CSS Analysis in Security Policy

CSS ETH Zurich

No. 142 • October 2013

RESILIENCE IN SECURITY POLICY: PRESENT AND FUTURE

The concept of resilience enjoys increasing popularity among security policy practitioners. It shifts the focus of security policy considerations from avoiding catastrophic events to mitigating their effects. There are great differences in the way it is applied practically worldwide. In preparing the Swiss Security Policy Report 2014, the question of whether the concept should also be anchored more strongly and broadly in Swiss security policy deserves critical consideration.

Implemented resilience: Girls play in flooded New York City. *Brandon Stanton / Humans of New York*

The concept of resilience has been a remarkable success story: In the past ten years, it has established itself as a core idea of crisis and disaster management in many different policy areas. Geographically, too, the impact of the concept is continually expanding: A growing number of states have identified the resilience of technical and social systems as a goal of their national and international crisis and security policy.

This development is based on the insight that in view of the diversity, complexity, and unpredictability of contemporary risks, complete security is impossible to guarantee – and that crises and disasters cannot be excluded altogether, despite the best possible preventive measures. Therefore, the focus of security policy considerations is increasingly shifting to the mitigation rather than the prevention of events. Resilience, referring to the ability of a system or society to recover quickly after experiencing a sudden shock or physical stress (cf. CSS Analysis No. 60), is exceptionally well suited to take on a key role in an era marked by insecurity.

Indeed, a comparison of several countries shows that modern security policy is hardly imaginable without the concept of resilience. However, there are great differences in how the political approaches are developed and significant difficulties regarding the concrete implementation of the concept. This allows important inferences to be drawn concerning countries such as Switzerland that are still in the process of establishing resilience as a concept in security policy or of improving its implementation. If resilience is to be applied in a targeted and gainful manner, four issues must be dealt with in practical terms: The nature of the desired resilience; the goals of resilience policy; the concrete instruments to be used in fostering resilience; and the question of how to measure current and future resilience levels.

Varying approaches to resilience

Three countries are commonly considered to be among those at the forefront of applying resilience: The UK, The US, and Singapore (see Table 1 for an overview). Their resilience policies can serve as examples to highlight both commonalities and differences in the way resilience is thought about and implemented today (see Box 1).

In **the UK,** the Civil Contingencies Act (2004) replaced older civil defence legislation, the strategies of which were seen to be inadequate for large-scale civil emergencies like the UK floods of 2000 and the Foot and Mouth Disease outbreak of 2001. The Act outlines how local arrangements for disaster or crisis prevention and response should be built upon "local resilience forums" that also support the British government's "National Resilience Capabilities Programme". Decisions about risk management should be made at the lowest appropriate level.

In **the USA,** there is a strong belief that disaster resilience should be everyone's business and is a shared responsibility among

© 2013 Center for Security Studies (CSS), ETH Zurich

citizens, the private sector, and government. This belief is premised on the resilience imperative as a transformational mechanism that requires long-term thinking and approaches to disaster management and was presented recently (2012) in the US National Academies report on "Disaster Resilience: A National Imperative". Much of this thinking focuses on how to develop strategic practices towards gaining disaster resilience, and on how to connect the theoretical resilience strategy to practices that might ultimately build national resilience.

In **Singapore,** building community resilience has become a fundamental objective in the national security discussion. The national approach to security through resilience is encompassed by the "Be As One" (2009–20011) concept and the government's "Let's Stand Together" Facebook page, suggesting the importance of collective action in the prevention of threats. In deploying the resilience approach for "a cohesive society" and "an engaged people", Singapore projects a central role for the citizen in addressing threats to the nation. This national security program is overseen at the ministerial level, but is largely operationalised at the community level through a wide range of engagement and risk communication resources.

The key commonality of these resilience approaches is that there is an emphasis on a role for the citizen based on the need to act as a "responsible" member of society. This responsibilisation of the population reflects several driving factors: experience with disruptive events like terrorist attacks and natural disasters, coupled with an insufficient state emergency response; the inability to know and predict dangers, and prevent them from happening; the increasing costs of disasters; the privatisation of critical infrastructures; and lastly, there is a growing desire within civil society to be involved in managing and mitigating risks.

But the policies in these countries also show the manifold way in which the resilience concept can be applied in security and disaster management policy, reflecting political, social, and cultural differences, the different contributions from the academic domain, and heterogeneous national security policy requirements. In other words, there is no single type of resilience – but *different types* of resilience for different contexts. Therefore, it is almost impossible to find catch-all solutions for resilience policy. Engaging with resilience in depth is best done by looking at four important issues: how resilience is expressed; what or who resilience is required for; how to build resilience; and how to measure and monitor resilience.

Resilience currently enjoys an international status as a panacea for modern security challenges.

What kind of resilience?

Resilience, being a coping process, can only be observed once a technical or societal system has been disrupted by an incident. The manner in which a sudden disaster or crisis is mitigated and the functionality or operability of a system is restored varies according to the incident and the system in question. The academic literature makes a distinction between two extremes: On the one hand, there may be a relatively swift recovery in which the system is restored to the exact functionality that it was at before the incident ("bounce back"); on the other hand, there may be a dynamic, adaptive, and often longer-lasting process in which the system adapts to the new situation upon restoration of its functionality through processes of learning and adjustment ("adaptation").

In this context, disaster response may have different meanings for various components of an affected system: Varying resilience processes involving both "bounce back" and "adaptation" may occur as part of the same coping process. There may be particularly strong variations in the processes depending on whether technical component or human individuals are affected. While the resilience of a fibre optic cable network, for instance, depends on how quickly it can restore an internet connection based on innate redundancies, resilience in the case of the operators or users of such a network can be better identified on the basis of their capability of dealing with the disruption. For instance, one may look at the ability to compensate for lost services as well as at the way in which experiences gained in the incident can lead to behavioural changes.

Thus, first of all, resilience should not be thought of vaguely as simply a desirable property. Instead, it is important to think about which kind of resilience is necessary under which specific circumstances. It is equally important to clarify the following questions: What is the desired normal state? How much change may be permitted in a political system?

Which aims and actors for resilience?

Secondly, it is important to clarify the aim of resilience policy: Who and what is to be made resilient? This also touches on the question of who or what is especially vulnerable and thus most at risk, and who or what is particularly important and thus in need of being made resilient. This may apply to (critical) infrastructures, but also to high-density urban areas or certain professional groups (e.g., medical doctors). Due

Table 1: Country comparison of resilience in the United Kingdom, United States and Singapore

Country	Resilience for what?	What kind of resilience	Which aims for resilience?	Which instruments?	How to measure resilience
UK	Disaster response; community preparedness; community risk dialogue	"Bounce back"	Subsidiarity: decisions about risk management to be made at lowest appropriate level	"local resilience forums": community risk registers; risk communication; engaging public	No
US	Disaster response; disaster preparedness; critical infrastructure; national security	"Adaptation"	Shared responsibility	Various: recognise that "independent efforts fulfil strategic needs".	Yes: CIP "Regional Resiliency Assessment Program"
Singapore	National security; terrorism; disaster response.	"Bounce back"	National security: "whole of government, whole of community" mind-set; citizen " responsibilisation"	Citizen engagement; popular media; partnerships for integration, collective action & shared awareness	No

© 2013 Center for Security Studies (CSS), ETH Zurich

Resilienzformen «Bounce back» vs. «Adaptation»

	Resilience: Bounce Back	Resilience: Adaptation
Applicable to:	Entities or system components whose value (or service) lies in a specific function.	Entities or system components whose value lies in the management and proper functioning of systems or system components.
Results in:	Static outcome, where the objective is a return to existing function.	Dynamic process that results in an adaptive response to disturbance.
Temporal span:	Resilience is attributed if normal function is returned quickly.	Longer; characterised by social learning and reflection.

Source: Giroux/Prior: «Factsheet: Expressions of Resilience – From ‹Bounce Back› to Adaptation»

to their political sensitivity, these are decisions that need to be made at the highest political levels.

Furthermore, it is necessary to state in concrete terms which actors are to be given responsibility for resilience. If resilience is identified as a target, it follows that to a certain extent, the population or the private sector are allocated some of the responsibility for responding to events with a security policy impact. This has been particularly obvious for some time in the case of critical infrastructures, where private infrastructure operators are actively harnessed for the pursuit of security policy goals through regulation and other means such as dialog with government agencies. However, the increasing involvement of non-state actors also creates a number of questions regarding the relationship between the state and its citizens: E.g., should elected governments hold responsibility – what are governments for if not to bear responsibility for their citizenry? If not, how closely should civil society be involved in broad risk-related decisions that affect them? Should some people be made more responsible than others? What is the capacity of different players to be responsible? Experience shows that the crux of the matter is finding a good balance between top-down state governance and fostering "bottom-up" forces. Too much state control may obstruct or reduce the resilience that is already inherent in the private sector or in civil society.

Tools for building resilience

Once the nature of resilience and policy goals are determined, the third consideration will concern how to actually foster the type of resilience that one wants. Clearly, different expressions of resilience and the resilience of different elements of society (people, communities, infrastructure, companies, the economy, etc.) require different resilience-building tools. Therefore, broad security policy focused on the need for resilience will only be as successful as the specificity and application success of resilience-building tools targeted at the various resilience sub-elements in a social system, whether social, technical, economic, or environmental.

Many security and disaster policies, including those mentioned from the UK, Singapore, and the US, are relatively vague about how resilience might be developed in communities, infrastructure elements, or the environment. Typical practical means to build resilience that are regularly highlighted by policy-makers include risk communication, regulation, engagement, and collaborative decisionmaking. This shows that it is usually possible to foster resilience through established means and that such fostering is already taking place. Thus, existing solutions can frequently be applied.

Measuring resilience

Monitoring the suitability of policy tools in meeting the policy's goals is the fourth consideration in making effective resilience security policy. Having the capability to *measure* resilience in different sub-elements of social systems is essential for answering some key questions about resilience: How much resilience does an entity have? How much does it need to meet the policy goals? How are the policy tools for building or influencing resilience working? In particular, some assessment of the 'baseline' level of resilience possessed by an entity (before policy implementation tools are used) is useful for informing the allocation of resources where they are most needed.

It is quite possible that sufficient resilience is already in place, even if it has not been labelled as such.

Characteristics like resilience (and vulnerability, sustainability, human well-being, etc.) are hard to assess directly, and are typically measured as an index – a 'pointer' derived from several measurable indicators. For example, a critical infrastructure resilience index might be composed of several factors like 'probability of failure', 'level of maintenance', and 'age of infrastructure'. An index is consequently only as good as the indicators it combines, and the data available (is it high quality data, and is it suitable?) for the indicators. The selection of indicators might be streamlined by engaging relevant stakeholders, while obtaining appropriate data can be improved if data collection techniques are developed when the resilience policy is established. Because of these questions and challenges, the measurement of resilience in security and disaster contexts remains vague and under-developed in most countries. The United States is most actively exploring resilience measurement, and the 'Regional Resiliency Assessment Program' represents a recent initiative in the context of critical infrastructure protection overseen by the US Department of Homeland Security. However, even though the US spends a lot of time and money on measuring resilience, huge difficulties remain.

Resilience in Switzerland: Present and future

In Switzerland, resilience-based approaches are still only found in a handful of policy fields, particularly in civil protection and critical infrastructure protection and in the context of cyber-risks. More specifically, the "Basic Strategy for Critical Infrastructure Protection" and the "Swiss National Cyber-Risk Protection Strategy" have explicitly referenced resilience as an entrenched policy goal since 2012. In preparation for the new Swiss Security Policy Report (2014), however, it would be good to give greater weight to the question of whether the concept should be more strongly and broadly anchored in Swiss security policy as well, in line with the international trend. In answering this question, the following issues should be considered:

Resilience currently enjoys an international status as a panacea for modern security challenges, as it leaves room for a new kind of subjective perception of security, despite the unpredictable nature of contemporary hazards. However, the experiences of other countries (UK, Singapore) show that when introduced as a mere buzzword, the concept of resilience has little impact and may even give rise to negative outcomes when raising false expectations. Therefore, a beneficial policy of resilience

© 2013 Center for Security Studies (CSS), ETH Zurich

must be diligently tailored to the requirements of the respective political context – there are no simple "copy/paste" solutions. If the resources for such careful deliberations are lacking, there is no point in establishing resilience as a new concept.

Furthermore, it is advisable to review the existing structures, institutions, and instruments for their resilience-enhancing properties. It is quite possible that sufficient resilience is already in place, even if it has not been labelled as such. In the specific case of Switzerland, for instance, there is evidence to suggest that institutions such as federalism, the militia system, or nationwide insurance coverage contribute to the general resilience of the population and of the Swiss political system. Therefore, a specific relabeling of existing solutions under the heading of "resilience" may not be necessary.

If an additional resilience policy is desired, the main challenge will be to conceptualize resilience not only as a vaguely desirable state of affairs, but as a concept that must be implemented through concrete steps. This means asking, and finding answers to, questions such as the following: How do we define the politico-social status of "normalcy" that is to be reattained by means of a resilience process? What and who is in need of resilience, and is to be targeted by interventions aimed at enhancing resilience? Who is to be made responsible for resilience? To what extent? Who is answerable for achieving it? And finally: How can efforts to enhance resilience transform the relationship between the citizen and the state? These are highly political and sensitive issues; however, an open debate is essential if Switzerland is to have a useful policy of resilience. The Security Policy Report 2014 is a good opportunity to initiate a broad debate on these questions in Switzerland.

Authors: Myriam Dunn Cavelty
dunn@sipo.gess.ethz.ch
and Tim Prior
tim.prior@sipo.gess.ethz.ch

Responsible editor: Christian Nünlist
analysen@sipo.gess.ethz.ch

German and French versions / other CSS Analyses / mailinglist:
www.css.ethz.ch/cssanalysen

ISSN: 2296-0244

Previous issues

© 2013 Center for Security Studies (CSS), ETH Zurich