CRN REPORT

Factsheet

Examining Resilience: A concept to improve societal security and technical safety

Zurich, June 2009

Crisis and Risk Network (CRN)
Center for Security Studies (CSS), ETH Zürich

Commissioned by the Federal Office for Civil Protection (FOCP)

CRN
Supported by ISN

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Authors: Elgin Brunner und Jennifer Giroux

Contact:
Center for Security Studies
Seilergraben 45–49
ETH Zurich
CH-8092 Zurich
Switzerland
Tel.: +41-44-632 40 25

crn@sipo.gess.ethz.ch
www.crn.ethz.ch

Contracting Entity: Federal Office for Civil Protection (FOCP)
Project supervision FOCP: Stefan Brem, Head Risk Analysis and Research Coordination
Contractor: Center for Security Studies (CSS), ETH Zurich
Project supervision CSS: Myriam Dunn, Head New Risks Research Unit; Andreas Wenger, Director CSS; Victor Mauer, Deputy Director CSS

Disclaimer: The views expressed in this focal report do not necessarily represent the official position of the Swiss Federal Office for Civil Protection, the Swiss Federal Department of Defence, Civil Protection, and Sport or any other governmental body. They represent the views and interpretations of the authors, unless otherwise stated.

TABLE OF CONTENTS

ABSTRACT

In recent years, the concept of resilience has gained traction within the systems design community. Recognizing that not all threats or disasters can be averted, some states are turning their attention to efforts that can enhance the flexibility and strength of technical systems and, more recently, of entire societies. While studies on the resilience of technical systems have been undertaken for quite some time, the societal aspect is a new development. In this regard, states are increasingly debating ways to enhance community or rather local resilience. This attention on the individual role in preparing and responding to emergencies is clearly a new trend that will be underlined throughout this report. In addition to examining some current definitions of and conceptual approaches to resilience, this report will also highlight the difference between *resilience* and another commonly used term, *redundancy*. From there, components of resilience within CI and society, respectively, will be addressed followed by some concrete examples of how states, and even international organizations, are incorporating resilience into their security strategies. It is evident in these examples that some states are focusing on technical resilience within CI, while others adopt a broadening approach to include societal resilience. With the latter, some states and local organizations are utilizing new technologies, such as social media and mobile phones, to expand their reach and improve access to civilians and representatives of the public and private sectors. These developments call attention to the various modern platforms that can be utilized to engage and mobilize communities, especially during emergencies. The final section discusses the role of resilience in Swiss policy and areas where societal resilience in particular could be strengthened.

1. INTRODUCTION

1.1 Resilience – conceptual framework and definitional cornerstones

Due to the challenges involved in protecting critical infrastructures and societies from various threats, resilience is gaining importance as a core conceptual approach. The rise of the risk paradigm among security experts – irrespective of whether they are focused on technological or societal features – and the acknowledgement that security can never be fully achieved are the main insights that have characterized the global security environment of our time. Increasingly, states are recognizing the uncertainty involved in ensuring a society's smooth functioning. Disruptions are inevitable, as it is difficult to identify and address all vulnerabilities and potential threats; thus, critical infrastructures and the core values of a society cannot be entirely protected at all times.

This raises the following fundamental question: *What happens when a disruption occurs?*

The concept of resilience addresses this very question, as it aims at covering:

> "The ability of social units to mitigate hazards, contain the effects of disasters when they occur, and carry out recovery activities in ways that minimize social disruption and mitigate the effects of future disasters."[1]

Therefore, resilience can be understood as the process of preparing and responding to the eventual actualization of the multiple and increasingly diverse risks. Resilience as a term, having become crucial to security and risk theory and practice, originated in various different disciplines and therefore integrates knowledge from psychology and social psychology, ecology and environmental science, engineering, and organizational behavior research.

On the structural level, two factors determine what is covered by resilience. First, due to uncertainty, every system or social unit should strive to be as flexible as possible. Such "resilient flexibility means avoiding situations where components of a system [or social unit] are 'too big to fail'".[2] In other words, a high resilience system distributes risk throughout the system, while in a low resilience system, risks are felt disproportionately. Second, since failures cannot be ruled out, the system or social unit has an inherent need to spot failures early in order to mitigate their consequences. Walker and Cascio provide definitions that further expand these characteristics.

Whereas Walker defines resilience as

> "[t]he capacity of a system to absorb disturbance and reorganize while undergoing change so as to still retain essentially the same function, structure, identity and feedbacks",[3]

Cascio views it as

> "[t]he capacity of an entity [...] to withstand sudden, unexpected shocks, and (ideally) be capable of recovering quickly afterwards."[4]

Such definitions enable us to comprehend *what* resilience is ideally about, yet they say nothing about *how* a system or societal unit can *become* resilient. All three of the highlighted definitions share the idea of adaptability/flexibility, while maintaining the essence of the system or societal unit (identity).In the words of Evans and Steven, this means that "resilience results from being able to face up to reality,

[1] Bruneau, M., S.E. Chang, et al. (2003). "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities", in Earthquake Spectra 19(4): 733–752.

[2] Cascio, Jamais (2009). "Resilience in the Face of Crisis: Why the Future Will Be Flexible" in FastCompany.com, April 2.

[3] Walker, B. et al. (2004). "Resilience Thinking: sustaining Ecosystems and People in a Changing Word", Washington: Island Press. Cited in Evans, A., Steven, D. (2009) "Risks and resilience in the new global era" in Renewal vol. 17, no. 1.

[4] Op. cit. Cascio (2009).

[and] improvise in the face of unfamiliar challenges",[5] while maintaining a coherent identity. Hence, resilience is fundamentally about both flexibility and the capacity to maintain the 'whole'. Therefore, resilience implies both strength and flexibility. In this sense, a resilient structure would bend, but not break in the face of an emergency.

Within this understanding, complexity is advocated as a problem-solving strategy. Complexity naturally coincides with diversity. Hence, the so-called risk paradigm, characterized by a diverse and complex security landscape, forges the structure of the potential remedy that resilience offers both as a concept and in practice. Not only do vulnerabilities increase with complex and diverse systems and social units, but the potential avenues for addressing a challenge and alleviating disruption are increased commensurately. Thus, the complexity and diversity of systems and social units means that resilience should be understood as the capacity to adapt in a dynamic environment. Accordingly, resilience is characterized by a positive correlation between complexity/diversity and adaptability.

The differentiation between technological systems and social units merits further discussion. When considering the potential breakdown of particular (critical) infrastructures, resilience in theory and practice focuses upon these infrastructures from a systemic perspective, most often with a technological focus. On a greater scale, the resilience of society as a whole is concerned when, due to cascading spill-over effects of a disruptive event, an entire community is affected. The focus is then no longer on a single system or sub-system of a particular (critical) infrastructure, but is broadened to include the interplay of multiple systems adding up to ensure the functioning of society at large. While systems resilience is a continuous driving force for improvement, on the societal level the human component is central. In the case of a major disruptive event, resilience is essentially contingent on the actions of people operating at the local level. At this particular stage, the visible role of governments and their agencies is minimal, and basically consists of coordinating activities. However, despite the efforts of local/civilian actors, ultimate responsibility for minimizing damage rests with the governments and their agencies when a disruptive event occurs at the national and/or transnational stages.

On the very practical level, both resilience layers – the societal and the systemic – require specific and particular approaches. In terms of societal resilience and developing an approach to building a resilient nation, Charlie Edwards pleads for the adoption of what he calls the 'four Es' of community resilience: engagement, education, empowerment, and encouragement.[6] Holding that community resilience is an everyday activity, governmental and administrative agencies are to engage in constant dialog and feedback with community members. This includes providing tools and resources such as educational platforms and outlets in order to promote the building of individual resilience. A key point, according to Edwards, is that individuals and communities need to be encouraged to play a role.[7]

For systemic-level resilience, Michel Bruneau has developed an organizational framework that conceptualizes and defines disaster resilience as consisting of four distinct organizational characteristics or factors – the R4 framework. The four factors are: robustness, defined as the ability of an entity to resist or fore-

[5] Op. cit., Evans and Steven (2009).

[6] Edwards C. (2009). "Resilient Nation". London: Demos, pp. 80ff.

[7] Ibid.

stall damaging or catastrophic events; redundancy, defined as an organizational unit's ability to provide alternative processes for inline or critical systems; resourcefulness, defined as a characteristic of an entity's tenacious response to, and creative solutions for, a disaster-related instance; and rapidity, defined as the ability to restore systems or processes quickly. Bruneau identifies the four different resilience domains – technical, organizational, social, and economic systems – and seeks to quantify these areas in order to measure resilience.[8] From an analytical perspective, however, measurability and quantification (of precisely fixed entities) is inherently incompatible with the core of the concept of resilience (which calls for adaptability and constant flexibility).

Lastly, can resilience be understood as a society or system's preparedness for the actualization of a disruptive event? Indeed, this seems the case. However, it is also true that we can never know exactly what we should be prepared for or how we should prepare for it. That is why, as some experts contend, "the most resilient systems are those that recognize that they may be insufficient against all possible outcomes."[9] Acknowledging this, the focus of resilience expands to include systemic learning processes.

1.2 Differentiating resilience and redundancy

Redundancy is one of the four components of Michel Bruneau's disaster resilience framework. It is defined as those system properties that allow for alternative options, choices, and substitutions in the case of failure or breakdown. The availability of redundancies increases resilience insofar as it decreases dependence upon particular and specific components of a system or social unit specifically by providing alternatives. Therefore, redundancy matches with the diversity element of resilience. Hence, redundancy is just one, albeit crucial, aspect of resilience; but resilience as a concept should not be reduced to redundancy – a resilient system or social unit is also robust while flexible, adaptive through its learning processes, has resources at its disposal, is capable of reacting quickly, and is maintained by engaged, educated, and empowered individuals. Furthermore, redundancy defined as the availability of alternatives discloses a tension in the relationship between resilience as a concept in general (and redundancy as one of its core elements in particular) and the pervasive neo-liberal paradigm of efficiency. While redundancy increases the diversity of potential responses and the flexibility of a system or social unit (and therefore its resilience), it is per definition inefficient to provide multiple solutions to an emerging problem rather than the one with the single best cost-benefit ratio.

[8] Bruneau, M. and Tierney, K.. "Resilience: Defining and Measuring What Matters". Mulitdisciplinary Center for Earthquake Engineering Research. And: King, M. A. and Zobel, C. W. "Applying the R4 Framework of Resilience: Information Technology Risk Management at Northrop Grumman". Southeast Decision Sciences Institute Annual Conference.

[9] Cascio, J. (2009). "Uncertainty and Resilience". Jan. 2. Available at: http://www.peopleandplace.net/perspectives/2009/1/2/uncertainty_and_resilience

2. TRAITS AND COMPONENTS OF A RESILIENT SOCIETY

As discussed thus far, all highly resilient systems possess the capacity to absorb major disturbances and reorganize while undergoing changes that allow them to retain their functionality and identity, or in other words, to maintain the essence of the system or societal unit. However, much like the concept of critical infrastructure, the concept of resilience is also evolving. As noted, states are increasingly coming to the understanding that the notion of protecting all critical infrastructures from threats – no matter what the cause – is unrealistic. Rather than focusing on the causes, efforts are underway to anticipate the consequences of CI breakdowns and damages.

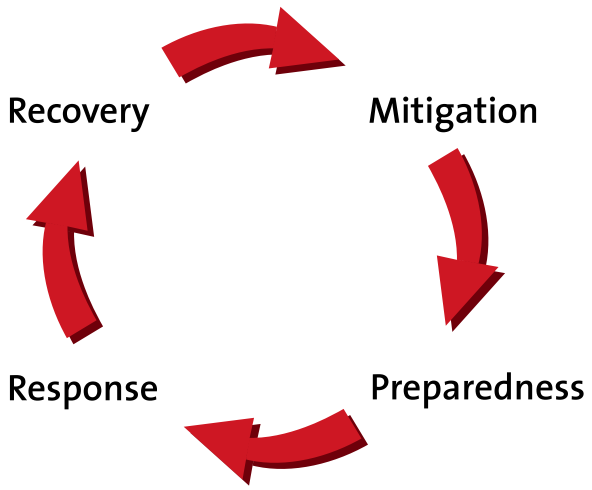

Figure 1: Resilience Cycle[10]

However, some common traits and components of a resilient system – both in the technical and in the societal domain – may be identified. Together, they share what can be defined as a process, as illustrated in Figure 1. Whether at the technical or social level, all systems experience this resilience cycle and its key elements of mitigation, preparedness, response, and recovery. As Edwards notes, mitigation refers to the strengthening of capabilities; preparedness refers to anticipating threats and emergencies that could lead to failures, identifying and utilizing capacity, and developing response plans; response refers to the actions taken with the goal of minimizing damage and disruption; and, finally, recovery refers to rebuilding and restoring.[11] At each phase, there is a role for individuals and industries to engage and be a part of prevention activities. For example, at the mitigation stage, government agencies can liaise with construction companies to recommend and/or explore new approaches to building transit infrastructure such as roads or bridges that are better suited to withstand a sizable storm, whereas at the preparedness phase, individuals can be informed of potential emergencies and responses needed, such as being aware of alternative transit routes. In the spirit of prevention, public and private entities enhance resilience by working together to strengthen the channels of communication and awareness.

2.1 Resilience and CI

Turning to specific traits, one of the major vulnerabilities of modern critical infrastructures – such as food supply chains, transport networks, and energy grids – is their interconnected, interdependent, highly complex nature. Within such systems – and indeed other connected systems – one failure can have a domino effect that leads to failures throughout the chain. This inability to absorb shocks and keep disturbances localized is characteristic of a low-resilience system. Therefore, in order to enhance the resilience of CI, its ability to absorb shocks must be strengthened. National grids, such as those in the United States and the United Kingdom, have a recent history of black-

[10] Edwards, p. 20.

[11] Ibid., pp. 19ff.

outs where the failures of a few power stations have set off cascades of regional power failures.[12] Such experiences can lead to additional disruptions and multiply effects by creating other negative outcomes, such as societal aggression or, in the case of extreme (low or high) temperatures, casualties. For example, a heat wave in 2003 led to power shortages in France due to the unusually large electricity demands. What was initially a technical problem became a health crisis in northern France as much of society, especially the most vulnerable part of the population, was unable to cope with the high temperatures, and many casualties were recorded as a result.[13]

Given that most critical infrastructures are controlled by the private sector, governments must be active in engaging and encouraging dialog with such industries that are essential to society. Thus, another component to enhancing resilience within CI is forging *partnerships* between vital nodes within in the public and private sector where critical infrastructure protection converge. In critiquing the United Kingdom's CIP, a report produced by Infinity, a business continuity corporation, noted the lack of communication and collaboration between the public and private sectors.[14] As the report noted, a "lack of joined up thinking across both Government departments and the private sector, has created many points of weakness in our Critical Infrastructure".[15] Therefore, opening the pathways to communication between these sectors that are conjoined through their significance to society is a crucial component to enhancing resilience within CI.

2.2 Resilience and the community

To date, there has been no blueprint design for creating a resilient organization/community. However, many characteristics of such a design have been identified – some of which have already been mentioned, such as flexibility and adaptability. Figure 2 expands on some of these characteristics with the view of applying them to a resilient society. Bringing these qualities together aggregates into the following four areas:

- Foresight and Planning: This involves a community's ability to discuss and anticipate the myriad threats to their systems and understand the potential impacts. This involves engaging individuals, collaborating, coordinating, and sponsoring dialog with all sectors.
- Trust & Partnering: Trust – both within CI and society – is a key element to developing supportive partnerships throughout the community. Trust within and between the public sector, the private sector, and local communities will enhance response and recovery, as sectors will be better equipped to respond collectively to emergencies.
- Strength and Flexibility: Adaptation to the changing environment while preserving identity. For example, having learned the detrimental effects that massive storms can have on communities, the residents of Fargo, North Dakota came together to help with sandbagging and prevent major flooding throughout their city.[16] Businesses

[12] Ibid. pp. 27ff.

[13] Bhattacharya, S. 2003. European heatwave causes 35,000 deaths. The New Scientist. 10 October. Available at: http://www.newscientist.com/article/dn4259

[14] Infinity. 2007. Providing Protection and Continuity: The UK's national security in the 21st Century. IPPR Research Commission on National Security for the 21st Century Available at: http://www.ippr.org/uploadedFiles/ipprcommissions/infinity_ippr_submission.pdf

[15] Ibid. p. 4.

[16] ABC News. 2009. Storm threatens Fargo, increases flood prediction. 23 March. Available at: http://kstp.com/article/stories/s843458.shtml?cat=1

and schools were quickly shut down, as volunteers from all walks of life came together to limit the potential devastation to their area. Such rapid, coordinated response not only requires trust, but also a great deal of strength and flexibility to adapt and respond to the circumstances.

- Leadership: Good leadership is essential to the effectiveness of any organization. Leadership provides objectives and establishes guidance. Though within the resilience discourse, the emphasis is on the responsibility of individuals, it is the leaders who establish frameworks and platforms for organized engagement.

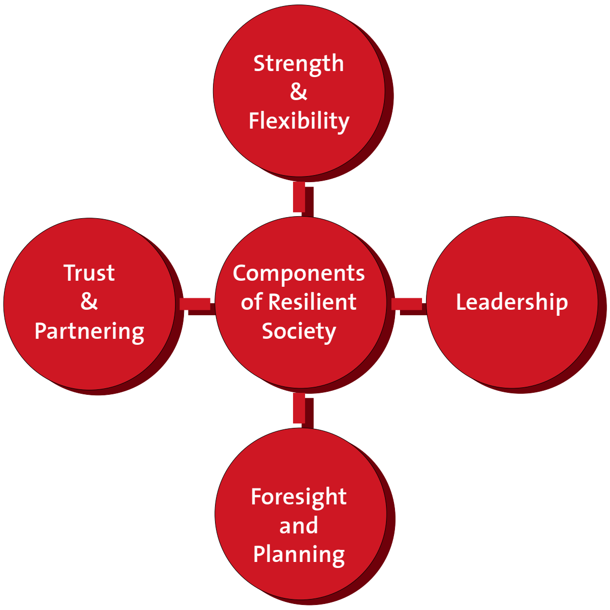

Figure 2: Components of a Resilient Society[17]

2.3 Technology and social resilience

Advances in technology have provided societies with ways of communicating and exchanging information at an ever-increasing rate. In the last decade, global use of more affordable mobile phones and accessible internet has exploded. In 2008, a reported 23 per cent of the world's population used the internet, while 60 per cent now own a mobile phone – for a total of more than one billion people using digital technology.[18] This is a favorable development not only for civil society, but also for government officials and emergency responders who seek new, efficient, and effective ways to connect with their communities. However, rather than focusing on ways to utilize technology only during an emergency, officials are realizing that such tools can be better suited for prevention activities that aim to help individuals be informed and prepared and thus better equipped to endure and rebound from a crisis. On the one hand, the products, services, and platforms developed through technological innovation can aid communities in prevention activities by creating opportunities and venues to forge community relationships, enhance community trust, and encourage information-sharing. On the other hand, it is now widely documented that mobile phone networks can become congested during an emergency;[19] thus, it is imperative to develop continuity plans that take into account such technological limitations *before* a crisis occurs. specifically closer

[17] These components were drawn from the various resources utilized for this factsheet. In particular, see Cascio (2009), Edwards (2009), Walker (2004). Also see, Evans, A. & Steven, D. 2009. Risk and resilience in the new global era. Renewal, 17(1). Available at: http://globaldashboard.org/wp-content/uploads/2009/Renewal_resilience_article.pdf

[18] The Daily Mail. 2009. Mobile phone use explodes as 60% of the world's population signs up for a handset. The Daily Mail Online. 3 March. Available at: http://www.dailymail.co.uk/sciencetech/article-1158758/Mobile-phone-use-explodes-60-worlds-population-signs-handset.html

[19] Goodwin, Bill. 2005. Mobile phones of little use in crisis. Computer Weekly. 19 July. Available at: http://www.computerweekly.com/Articles/2005/07/19/210901/mobile-phones-of-little-use-in-crisis.htm

investigation of how these tools are being used renders a number of examples.

- *Mobile Phones*: Many governmental agencies and organizations now use Short Messaging Services (SMS) delivered by mobile phones to provide a steady stream of alerts. For example, the Los Angeles Fire Department (LAFD) has a text message service called "LAFD Alert" that notifies users of incidents throughout Los Angeles.[20] During recent wildfires in California and Australia, such texting services have provided a way for responders to quickly communicate with civilians. These exchanges are useful not only for limiting casualties, but in some cases also for limiting damages. Noting the importance of such technology, the US Department of Homeland Security's (DHS) Ready.Gov program and the American Red Cross have added mobile phones and chargers to the list of basic supplies that citizens should have in their emergency preparedness kits.[21]
- *Social Media: Web 2.0 Tools:* Social networking tools have emerged as powerful platforms for individuals and communities – brought together through interests, affiliations, or geography – to come together, exchange information, and mobilize around interests and events. "Web 2.0 refers to the evolution of the Internet into a tool for harnessing collective wisdom through information sharing, rather than seeking information only from static sites."[22] In recent years, private companies and social entrepreneurs have launched a large number of community platforms such as MySpace, Facebook, LinkedIn, Twitter, YouTube, or blog-hosting services. While commonly used for general consumer purposes – such as sharing articles, pictures, and videos for promotional purposes and/or within one's personal network – these tools have entered a new dimension. Activists and emergency personnel are beginning to use such low-cost platforms to transmit information quickly, mobilize people, provoke action, and provide a mechanism for feedback. However, it should be noted that all of these platforms are vulnerable to manipulation and fraudulent activity,[23] so while governments can leverage these platforms to enhance community engagement, they must also be mindful of the limitations.
- *Emergency Response and Communication*: Learning from the devastation of Hurricane Katrina in August 2005 and the poor coordination between emergency personal and civilians, the LAFD has begun using a variety of web 2.0 tools such as Twitter, Flicker, blogs, and live internet radio to provide a constraint stream of information utilizing all types of media platforms.[24] They used the micro-blogging site Twitter to post information briefs about fires or other emergencies that the LAFD responds to while utilizing a blog to discuss emergencies and responses in greater detail.[25] To date, they have roughly 4,500 followers on their Twitter account and are also exploring various

[20] http://groups.google.com/group/LAFD_ALERT

[21] 2009. Ready.Gov, Red Cross Adding Mobile Phones To Basic Emergency Preparedness Supply Kit Recommendation. Available at: http://incaseofemergencyblog.com/2009/05/18/breaking-news-readygov-red-cross-adding-mobile-phones-to-basic-emergency-preparedness-supply-kit-recommendation

[22] Sternstein, A. 2009. State department promotes Internet diplomacy. Nextgov.com. 1 June. Available at: http://www.nextgov.com/nextgov/ng_20090601_2467.php?oref=rss

[23] Jackson, W. 2009. Tweeters beware: All is not secure on the cyber front. Government Computer News. 20 July. Available at: http://gcn.com/Articles/2009/07/20/Cybereye-Twitter-social-network-security-warning.aspx

[24] Havenstein, H. 2007. LA fire department all a 'twitter' over web 2.0. Computer World. 3 August. Available at: http://www.pcworld.com/article/135518/la_fire_department_all_atwitter_over_web_20.html

[25] Twitter: http://twitter.com/LAFD; blog: http://lafd.blogspot.com/

other social media platforms to test effectiveness. As Ron Meyers, a spokesman for the LAFD, notes:

> "We have about 80 Web 2.0 projects in the works right now, we bring them in slowly, keep them if they work and if they're not sustainable, we move on."[26]

The US Federal Bureau of Investigation (FBI) has also set up a Facebook fan page, a YouTube page, and a Twitter account in order to "expand its ability to share information with millions of social media users" and provide another venue to enlist public support, as well as for communication with government officials.[27] The FBI is also experimenting with the use of FBI widgets[28] and testing the usefulness of other virtual tools such as 'Second Life.'[29] Thus far, more than 350,000 people in 80 countries have downloaded a "Most Wanted" application for iPhones and iPod Touches. "To reach out to the public, we need to be where people are, and we know tens of millions of people spend their time in social media sites," noted John Miller, the FBI's head of public affairs.[30] Such developments can also be found in the use of blogs, which are proving to be a promising tool for government to use and engage citizens over the web. The US Transportation Security Administration (TSA) blog, Evolution of Security,[31] is using its blog, for example, to communicate with travelers.[32]

- Corporations such as Microsoft are beginning to design such software aimed at improving emergency response and easing communication. For example, Microsoft has recently launched a new platform called "Microsoft Vine",[33] which they are beta-testing in US cities. Microsoft is working with emergency management to create a service that provides "a local platform to communicate in all situations, especially during emergencies".[34] Vine not only allows members to communicate, but also allows them to map areas of concern and to provide rapid notifications that can be tailored to individuals or the group. Microsoft is beta-testing the product in selected cities, such as Seattle, working with emergency management agencies to test the above concepts. However, the feasibility and reliability of such platforms need to be tested for effectiveness.

[26] De Turenne, V. 2008. LA Fire Department's a Twitter with web 2.0. Los Angeles Times. 25 July. Available at: http://latimesblogs.latimes.com/lanow/2008/07/do-you-twitter.html

[27] Bain, B. 2009. FBI expands use of social media. Federal Computer Week. 18 May. Available at: http://fcw.com/Articles/2009/05/18/Web-FBI-social-media.aspx?p=1

[28] For example the FBI has developed various modules (wigets) that contain links to FBI sites that discuss news, history, fugitives, sex offenders and missing kids. The FBI offers this service for people to post on their personal websites and blogs. This effort aims to share frequently updated information and hopefully catch more fugitives and find missing children through broader engagement with the web community.

[29] See: http://www.fbi.gov/page2/may09/socialmedia_051509.html and http://www.fbi.gov/page2/may09/gallery_050809f.html

[30] Bain, 2009.

[31] http://www.tsa.gov/blog

[32] Beam, C. 2009. Those airport security guys have a good blog. St. Petersburg Times. 5 May. Available at: http://www.tampabay.com/news/perspective/article998343.ece

[33] http://www.vine.net

[34] McKay, J. 2009. Microsoft Launches Social Media Tool. Available at: http://www.emergencymgmt.com/disaster/Microsoft-Launches-Social-Media.html

3. RESILIENCE IN PRACTICE

Resilience is clearly becoming increasingly important for modern societies as states come to accept that they cannot prevent every risk from being realized, but rather must learn to adapt and manage risks in a way that minimizes impact. However, a brief survey of countries and their approaches to resilience shows that there are many different examples. Some countries continue to approach resilience within technical systems only, while others are moving to a more holistic approach that embraces engagement throughout all sectors. Advances made through community platforms (online) and examples of community engagement during emergencies have led some states to look more to the individual as a key component in security planning. There is an increasing number of state-sponsored websites providing the general public with emergency information and preparedness tools. In addition, 'Transition Towns', which are local movements that aim to prepare communities to cope with challenges caused by energy supply and environmental change, constitute a grassroots effort to build societal resilience.[35] The following section cites some examples where resilience is being introduced and/or incorporated.

- *Australia*: In Australia, resilience is considered a key element in the national critical infrastructure protection plan and, more recently, in community preparedness.[36] Recognizing that organizations cannot anticipate nor plan for every challenge, the Australian authorities have not only promoted the idea of developing business continuity and risk management plans "to help prevent what can be prevented and protect what can be protected", but also called for 'organizational resilience' to help organizations "cope with what cannot be prevented or protected".[37] To bring the business community together, the Trusted Information Sharing Network (TISN) was developed to provide a platform for the owners and operators of critical infrastructure to exchange information and coordinate their activities. In addition, the TISN Resilience Community of Interest has been launched to promote the idea of organizational resilience to the corporate sector and the CI community.[38] This website provides information, defines terms, describes approaches, and highlights tools such as the Resilience Maturity Model Quick Assessment Tool, which is still in the testing phase.[39] More recently, government officials announced the Disaster Resilience Australia Package, which aims "to help local communities threatened by wildfires and other disasters".[40] A portion of the funding will go towards improving e-security by ensuring that "Australian Internet users have access to information on cyber threats, vulnerabilities in their systems, and information on how to better protect their information technology environment," as well as "upgrading wireless emergency communications capabilities during major national security or disaster events."[41]
- *Canada*: The Canadian Public Safety department (Public Safety Canada) has adopted an all-hazards approach and mainly focuses on enhancing the resilience of its critical infrastructures. This is documented in the "Working Towards a National Strat-

[35] http://www.transitiontowns.org

[36] See, for example, a brochure on community resilience: http://www.socialinclusion.gov.au/LatestNews/Documents/Building-communityresiliencebrochure.pdf

[37] http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_CriticalInfrastructureProtection#c8

[38] http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/Aboutthe-TISN_ResilienceCommunityofInterest

[39] *Ibid*.

[40] Occupational Health and Safety. 2009. Australia creating national computer emergency response team. 20 May. Available at: http://ohsonline.com/articles/2009/05/20/australia-creating-national-computer-emergency-response-team.aspx

[41] *Ibid*.

egy and Action Plan for Critical Infrastructure",[42] which was developed in coordination and collaboration between the federal, provincial, and territorial governments. Such cross-territorial partnerships and exchanges between Canada's public and private sectors are important to strategy development. So far, no efforts have been made to examine community resilience and individual engagement.

- *Sweden*: The Swedish Civil Contingencies Agency (SCCA), established in January 2009, has launched a comprehensive approach to societal security within Sweden.[43] Adopting an all-hazards approach, the SCCA focuses on the resilience of Sweden's critical infrastructure in addition to addressing security issues that affect society, ranging from small to large traffic disturbances, technical failures, and more serious emergencies that demand federal engagement.[44] In this respect, Sweden is leading among the Nordic nations in terms of integrating the concept of resilience – in both the technical and the societal spheres – into its security policy.

- *United States:* Resilience is surfacing more frequently throughout the United States. Historically this concept has been used to in the area of technical systems and infrastructure, though recent developments show a move to introduce resilience into society by recognizing the individual role in preventing and/or mitigating disasters. This approach, which originated at the local level is now being recognized at the federal level as demonstrated in by National Security Council which formed a new directorate in May 2009 that will focus on resilience in the form of "preparedness and response for a domestic WMD attack, pandemic or natural catastrophe".[45] In addition, the adoption of resilience, especially within the community, is also found in recent statements made by the Federal Emergency Management Agency (FEMA),[46] which has highlighted the role of the individual in disaster response and management, and through the Department of Homeland Security (DHS), which has launched Ready.gov, a website that provides a source of guidance on disaster preparedness and response for communities.

- *United Kingdom:* With regard to managing risks, the United Kingdom has been fairly aggressive in addressing the risks outlined in its National Risk Register.[47] Such measures include the creation of new legislation, launching and/or enhancing civil protection structures, and sponsoring a nationwide discussion on risk management. While such activities have hitherto centered on formal institutions and organizations within technical systems and critical infrastructures, the government

[42] Public Safety Canada. 2008. Working Towards a National Strategy and Action Plan for Critical Infrastructure, Draft for Consultation. Available at: *http://www.publicsafety.gc.ca/prg/em/cip/_fl/nat-strat-critical-infrastructure-eng.pdf*

[43] *http://www.raddningsverket.se/templates/SRSA_Page____24815.aspx*

[44] Englund, L. & Lundberg, J. 2008. Country Survey of Sweden 2008. International CIIP Handbook, Center for Security Studies, ETH Zurich, p. 396. Available at: *http://www.crn.ethz.ch/publications/crn_team/ciip_by_chapter/partI/sweden.pdf*

[45] Hsu, S.S. 2009. Obama Integrates Security Councils, Adds New Offices. The Washington Post. 27 May. Available at: *http://www.washingtonpost.com/wp-dyn/content/article/2009/05/26/AR2009052603148.html*

[46] For examples of where FEMA discusses resilience and the role of individuals in preparing for and responding to emergencies, see: *http://www.domesticpreparedness.com/Resilience/Resilience_Tips/FEMA_(Federal_Emergency_Management_Agency)_and_SEMA_(State_Emergency_Management_Agency)_Urge_Flood_Preparedness and http://www.fema.gov/hazard/wildfire/ca_2007.shtm.*

[47] According to the United Kingdom's National Risk Register, risks are made up of threats like terrorism and organized crime; hazards such as flooding, heat waves, and snow storms, as well as major accidents. *http://www.cabinetoffice.gov.uk/reports/national_risk_register.aspx*

has recently become more interested in the concept of resilience that embraces both technical and societal components. In 2007, the Centre for the Protection of National Infrastructure was established in order to address vulnerabilities, risks, and responses. This effort to look at ways to reduce vulnerabilities was and continues to be driven by an effort to enhance the resilience of the United Kingdom's critical infrastructures. The private sector has also been moving in this direction, as illustrated by the Shared Capability Advisory Network (CNI Scan), which also seeks to encourage dialog and planning within the framework of resilience.[48] However, as Edwards notes, while such efforts are a step in the right direction, they still fall short of recognizing "the brittle nature of society".[49] The United Kingdom has also launched a comprehensive website "UK Resilience"[50] that provides various resources on business continuity, emergency planning, and civil engagement. A more recent platform is the Direct.gov online resource, which is aimed at bridging the gap between the federal and local levels.[51] Visitors can find information on preparedness, advice for community groups and volunteers, and specifically identified risks for a given town or region. The "Preparing for Emergencies" booklet – available in multiple languages – is a guide for individuals that was delivered to British residents homes and is also available on the web.[52]

- *United Nations:* A key element of resilience is the significance placed upon the society as a whole, largely emanating from the local level. However, the international community, and this regard the United Nations (UN), has a role in the resilience debate in that it can create platforms for dialogue, sharing and exchanging in best practices, and the promotion of frameworks and tools for states, especially those that are less-developed, to utilize. This is already in the works, as seen in the 2007 UN International Strategy for Disaster Risk Reduction (UN-ISDRR) meeting where the theme was 'Disaster Risk Reduction Begins at School.' This approach was based on two criteria "(1) it is in line with the Priority 3 of the Hyogo Framework for Action 2005-2015: 'Use knowledge, innovation and education to build a culture of safety and resilience at all levels'; and (2) schools are the best venues for forging durable collective values; therefore they are suitable for building a culture of prevention and disaster resilience."[53] States can use such platforms not only to learn about new ways of capitalizing on existing resources within their communities, in this case the classroom, but also to identify new approaches to incorporating resilience into emergency plans.

[48] See: http://www.cniscan.org/

[49] Edwards, p. 30.

[50] http://www.cabinetoffice.gov.uk/ukresilience.aspx

[51] http://www.direct.gov.uk/en/Governmentcitizensandrights/Dealingwithemergencies/Preparingforemergencies/index.htm

[52] http://www.direct.gov.uk/en/Governmentcitizensandrights/Dealingwithemergencies/Preparingforemergencies/DG_176035

[53] http://www.unisdr.org/eng/public_aware/world_camp/2006-2007/wdrc-2006-2007.htm

4. IMPLICATIONS FOR SWITZERLAND

Resilience is one of the five core principles for the protection of critical infrastructures in Switzerland. The others are:

- A holistic approach to risk management that embraces an
- all-hazards threat spectrum
- maintaining proportionality between the protective provisions taken and the risk estimate, and
- the principle of subsidiarity between public and the private infrastructure operators.[54]

Like many of the countries in section 3, Switzerland regards resilience as crucial to the protection of critical infrastructures and strives to reestablish normalcy as quickly as possible after the occurrence of a disruptive event. As noted in section 1.1, Bruneau's disaster resilience framework contains four elements (4R), whereas Swiss resilience policy contains five: First, the robustness of the individual system – of society as a whole, an individual sector or a particular infrastructure component; second, the availability of redundancies; third, the capacity to mobilize supporting measures; fourth, the rapidity of these supporting measures; and as fifth and new element, the Swiss model includes the overall capacity of society to cope with a crisis situation. As for the challenges involved in implementing Swiss resilience policy, these are mainly contingent on the capacity to mobilize supporting measures and the rapidity of this mobilization.

With the integration of its resilience concept and policy into the broader approach to civil protection and risk management, Switzerland is in line with those countries that regard resilience as the only suitable alternative to the unrealistic goal of providing an entirely secure environment for their inhabitants. While efforts to prevent disruptive events are indispensable and deserve full attention and substantial allocation of resources, societal and systemic resilience is equally important in order to generate the levels of trust and comfort that a society needs if it is to prosper. The durable civil protection facilities and networks that Switzerland constructed in the Cold War and still maintains can be seen as an earlier version of what is now known as resilience. However, civil defense encompasses more than providing shelter for each and every citizen in the case of war. The major challenge for Swiss resilience policy is to cope with the constant dynamics and flexibility inherent to the concept. In the field of resilience, best practices can never be established or achieved. They are constantly changing, and must be revised through continuous learning processes. Coping with such demands represents a major challenge not only to Swiss agencies, but also to executive and administrative agencies in general.

Within the public sector, resilience in Switzerland is currently embraced at both the federal level, which includes stakeholders from various government agencies, and at the cantonal, regional, and local levels. While coordination of resilience measures at these levels is important for the efficiency of Swiss protection and recovery policies, a coherent and effective communication strategy between the various levels and for addressing the affected population is equally important. Moreover, individuals should also be invited into the emergency preparedness process. As demonstrated in the United Kingdom and the United States, for example, individuals can be a part of prevention activities and information sharing. Furthermore, Switzerland can use many of the communication tools and approaches described to begin to facilitate the process of societal resilience

[54] Cf. Grundstrategie des Bundesrates zum Schutz Kritischer Infrastrukturen. Basis für die nationale Strategie zum Schutz Kritischer Infrastrukturen. Available at: http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski.html

building. In terms of disaster response, the federal level can encourage local and cantonal disaster response exercises where various municipal, cantonal, and regional agencies – as well as businesses and individuals – are invited to participate. For example, Los Angeles holds the annual Operation Golden Phoenix series of disaster training exercises, where anthropogenic or natural disasters are simulated and "local, state, federal, tribal, academic, nongovernmental and private sector entities" practice responding to the emergency.[55] Among the benefits of this activity are the development of personal relationships at the local and regional levels, capacity building, and enhanced trust between the various stakeholders. In terms of the components of a resilient society as described in figure 2, these are essential elements. In addition to encouraging and, to a certain degree, facilitating such exercises, the federal government can fill the 'emergency gap', when necessary, by providing "transportation, communication bandwidth and portable electrical power".[56]

Leveraging technology, as noted in section 2.3, is another area where local, regional, and federal governmental agencies can enhance societal resilience. Mobile phones, digital cameras, and the plethora of online platforms have only made societal engagement more accessible and affordable. As shown above, channeling such capacities will be a significant element in societal resilience policy in the years to come. Websites such as those developed in the United Kingdom and elsewhere, which provide emergency preparedness and response tools and resources for civilians in addition to engagement in the classroom, as demonstrated through the UN-ISDRR, are useful as initial steps in inviting society to participate. Other tools, such as Twitter and SMS messages, can further solidify the link between society and responders. In developing a resilience strategy that incorporates the individual role, Switzerland can reference such examples and further expand upon the role of technology in city, canton, regional, and federal emergency planning.

[55] Ganyard, S.T. 2009. All disasters are local. New York Times. 18 May. Available at: http://www.nytimes.com/2009/05/18/opinion/18ganyard.html.

[56] Ibid

5. ANNEX: INTERNET RESOURCES ON RESILIENCE

Resilience Alliance

http://www.resalliance.org

The Resilience Alliance is a research organization comprising scientists and practitioners from many disciplines who collaborate to explore the dynamics of social-ecological systems. The body of knowledge developed by the Resilience Alliance encompasses key concepts of resilience, adaptability, and transformability and provides a foundation for sustainable development policy and practice.

Global Dashboard

http://www.globaldashboard.org

Global Dashboard explores global risks and international affairs, bringing together authors who work on foreign policy in think-tanks, government, academia, and the media.

Los Angeles Fire Department (LAFD)

http://lafd.org/

The LAFD provides a variety of tools to engage the residents of Los Angeles and enhance preparedness so that the community is able to respond and rebound quickly from a disaster. This website is an example of how local emergency responders can provide resources to individuals through various media channels.

Ready.gov

http://www.ready.gov/

Ready.gov is the home for the US Department of Homeland Security *Ready* campaign, which aims to build societal resilience by providing educational resources for individuals, businesses, and communities. Similar to the United Kingdom Resilience website, Ready.gov is geared towards enhancing prevention activities and creating awareness about emergencies.

Social Inclusion

http://www.socialinclusion.gov.au

Social Inclusion is an initiative of the Australian government that has introduced a section on Community Resilience. The initiative aims to promote partnerships between the public and private sector with the goal of addressing economic and social disadvantages and building inclusive and resilient communities. There is also a brochure on this approach:

http://www.socialinclusion.gov.au/LatestNews/Documents/Buildingcommunityresiliencebrochure.pdf

Stockholm Resilience Centre

http://www.stockholmresilience.su.se/2.aeea46911a3127427980003200.html

The Stockholm Resilience Centre seeks to advance transdisciplinary research on the governance of social-ecological systems, with a special emphasis on resilience – the ability to deal with change and continue to develop.

United Kingdom Resilience

http://www.cabinetoffice.gov.uk/ukresilience.aspx

This website provides information on various threats with the aim of improving emergency preparedness and societal resilience. There are resources for civil protection practitioners, individuals, and emergency responders.

United Nations International Strategy for Disaster Risk Reduction

http://www.unisdr.org/

This site is an example of how the United Nations is incorporating the concept of resilience. Recognizing the human, social, economic, and environmental losses that can occur from natural hazards and related technological and environmental disasters, this strategy aims to build disaster-resilient communities. The site offers a variety of resources and guidance for member states seeking to promote awareness and disaster reduction.

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** specializes in research, teaching, and information services in the fields of international relations and security policy. The CSS also acts as a consultant to various political bodies and the general public. The Center is engaged in research projects with a number of Swiss and international partners, focusing on new risks, European and transatlantic security, strategy and doctrine, state failure and state building, and Swiss foreign and security policy.

The **Crisis and Risk Network (CRN)** is an Internet and workshop initiative for international dialog on national-level security risks and vulnerabilities, critical infrastructure protection (CIP) and emergency preparedness.
As a complementary service to the International Relations and Security Network (ISN), the CRN is coordinated and developed by the Center for Security Studies at the Swiss Federal Institute of Technology (ETH) Zurich, Switzerland. (www.crn.ethz.ch)