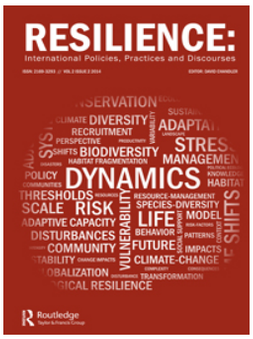

Routledge
Taylor & Francis Group

Resilience
International Policies, Practices and Discourses

ISSN: 2169-3293 (Print) 2169-3307 (Online) Journal homepage: https://www.tandfonline.com/loi/resi20

# The nation-state, national security and resilience in the age of globalisation

Christian Fjäder

**To cite this article:** Christian Fjäder (2014) The nation-state, national security and resilience in the age of globalisation, Resilience, 2:2, 114-129, DOI: 10.1080/21693293.2014.914771

**To link to this article:** https://doi.org/10.1080/21693293.2014.914771

*Resilience*, 2014
Vol. 2, No. 2, 114–129, http://dx.doi.org/10.1080/21693293.2014.914771

# The nation-state, national security and resilience in the age of globalisation

Christian Fjäder*

*National Emergency Supply Agency (NESA), Pohjoinen Makasiinikatu 7A, 00131 Helsinki, Finland*

This article explores the evolving role of sovereign governments in the provision of security in an increasingly complex and uncertain global world (in which the demand for security is increasing, whilst simultaneously the capability of the nation-states to manage it is being challenged) and the concept of resilience as a strategy to meet these challenges. In order to analyse the rise of resilience, national security and national resilience strategies from a number of countries are examined. It argues that whilst national resilience features prominently in national security strategies, its definition and goals remain ambiguous. Moreover, whilst resilience can be a pragmatic approach to security challenges, its relationship with national security and the state's responsibility as security provider requires further clarification. The article aims to contribute to the emerging discourse around the concept of national resilience, as well as to the identification of policies and practices required for establishing a strategic approach to national resilience.

**Keywords:** resilience; nation-state; national security; globalisation; critical infrastructure protection

## Introduction

> The time has come for the protection mindset to be broadened – to embrace the broader concept of resilience. The aim is to build a more resilient nation – one where all Australians are better able to adapt to change, where we have reduced exposure to risks, and where we are all better able to bounce back from disaster. (The Hon Robert McClelland MP, Attorney-General, 9 December 2009, Australian Government Critical Infrastructure Advisory Council)[1]

This article deals with emergence of the concept of 'national resilience' in national security agendas, stemming from a notion of the broadening variety of 'new' security threats, national vulnerabilities arising from global interdependence and an overarching condition of uncertainty, under which national security is now required to operate. The basis of the article is an examination of national security strategies, related documents and statements, and in particular policies adopted for critical infrastructure resilience in Australia, Canada, the Netherlands, New Zealand, the UK and the USA.

All the strategies examined display a growing concern with the broadening threat environment and its uncertainty. Whether intentional or not, the strategies relay the notion

*Email: Christian.fjader@nesa.fi
The views expressed are those of the author and do not reflect the official policy or position of the National Emergency Supply Agency or the Finnish Government.

[1] Australian Government, "Australian Government Critical Infrastructure Resilience Strategy," http://www.tisn.gov.au/Documents/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.pdf (Accessed July 3, 2013), 6.

of a growing demand for security. At the same time, however, it has been suggested that the provisioning of security has become increasingly difficult for the nation-state, as its span of control does not efficiently correspond with the transnational threats at the heart of this emerging uncertainty. Moreover, the concept of uncertainty suggests that threats are increasingly harder to recognise and unpredictable in timing and scale. As a result, the concept of security can be seen as having a decreasing utility, as it is not possible to prepare and respond to all imaginable threats effectively, and especially cost-effectively. This in turn has created favourable conditions for a resilience approach to national security. Resilience has indeed been increasingly promoted as a potential solution to this dilemma. However, the nation-state has nonetheless retained its core responsibilities for traditional national security, which is more preventive and territorial in nature, and not always aligned with the resilience approach.

This article consequently examines the concept of resilience, which has been characterised as the ability to withstand sudden shocks and recover (or 'bounce back') from them, in the context of the nation-states' responsibility for the provisioning of security. In order to establish what resilience signifies in the context of national resilience, as well as how it could be applied in relation to the nation-state's responsibility for the provisioning of national security, the article examines the evolving role of the nation-state in the provision of positive political goods in the age of globalisation, specifically within the context of the ever broader concept of national security, including in relation to Critical Infrastructure Protection (CIP): the protection of what is most critical for the survival of a nation and the well-being of its citizens. It argues that, whilst resilience can be an effective strategy against uncertainty, its application for national resilience is not entirely straightforward. In addition to determining the relationship between resilience and the nation-state's responsibility for security, in order to establish a strategic approach to national resilience one needs to consider how resilience contributes towards the security goals of the state, as well as what the precise goals of resilience are. Perhaps the most challenging task, however, is to establish a measure of success; how would one determine whether a nation-state is resilient? This article aims to contribute to the emerging discourse around the concept of national resilience, as well as to the identification of policies and practices required for establishing such a strategic approach to national resilience.

## The nation-state and globalisation

Nation-states have long been considered the principal agents in the modern world system. The emergence of the welfare state after WWII introduced a new type of a protective state that aimed to guarantee the welfare of its citizens by offering social services, health care, education and social benefits in the form of the provision of social security and unemployment benefits. As a result of this evolution, the modern nation-state's core responsibilities are now seen to focus on the provision of positive political goods, such as security, health care, education, law and order, economic opportunity and critical infrastructure, i.e. the protection of the overall well-being of its citizens. As such the state maintains a central role in the economic, political, social and cultural life of its citizens that is both pervasive and persistent.

The concept of globalisation emerged in the 1990s in the aftermath of the end of the Cold War and the resulting 'new borderless world', stemming from the opening of markets and an emerging technological revolution in telecommunications and information technologies, which seemed to make the world smaller and increasingly interdependent.

Due to its multifaceted nature, globalisation is hard to define in a coherent manner, definitions ultimately depending on what particular angle of globalisation one is interested in. Whilst the majority of accounts refer to the economic transformation caused by globalisation, it is in fact a multifaceted phenomena of deterritorialisation and increasing interconnectedness that has multiple impacts on nation-states, ranging from cultural, security, social and political impacts to structural pressures.[2]

In terms of globalisation's impact on the role of the nation-state, three broad positions have emerged: the 'hyperglobalists', 'sceptics' and 'transformalists'. The 'hyperglobalists', for instance Kenichi Ohmae and Susan Strange, viewed globalisation as a fundamental challenge to the role of nation-states and concluded that it constitutes a challenge to the nation-state through the evident loss of control over territory, which in turn leads into the loss of sovereignty. Moreover, the 'hyperglobalists' assumed that because the nation-state's capability to offer public goods, including security, and regulating the economy, had declined, or even all but disappeared, the nation-state has become an obsolete construct in the age of globalisation.[3] Ulrich Beck, for instance, has argued that globalisation represents the weakening of state sovereignty and state structures,[4] whilst others, such as Susan Strange, have argued that the process of deterritorialisation is an integral part of the process of globalisation, producing an 'end of geography' and thus, eroding of the core of the nation-state's power over its most central function, the control over territory.[5]

The 'sceptics', for instance Paul Hirst, Stephen Krasner and Robert Gilpin, on the other hand, have principally argued that globalisation has in fact produced little new to territoriality and state sovereignty, rejecting the notion of the nation-state as a 'victim' of globalisation.[6] The 'transformalists', including scholars like Anthony Giddens, James Rosenau, David Held and John Ruggie, reject the 'hyperglobalist' view, but concede that globalisation produces a spatial reorganisation of economic, political, cultural and social life that impacts on the role of the nation-state. The 'transformalists', however, argue that globalisation does not automatically diminish the nation-state's importance, but that instead the potential impact depends on the state's own reaction to it.[7]

## Globalisation and the transformation of 'national security'

The traditional concept of national security derives its origins from a line of modernist political and sociological thought from Thomas Hobbes to Max Weber,[8] insisting that the state needs to have the absolute monopoly upon the legitimate use of physical force and

---

[2] Stanford Encyclopaedia of Philosophy, "Globalization," http://plato.stanford.edu/entries/globalization/ (Accessed May 3, 2013).

[3] David Held and Anthony McGrew, "Globalization," The Global Transformations Website, http://www.polity.co.uk/global/globalization-oxford.asp (Accessed March 29, 2014).

[4] Ulrich Beck, "The Cosmopolitan Perspective: Sociology of the Second Age of Modernity," *The British Journal of Sociology* 51, no. 1 (2000): 86.

[5] *Susan Strange, The Retreat of the State: Diffusion of Power in the World Economy* (New York: Cambridge University Press, 1996).

[6] Held and McGrew, "Globalization."

[7] Ibid.

[8] Thomas Hobbes, ed., *Hobbes's Leviathan Reprinted from the Edition of 1651 with an Essay by the Late W.G. Pogson Smith* (Oxford: Clarendon Press, 1909), http://oll.libertyfund.org/index.php?option=com_staticxt&staticfile=show.php%3Ftitle=869&Itemid=99999999 (Accessed October 5, 2013); Max Weber, "Politics as a Vocation," in *Essays in Sociology*, ed. H. Garth and C. Wright Mills (New York: Macmillan, 1946), 26–45.

that security is the core responsibility of a nation-state. Based on this traditional view of national security, the *raison d'etre* of the nation-state is the provisioning of security through the creation of a professional security bureaucracy (for example, border security, military, law enforcement and paramilitary organisations) to manage external and internal threats to national security. Moreover, the scope of the traditional national security concept was above all maintaining security within a geographically defined territory in order to protect the survival of the state against both external and internal threats.[9]

The inclusion of new security threats, however, principally non-military threats, mostly posed by non-state actors, such as international terrorism, organised crime, pandemics, natural disasters, drug trafficking and people trafficking, into the national security agendas, presented the state with both new challenges and, arguably, new opportunities. If globalisation has been seen to transform the role of the nation-state, in a similar manner it has been argued as having transformed the concept of national security. The non-state nature of many of these new threats has prompted those in agreement with the hyperglobalists to question whether the nation-state is adequately equipped to efficiently deal with such transnational threats.

Barry Buzan, however, argues that despite the declining role of the state in the management of the economy, the state still remains the principal security provider because it is the only societal organisation that has both the capacity to act and the authority to define what represents a security threat. Since there is no global government or society that could replace the nation-state, the nation-state is simply the best available institution to take its place.[10] Moreover, Keith Krause argues that in fact the role of the state has expanded, due to the securitisation of non-traditional threats. Consequently, the responsibilities of the state now include protecting citizens from the threat of violence and creating not only the conditions for economic and social well-being, but also for the preservation of their core values and identity. Furthermore, Krause argues that states seek to distinguish the 'national security' agenda from the more day-to-day political 'problems' by emphasising the urgent, existential or pervasive nature of security threats.[11] Hence, at least partially due to the securitisation of non-traditional threats, the nation-state has managed not only to maintain its mandate to regulate security, but to decide what constitutes a security issue and through the mandate to define the national interest, to dictate the agenda for national security.

The centrality of the state is emphasised in 'securitisation' analysis, a theoretical approach to security developed and advanced by the so-called 'Copenhagen school', largely formed around the researchers employed at the Copenhagen Peace Research Institute, but in particular based on the work of Buzan and Ole Waever.[12] The concept of securitisation suggests that security is essentially a speech act, within which an actor

---

[9] For more discussion, see N.M. Ripsman and T.V. Paul, *Globalization and the National Security State* (Oxford: Oxford University Press, 2010).

[10] Barry Buzan, "What is National Security in the Age of Globalization?" Refleks, Department of Foreign Affairs, Oslo, http://www.regjeringen.no/nb/dep/ud/kampanjer/refleks/innspill/sikkerhet/buzan.html?id=493187 (Accessed July 3, 2013).

[11] Keith Krause, "National Security in the Age of Globalization: A Brainstorming Note," Refleks, Department of Foreign Affairs, Oslo, http://www.regjeringen.no/nb/dep/ud/kampanjer/refleks/innspill/sikkerhet/krause.html?id=493206 (Accessed July 3, 2013).

[12] The following have been considered as the foundational pieces of work of the Copenhagen school: Barry Buzan, Ole Waever, and Jaap de Wilde, eds., *Security: A New Framework for Analysis* (Boulder, CO: Lynne Riener, 1997); Ole Waever, "Securitization and Desecuritization," in *On Security*, ed. R.D. Lipschutz (New York: Columbia University Press, 1995), 46–86.

presents an issue as an existential threat to a particular object, prompting immediate and extraordinary measures to secure it.

Consequently, by successfully articulating a threat or an issue in terms of 'security', an issue moves from the realm of 'normal' politics into the realm of security politics, whether this threat is 'real' or not. Merely presenting an issue as an existential threat gives it a real meaning and leads to security responses. The Copenhagen school originally identified five focus sectors for security studies – economic, environmental, military, political and societal – but eventually a variety of human security topics emerged as subjects of study. According to the Copenhagen school, however, moving an issue to the realm of security represents a failure and, hence, there is a preference for desecuritisation, i.e. moving issues back to 'normal politics'. Consequently, the broadening of the security agenda is not necessarily intentional. The 'Paris school' of securitisation further argues that in addition to the speech act itself, political agency, audience and context determine whether securitisation is effective.[13] As will be discussed below, the problem of which aspects of social, economic and environmental relations should become 'securitized' is central to discussions of how to understand and to manage the concerns of traditional national security and of developing concerns with national resilience and to the role of the nation-state within this.

### *National security strategies in the 'age of uncertainty' and the rise of resilience*

The proliferation of 'new security threats' and the urgent need for the government to respond to them, a sense of vulnerability stemming from global interdependency and a resulting notion of uncertainty, feature prominently in the national security strategies of Australia, Canada, the Netherlands, the UK and the USA. Britain's national security strategy – 'A Strong Britain in the Age of Uncertainty' – for instance, states that Britain is more vulnerable to global threats 'because we are one the most open societies, in a word that is more networked than ever before' (3). It also refers to a multitude of new threats, including those posed by non-state actors, e.g. terrorism, security of national energy, food and water supply and climate change as the sources of threat to Britain's national security.[14]

Following a similar logic, Canada's national security policy – Securing an Open Society: Canada's National Security Policy – states:

> There can be no greater role, no more important obligation for a government, than the protection and safety of its citizens. But as all Canadians know, we live in an increasingly interconnected, complex and often dangerous world.[15]

---

[13] Thierry Balzacq, "The Three Faces of Securitization: Political Agency, Audience and Context," *European Journal of International Relations* 11, no. 2 (2005): 171–201. It should be noted that there is also the 'Critical Security Studies' approach (sometimes referred to as the Aberystwyth school), which rejects the traditional security approach and the state's moral authority in security. Instead, it argues that security is inter-subjectively created and that different world views and discourses on politics result in different views and discourses about security. Consequently, as Ken Booth puts it, 'security is what we make it', see Ken Booth, "Security and Self: Reflections of a Fallen Realist," in *Critical Security Studies: Concepts and Cases*, eds. Keith Krause and Michael C. Williams (London: UCL Press, 1997), 38–9.

[14] HM Government, "A Strong Britain in the Age of Uncertainty: The National Security Strategy," https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf (Accessed March 28, 2014).

[15] Government of Canada – Public Safety Canada, "Securing an Open Society: Canada's National Security Policy," http://www.publicsafety.gc.ca/cnt/ntnl-scrt/scrng-eng.aspx (Accessed March 26, 2014).

Australia's National Security White Paper (2013), on the other hand, is a good example of the national security goals of a modern nation-state, mixing traditional security missions towards the safeguarding of national sovereignty and the new paradigm towards establishing national resilience. The strategy states that Australia's national security objectives are:

> … to ensure a safe and resilient population; to protect and strengthen our sovereignty; to secure our assets, infrastructure and institutions; and to promote a favourable international environment. These objectives anchor decision-making and planning for the national security community.[16]

The Netherlands, on the other hand, adopted an overarching international security strategy in order to respond to large-scale and rapid changes in the global system, whether they are economic, political or security related in nature. The strategy underlines uncertainty and the difficulty to distinguish between internal and external security in this new reality.[17]

Due to the multitude of threats, perceived uncertainty and complexity of global interdependencies, most national security strategies appear to have now adopted a risk-based 'all hazards' and 'all of society' approach as the new paradigm. More significantly, however, the concept of resilience has been promoted as a fundamental element of this new paradigm. Moreover, in addition to Australia, Canada and the Netherlands have also already adopted specific resilience strategies, whilst the US government has made critical infrastructure resilience and security as one of the core missions of the Department of Homeland Security (DHS). The concept of 'national resilience', however, nonetheless remains rather undefined and ambiguous. Consequently, one needs to consider what 'national resilience' signifies and how it relates to national security.

## Definitions of 'resilience': what is 'national resilience'?

Despite the concept's prominence in national security strategies, there is no single definition of resilience that could be directly applied to the purposes of national resilience, as it relates to national security, civil emergency management and CIP. The definitions of the concept of resilience vary depending on the point of view and field of science in question, for example in material sciences, psychology, ecology and economics. The most common and colloquial use of the term resilience, however, derives from the material sciences, in which the term is used prevalently in engineering design, and in particular towards understanding the behaviour and properties of specific materials in relation to their purpose, for example in the design of structures, such as support beams and bridges. In this context, the measure of resilience is defined based on how much force (or 'stress') the material can withstand without breaking or permanently altering its shape under stress, how much it bends under stress and how fast it returns to its original shape after the stress or force is relieved. Consequently, utilising the definition of resilience, as it is understood in material science, would suggest 'something is resilient if it can resist external forces, shocks, and disturbances and can quickly return to its normal state'.[18] Following this logic,

---

[16] Australian Government, "National Security Strategy," Canberra, http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=167267 (accessed April 28, 2014).

[17] Government of the Netherlands, "A Secure Netherlands in a Secure World: International Security Strategy," http://www.government.nl/documents-and-publications/notes/2013/06/21/international-security-strategy.html (Accessed March 24, 2014).

[18] Patrick Martin-Breen and Marty J. Anderies, "Resilience: A Literature Review," Rockefeller Foundation, 2011, http://www.rockefellerfoundation.org/blog/resilience-literature-review (Accessed June 5, 2013), 43.

individuals, communities and societies are resilient if they can withstand and recover (or in colloquial terms 'bounce back') from shocks, such as a death of a loved one, loss of a job or a natural disaster such as an earthquake or flood.[19] The challenge with this application of the concept to societal resilience is that it requires a relatively precise definition of what is considered the state of normalcy (i.e. the normal state, equilibrium, business as usual, etc.), which either has to be preserved or is the target for recovery. Whilst this is often relatively straightforward when the scope is limited to an individual, a single system or otherwise clearly defined entity, defining the state of normalcy for a complex system such as a nation, is far from straightforward, as is defining the required risk appetite and recovery objectives in the national context.

The resilience of systems, on the other hand, in the simplest of terms refers to the capability of the system to maintain its subscribed function even in the event of a disruption and thus, continue to operate within the parameter of what could be considered 'normal' or 'business as usual'.[20] What complicates the resilience of systems is that it is relatively hard to find a system that is so isolated that it would not depend on a complex web of interdependencies for its functions. Consequently, the target of resilience/recovery can in fact be a sum of 'normals', which needs to be individually determined for each function that the system is supposed to produce or enable. An alternative approach to the resilience of systems is to refer to resilience as the system's response to emergencies, specifically as it relates to the (autonomous) 'capacity of a system to absorb disturbance, undergo change, and retain the same essential functions, structure, identity, and feedbacks'.[21]

Resilience in complex adaptive systems, on the other hand, such as the ecosystem and social systems, is understood as a combination of an ability to resist, recover from and reorganise in response to a shock or a crisis. The key to resilience is thus adaptability, which is enabled by the non-linear nature of the relationship between constituent parts of the system. Consequently, the definition of 'normal' in complex adaptive systems adapts to match the new circumstances and focuses on the ability to maintain the core function/s of the system, even if the system structure may change, or even collapse in the process.[22]

The definitions of 'resilience' in relation to critical infrastructure have been equally diverse. Recognising this, the National Infrastructure Advisory Council (NIAC) report on CIP in the United States suggested a common definition for 'critical infrastructure resilience' as 'the ability to reduce the magnitude, impact, or duration of a disruption', and 'resilience' as 'the ability to absorb, adapt to, and/or rapidly recover from a potentially disruptive event'.[23] According to the report, resilient critical infrastructure has three principal characteristics: robustness – the ability to maintain critical functions and absorb the impact in the event of crisis or disruption; resourcefulness – the ability to prepare for, respond to and manage a crisis or disruption through establishing and maintaining adaptive capacity and flexibility to redirect resources and assets; and rapid recovery – the ability to return to normal operations as quickly and efficiently as possible.[24]

---

[19] Ibid.
[20] Martin-Breen and Anderies, "Resilience," 7.
[21] Mareile Kaufmann, "Emergent Self-Organisation in Emergencies: Resilience Rationales in Interconnected Societies," *Resilience: International Policies, Practices and Discourses* 1, no 1 (2013): 55.
[22] Martin-Breen and Anderies, "Resilience," 7.
[23] National Infrastructure Advisory Council (NIAC), "Critical Infrastructure Resilience," NIAC, Washington, DC, 2009, http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf (Accessed August 8, 2013), 2.
[24] Ibid., 13.

The definition for the concept of societal resilience, on the other hand, is difficult to pinpoint, as it ultimately depends upon what type of resilience is sought after and towards what end. In general, it appears that the national resilience, security and CIP strategies reviewed here have a tendency to declare very broad objectives, aiming at building a 'resilient country' that is able to withstand and recover from disasters and any unexpected events ('all hazards' approach). This, however, is not adequate, especially in terms of determining whether resilience has indeed been established, to what exactly and to what extent.

Philippe Bourbeau, on the other hand, refers to three types of (societal) resilience, each representing a different ontology: resilience as maintenance, emphasising utilising the capability for adaptation towards the maintenance of the *status quo*; resilience as marginality, aiming at keeping the changes produced by a crisis or shock as marginal in order to safeguard against changes to existing structures or policies; and resilience as renewal, with an aim to transform, even potentially remodel, the existing structure and policies, relying on diversification between multiple structures and institutions acting as fall backs.[25]

Demos, a British think tank, published a research report in 2009 entitled *Resilient Nation*, which states that resilience in this context should be understood as 'the capacity of an individual, community or system to adapt in order to sustain an acceptable level of function, structure and identity'.[26] Moreover, the report stated that the 'next generation of resilience relies on citizens and communities, not the institutions of state'.[27] This representation of societal resilience would seem to support Jonathan Joseph's view that resilience has an inherently neoliberal ontology, emphasising individual responsibility for preparedness and a minimal government role.[28]

These definitions, however, overlook an important question regarding societal resilience, specifically in regards to underlining the logic of resilience: is it desirable in the first place? As Joseph points out, disruptions and crises can be also have a constructive impact if they lead to learning and adapting towards positive renewal.[29] Kaufmann takes a similar position, but goes even further by arguing that, in the worst case, resilience could be very costly and lead to results that are not desirable, pointing out that 'resilience can apply to forces that are constructive as well as detrimental for human survival, as for example in the form of resilient viruses'.[30]

## Resilience and national security: towards a 'resilient' country

The following section will focus on examining what the role of the nation-state could be in providing resilience in the age of globalisation, in particular in reference to national security and CIP. How could one build a resilient nation-state? How does national resilience compare against the concept of national security, one of the core responsibilities of the state, and what value added is it expected to bring? What type of security and resilience can the nation-state realistically commit to and what could its goals be?

---

[25] Philippe Bourbeau, "Resiliencism: Premises and Promises in Securitization Research," *Resilience: International Policies, Practices and Discourses* 1, no. 1 (2013): 11–16.
[26] Charlie Edwards, *Resilient Nation* (London: Demos, 2009).
[27] Ibid.
[28] Jonathan Joseph, "Resilience as Embedded Neoliberalism: A Governmentility Approach," *Resilience: International Policies, Practices and Discourses* 1, no. 1 (2013): 39.
[29] Ibid., 42.
[30] Kaufmann, "Emergent Self-Organisation in Emergencies," 65–7.

On the surface, resilience may appear a convenient strategic option, especially under the conditions of financial scarcity, as adaptability and agility arguably enable better use of existing resources, and is almost certainly cheaper than security. However, taking into consideration the nation-state's core responsibility to protect all citizens, the problem of acceptable losses and the acceptable level of risk is not a comfortable topic, albeit unfortunately unavoidable when contemplating the application of the resilience concept in a national context. For example, the prioritisation of one region, or a critical industry, over others, for the sake of greater common good can be problematic. Take for an example, a situation where there is a decision to prioritise the resilience of the electricity supply to a densely populated area with a plenitude of critical (national) infrastructure over the supply to a more remote area with a sparse population and little industrial or business activity. What happens if even one person in the remote area, which has been considered secondary, dies because lack of heating or inability to call the emergency services for help because mobile phone services are not working? Yet, if the strategic objective is making a nation more resilient, prioritisation is necessary and in some cases could produce difficult value choices. Whilst the general principle is that emergency and rescue services are made available nationwide, resilience-based resource prioritisation may well produce inequality between regions and constituencies as prioritisation is a necessary component of a resilience strategy.

Moreover, considering the potential vagueness of what exactly is considered as 'resilient', in order to build resilience in a meaningful manner it needs to be first established what the objective is, i.e. resilience of what and against what?[31] This in turn tells us what type of resilience is required. In case of societal (or national) resilience, one needs to also ask the difficult ethical question – 'resilience for whom?' – as building national resilience necessarily involves making prioritisation choices and thus entails the potential for creating inequality during a disaster and in its aftermath. Resilience does not always benefit everyone. It is not possible to protect all elements of critical infrastructure everywhere and against all threats, e.g. electricity transmission cables or pipelines, and recovery is always incremental as repairs take time and a concentration of resources. Above all, however, it is necessary to differentiate success from failure. In order to achieve this, it needs to be determined what qualifies as 'resilient'. Does resilience aim to ensure the availability of critical resources, or their recoverability? Finally, the distinction between national security and resilience must be determined in order to decide what the resilience goals for the nation should be.

## Resilience versus security

One of the core questions for establishing a national resilience strategy is to determine how resilience corresponds with the state's responsibility to manage national security. Is resilience an integrated component of national security, or is it an alternative to it? If the latter holds, what value added can resilience bring to the table in comparison to national security? On the other hand, if resilience is complimentary to national security, how should one balance between the two?

The principal differences between security and resilience are evident: in both spatial and temporal scope and objectives the two are interrelated, but arguably separate concepts. First of all, security is essentially preventive and proactive in nature, aimed at protecting the state and the citizens against threats, identified and assessed through the means of

[31] Martin-Breen and Anderies, "Resilience," 55.

intelligence and law enforcement, or risk assessments based on past actual events. In terms of its temporal scope, security as a strategy aims to stop the threat before it materialises or escalates, or in the worst case to defeat it as soon as possible. Spatially, security is usually relatively specific, focusing on persons, organisations, facilities and territory. If the object of security is destroyed, disrupted or compromised, this constitutes a failure. Security is thus relatively specific in terms of its objectives, and its rate of success is generally verifiable. Resilience, on the other hand, is a combination of proactive and reactive measures aiming at reducing the impact but not at preventing threats as such. On the contrary, resilience as a concept suggests that preventive measures have not had a full effect, and it consequently focuses on minimising disruption to critical services to the society once an event has nonetheless happened.

Perhaps because of this logic, most of the resilience strategies would also appear to subscribe to an 'all hazards approach', accounting for all forms of human, technical and natural threats, ranging from terrorism and sabotage to technical system failures and natural disasters.[32] Resilience also tends to be spatially less defined, often referring to providing resilience to a complex system, value chain or function that can be both spatially and temporally spread out. Resilience also, unlike security, suggests an ability to adapt to disruptions and recover from them to the state of normalcy within an acceptable timeframe, rather than attempting to 'defeat' the disruption or its source. Consequently, resilient systems are often described as self-learning, self-organising and innovative, a combination of which provides them with the capability to continue functioning, rather than to be safeguarded against disruption or being compromised in another manner. This approach, however, is problematic in terms of setting measurable and verifiable objectives for the strategy. At what stage exactly is resilience judged as having been successful?

Whilst security and resilience are different in their temporal and spatial properties, I would argue that both are required for the new national security paradigm referred to in national security strategies. The critical question for decision-makers is rather how the two relate to each other and how to balance between the two in terms of objectives and the optimal use of resources. This is not entirely straightforward, but doable nonetheless. On the one hand, security and robustness are essential elements of resilience, with a specific aim to reduce the likelihood of a major event and limit its impact in order to avoid irreparable damage and loss of life, as well as to facilitate efficient recovery by maintaining the most essential structures and resources as intact as possible. On the other hand, resilience could be seen as an integrated element of national security, with a specific aim to provide a solution for preparedness against unforeseen and sudden threats, against which it is not possible, or at least not cost-effective to use a preventive security approach. In any case, the strategic objective should be lowering the risk of disruption in the most essential functions to an acceptable level, whilst ensuring that the essential functions of the society as a whole can be recovered in a reasonable time and with reasonable cost. The increasing private ownership of critical infrastructure and the dependence of private operators on the global supply chain, however, complicate this task. The following section will address the question of the nation-state's capability to determine resilience goals and direct them in this complex environment.

[32] OECD, "Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security," 2008, http://www.oecd.org/daf/inv/investment-policy/40700392.pdf (Accessed June 8, 2013), 6.

**Resilience of privately owned critical infrastructure: what role for the state?**

An increasingly important field of national security is CIP, the policy field dedicated to the protection of national critical infrastructure, which delivers, enables and supports the provision of critical services to the citizens, communities and the economy. CIP relies on definitions of 'critical' and, thus, that of 'critical infrastructure', for its scope and mission. Whilst these definitions vary from country to country, in most cases 'critical' refers to infrastructure that provides life sustaining and essential services required for the economic and social well-being of citizens, national and public security and key government functions.[33] The sectors typically considered as critical infrastructure are: energy, water services, communications, transport, food supply chains, health, banking and finance, national security and defence-related assets. The definitions of 'infrastructure' still tend to focus on physical infrastructures, but some countries now also include intangible assets, such as supply chains that enable the functioning of physical infrastructure and/or deliver critical services.[34] For instance, the Australian government's *Critical Infrastructure Resilience Strategy* (2010) defines critical infrastructure as:

> … those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security.[35]

One of the most fundamental challenges to establishing a national resilience strategy, however, is to solve how the privately owned and operated critical infrastructure is integrated into the strategy. The shortage of financial assets available to infrastructure investments has increased the use of project financing models utilising a Private–Public Partnerships (PPP) in infrastructure investment and operations. Also, in general, the share of privately owned and operated infrastructure has increased globally, especially in the OECD member states, where critical infrastructure is mostly either completely or partially owned by the private sector. For instance, the DHS has estimated that in the USA approximately 85% of critical infrastructure is privately owned and operated.[36]

Whilst the private ownership of infrastructure has arguably created financing and operational efficiency, it has also intensified the state's dependency on private institutions for the delivery of basic services, not only under normal circumstances, but also under exceptional circumstances. Moreover, whilst governments impose at least some level of regulation regarding the expected service levels of infrastructure services, as well as the minimum standards for security, risk and business continuity management, in principal, at least, these infrastructures are operated on business terms with an objective to maximise the revenue on investment. Consequently, proposed investments in redundancies and robustness need to primarily satisfy the business criteria, rather than the national security criteria. The difficult question for the state thus becomes solving the possible gap between national security interests and the business interests of critical infrastructure owners and operators with regard to redundancy and robustness investments. There is certainly a delicate balance to be found here, as further regulation may become a disincentive instead

[33] Ibid., 3.
[34] Ibid., 6.
[35] Australian Government, "Australian Government Critical Infrastructure," 8.
[36] Department of Homeland Security (DHS), "Office of Infrastructure Protection Strategic Plan 2012-2016 National Protection and Programs Directorate," Washington, DC, 2009, https://www.dhs.gov/sites/default/files/publications/IP%20Strategic%20Plan%20FINAL.pdf (Accessed July 3, 2013).

of an incentive, and subsidising may represent a market intervention and thus potentially create a market distortion through enhancing the competitive advantage of selected market players over others. Finally, if 'resilience' has a neoliberal ontology, as Joseph has suggested, there appears to be a dichotomy between two approaches: the principle that the private sector owners and operators are best placed to manage the security of critical infrastructure within the framework of their normal risk and business continuity management programmes, and the state-centric position that considers critical infrastructure as a central national security issue. If one would accept that critical infrastructure has been a subject of securitisation in national security agendas, perhaps desecuritisation should be at least considered with this dilemma in mind?

The securitisation of critical infrastructure, which would be likely to lead to increasing state ownership in the name of national security and imposing limits on private and foreign ownership, would not necessarily be the best option for infrastructure resilience. Nonetheless, a great number of governments do exercise it. For instance, Bothlin et al. have noted a trend of security concerns already becoming a significant driver of telecommunications infrastructure development around the world.[37] A good example of this are the national security-motivated exclusions the Chinese telecoms equipment provider Huawei has faced in Australia, the USA and the UK when bidding for telecommunications and information network infrastructure projects. With the proliferation of national cyber security strategies and increasing concerns over the importance of Information and Communications Technology and the Internet on national security and the economy, this trend is likely to increase.

The increasing share of national ownership of critical infrastructure is in fact an example of the nation-state 'fighting back' to maintain control over national security. An OECD report on the role of foreign investment policies and national security found that all 39 countries surveyed applied discriminatory measures against foreign investment in critical infrastructure sectors, albeit in many cases such discriminatory policies were minor in nature. Out of the 39 countries surveyed, 29 countries imposed restrictions on Postal and Telecommunications services, 28 on the energy sector, 25 on radio and television, 22 on agriculture and defence, 18 on potable water services and 17 on banking and finance.[38] In terms of restriction mechanisms, some applied blanket restrictions, in some cases imposing a total ban on limited infrastructure sectors, whilst the majority relied on sector-specific licensing and investment approval procedures that could be used to block foreign investment in critical infrastructure or national security related sectors.[39] One of the most extensive mechanisms for controlling the foreign ownership of infrastructure in the OECD is the US Committee on Foreign Investment in the United States (CFIUS), which is run by the Treasury and includes members from the other Federal departments and operates based on the mandate granted by the Foreign Investment and National Security Act of 2007 (NINSA). As part of the certification process, CFIUS conducts risk-based assessments on the national security impact of the proposed foreign investments. The definition CFIUS utilises to screen proposed a foreign critical infrastructure investment is somewhat narrower than the general definition for what qualifies as 'critical': 'systems and assets, whether physical or virtual, so vital to the

[37] OECD, "Infrastructure to 2030: Telecom, Land Transport, Water and Electricity," 2006, http://www.oecd.org/futures/infrastructureto2030/infrastructureto2030telecomlandtransportwaterandelectricity.htm (Accessed July 5, 2013), 19.
[38] OECD, "Protection of Critical Infrastructure," 7.
[39] Ibid.

United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security'.[40]

Whilst CFIUS declarations are voluntary – typically less than 200 cases are subject to national security review[41] and only a few selected foreign investments have been formally stopped under FINSA[42] – many transactions are voluntarily abandoned by the foreign acquiring parties due to concerns that if remedial measures were taken they would not pass the CFIUS review and would be eventually stopped under FINSA. One primary example of this is the Chinese telecommunications equipment manufacturer Huawei, which was forced to abandon its 3Com transaction in 2008, acquisition of 3Leaf Systems in 2010 and to pull out of its intended acquisition of Motorola's network business.[43]

The Netherlands, on the other hand, does not refer to discriminatory investment policies in its approach and has expressed scepticism of the effectiveness of such policies for CIP.[44] The Australian Government takes a similar position, committing itself to a non-regulatory approach to critical infrastructure,[45] stating that regulation is not the most suitable tool for setting security and risk standards, but rather that the owners and operators of critical infrastructure are best placed to set these objectives and to manage them.[46] This markets-based approach to CIP has created a proliferation of PPP in CIP that focus on the distribution of CIP awareness and education and that facilitate information exchange between the state, business and civil society organisations. CIP PPPs are indeed arguably useful tools for promoting a resilience culture and the sharing of information and best practices, but they also have a tendency to get complex and diffused as interdependencies between critical infrastructures increase to such an extent that it is hard to recognise the mesh of interconnections.[47]

However, PPPs tend to work properly only when they are formed around a relatively small group of actors that already have established links of trust between them. PPPs also are not particularly effective tools for addressing risks that are not business risks, but from

[40] US Treasury, "Committee on Foreign Investment in the United States (CIFIUS)," http://www.treasury.gov/resource-center/international/Pages/Committee-on-Foreign-Investment-in-US.aspx (Accessed September 21, 2013).

[41] Christine Laciak and Robert Schlossberg, "US: CIFIUS Review," The Antitrust Review of the Americas 2014, Global Competition Review, http://globalcompetitionreview.com/reviews/54/sections/182/chapters/2137/ (Accessed January 7, 2014).

[42] On 28 September 2012, President Obama used the authority granted to him under FINSA to block a Chinese acquisition of a US energy firm. Congressional Research Service, "The Committee on Foreign Investment in the United States (CFIUS)," http://www.fas.org/sgp/crs/natsec/RL33388.pdf (Accessed July 9, 2013).

[43] Nokia Siemens Networks consequently grabbed the deal, whilst unconfirmed rumours suggested that Huawei was prepared to pay considerably more for Motorola's wireless networks business.

[44] OECD, "Protection of Critical Infrastructure," 8.

[45] Albeit the Australian government stopped Huawei's participation in the National Broadband Network based on security concerns in 2012. The Attorney General's office commented that the decision was in line with the government's approach to ensuring the security and resilience of Australia's critical infrastructure. M. Lu Yueyang, "Australia Bars Huawei from Broadband Project," *The New York Times*, March 26, 2012, Technology, http://www.nytimes.com/2012/03/27/technology/australia-bars-huawei-from-broadband-project.html?_r=0 (Accessed September 21, 2013).

[46] Australian Government, "Australian Government Critical Infrastructure," 14.

[47] For discussion on the challenges and potential role for the CIP PPPs, see Myriam Dunn Cavelty and Manuel Suter, "Public-Private Partnerships are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection," *International Journal of Critical Infrastructure Protection* 2, no. 4 (2009): 179–88.

a national duty of care point of view are nonetheless unacceptable. In the meanwhile, the accountability of private operators tends to be limited to negligence in relation to duty of care legislation at the worst, whilst the principal motivation for establishing resilience is avoiding loss of revenue, customers and reputation. Given that the state retains the accountability for the provision of public goods and national security, the state must find a working strategy to address this gap.

Taking into consideration the complexities involved in the definition, ownership and management of critical infrastructures, perhaps it would be best for a national resilience strategy to focus on solving how the most critical functions of the society are maintained in a significant event, with an assumption that not all the services provided by critical infrastructure are available, at least on an equal basis to all segments of the society. Consequently, governments could concentrate their efforts towards securing infrastructure that must always be available, i.e. life sustaining services such as electricity, health services and water service, as well as national security and defence assets. The other critical infrastructure would then operate genuinely on commercial grounds under normal circumstances and the government would only involve itself as a contractual party with specific expectations for service and recovery levels under exceptional circumstances. Moreover, in order to achieve service and recovery levels that cannot be justified under normal commercial grounds, the government could utilise financial instruments, such as loans and guarantees, to subsidise the robustness and recovery investments. These subsidies should not provide the recipients a competitive edge over others under business as usual conditions.

In case of a serious disruption, the government would pay for operational costs related to the recovery operations within the agreed Recovery Time Objectives (RTOs). Hence, the government would essentially buy a recovery service, in line with what companies do to secure continuity of their critical operations. Once the service levels, or RTOs, have been agreed upon, the contractual parties would have the appropriate incentives for meeting the target levels and suffer fines for failing them. Whilst there would certainly be complexities involved with such an approach, it is quite clear that a contractual agreement would be more enforceable than any standard, decree or best practice in the context of a PPP for CIP. For such a strategy to succeed, however, the definition of what is critical, how and to what extent, both in terms of impact and time, is absolutely critical. It would, nonetheless, be a pragmatic option and effectively avoid the temptation to securitise critical infrastructure. If the sharing of business risk is accounted for in PPP infrastructure projects, why is the same principle not applied to catastrophic risk where government has a more natural role as the ultimate guarantor?

## Is resilience at odds with the core responsibilities of the nation-state?

Resilience strategies tend to follow risk and business continuity management principles and can be a cost-effective option, as the provisioning of security, robustness and redundancies for all sectors of critical infrastructure and services would be tremendously expensive, and would still not guarantee that significant disruptions do not take place. As has been argued, the differences between resilience and security are evident in both their spatial and temporal objectives. Security as a preventive discipline relies on stopping threats before they happen and hence, failure is often total if the threat is not stopped. Resilience, on the other hand, focuses on the ability to withstand and adapt to unexpected events and shocks and aims to keep

essential services running, at least a minimum level. The underlying logic of resilience is thus avoiding total failure. A resilient nation would thus not only be able to 'bounce back' when faced with the unexpected, but also have the ability to maintain a level of stability through securing at least a minimum level of basic services at all times and under all circumstances and/or recover such services within a reasonable time to minimise the adverse impact of disasters and disruptions to the citizens' safety, security and overall well-being. Thus, in a broad sense, resilience can be seen as a cost-effective insurance protection against the perceived challenge of uncertainty.

However, it is quite clear that national resilience, as a concept, challenges the traditional role of the state in the provision of security. As has been argued, implementing a national resilience strategy necessarily involves making choices, manifested in the prioritisation of critical services, and resulting in a level of inequality under exceptional circumstances. Hence, resilience implies a necessary compromise of the state's responsibility for the provision of basic services equally across its territory and constituencies. Taking into consideration that resilience, in the context of national security, has emerged at least partially because of the importance placed on 'new' threats (for example, economic, societal and environmental threats), emphasising resilience and an all-hazards approach, instead of traditional preventive security, can be seen as an entirely pragmatic response. The application of resilience in this context, however, requires the nation-state to agree on a new social contract with its citizens, based on a mutual understanding that acknowledges at least a partial shift from prevention of threats to management of the impacts of threats.

## Conclusion

This article has explored the evolving role of sovereign governments in the provision of security and positive political goods in an increasingly complex and uncertain global world, and the concept of resilience as a strategy to meet these challenges. The inclusion of a variety of new threats (such as the economic, environmental and societal) to the national security agenda, as well as securitisation of critical infrastructure, has created favourable conditions for a resilience approach to national security. However, the nation-state has nonetheless retained its core responsibilities for the traditional national security approach, which are more preventive in nature and are not always aligned with the resilience approach. Hence, nation-states should find an appropriate balance between preventive (security) and reactive (resilience) that corresponds with their particular needs, as well as the values of the society.

This, however, requires the government to articulate what the benefits and risks are with such an approach and use this as a basis for a renewed social contract with its citizens that clarifies the state's response before, during and after a catastrophic event. Consequently, it could be argued that a resilient state is a state that has the ability to ensure that its citizens are *reasonably* safe from physical harm, receive quality education, have an opportunity to prosper and can live their lives according to the standards set by their identity, culture and values. However, if critical infrastructure resilience remains a core national security issue, but the government nonetheless maintains a neoliberal stance in terms of considering its private operators and owners as responsible for the security and resilience of critical infrastructures, perhaps the desecuritisation of CIP should be at least considered?

## Notes on contributor

Christian Fjäder is a Manager at the National Emergency Supply Agency, Helsinki, Finland. He is an expert in security, risk and resilience management with extensive experience in regional and global roles in Australia, Asia, Europe and South America. In addition, he has research and consulting experience in international relations, geopolitics and global risk. He has a PhD in International Relations from the University of Sydney and a MBA from Bond University, Australia.