Dezember 2016

Österreichisches Institut für Internationale Politik
Austrian Institute for International Affairs

‘Keep Calm and Carry on’? Resilience and UK Security Policies

Working Paper 91/2016

Sarah Ponesch

Abstract

In the UK context of National Security Strategies and Critical National Infrastructure Protection, resilience is understood as a result of, or an answer to, an ever changing, complex and interconnected world in which even a tiny event can have a huge impact. Resilience incorporates the need to adapt to an almost infinite variety of hazards and risks and could therefore be called an all-hazards approach in the wider realm of security. However, an analysis of UK security policy documents and qualitative in-depth interviews with a variety of stakeholders shows it is more than that. Resilience is framed as a means to address change in general. It includes not only the negative aspects of globalisation but also its opportunities. Moreover, resilience is understood as a whole-of-government, if not whole-of-nation attempt to 'connect the dots' and overcome the 'silo thinking' in order to see the 'bigger picture'. Therefore, resilience, in the UK, is often understood as a form of culture rather than a tool, instrument, concept or approach. In order for it to 'function', resilience has to overcome and reach beyond simple top-down or bottom-up approaches. It has to be lived.
Keywords: *resilience, security, risk, change, critical infrastructure, United Kingdom*

Zusammenfassung

Das vorliegende Arbeitspapier beschäftigt sich mit der Ausgestaltung von Resilienz in Großbritannien, speziell in Bezug auf die jeweiligen Nationalen Sicherheitspolitiken sowie den Schutz Kritischer Infrastrukturen. Dabei wird anhand von Interviews mit staatlichen und nicht-staatlichen Akteuren sowie einer Policy-Analyse relevanter Dokumente sichtbar, dass Resilienz im Falle von GB nicht allein die Kurz- sondern ebenso die Langzeitperspektive inkludiert. In diesem Sinne zielt Resilienz nicht allein auf die Fähigkeit ab sich von Krisen zu erholen sondern sie wird ganz allgemein als unumgängliche Antwort auf eine Welt im Wandel verstanden. Dabei soll es vor allem darum gehen, das große Ganze in den Blick zu nehmen und jenseits von Silodenken der voranschreitenden Komplexität gerecht zu werden, in dem duale Ansätze von „bottom-up" und „top-down" überwunden und in Form einer „Resilienzkultur" gelebt werden.
Schlüsselwörter: *Resilienz, Sicherheit, Risiko, Wandel, Kritische Infrastruktur, Großbritannien*

Author

Mag. Sarah Ponesch is a researcher at the Austrian Institute for International Affairs (oiip). Her main research interests include in the interconnections between (Queer-)Feminist and Postcolonial Studies, Critical Security Studies (CSS) and Science, Technology & Society (STS). She currently works on a project about the governance of resilience, which is funded by the anniversary fund of the Österreichische Nationalbank (OeNB Jubiläumsfonds).

This work was supported by the Österreichische Nationalbank (Anniversary Fund) under grant no. 16601 and is carried out in cooperation with the Donau University Krems.

Introduction

> *It is a challenge to define what resilience is and what it means in practice for organizations and professionals. (Higgins, Business Continuity Institute, 02:20)*

There is no absolute agreement about what resilience means, does and should do. It is sometimes understood as a buzzword (Walsh, 2013), a value (Zebrowski, 2016), a tool, or a mode of governance (cf. Joseph, 2013). However, although highly context-dependent, it seems to include several main characteristics, which are commonly shared by academics, security policy actors and UK stakeholders alike. The aim of this working paper is to identify the similarities and differences between the various actors about what resilience means, what its (dis)advantages are and how it unfolds in practice. It tries to trace what the paper identifies as the UK specificity of resilience as a 'culture', and as an answer to an ever-changing world. Thereby it includes questions about short and long term aspects and challenges and opportunities regarding a new understanding of an uncertain future. It does so by analysing UK security policies, namely the National Security Strategies (NSS) as well as its stand on Critical National Infrastructure Protection (CNIP), and drawing on interviews with various (non-)state UK stakeholders.[1]

This paper will at first discuss the historical and current (institutional) resilience approaches and implementations in the UK. Second, it will address the question if, and if so, how, resilience has changed the relevant stakeholder landscape and the distribution of responsibilities between them. Third, the paper will discuss the various modes at work in what UK stakeholders have called 'resilience culture'. It then elaborates the roles of values and leadership in this context. Fourth, the paper will demonstrate that resilience is understood as an answer to change in general and thus asks how resilience can or should work in practice. After touching upon its (dis)advantages as well as its relationship with security, this paper will conclude by giving an outlook for the future of resilience and resilience future(s) with regards to UK national security policies.

[1] The author conducted five interviews with high level UK resilience stakeholders working for (non-)governmental as well as private business organisations. They were carried out in London between May and June 2016.

Now and then – UK resilience in its historic and current dimensions

First mentioned by the National Security Strategy (NSS) in 2008[2], resilience introduced a shift from the narrow realm of traditional defence to 'softer' elements of security policies (cf. Pospisil & Gruber, 2016). While resilience in the international context was closely linked with the topics of climate change and (lack of) natural resources, its introduction on a national level focused on disaster control and crisis management (cf. Manyena, 2006). However, this limited focus subsequently was broadened.

At current, resilience ranges from the protection of critical national infrastructure to civil emergencies, pandemics or terrorist attacks. Contrasting some scholarly accounts which argue that resilience signifies the drawback of the state and the externalisation of its responsibilities (cf. Joseph, 2013), the state, interestingly, took over more responsibility following the introduction of the new civil contingency policy after the end of the Cold War. The most severe change can be identified as a closer engagement of central state departments and the Civil Contingencies Secretariat in regard to civil emergencies (cf. Pospisil & Gruber, 2016; Smith, 2003). At a bureaucratic level, the Civil Contingencies Secretariat (CCS) is the key governmental player when it comes to resilience and security policies. It is part of the National Security Secretariat and includes various tasks which are described as follows:

- *The National Risk Assessment and National Risk Register (identifying and assessing risks to national safety and security arising from terrorism, major industrial accidents and natural hazards, over 5 years)*
- *The National Security Risk Assessment (identifying global risks to UK security interests, in a 5 to 20 year timeframe)*
- *Leading a cross-government resilience capabilities programme to improve public sector response to such emergencies*
- *Contingency planning and capability building for the risks of catastrophic emergencies*

[2] 'Traditionally, the Government has been expected to deal with the threats and risks to national security through the Armed Forces, the police, border staff, and the intelligence and security agencies. Increasingly, the changing nature of the threats and risks, and our improved understanding of the best way to respond to them, demand broader partnerships. We will build on the coalition of public, private and third sectors already involved in counter-terrorism. We will work with owners or operators to protect critical sites and essential services; with business to improve resilience; with local authorities and communities to plan for emergencies and to counter violent extremism; and with individuals, where changing people's behaviour is the best way to mitigate risk' (HM Government, 2008, p. 8).

- *Policy for secure and resilient national infrastructure, and corporate resilience in the private sector (Centre for Science and Policy, University of Cambridge, 2016)* [3]

Furthermore, the secretariat is meant to support the Prime Minister as well as the cabinet especially in relation to questions about civil emergency planning and response.

In contrast to the common assumption about resilience as a rather short-term ability to 'bounce back' from a crisis, the respondents stressed the importance of including short as well as long term perspectives. What resilience actually encompasses when looking at the 'bigger picture' is illustrated by the graph shown below, which was depicted by one of the interview-ees (Interview 2):

Resilience

Timescale	Acute	Chronic
Nature of disturbance	Shock	Stress
Respond to disturbance	Continuity	Adaptability

However, one critical aspect is the question of how to differentiate between short and long-term aspects. As Emily Hough from Crisis Response Journal (CRJ) claims, '[i]t is like being in the eye of a storm. You don't know when the worst of it is over. You think this is a shock now, but it might just be the edges of a storm and it's going to be a hell of a lot worse – but how to define long-term within that context?' (Hough, CRJ, 34:48). The illustration highlights one aspect about resilience that the main stakeholders in the UK context identified as key: its proactive element. This particularly involves the inclusion of *impact* as well as *cause* and can be described as follows:

> *So you are really sort of thinking about risk mitigation not just as impact mitigation, you are thinking about it in terms of cause mitigation as well. And that is thinking which is very, very much, characteristic of resilience. Because you are not just looking at the response element. You are looking at the cause or the long term, the context and so on. (Interview 2, 18:54)*

[3] CSaP, see http://www.csap.cam.ac.uk/organisations/civil-contingencies-secretariat/

As described by one interviewee, this shift in the application of resilience resulted from the 2010 National Security Strategy. Back then the strategy was still based on what can be called an 'all-risks approach' where the consequences of certain risks were understood as common, but there still were separate planning processes going on. This changed with the state minister of security at that time, Lady Neville-Jones, who addressed this former practice as a waste of (human) resources. Instead of treating the identified risks and their respective state departments and actors as separate issues, she argued for a joined up effort towards the respective matters:

> *You counter-terrorism people, you civil emergencies people, you are going to work out a single framework whereby we will understand the common consequences of things. And we will prepare the capabilities, plans etc. to deal with them. … But where we need to think separately about terrorist threats, or accidents, or errors or other forms of risk then we will do so. So there is this phrase of this coming together of all risks to have certainly more efficient and I think more effective approach to thinking about resilience. (Interview 2, 41:04)*

These developments point towards a shift in the general assumptions about the future. While the threats to a state like the UK were formerly understood as calculable, this perception changed after the end of the Cold War and especially since 9/11 (cf. Aradau & Munster, 2011) and, especially in the case of the UK, 7/7[4]. Resilience strongly resonates with the fact that security *no longer* can be guaranteed due to the permanent (latent) presence of known or unknown risks (Corry, 2012; Pospisil & Gruber, 2016). Instead of solely relying on the knowledge of risk assessments, this new perspective rests upon and reproduces the assumption that '[w]e [the UK] are entering an age of uncertainty' (HM Government, 2010, p. 3). Although this one is taken from the old NSS from 2010, it resonates with recent statements, along which 'the world is more dangerous and uncertain today than five years ago' (HM Government, 2015, p. 3). Here, unpredictability and uncertainty are even more pronounced than in the NSS 2010. Especially in light of these changes, UK security policy designs resilience to be an adequate answer to the supposed increase in the potentiality of danger and uncertainty but, as we will see, also as an enabler of new opportunities.

[4] The term 7/7 refers to a series of suicide bombings targeting the London transport system on 7 July 2005.

Resilience culture, leadership and values in the UK

While the rise of resilience in the context of national security policies chimes with an international trend since the 2000's in states like the US, Israel, Singapore or Australia, it has very specific national connotations. One factor that the interviewees identify as key is the element of leadership, or more specifically '*visionary* leadership' (Hough, CRJ, 44:36; highlighted by author), as a central aspect for the success of resilience. Moreover, the interviews unanimously connect such leadership characteristics with the embracement of specific values, thus fostering a certain UK self-image or national identity (cf. Interview 2; Caddick, Pricewaterhouse-Coopers (PwC); Hough, CRJ). As Martin Caddick from PwC highlights, 'if I wanted to create a resilient organisation … it starts from the top. … You need to understand what you're about and you need to communicate that clearly. I think the same is true nationally as well. This is what we stand for, these are the things that matter to us' (Caddick, PwC, 53:04). Caddick goes further and claims that

> *the key to understanding resilience is understanding what's important to you: to you as a business, to society, to the government. Understanding the things that you depend on, and the factors that make those dependencies more or less resilient. And managing that. You don't know what's going to happen, but you can make yourself better able to respond and more likely to survive. (Caddick, PwC, 32:20)*

In this sense, resilience becomes a mechanism to deal with uncertainties while nevertheless following certain goals that may change over time but are still guided by very specific visions and values, be they for an organisation or a society. Resilience, hence, does not necessarily mean to simply 'going with the grain', but instead to identify and to realise necessary achievements in spite of increasing interdependency and change across the globe. In accordance, the NSS (2010) describes the UK's 'place in the world' like this:

> *Our strategy reflects the country that we want to be: a prosperous, secure, modern and outward-looking nation, confident in its values and ideas. Our national interest comprises our security, prosperity and freedom. We must be a nation that is able to bring together all the instruments of national power to build a secure and resilient UK and to help shape a stable world. Our outlook will be characterised by flexibility and resilience*

> *and underpinned by a firm commitment to human rights, justice and the rule of law. (HM Government, 2010, p. 10)*

Although this strategy is six years old, it still holds true for the current self-proclamation of the UK. The aspects of its openness as well as its central role in the world market and its global influence in promoting its values are considered as the main building blocks of the nation (see HM Government, 2105). Against this background, I argue that security policies in general and NSS's in particular are part of an intended, policy-led nation-building process. Thus, they simultaneously signify a nation claim while at the same time producing the very object they rely on – the nation.

The openness of the UK is continuously mentioned as a great opportunity concerning the free market, but at the same time framed as leaving the nation vulnerable to a whole variety of threats and risks, 'natural' as well as 'human made' (HM Government, 2010; HM Government, 2015). The known and unknown risks resulting from the interconnectedness of the UK, the networks of institutions, people, technologies and things, are especially relevant when it comes to the protection of Critical National Infrastructure (CNI) as 'the networked world creates great opportunities but also new vulnerabilities. In particular, protecting virtual assets and networks, on which our economy and way of life now depend, becomes as important as directly protecting physical assets and lives' (HM Government, 2010). Resilience, then, can be understood as 'an intelligent program to keep yourself [and your CNI; *author's note*] healthy… And healthy appropriate to your lifestyle. You know, to the things that you want to do' (Caddick, PwC, 33:13).

Since more than 80 percent of the UK CNI is run or owned by private companies, the cooperation between state and private businesses is crucial when it comes to their functioning. Therefore, Public-Private-Partnerships are perceived as unavoidable. This leads to the question of the distribution of responsibilities (HM Government, 2015, p. 44). Based on the Civil Contingencies Act of 2004, a regulatory framework legally obliges CNI companies to meet certain standards.[5] Yet, as the interviews showed, the act is no longer understood as sufficient to meet the necessary requirements to enhance resilience on a broader level. Instead, the inter-

[5] 'Resilience, generally as a concept, is something that we are working on at an international standards level' (Hall, London First, 02:25).

views emphasise the fact that Civil Contingencies Act, being more than ten years old, needs to be updated in order to address the present needs. As stressed by one interviewee, one major shortcoming in this regard is the neglect of 80 percent of the businesses, since the act solely aims at the inclusion of local authorities and key providers (Hall, London First, 08:05). In addition, although it is used as a major source for the implementation of resilience, the Contingency Act never actually mentions the word resilience (see Civil Contingencies Act, 2004).

The question of how the government can ensure the basic requirements of CNIP is another aspect that needs to be taken into account. (cf. Hall, London First). Implementing legally binding instruments is thereby an ambiguous task: while they are perceived as important in order to get private businesses to implement certain standards to ensure the resilience of CNI (Hall, London First), they themselves may result in repercussions on smaller businesses (Hough, CRJ). Such instruments could thus reinforce the concentration of financial powers in the hand of only a few big companies. Hence, the trick is to get companies to invest in resilience, as 'something that they are not really interested in doing' (Hall, London First, 10:32), while at the same time keeping the balance between big players and SMEs. This is no easy task since, according to Emily Hough, regulations are

> *absolutely well thought out, there to protect everywhere down the chain, but by doing so you can make it impossible for smaller organisations to take part because the barriers are prohibitive. It can demand resources that SMEs simply don't have. They don't have big administrative departments or HR departments and that's an overlooked effect that just concentrates the financial power in bigger groups. (Hough, CRJ, 41:06)*

When asked about the tensions between short-term profits of privately run CNI and the long-term goal of their continuous functioning for society's basic needs, the interviewees unanimously agreed that some businesses – including those in charge of CNI – are mainly interested in short-term profits, which inherently contradicts resilience. 'Money saving and efficiency is the enemy of resilience. You know, resilience likes redundancy, resilience likes buffer stock' (Caddick, PwC, 44:32). Thus, resilience 'can't be done just on a cost basis. It is more than just cost, you need to factor resilience in' (ibid., 46:07). It is precisely these kinds of tensions that create a 'conflict between the private sector and the public good' (Hough, CRJ, 36:42). It may be argued that these new forms of PPP's are able to foster or to enable a stronger implementation of resilience. Yet, it cannot be overlooked that

> *a lot of it [CNI] is in the hands of private sector, yet the ramifications if something were to happen, are very, very public, and not least to mention who would pick up the bill and so forth. And these are just the areas that we have anticipated. But the last ten years have shown that we cannot possibly predict the type of crisis and emergency that we will face in the future. We have got an idea, but we don't know how that will manifest itself and in what form. (ibid., 06:08)*

As an answer to the difficulties in the distributions of responsibility, respondents (cf. Hall, London First; Higgins, BCI) highlight the importance of (inter-)national standards that are currently in the making (ISO22316) or have already been published in 2014 (BS65000). This relates to another question necessary to be addressed, the question of uncertainty and risk (management).

Resilience as the culture of change?

> *It's not just about reacting to threats in the marketplace, it's about reacting to changes in the marketplace. (Caddick, PwC, 21:07)*

As the two exemplary extracts from the NSS of 2010 and 2015 have shown, the idea of resilience reflects the idea of an uncertain future. This future is regarded as being full of increasingly diverse risk perceptions, which are drawn by National and Local Risk Registers alike. The identified risks are thereby ranked along the lines of likelihood and impact, thus creating a system of guidance for their prioritisation in the (National) Security Strategies (see HM Government, 2015). Nevertheless, this risk assessment approach is no longer sufficient in light of the radical changes in a world that is widely regarded as being more and more unpredictable (cf. Pospisil, 2013):

> *The world is changing rapidly and fundamentally. We are seeing long-term shifts in the balance of global economic and military power, increasing competition between states, and the emergence of more powerful non-state actors. We are increasingly likely to have to deal with unexpected developments. (HM Government, 2015, p. 15)*

Or as one of the interviewees states, 'probability is a useless measure. In risk matrices based on probability and impact, it is increasingly hard to gauge probability in unpredictable and complex systems. But it's not just probability – because when you look at potential impact, it's becoming equally hard to predict the impact of a risk' (Caddick, PwC, 30:51). Caddick challenges conventional risk management approaches, and claims that there is 'a lot of chance in impact. So you can't really predict the impact. So what use is risk management?' (ibid., 31:28). Further, resilience not only includes the possibility to deal with these kinds of uncertainties, but takes on this ability as one of its *main characteristics*. In this sense, resilience fosters the proactive engagement with the kinds of changes that can neither be predicted nor prevented.

When asked about whether resilience applies in the same way for counter-terrorism as it does, for example, for disaster management or cyber security Deborah Higgins from the Business Continuity Institute (BCI) says that

> *it is everything. It is not just about hazards though. Not just things that go wrong. It is change generally. Rather than all hazards, the new international standard for organisational resilience [and resilience in general; author's note] is talking about adapting to change. Change could be a hazard, fire, flood, cyber, terror, as much as it could be an aggressive hostile take-over in your market place, and damage to your business from a competitor. What makes organisations resilient is being able to, having the capability to adapt to that. (Higgins, BCI, 31:57)*

What this general capacity or inherent quality of resilience means in relation to change, notwithstanding negative or positive, will be discussed in the following chapter.

Means to an end or means in itself?

In contrast to the common understanding of resilience being bound to change, there is disagreement about the question of what resilience actually is. Although strongly related to the previous discussion about resilience culture, leadership and values, it seems to be unclear whether it is a *goal* in itself or a *tool*, an *instrument* or *approach* to achieve something else, e.g. a strategy. Resilience, then correlating with the call for a strong national identity, is regarded as a possibility to deal with the ongoing dynamics of an ever changing world in order to achieve a certain goal which is not resilience itself. Instead, it is perceived as 'a means to an end not a means in itself' (Interview 2), which then can be understood as an instrument to arrive at a very specific aim. However, this position was opposed by other interviewees who claimed that resilience itself should be the goal to aim for:

> *Resilience can be thought of as a goal to aspire to, a desired state, it provides a strategic rationale for many of the protective functions. The word resilience is creeping into an organization's policies and plans, but there is no exact science or guidance of how to do it. (Higgins, BCI, 45:35)*

Contrasting this understanding, one perspective offered during the interviews was that 'resilience applies or it doesn't apply but it is not a finite journey. Because you are always going to be working towards it, and you think of change, and you are going to be more and more progressive. So it's not a destination, it's a journey' (Hall, London First, 17:02). As already discussed, resilience gets exposed to its own vagueness at this point.

These tensions within the notion itself are exemplified by the following positions: one interviewee claims that 'resilience is a fundamental aspiration that we should be working towards. It is absolutely vital in every sense. That's personal resilience, that's professional resilience, that's critical infrastructure resilience, disaster resilience – all these things. But how to bring them all together?' (Hough, CRJ, 07:32). What seems to oppose this statement is the suggestion of another interviewee to always ask *why exactly* a person values resilience. While it seems to be the case that resilience has almost become self-evident – which is often described as one of the main challenges regarding the question of what it can and should do – the interviewee states that it is exactly the engagement with this supposed self-explanation that can lead people towards identifying their goals. 'Resilience has no inherent, in nature, intrinsic

value. It has value because it enables you to do something else, or be something else, or achieve something else. So in that sense I would always regard resilience as an *enabler*' (*highlighted by author*; Interview 2, 24:32).

What links the varying positions of the interviewees is the idea that resilience should not mean to adapt to just *anything,* but instead it should serve as an enabler to achieve *something specific*, like an organisational, personal or national *strategy.* What is considered important in this regard is being clear about your values as well as your goals, or in other words, 'resilience is being true to where you come from but achieving where you want to go' (Interview 2, 29:17). This idea is further exemplified by the following citation from the NSS 2010:

> *Any strategy for our national security must begin with the role we want Britain to play in the modern world. In a world that is changing at an astonishing pace, Britain's interests remain surprisingly constant. We are an open, outward-facing nation that depends on trade and has people living all over the world. (HM Government, 2010, p. 4)*

Therefore, resilience could be understood as a necessary answer to an ever changing world by including capacities such as adaptability, flexibility, coping, redundancy or absorbance. Coming back to the question of leadership and values, it seems that resilience could serve as a means to protect the relatively stable national interests, not in spite of but *through* or *because of* these obviously fluid qualities.

Resilience at work – Connecting the dots, permeating the silos

Another consensus about resilience is its capacity of 'seeing the bigger picture', having the 'birds eye view', 'connecting the dots' or in other words 'not to develop something new. It is a different way of looking at what you already do' (Higgins, BCI, 44:47). Resilience not only aims at a multi-actor as well as multi-level approach, but *demands it* in order to work. Or, in other words,

> *the fundamental metaphor I always reach for when talking to people about resilience is joining the dots. And that kind of implies it is multi-actor. You got people who do this,*

> *you got people who do this, you have got people who do both. But you've got to get them all working together. (Interview 2, 37:35)*

Looking at the multi-actor element, resilience is commonly described as enhancing cooperation between the already established stakeholders, while also including new ones. The idea that resilience necessitates the cooperation of various levels and actors of state, business organisation and society is thus widely accepted. Or, as the NSS (2015) states, '[t]he UK's resilience depends on all of us – the emergency services, local and central government, businesses, communities and individual members of the public' (HM Government, 2015, p. 43). This was already described in the NSS of 2010, which states that

> *we need to build a much closer relationship between government, the private sector and the public when it comes to national security. Of course, the Government has a crucial role to play, and we will certainly fulfil our responsibilities. But we all have a part to play in keeping the country safe – be it from terrorists, cyber-attack or natural disasters. (HM Government, 2010, p. 5)*

The main question, then, remains how to achieve an improved cooperation between the various stakeholders? How can and shall resilience actually work? The NSS 2015 stresses that the government promotes and practices 'local cross-border coordination between responders, where required' (HM Government, 2015, p. 44). In cases of extraordinary emergencies, especially the ones that impact the UK as a whole, they link the UK government's emergency coordination structures with the ones of the devolved administrations in order to guarantee a coordinated response.

This is regarded as particularly relevant in events that affect the CNI (ibid.). One interviewee points out that the civic engagement in the coalition of stakeholders fostering resilience does not have to be newly invented all together, but could rest upon older institutional measures which were installed during the Cold War. The respondent claims that 'we need some sort of organised structure like that [civil defence during the Cold War; *author's note*] to assemble the volunteers. Because I think that the threats today, and it's not just terrorism, are so great that we can't just cobble it together when something happens' (Hall, London First, 05:56). This suggestion resonates with other recent recommendations in Germany (FAZ, 21-08-2016) or Sweden (see Gruber, 2016), which advocate for the revival of older civil defence instruments.

Still, this does not fully address the question from above, which not only relates to the organisational aspect of the coordination of emergencies but also to resilience in general, including its 'vision'. There is no straightforward answer, but, according to Deborah Higgins from the BCI, it certainly includes 'further collaboration between business functions and fostering a culture of resilience aligned to the values and beliefs of the organisation' (Higgins BCI, 46:53). Again, this citation resonates with the section about values discussed above while connecting it to the question of how resilience works in practice.

According to the interviews, resilience can only work top-down *as well as* bottom-up. More specifically, one could argue that it has to precisely overcome these dualisms and be applied to policy culture, or even culture in a much broader sense, in order to work. Three major topics raised in this regard are *awareness*, *knowledge* and *cooperation*. Identified as the main building blocks, they help enhance resilience through the multifaceted layers of the state, private businesses and society. As mentioned by one interviewee, it is essential not to rely on 'accepted wisdom' (Hough, CRJ) without questioning it and asking 'how much have they actually listened?' (ibid., 23:41). Further,

> *in large organisations you have to have roles and structures, and I understand that. But when you are sitting through the 100th most boring meeting that you have sat through in the last year, it is easy to switch off and reduce the issues to safe words, accepted terminologies and long-established policies and plans. You need to actually bring the issues to life again, to show the possible ramifications of an incident, without being hysterical about it. One possible solution could be to bring more creative vision back into training, to challenge people's assumptions and bring them out of their comfort zones. (Hough, CRJ, 24:04)*

Resilience, hence, seems to include different elements or roles with respect to where one stands. While UK resilience is essentially based on leadership, which, as already mentioned, comes down to identifying and following your very own strategy, resilience also has be rooted and lived through a culture that goes through various 'degrees and levels' (Higgins, BCI, 00:36:36). One of the many difficulties here is to overcome the habit that 'everyone falls back on what they know' (Hough, CRJ, 24:32). A telling comment by one of the interviewees claims that

> *you have got to allow people to be able to think, so they have resilience firmly underpinning all their actions. And everyone in whatever sector or department has to understand that resilience should be a fundamental tenet of that. Everything they do, both as standard good practice for the success of an organisation, and to withstand any external shocks. They must be able to think about it and have the autonomy and the permission to act as they see fit. And they must be allowed, indeed encouraged, to think creatively without fear of reprisal, being pilloried in the media or being 'punished' in some other way. (Hough, CRJ, 11:16)*

However, what happens if the leadership vision of resilience clashes with the interests of communities or individuals? In order to summarise this tension, one of the main challenges remains that '[r]esilience governance in the realm of nation-state based security policy necessarily has to face the paradox of inducing a societal process in a top-down, or "macro-structural" manner' (Pospisil & Gruber, 2016, p. 4; cf. Wilson, 2014). Hence, if the two starting points from 'above' and 'below' do not work together, or maybe even if they are not overcome, resilience cannot work. In this sense '[t]he challenge is how. Because everyone is already doing what they regard their responsibilities and their activities. So to me it is the coordination of it all – whose role and whose job is it to coordinate all of this together. At a governmental level that is the challenge' (Higgins, BCI, 48:59). In other words,

> *[you have] all these lovely departments in silos and there is nobody in government controlling it, you know linking it together, in a concerted way. And that's the weakest part I think in the governance of resilience. Until you have someone in charge, either a minister of civil affairs or a minister of resilience, someone who can join the dots, I don't think you have true governance. (Hall, London First, 05:13)*

Resilience, as the interviews show, aims at permeating the boundaries between the different 'silos', be it governmental departments, responsibilities or activities. As one interviewee stresses, 'people still are not recognising the interdependencies and the mesh that has to be created between public sector, private sector, all the disciplines, citizens themselves… between security NGOs who have got to learn to talk to the military, the military, which has to engage with NGOs' (Hough, CRJ, 05:11). Pointing out a critical aspect, the respondent elaborates that 'they do it at the moment but with great suspicion, because there are implications

for their own personal security and safety and of those they are trying to assist' (ibid., 05:22). Yet, it is important to stress that this does not mean 'merg[ing] all the silos together [into] […] one massive super department' (Hall, London First, 18:31). Instead, 'they just have to break down the barriers, make them more permeable, so that joining the dots, as we say, can be easier' (ibid.).

The silo metaphor is stressed widely among respondents: '[g]overnment is better than it used to be but remains in the idea of silos and activities. Government will always be siloed. And our job is to make them porous and lower. But sometimes they go quite high' (Interview 2, 51:51). While these measures to improve cooperation between the different departments as well as between state, private industry and civil society are highlighted as being necessary in order to foster resilience, and therefore inherently positive, there seems to be another, precarious side to resilience – both of which will be discussed in the next chapter.

Resilience and its (dis)advantages

> *Resilience to one person or organisation may mean something different to another. I have never met anybody who said they don't want to be resilient. That's not something anybody would say, because you like to be resilient and bounce back from misery, from ill health, from any kind of disaster. It is often heard after the terror attacks, about how resilient people were, the city was, the communities have been. These are all positive uses of the word, but they mean different things in different contexts. Some people say the word is overused and ill-defined. (Higgins, BCI, 40:32)*

Some of the obvious challenges resilience poses have already been discussed or touched upon in the previous chapters: First, what is resilience even – just another buzzword or a whole new way of seeing the world? Second, how can resilience actually work? And third, how is it possible to foster the 'resilience culture' without (m)any 'actual events' like emergencies, accidents, attacks or disasters that prove its necessity?

When it comes to the 'essence' of resilience, people have very different ideas about what it means – a fact that got very clear throughout the process of discussing with a variety of stakeholders. The ongoing lively academic debates about what resilience means, does and should

do, underline this. Further, 'resilience is bigger than [for example] emergency management and cyber security. It is a little bit too big some people would say' (Higgins, BCI, 20:42). One could even argue that 'it appears that everything (organizations, cities, nations) and everybody (from schoolteachers to the U.S. president) can and should be resilient' (Comfort, Boin, & Demchak, 2010, p. 1). Who or what, actually, can be resilient? One exemplary answer arising from the interviews is that 'systems have to be resilient, networks have to be resilient, organisations have to be resilient and people have to be resilient' (Hall, London First, 17:02). Sure enough, this encompasses a wide range of potential targets for resilience policies, yet it fails to address the key question of how these various actors can work together in 'creating' resilience, and what happens if, for instance, the resilience of one contradicts the resilience of another.

Although there is consensus about the fact that resilience has yet to be implemented to a greater extent, the question of the current 'degree' of implementation is perceived differently. While some interviewees claim that a great deal has already been achieved, others state that resilience is far away from having sunk into the different layers of the state, private businesses and civil society. As one interview partner puts it, 'I haven't seen resilience plans or policies in place. Because I'm not sure we are there yet, I think we are quite early on in having policies and plans in place that relate to resilience' (Higgins, BCI, 45:35). Another interviewee points out that 'it's as vital as bottom line, it's as vital as money, it's as vital as the air that we breathe, in order to fulfil organisational and personal goals and to thrive. But I don't think we are at a stage where we are close to that in any way' (Hough, CRJ, 07:51). Relating to the debate about how to live the 'resilience culture', Deborah Higgins, BCI, makes the following statement:

> *What makes an organisation resilient? Often it is that intangible softer factors that are very hard to practice and measure, they are reason that an organisation survived something, because they had that type of culture. So the challenge for us as practitioners is: How do we bring all that together? This is the debate we are having at the moment, nationally and internationally: How do we measure it? How do we know how resilient we are now? How do we know if we have improved? (Higgins, BCI, 07:32)*

Regarding fostering a resilience culture, Higgins acknowledges the challenge that 'if it hasn't happened to you, it is putting money into something that might never happen. It is always

difficult' (Higgins, BCI 16:25). This aspect was highlighted by a fair number of interviewees and strongly relates to the issues discussed above, namely a certain resilience culture which should be promoted and lived across various degrees and levels of state and society. Thus, 'you can't be resilient in bits, you can either be resilient or you can't' (Interview 2, 15:32). If 'the whole organisation is not on board with what you are there what you are trying to achieve and that whole culture is missing, there is always going to be gaps and disasters' (Higgins, BCI, 25:41). In more general terms, resilience 'is about a changed environment, where horizon scanning and situational awareness comes in which is important for resilience. If you are not aware, you can't take the opportunities and advantages. You can't survive and thrive if you don't adapt or take opportunities if you could have' (ibid., 35:14).

These remarks point towards an issue that is key when it comes to the (dis)advantages of resilience: the future. As already discussed in the previous sections, resilience goes hand in hand with the idea that the future is inherently uncertain and full of risks, but also full of opportunities that often cannot be known in advance. In this sense,

> *resilience is giving people and institutions and organisations the ability to react in a different way to the unforeseen, and to turn what could be a negative or a disaster into a positive. And that does not mean to get rid of all the old accepted ways of preparedness, training, command, leadership at this stage. But we must accept that sometimes things are going to go wrong or that events will unfurl in completely unanticipated ways – I am thinking of the 2011 Japanese earthquake and tsunami in particular. (Hough, CRJ, 14:23)*

Thus, along with the perception of threat and risk, the question of the relationship between security, defence and resilience comes back into the foreground (cf. Pospisil, 2013).

Security, defence and resilience – an uneasy relationship?

> *[E]nsuring a secure and resilient UK – protecting our people, economy, infrastructure, territory and way of life from all major risks that can affect us directly – requiring both direct protection against real and present threats such as terrorism and cyber-attack, resilience in*

> *the face of natural and man-made emergencies and crime, and deterrence against less likely threats such as a military attack by another state (HM Government, 2010, p. 22)*

How does resilience relate to security and defence? This is yet another question without a straightforward answer. While some scholars argue that resilience replaces security (Evans & Reid, 2014), others stress that resilience is a kind of enhanced security (cf. Coaffee & Wood, 2006; Fjäder, 2004) and still others argue that it couples up with security, such as leading to what Pospisil & Gruber (2016) have called a resilience-security-nexus. Whether resilience does replace security or goes hand in hand with it, the question of its relationship has not yet been sufficiently discussed.

Except for a different interpretation of resilience as a reincarnation of older civil defence measures (cf. Duffield, 2011; Zebrowski, 2013), it is widely regarded at current that resilience followed and thus opened up the narrow realm of defence at the end of the Cold War era (cf. Pospisil & Gruber, 2016). The interviewees adhere to a position that may be illustrated by the statement that 'if national security is the framework then I think security nests neatly within resilience' (Interview 2, 23:42). However, one interviewee modifies this claim by stating that '*in practice* resilience is being maybe put under security. In fact, security is a subset of resilience not the other way around. […] And what's more is that defence is a subset of resilience' (highlighted by author; Caddick, PwC, 17:45). What seems to be commonly accepted, though, is the assumption that there is no absolute security and that resilience is a way of dealing with that fact, as exemplified by the following statement:

> *Because you could have the best security in the world. That's the discussion: there is world-class security in place in many cases but there are examples where it is breached. Why is it breached? It can't always be a failing of intelligence. And it isn't always because we did not respond correctly. You're never going to have absolute security or resilience. It is the degree and the level of protection that you can provide and the reduction of the impact on the community and on your business. We should be all trying to achieve the highest level of resilience that we can. But completely is not possible. I don't believe anyone who says that. (Higgins, BCI, 25:22)*

Conclusion – resilient futures or the future of resilience

Who is best qualified to define the values that are backed up by and lived through a resilience culture? How is it possible to promote this idea through leadership and a deep implementation throughout the various levels of society and state? What happens if, and that is and will be the case eventually, interests between the various stakeholders differ or even contradict each other? How can resilience be practised in the everyday without falling into the traps of simply repeating 'common knowledge' or 'accepted wisdom' and doing what has always been done? How to best address the problematic tensions between the public good and the privately run or owned CNI? While this working paper did not attempt to answer all of these questions, it at least tried to hint at some possible directions.

As we have seen, resilience in the UK context is strongly linked to change and the ability to see the 'bigger picture'. It is therefore understood as an inherently holistic way of understanding the world. By challenging the 'old silo thinking', it focuses on the interconnectedness of people, things and technologies as complex networks of support but also dependency, which brings questions of risk and vulnerability into play. Furthermore, it seems that resilience is understood as an almost inevitable answer to the ever changing nature of our globalised world. In this sense, it aims at dissolving the tensions between short and long term aspects, top-down and bottom-up elements, and challenges and opportunities. However, while it seems to promote inclusion as well as awareness raising, participatory knowledge and cooperation across boundaries between state and non-state actors, it seems that its ambitious tasks in defining the 'resilience culture' have not yet been fully internalised through the multifaceted layers of the state, private businesses and society.

To summarise, the questions above seem to be theoretical only at first sight since they have immediate practical implications. How will future UK security and resilience policies, including the National Security Strategy and CNIP, look like in light of the BREXIT referendum and its consequences? And finally, connected to this question is a broader one, namely how do we differentiate between the times when we want to be resilient and the times when we want to resist?

Bibliography:

Aradau, C., & Munster, R. van. (2011). *Politics of catastrophe: genealogies of the unknown*. London; New York: Routledge.

Blasius, Rainer (2016): *Den Notstand denken.* Frankfurter Allgemeine Zeitung, 21.08.2016.

Comfort, L. K., Boin, A., & Demchak, C. C. (Eds.). (2010). *Designing resilience: preparing for extreme events*. Pittsburgh, Pa: University of Pittsburgh Press.

Corry, O. (2012). Securitisation and "Riskification": Second-order Security and the Politics of Climate Change. *Millennium - Journal of International Studies*, *40*(2), 235–258. https://doi.org/10.1177/0305829811419444

Duffield, M. (2011). Environmental Terror: Uncertainty, Resilience and the Bunker. *School of Sociology, Politics and International Studies,* University of Bristol.

Gruber, B. (2016). Going Side by Side: Defence and Resilience in Swedish Security Policy. *oiip Working Paper*, Vienna.

HM Government. (2008). *The National Security Strategy of the United Kingdom Security in an interdependent world*, London, HM Government.

HM Government. (2010). *A Strong Britain in the Age of Uncertainty: The National Security Strategy*, London, HM Government.

HM Government. (2015). *National Security Strategy and Strategic Defence and Security Review 2015. A Secure and Prosperous United Kingdom.* London, HM Government.

Joseph, J. (2013). Resilience as embedded neoliberalism: a governmentality approach. *Resilience: International Policies, Practices and Discourses*, *1*(1), 38–52. https://doi.org/10.1080/21693293.2013.765741

Manyena, S. B. (2006). The Concept of Resilience Revisited. *Disasters*, *30*(4), 434–450.

Pospisil, J. (2013). Die Neukonfiguration von Resilienz im Zeitalter von Risiko. *Österreichische Zeitschrift Für Politikwissenschaft*, *43:1*.

Pospisil, J., & Gruber, B. (2016). Resilience and the transformation of sovereign security: a look at policy challenges and interests. *Resilience*, *4*(3), 202–216. https://doi.org/10.1080/21693293.2016.1210256

Smith, J. (2003). This turn required other temporalities. *Parliamentary Affairs*, *56*, 410–422.

Walsh, B. (2013, August 1). Adapt or Die: Why the Environmental Buzzword of 2013 Will Be Resilience. *TIME*. Retrieved from http://science.time.com/2013/01/08/adapt-or-die-why-the-environmental-buzzword-of-2013-will-be-resilience/

Zebrowski, C. (2013). The nature of resilience. *Resilience: International Policies, Practices and Discourses*, *1*(3), 159–173. https://doi.org/10.1080/21693293.2013.804672

Zebrowski, C. (2016). *The value of resilience: securing life in the 21st century*. Abingdon, Oxon; New York, NY: Routledge, is an imprint of the Taylor & Francis Group, an Informal business.

Interviews:

Hall, R. (London First), 31.05.2016, London, UK (Interview 1)

Interview 2, 31.05.2016, London, UK

Higgins, D. (BCI), 22.06.2016, London, UK (Interview 3)

Caddick, M. (PwC), 23.06.2016, London, UK (Interview 4)

Hough, E. (CRJ), 24.06.2016, London, UK (Interview 5)