de la Formation et de la Recherche Stratégiques 2011: 69).[[4]](#footnote-4)

The consequences of such a view are, however, politically complex. While it looks like this is advocating the Anglo-Saxon view of resilience as adaptation rather than resistance, the report goes on to defend aspects of the French system against Anglo-Saxon ‘individualism’ while also noting that the Anglo-Saxon approach is not necessarily compatible with French forms of capitalism. It is argued that it is not easily to change centuries of doing things a certain way, especially when centralisation brings certain benefits such as equal access to public services. Indeed the report, echoing a wider feeling in France and indeed in other European countries, says that it is still necessary to reaffirm the importance of this social model of equal access (rather than individual rights), emphasising the fundamental difference between this approach and the Anglo-Saxon model (Conseil Supérieur de la Formation et de la Recherche Stratégiques 2011: 10, 29).

We might say that this reflects a wider distrust of Anglo-Saxon models of individual behaviour, something we also found in French responses to the use of resilience in the White Paper on Defence and National Security. It reflects a continued belief in the role of the state as providing security and protection. Instead of neoliberal governance through denial of its obligations, this might be said to reflect a more progressive European tradition that sees the state as still obliged to protect people. In actual practice, however, this may not necessarily be the case. Recent policy develops do acknowledge the need for the state devolve powers, but this might indeed create a more confusing situation whereby the state seems to express its will to take a step back from its protective role, while not really being prepared to properly do so.

While still not particularly prominent in its policies, the emergence of resilience in EU policy making does raise questions about the purpose of EU strategy in these areas. In the case of European infrastructure protection we see resilience playing a limited role that is often synonymous with protecting the actual infrastructure and restoring its functioning in the case of a disaster. The transborder nature of infrastructure highlights the difficulties the EU faces in trying to coordinate collective action across the different member states. Not surprisingly, the main emphasis in the policy documents is for better, more coherent and more coordinated actions. In terms of the role of the Commission, it sees itself mainly as a facilitator that encourages such coordination through suggestion, policy recommendation, good practice, peer review, standardisation and evaluation and other measures that we have described as representing ‘governance from a distance’.

In the case of environmental policy we find resilience promoted as a response to climate change with emphasis on the need for adaptability in the face of developments that are increasingly difficult to control. More prominent here is the need for adaptability, making these arguments for resilience more like those of the Anglo-Saxon countries. This view tends to accept systemic crises and change as inevitable and therefore emphasises adaptation as the only realist response. Attention is shifted away from large-scale state intervention to protect and prevent in favour of government support to help citizens prepare and adapt in order to better cope with adversity. Emphasis is placed on pragmatic and ‘best fit’ solutions.

Some of the arguments relating to climate change response contrast with other arguments in favour of resilient infrastructure and highlight tensions in the EU’s understanding of resilience. Looking at some of the EU’s arguments about critical infrastructure protection, it is clearly not the case that the EU has abandoned the state’s role to protect and prevent. However, the adaption strategy for climate resilience does place greater emphasis on acquiring better understanding, involving the private sector, and better informing the community about how to deal with crises. Rather than putting more money into physical infrastructure protection, there is emphasis on management programmes. This goes some way towards the Anglo-Saxon approach without fully abandoning the idea that the role of the state is to protect people rather than to ‘help them to help themselves’ as the UK approach argues (Cabinet Office, 2011a: 4).

As it gets promoted more ardently, resilience will surely become more prominent within the already existing mechanisms of governance from a distance. What is questionable is whether this form of governance is really neoliberal in character as the governmentality critics would suggest is the case in the Anglo-Saxon approach to resilience. Hence while we find the *mechanisms* of governance or governmentality present in the way the EU seeks to work through the ‘conduct of conduct’, we do not really find a strong neoliberal *rationality* that attempts to instil in this conduct neoliberal values of enterprise and competitiveness. While EU policy accepts and promotes things like the private provision of infrastructure and services and seeks to build a network of private and quasi-private bodies, the strategy of distant coordination is more a product of the peculiar nature of the EU and the relation to member states rather than a stronger, more assertively neoliberal form of governance.

Summarising the situation of the EU’s uptake of resilience, it can be seen as based less on ideological commitment to Anglo-Saxon or neoliberal values, than to pragmatic considerations of infrastructure and civil protection and coordination issues relating to the Member States and other actors. Nevertheless, this does result in a form of ‘governance from a distance’ that shares features of the Anglo-Saxon and neoliberal approaches to governance and might indeed even be described as governmentality. The EU’s approach is to give preference to ‘conducting conduct’ through facilitation and suggestion wherever this is possible. This less direct form of governing is nevertheless backed up with regulative techniques, notably benchmarking, monitoring, best practice and peer-review.

The term has recognisability and it is seen as worthwhile to emphasise resilience in certain areas of policy making. But this fails to go much beyond using it as a fashionable buzzword and it fails to really acquire a deeper meaning. In the UK, policy in these areas invokes notions of individual and community responsiveness, awareness and preparedness, but these elements are underdeveloped in the EU’s arguments for resilience even if they have some presence in the area of environmental politics and the need for climate change adaptation. Nor is there any of the dynamism found in Anglo-Saxon approaches which go beyond the idea of protection and returning to normal, to emphasise how crises provide opportunities to build new relationships and generate new ways of operating (Arnold, Mearns, Oshima, and Prasad 2014: 5).

Instead, a considerable amount of the EU’s concern is directed at problems of coordination, both across different member states and over different areas and scales. Attempts to develop an EU approach are channelled through questions concerning areas of competence and subsidiarity. While there is a strong emphasis on cooperation, learning and shared practice, this raises questions about the purpose of cooperation and whether this is undermined by differences of priority and understanding. For example, member states may have different national security priorities, different expectations and a different relationship with their citizens, civil society and the private sector. This is particularly the case with a notion like civil protection which combines a security dimension with a relationship with civil society or community – something that various significantly across Europe and which is also affected by different legal systems and constitutional settlements

Nevertheless, the Commission has for a long time been emphasising Europe’s global challenges, particularly in relation to new threats, a more competitive global environment and Europe’s less secure position in the world. While not presented in a particularly innovative or dynamic way, the connection between resilience and adaptation is slowly developing, set within the context of the neoliberal tendencies of Europe 2020 and its arguments for socio-economic restructuring. For this reason, and regardless of the difficulties in presenting the Anglo-Saxon ‘vision’ of resilient Europe, the EU is gradually putting in place the kind of framework that would allow resilience to come to the fore as a major idea. Due to the dynamics of governance from a distance with its dissemination of policy proposals, standardisation procedures, use of indicators, benchmarks and more compelling forms of obtaining compliance, we might, despite opposition, expect the EU to move in the direction of the Anglo-Saxon view of resilience, albeit with significant internal tensions.

**Conclusion**

We can summarise the differences in cases in the following way. The UK and US share an Anglo-Saxon approach to resilience in infrastructure, disasters and emergencies. We can describe this approach as governmentality because it seeks to govern from a distance, devolve responsibility to individuals and communities, place heavy emphasis on the role of the private sector, invoke innovation and enterprise, and combine emphasis on adaptation with a view of resilience as transformation of communities. By contrast the French and German approaches to infrastructure and domestic emergencies has only just started to talk of resilience, often without the above connotations. Hence resilience does not play the same role as a tool of governmentality – indeed, its place in the wider discourse causes certain tensions and contradictions. This is also the case with the EU, although we saw that the EU has its own reasons for developing the idea further.

This leaves us to return to the UK approach in order to raise the question of whether there are in fact some contradictions and tensions in the Anglo-Saxon approach itself. While the UK approach looks like neoliberal governmentality, does it actually meet all of the elements of governmentality mentioned above? We might say, first of all, that the UK approach is perhaps not so ‘distant’ as it first seems. This is not as contradictory as it first seems since our understanding is that neoliberalism seeks to ‘create’ free subjects. It should therefore not be a surprise to find the UK state playing a leading and directing role. Although the UK’s Critical Infrastructure Resilience Programme encourages ‘voluntary cooperation’, it admits that stricter legislative powers may also be used. We also noted how the preferred form of ‘governance from a distance’ is supported by extensive monitoring techniques, information gathering and various forms of assessment and performance measurement. Hence the notion of community resilience should be tempered with the knowledge that the state contains to play the dominant role and that it maintains considerable powers of intervention and enforcement. This is particularly the case, as we saw in the last chapter, where questions of national security are involved. Counterterrorism measures are coercive, regardless of appeals to community resilience. However, while there is less need for coercion as in cases like flood protection, there is still a strong top-down element to the ‘devolution’ of responsibilities.

We will pick out a couple of critical interventions to make this point. First, the work of Tudor Vilcan can be used to examine the practices of flood protection in the UK and to question whether community resilience really is a genuine thing. Vilcan notes the aim of the strategy is to ‘re-orchestrate’ the distinction between the state as protector and the passive public as one between ‘state as enabler and individuals as active participants’ (Vilcan 2017: 33). Paradoxically, of course, it is the state that does the re-orchestrating. How does empowerment of the community work? Who is to be listened to? Vilcan’s study of resilience-building for flood protection finds that the government ‘frames’ empowerment in a certain way that narrows the voices of the community which is effectively reduced to members of flood groups. These flood groups rely on a few key people and are certainly not representative of the whole community. Moreover, the government’s flooding Evaluation Report avoids political questions, framing engagement with the community in terms of an awareness raising exercise, fed down to the community level in the manner of an outreach programme (Vilcan 2017: 39-40). This suggests that community resilience is more of a government fabrication, rather than an organically emergent community concern. Moreover, as O'Brien and Read suggest (2005: 359), public awareness campaigns often have little impact on preparedness at the individual and local level.

The critical intervention by O'Brien and Read is also useful in challenging some other aspects of the UK approach to resilience in this field. They question the government’s priorities in a number of ways. They argue that many of the changes claimed under the framework of the Civil Contingencies Act are really codifications of existing practices with most responsibility continuing to fall upon emergency responders. Where the government has made significant structural changes to civil protection, they raise questions of whether the government really has taken a more holistic approach, or whether it is actually focusing on selected areas (O'Brien and Read 2005: 356). In particular, they note that while the amount spent on civil defence has increased, the figure is miniscule in comparison to the amount spent on the UK’s counterterrorism activities (O'Brien and Read 2005: 358).

As we move on to look at overseas interventions we might conclude, therefore, that building local, national and transborder resilience is certainly a developing field. But it is an uneven field, with many of the old practices, discourses and government priorities still evident and with significant tensions over both understanding and implementation of resilience-building measure. This clearly applies, to France, Germany and the EU, but it is also evident in the Anglo-Saxon approach, despite this being the dominant one in this area.

1. La résilience se définit comme la volonté et la capacité d’un pays, de la société et des pouvoirs publics à résister aux conséquences d’une agression ou d’une catastrophe majeures, puis à rétablir rapidement leur capacité de fonctionner normalement, ou à tout le moins dans un mode socialement acceptable. Elle concerne non seulement les pouvoirs publics, mais encore les acteurs économiques et la société civile tout entire. [↑](#footnote-ref-1)
2. Un PIV est un établissement, une installation ou un ouvrage sis sur le territoire national dont le dommage, l’indisponibilité ou la destruction par suite d’un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement : - d’obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ; - ou de mettre gravement en cause la santé ou la vie de la population. [↑](#footnote-ref-2)
3. Une infrastructure critique est un « point, système ou partie de celui-ci, situé dans les États membres, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l’arrêt ou la destruction aurait un impact significatif dans un État membre du fait de la défaillance de ces fonctions ». [↑](#footnote-ref-3)
4. La résilience d’un système technique, humain ou social ne réside pas dans sa simple capacité de robustesse ou de « résistance » à des phénomènes menaçant son intégrité et sa pérennité. La résilience d’un système réside dans son agilité, aussi bien humaine que systémique, proper à engager les transformations nécessaires avant la rencontre de ses points de rupture. [↑](#footnote-ref-4)