

# Trends in Resilience: Spotlight on Teaching & Learning Resilience.

## SKI Factsheet No. 9

**Report****Author(s):**

Giroux, Jennifer

**Publication date:**

2012-12

**Permanent link:**

<https://doi.org/10.3929/ethz-a-009978867>

**Rights / license:**

In Copyright - Non-Commercial Use Permitted

**Originally published in:**

CSS Risk and Resilience Reports

# BRG REPORT

---

## Trends in Resilience: Spotlight on Teaching & Learning Resilience SKI Factsheet No. 9

Zurich, December 2012

Risk and Resilience Research Group  
Center for Security Studies (CSS), ETH Zürich

Commissioned by the Federal Office for Civil Protection (FOCP)

Author: Jennifer Giroux

© 2012 Center for Security Studies (CSS), ETH Zurich.

Contact:

Center for Security Studies (CSS)

ETH Zurich

Haldeneggsteig 4, IFW

CH-8092 Zurich

Switzerland

Tel.: +41-44-632 40 25

[www.css.ethz.ch](http://www.css.ethz.ch)

Contracting entity: Federal Office for Civil Protection (FOCP)

Project lead FOCP: Stefan Brem, Head Risk Analysis and Research Coordination

Contractor: Center for Security Studies (CSS), ETH Zurich

Project supervision CSS: Tim Prior, Head Risk and Resilience Team; Oliver Thränert, Head Think Tank,

Andreas Wenger, 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.

# CONTENTS

INTRODUCTION .....	4
1 TEACHING RESILIENCE: WHY?.....	6
1.1 General role of training for key CIP concepts.....	6
1.2 Conceptual clarity: key definitions.....	7
1.3 Conceptual Clarity: Context & Theory.....	7
1.4 Application.....	8
2 TEACHING RESILIENCE: WHO & WHERE? .....	10
2.1 Educational System: University Training .....	10
2.2 Resilience training by Governments .....	12
2.3 Private Sector resilience training .....	13
2.4 Resilience training conducted by International Agencies .....	13
3 CONCLUSIONS AND IMPLICATIONS FOR SWITZERLAND.....	14
3.1 Implications for Switzerland.....	14
4 BIBLIOGRAPHY .....	17

## INTRODUCTION

The concept of resilience in homeland security (HS) and critical infrastructure protection (CIP) continues to gain traction and relevance in a 21<sup>st</sup> century risk environment characterized by volatility, uncertainty, instability, vast acceleration and interactivity. Indeed, in today's world threats are unpredictable and cross-cutting between various policy domains, interests, and sectors. While there have been, and continue to be numerous efforts to conceptualize, define, and measure resilience<sup>1</sup> (for homeland security purposes), there is also an emerging trend in the growth of training and certificate programs that specifically focus on critical infrastructure resilience, as well as building societal resilience in general. Of course, this trend fits the current resilience trajectory. Resilience (the ability of a system to resist, absorb, recover from or adapt to disruptions or changes in condition) is not only gaining in popularity<sup>2</sup> within the HS/CIP

domain, but rather than simply being considered a buzzword (often associated with words like adaptability, agility, and flexibility) its use in this domain is also contributing to the development of the term's conceptual depth and maturity. Evidence of this is found in numerous areas from strategy documents to academic debates and more recently educational development.

The establishment of courses, training, and degree programs that aim to give CIP scholars and practitioners the conceptual and practical background to deepen their understanding of resilience merits further examination. Several questions motivate this report: Are such training programs necessary? Which actors and organizations are offering training, via what medium and for what purpose? This Factsheet was also inspired by the 2012 Critical Infrastructure Symposium in Arlington, Virginia (USA) where discussions on teaching and learning resilience (within CIP) played a prominent role.

This two-day meeting is an annual gathering (since 2010), hosted by the Infrastructure Security Partnership (TISP), that aims to provide a meeting platform for experts and institutions promoting critical infrastructure protection and resilience (CIP/R) programs

<sup>1</sup> To document this trend see studies such as: Scalingi, Paula. «Moving Beyond Critical Infrastructure Protection to Disaster Resilience.» In *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*, by John A. McCarthy, 49–72. Washington: George Mason University, 2007; Bolton, M.J. and Stolcis, G.B. (2008), *Overcoming Failure of Imagination in Crisis Management: The complex Adaptive System*, in *The Innovation Journal: The Public Sector Innovation Journal*, 13 (3); Brunner, Elgin and Jennifer Giroux (2009). Factsheet: Examining resilience – A concept to improve societal security and technical safety. Zurich: Center for Security Studies (CSS), ETH Zurich; Evans, A. and D. Steven (2009), *The Resilience Doctrine*, in *World Politics Review*; Cascio, J. (2009), *Uncertainty and Resilience*, in *People and Place* 1(2); Walker, Jeremy and Melinda Cooper (2011), *Genealogies of Resilience From Systems Ecology to the Political Economy of Crisis Adaptation*, in *Security Dialogue* 14(2); Bara, C. and Brönnimann, G. (2011), *Resilience: Trends in Policy and Research*, *Focal Report 6 – Risk Analysis*, Center for Security Studies, ETH Zurich; and Haggmann, J. and Prior, T. (2012), *Measuring Resilience: Advantages and disadvantages of possible resilience indicators*, *Focal Report 9 – Critical Infrastructure Protection*, Center for Security Studies, ETH Zurich *forthcoming*

<sup>2</sup> This popularity refers to the use of resilience in various CIP security strategies, discussions, etc. as the key concept in an age of volatility and uncertainty. In terms of strategies and policy documents, see for example; Buckle, P., G. Marsh, et al. (2001). *Assessing Resilience & Vulnerability: Principles, Strategies & Actions*. Guidelines prepared for Emergency

Management Australia. 2001; Bundesministerium des Innern. *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)*, 2009; Federal Council (2009). *The Federal Council's Basic Strategy for Critical Infrastructure Protection – Basis for the national critical infrastructure protection strategy*. Berne: 18 May 2009; *Critical Infrastructure Resilience: Final Report and Recommendations*. National Infrastructure Advisory Council (NIAC), 2009; *National Infrastructure Protection Plan (NIPP): Partnering to enhance protection and resiliency*, DHS, 2009; *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*, Cabinet Office, 2010; *Chemical, Biological, Radiological, Nuclear and Explosives Resilience Strategy for Canada*, 2011.

and professional services. The Symposium’s main goals were to:

- ◆ Promote the exchange of ideas and experiences among students, educators, practitioners and government officials developing CIP/R programs and professional services.
- ◆ Offer resilience training and professional development to educators and practitioners.
- ◆ Strengthen CIP/R professional, research and educational networks and establishing a broader CIP/R community of practice.

More specifically, however, the 2012 meeting also offered the “Infrastructure Higher-Education Workshop”, which provided an overview of resilience teaching within CIP/HS educational programs. It also provided a platform to gather input and feedback on the practicality and effectiveness of resilience training. While this workshop focused on university education, it prompted questions on the activities of government and businesses in regards to adapting training to fit newly-adopted resilience frameworks and approaches. Naturally, given the prominence that teaching resilience played at the workshop, and coupled with the emergence of training modules in this field, this factsheet places a spotlight on the trend in resilience training and reflects on some of the early developments.

The discussion begins by identifying four main factors that explain the utility and relevance of resilience training. This is followed by a more practical discussion that draws out the actors and organizations that have developed resilience training modules in order to examine the various approaches. We conclude by providing some ideas that may support the development and institutionalization of training programs in Switzerland. Overall, we found the

development of resilience training and education to be a favorable development. This is most notable in the way that teaching can bridge the theoretical and conceptual discussions between the academic and practitioner spaces by working to remove the layer of abstraction that continues to cloud the concept of resilience within the HS/CIP domain.

# 1 TEACHING RESILIENCE: WHY?

In the last decade, states and organizations have increasingly injected, incorporated, and adopted the term resilience into their security dialogue. This injection has, on the one hand, occurred at an abstract level, such as using the term in a presentation at a meeting or statement within the media.<sup>3</sup> On the other hand, it has been applied more concretely within policy and strategy documents.<sup>4</sup> Whether abstract or concrete, its use has grown in reference to critical infrastructures, individuals and communities, and in relation to urban spaces. Needless to say, resilience, either framed as a process (*i.e.* building resilience) and as an outcome (*i.e.* being resilient), now plays a prominent role in today's risk management world.

As people grasp for the concepts and tools to deal with a complex world, resilience training and education becomes increasingly important for the following four reasons. Firstly, it is important to understand and inform what the key concepts within CIP are (such as public-private partnership (PPP) and more recently resilience). Secondly, training for the conceptual clarity and definition of resilience, and differentiating it from other terms, like risk management is fundamental. Thirdly, developing conceptual clarity and understanding in relation to the context and theoretical underpinnings of resilience is important. Finally, it is important to train people in the appropriate application of resilience. In the following we describe these reasons in more detail.

3 For example: "UN calls on Pakistan to strengthen disaster resilience", UN News Centre, 20 November 2012. Available at: <http://southasia.oneworld.net/news/un-calls-on-pakistan-to-strengthen-disaster-resilience#UO6cEKywXzE>

4 See footnote 2 for examples of strategy and policy documents. Also see: Bara, C. and Brönnimann, G. (2011), Resilience: Trends in Policy and Research, *Focal Report 6 – Risk Analysis*, Center for Security Studies, ETH Zurich.

## 1.1 General role of training for key CIP concepts

First, on a broad yet fundamental level, training is important as it involves the process of enhancing the skills, capabilities, subject-matter clarity and knowledge within a particular area. For instance, within the CIP domain, where public-private partnerships (PPPs) are crucial, numerous training programs, seminars, and specializations have emerged within the last decade that examine the various facets of PPPs. Theoretically, trainees are introduced to concepts such as network governance, for example. Practically, they are taught about policy and application, such as identifying CI projects, engaging stakeholders, and/or how to work with public and private partners during a crisis.<sup>5</sup> Consequently, PPP within CIP education has become a field rich in material and resources, while also providing researchers and practitioners with the knowledge and tools to better operate in (or study) this domain.

Similarly, given the growing importance of resilience within HS/CIP dialogue, such training is also needed. More explicitly, as resilience continues to play a role in (security) policy and strategy, principally in the areas of risk and crisis management, then trainees and practitioners of HS/CIP need to be imbued with the relevant knowledge in order to develop the necessary skills and capabilities to *implement* a resilience framework.

5 For example: the Institute for Public-Private Partnerships (IP3) offers training programs ([www.ip3.org](http://www.ip3.org)); the World Bank hosts an annual PPP event (<http://wbi.worldbank.org/wbi/about/topics/public-private-partnerships>) as well as courses on collaborative governance; the United States FEMA Emergency Management Institute offers an introduction to PPP (<http://training.fema.gov/EMIWeb/IS/is660.asp>).

## 1.2 Conceptual clarity: key definitions

Second, training and educational programs can offer conceptual clarity, particularly as it relates to the relationship that resilience has within processes of risk management. CIP practitioners and risk/crisis managers (both in the public and private sector) must be aware of the distinctions, relationship and relevance of resilience and risk management. On the one hand, risk management strategies identify, prioritize, and mitigate risks, whereas resilience can be viewed as an approach to risk management.<sup>6</sup> Yet, as van Opstal argues, resilience can also be something that “requires a different set of capabilities and competencies than conventional risk management”.<sup>7</sup> In addition to such conceptual distinctions, this discussion would also include providing practitioners (and trainees) an overview of policy, strategy, and practical application of critical infrastructure protection and resilience from an all-hazards perspective. Again, this conceptual clarity of resilience is important for educating current and future HS/CIP professionals as it gives the subject-matter clarity, which will in turn improve implementation efforts. In other words, only by fully understanding the concept will they be able to see how to incorporate it into existing risk and crisis management frameworks.

## 1.3 Conceptual Clarity: Context & Theory

Third, conceptual relevance and theoretical foundations must be an important starting point in any training program. The potpourri of potential hazards that the modern risk manager must consider includes so-

cial (such as non-state violence, cyber-attacks, pandemic influenza), natural (such as hurricanes, tsunamis, earthquakes, floods) and technical hazards (such as industrial accidents and power outages).<sup>8</sup> Such events often carry an element of surprise – whether it is the general characteristics, scale, and/or impact – and have a tendency to uncover new, unforeseen vulnerabilities. One simply has to draw from a few recent cases to capture this aspect. In 2012, Hurricane Sandy made history as a large storm that caused massive flooding, destruction, and power outages across parts of New York and New Jersey. Not only was the scale of the storm unique, but also the way that it combined with typical winter weather systems. The blizzards that affected parts of North America, once Hurricane Sandy made landfall, were unanticipated. The 2011 combined earthquake-tsunami caused a nuclear disaster in the Fukushima region that has had various repercussions for global nuclear energy supply chains and the nuclear energy industry generally. For example, Switzerland and Germany have decided to phase-out nuclear energy. This ‘hazard complexity’ is matched with the complexity of contemporary society; characterized by socio-technical systems, or as Lawson aptly defines “large, complex systems in which the lines between the social and the technological, the human and the machine are increasingly blurry.”<sup>9</sup>

Together, hazard and social complexity are challenging the ability of states to guarantee security by providing protection from (or only mitigating) threats that manifest somewhat randomly in space and time. This inability results in myriad and unforeseen consequences in today’s highly complex societies. Not only does this have interesting implications for the political relationship between the governing and the gov-

6 See: US Homeland Security Studies and Analysis Institute (2010), *Risk and Resilience: Exploring the Relationship*; Suter, Manuel. (2011), *Focus Report 7. Resilience and Risk Management: Exploring the Relationship between the two Concepts and Comparing their Use in Policy Documents on Critical Infrastructure Protection*, Center for Security Studies, ETH Zurich.

7 Opstal, D. v. (2012, December). *The Resilience Imperative*. George Mason University CIP Report, p2.

8 Also worth considering the different ways that hazards can be structured. For example, see Switzerland’s national disaster risk assessment methodology: [www.risk-ch.ch](http://www.risk-ch.ch)

9 Lawson, S. “A Domain Like Cyberspace”, *Forbes*, 4 August 2011. Available at: <http://www.forbes.com/sites/seanlawson/2011/08/04/a-domain-like-cyberspace/>



erned, it also points to a shift away from a strict security mindset to one of dynamism. Where threat in the former is ‘knowable’, calculable, and predictable, resilience predominates in the latter, where risks are ever-evolving and challenge the predictive capacities of security providers, and crisis management strategies when risks actually manifest into events.

With the above in mind, HS/CIP professionals can benefit from educational programs that not only introduce them to the concept of resilience, but also explain why it is an important idea, tool, and framework to deal with the fundamental governance changes brought on by the complexity of hazards and systems. Put another way, they need to understand why this concept has become so prominent and what it means for how societies deal with uncertainty and volatility. Indeed, this ties into the limits of protective capacity in today’s world. The reason why resilience has become an attractive or intriguing concept for scholars and practitioners alike is that does not refer to the absence of threats, surprises, or shocks, but rather accepts and expects them. Hence, protection, while still important, loses currency. By contrast, enhancing the ability of a system (including society) to quickly and efficiently reorganize and rebound from a potentially catastrophic event gains in value.

### 1.4 Application

The fourth and final point pertains to conceptual application. If resilience provides the complementary framework for risk management that helps to deal with the surprises, disruptions, and cascades that are bound to occur, then what should practitioners have in their toolkit? Discussions on resilience stress the ability of system flexibility (expressed in the capacity to quickly adapt to change) and adaptability, both of which allow a system to respond, reorganize and renew despite being challenged by extreme shocks and adverse events. Yet what are the entry points that might allow a practitioner to enhance flexibility, and how are they different between sectors or domains? In this respect, the educator can highlight that one approach does not fit all (*i.e.* entry points for improving flexibility will be different within CI sectors as well as between social systems more generally).

In addition, the practical application of resilience can also be improved by breaking apart the concept’s component parts (Figure 1) to provide additional practical guidance and application insight. By doing so, it is evident that approaches to resilience can be influenced by different governance levels (strategic, operational, and tactical), by different hazards (delib-

Levels	Spectrum	Levels of Impact
<ul style="list-style-type: none"> <li>◆ Strategic</li> <li>◆ Operational</li> <li>◆ Tactical</li> </ul>	<ul style="list-style-type: none"> <li>◆ Deliberate attacks</li> <li>◆ Accidents</li> <li>◆ Natural Disasters</li> <li>◆ Misc. Failures (such as deterioration)</li> </ul>	<ul style="list-style-type: none"> <li>◆ Sector Specific</li> <li>◆ Individual</li> <li>◆ Community</li> <li>◆ National</li> <li>◆ International</li> </ul>

Figure 1: Unpacking resilience would mean identifying how resilience is applied and how it influences the various governance levels (strategic, operational, and tactical) as well as assessing levels of impact. Adopted and modified based on Full Spectrum Resilience discussion.<sup>10</sup>

10 Boone, W. E., & Hart, S. D. (2012). Full Spectrum Resilience. CI Symposium (pp. 1–10). Arlington : The Infrastructure Security Partnership.

erate attacks, technical accidents, natural disasters or any other type of failure that results in a large crisis or disaster), or in relation to the CI sector in which the approach is deployed (individual, community national, regional/international). While there might be some commonalities in response regardless of crisis, some hazards may draw out certain types of vulnerabilities and issues. For example, a terrorist or mass shooting incident may have a strong psychological (fear) component that particularly impacts the individuals and community targeted in the violence, therefore influencing the operational governance level.

In addition, the risk management and crisis management wheels could also be utilized to identify where resilience is or can be applied. For example, Brunner and Giroux described what resilience might look like within a crisis management framework.<sup>11</sup> During each phase – mitigation, preparedness, response and recovery – trainees participating in resilience course/training could examine the role and engagement strategies for individuals and industries. This is one of the unique attributes of resilient systems – they rely on self-organized governance from within the system rather than by hierarchy and strict chains of commands. This makes non-official actors (such as individuals and business owners) a very important part of the risk and crisis management process. To illustrate, in order to mitigate the effects of future storms, state officials in New York and New Jersey are now liaising with engineers and construction companies to recommend and/or explore new approaches to building infrastructure that can endure future and more powerful storms.

---

<sup>11</sup> Brunner and Giroux, 2009, p. 9.

## 2 TEACHING RESILIENCE: WHO & WHERE?

In the last decade, educational programs for homeland security (HS) and CIP have grown rapidly. In Europe, there are civil protection educational courses as well as disaster management courses embedded in degree programs. For example, the University of Bonn in Germany offers a Master's Degree in "*Katastrophenvorsorge und Katastrophenmanagement*" or, in English, catastrophe provision and management (KAVOMA).<sup>12</sup> Within the United States, the academic field of HS did not truly emerge until 2006. Even so, higher learning institutions now offer over 100 degree programs and certificate programs in HS alone, with roughly 70 courses offered for CIP instruction.<sup>13</sup> Similarly, Canada has a number of graduate and undergraduate programs in which HS/CIP courses are provided (embedded in degree programs focused on areas such as IT security and emergency management). Carleton University, for example, offers an interesting interdisciplinary Master's program on infrastructure protection and international security,

however, like other programs,<sup>14</sup> is yet to offer a course on resilience within HS/CIP.<sup>15</sup>

In addition, there are numerous private and public sector training programs (though an exhaustive scan of these resources was not conducted for this report). In the following subsections we provide a brief summary of the notable resilience training and education programs (see summary in Table 1), including a list of courses. In this factsheet, we focus only on those programs that address resilience within the framework of HS/CIP and thus do not include the numerous resilience courses and programs that address the psychological dimensions of resilience<sup>16</sup>.

### 2.1 Educational System: University Training

A cursory overview of resilience training within universities highlights some specific short courses

**Table 1: Summary of organizations providing some form of resilience training in HS/CIP**

Country/Body	Type	What
George Mason University (GMU)	University	Certificate program and courses
United Nations University Institute for Sustainability and Peace	University	Postgraduate course
Swedish Civil Contingencies Agency (MSB)	Public	Professional exchange programs/field visits
The Infrastructure Security Partnership (TISP)	Private	Webinars & seminars
UN office for disaster risk reduction (UNISDR)	International	Educational webinars

<sup>12</sup> See: <http://www.kavoma.de>

<sup>13</sup> Data retrieved during the "Infrastructure Higher-Education Workshop" at the 2012 CI Symposium in Arlington, VA. For CIP specifically there are 2 degree programs, 1 training program, and 1 concentration.

<sup>14</sup> For example the Center for Homeland Defense and Security at the Naval Post Graduate School offers a Master's in Homeland Security, though like Carleton do not focus.

<sup>15</sup> See: <http://www.carleton.ca/ipis>

<sup>16</sup> Such courses are particularly delivered in private sector management and leadership courses.

and one larger effort. In terms of shorter courses, in 2011 the United Nations University Institute for Sustainability and Peace (UNU-ISP), Tokyo, provided a five-week postgraduate program on Building Resilience to Climate Change.<sup>17</sup> While not focused on CIP, it did address themes like community/societal adaptation, risk and uncertainty.<sup>18</sup>

One of the more notable programs is conducted by the George Mason University (GMU) Center for Infrastructure Protection and Homeland Security (CIP/HS), Virginia. In 2010, they partnered with the Department of Homeland Security (DHS), Office of Infrastructure Protection, to develop a new higher education curricula focused on infrastructure protection, with resilience serving as a core theme. The goal of the course was to create a prototype for graduate courses and certificate programs.<sup>19</sup> According to Hardy “a key objectives of the CIP/HS Education and Training Program is to equip professionals with the education and skills to understand the Nation’s critical infrastructure protection and resilience missions.”<sup>20</sup> In doing so, they conclude each course with evaluations that assess whether students can apply the knowledge and skills acquired in the classroom to their work in protecting critical infrastructures.

The certificate program, which is comprised of the following five courses, shows the prominence that resilience plays:

- ◆ foundations of CIP and resilience<sup>21</sup>

17 See: <http://isp.unu.edu/grad/credited/cecar/index.html>

18 It is unclear, whether this course will be offered in the future, or expanded to capture other themes. For a full list of the courses offered in this program see: <http://isp.unu.edu/grad/credited/cecar/courses.html>

19 Hardy, D. (2010, August). Joint George Mason University and Department of Homeland Security Initiative on Critical Infrastructure Higher Education Programs. *George Mason University CIP Report*, pp. 12–18.

20 Ibid.

21 To see the syllabus for this course see: [http://cip.gmu.edu/archive/CIPHS\\_Graduate\\_Course\\_1\\_Introduction\\_to\\_Critical\\_Infrastructure\\_Protection\\_and\\_Resilience.pdf](http://cip.gmu.edu/archive/CIPHS_Graduate_Course_1_Introduction_to_Critical_Infrastructure_Protection_and_Resilience.pdf)

- ◆ partnership and info sharing for CIP and resilience<sup>22</sup>
- ◆ assessing and managing risk to CI systems<sup>23</sup>
- ◆ CIP, Resilience, and cybersecurity<sup>24</sup>
- ◆ advanced topics in CIP and resilience

The first course, ‘Foundations of CIP and Resilience’, serves as an introduction to CIP and the emergence of the risk environment. In addition to the conceptual background, this course also distinguishes between the network of actors and factors, like public and private sector roles and responsibilities, as well as voluntary approaches vs. regulatory approaches. The second course, ‘Partnership and Info Sharing for CIP and Resilience’, not only provides conceptual background on the role of partnerships (and PPPs in particular) in CIP but also incorporates information sharing exercises. The third and fourth courses are more research and analysis oriented, while the fifth course in ‘Advanced topics in CIP and resilience’ is a project-specific class where groups of 2–4 trainees build a CIP program at sector or sub-sector level. They also participate in cyber-attack and natural disaster exercises to see how the CI is impacted during a crisis scenario.

More uniquely, bridging policy and education, the syllabus has been developed to address the core competences identified in the US National Infrastructure Protection Plan. These core competences include:

- ◆ risk analysis (GMU provides: course 1-general; course 3-in depth examination; course 4-cyber focus)

[cal\\_Infrastructure\\_Protection\\_and\\_Resilience.pdf](#)

22 To see the syllabus for this course see: [http://cip.gmu.edu/archive/CIPHS\\_Graduate\\_Course\\_2\\_Critical\\_Infrastructure\\_Protection\\_and\\_Information\\_Sharing.pdf](http://cip.gmu.edu/archive/CIPHS_Graduate_Course_2_Critical_Infrastructure_Protection_and_Information_Sharing.pdf)

23 The syllabus for this course was not found online.

24 To see the syllabus for this course see: [http://cip.gmu.edu/archive/CertificateCourse4\\_CriticalInfrastructureProtectionResilienceandCybersecurity.pdf](http://cip.gmu.edu/archive/CertificateCourse4_CriticalInfrastructureProtectionResilienceandCybersecurity.pdf)

- ♦ protective measures/mitigation strategies development (GMU provides: course 1- alternative analysis; course 1 & 5- papers and analysis)
- ♦ technical and tactical expertise (sector-specific) (GMU provides: course 1-general; courses 1–5 mini case studies)
- ♦ partnership building/networking (GMU provides: course 1 (general) courses 1, 4, 5 threat response and incident management exercise)
- ♦ metrics and program evaluation (GMU provides: course 1, 3, 5 papers and projects)
- ♦ information collection and reporting (GMU provides: course 2 info sharing exercise)
- ♦ program management (GMU provides: all courses – but specialized in course 5)

A final point worth mentioning about this program is the role of case studies in training, which are utilized through the courses to reinforce key concepts and lexicon (linking theory and practice). Within the program they have developed one case study in particular is the I-35W Mississippi River bridge collapse in 2007.<sup>25</sup> Cases like this one work well for discussions on CIP and resilience as they involve a nexus of multiple infrastructure nodes that interact with society (such as a bridge serving as a key transit route). It can engage robust critical thinking about how to deal with complex socio-technical systems (such as interdependencies, interrelationships, etc.) and consequences caused by disruptions, and captures the challenge of planning and response in a high-vulnerability and multi-threat environment.

## 2.2 Resilience training by Governments

There are a few government efforts worth highlighting. As part of the Making Cities Resilient campaign, for example, Sweden and the United Kingdom have

<sup>25</sup> For the full case study see: [http://cip.gmu.edu/archive/Case-Study\\_LearnerVersion.pdf](http://cip.gmu.edu/archive/Case-Study_LearnerVersion.pdf)

engaged in city-to-city learning exchange.<sup>26</sup> In 2011, representatives from two Swedish municipalities where hosted by the UK Environment Agency, and two local municipalities in the United Kingdom, where they learned about flood mitigation in England and about problems and solutions in other cities that face flooding risks. Such exchanges provide hands-on learning opportunities in the field and establish platforms that support shared ideas, lessons learned and best practices concerning risk and resilience. These mechanisms should continue to be utilized and adopted in other city-to-city or country-to-country exchanges. In fact, while time in the classroom is useful for learning concepts, definitions, etc., field visits are also important for showing the practical application of resilience.

In the United States, resilience is certainly found in numerous policy documents. However, training within the framework of the Department of Homeland Security (DHS) Infrastructure Protection and Resilience<sup>27</sup> appears to be more focused on HS/CIP in general, rather than offering modules that explicitly focus on the relationship between resilience and risk management, for example. In addition, although the US Army's 'Master Resiliency Training Course,' a joint 2-week course with the University of Pennsylvania is focused on psychological resilience, it is nonetheless worth mentioning due to the program's comprehensiveness.<sup>28</sup> It may also signal the trajectory of training in the United States as it relates to future efforts to teach resilience to individuals and communities, particularly those in disaster-prone areas.

<sup>26</sup> See: <http://www.preventionweb.net/english/professional/trainings-events/events/v.php?id=24437>

<sup>27</sup> See: <http://www.dhs.gov/infrastructure-protection-and-resilience>

<sup>28</sup> See: <https://www.resilience.army.mil/MRTfacilitators.html>

### 2.3 Private Sector resilience training

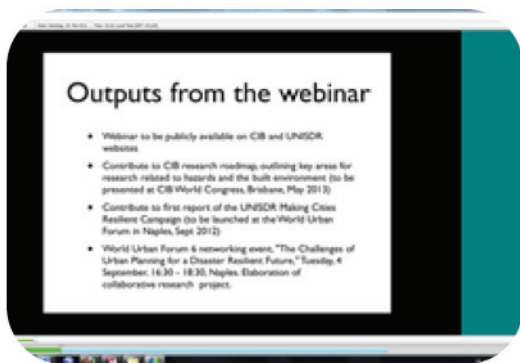
Within the private sector we found a number of resources offering training for business continuity and, increasingly, business resilience – both of which focus on psychological and leadership components. For instance, Management Advisory Services in the United Kingdom offers resilience training for managers and individuals, though it is focused on personal control and staff management.<sup>29</sup> In terms of psychological training in this domain, training offers professionals tools to deal with and bounce back from malaise in times of failure or significant disruption as well as how to maintain a strong posture to lead staff through adverse events.

More relevant to the field of HS/CIP, the Infrastructure Security Partnership (TISP) offers a series of Webinars focusing on regional, community and infrastructure resilience challenges in the United States that are associated with impeding a reduction of the impacts caused by disasters. A one-day training course addresses the topic of 'Building Resilient Regions and Infrastructure through Risk-Based Mitigation: Regional Continuity of Operations.'<sup>30</sup>

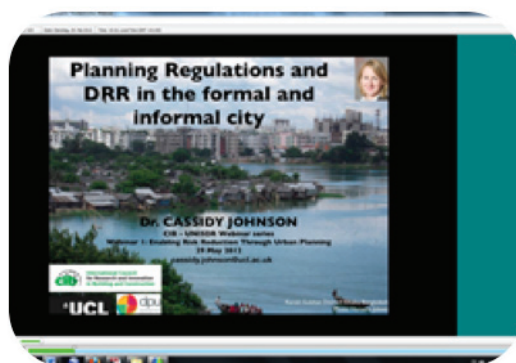
### 2.4 Resilience training conducted by International Agencies

As part of the Making Cities Resilient campaign, the International Council for Research and Innovation in Building and Construction (based in the Netherlands) and the UN office for disaster risk reduction (UNISDR) launched a series of Webinars in 2012 on building disaster-resilient cities. While this does not fit directly within the HS/CIP framework, it is closely related because it focuses on urban spaces, from households to complex socio-technical systems. The webinars utilize panel presentations by experts from various domains, sectors and countries, as well as discussion sessions to engage those attending the Webinar. Overall, "the goal of this training is to inform future research in building, construction and disaster resilience" as well as to "inform the first annual report of the UNISDR Making Cities Resilient Campaign [that was] prepared in 2012."<sup>31</sup> Courses offered in the program include:

- ◆ enabling risk reduction through urban planning
- ◆ engaging multiple stakeholders
- ◆ local government self-assessment tool



Introduction to Risk Reduction webinar



Webinar presenter and affiliations

Figure 2: Screenshot of UNISDR webinar tool

29 To see what this program offers see: <http://www.mas.org.uk/development-programmes/resilience-training.html>

30 See: <http://www.tisp.org/index.cfm?cdid=12809&pid=10231>

31 See: <http://www.unisdr.org/campaign/resilientcities/webinar>

### 3 CONCLUSIONS AND IMPLICATIONS FOR SWITZERLAND

The rise of the concept of resilience in HS/CIP and its emergence in training and education programs further embeds the shift in security thinking towards this newer direction. In short, resilience accepts the uncertainty brought on by complexity and thus acknowledges that certain disruptions are inevitable. Therefore, equipping scholars and practitioners with the concepts, understanding and tools to quickly and efficiently reorganize and rebound from disruptive events is becoming essential in the modern age. While this factsheet attempted to remain focused on resilience training in HS/CIP, resilience building expands over a broad range of areas: including psychological training for individuals, business continuity for organizations, community or society coherence and resourcefulness, and addressing critical infrastructure protection at both a national level and international vulnerabilities – all of which offer insights into different ways of training for the resilience approach.

However, the road ahead toward well-trained resilience professionals is not entirely clear cut. Certainly, we know and understand that resilience is an exceedingly popular term. But its application and utility is still being debated within policy and academic circles. What it really means in theory and practice is still arguably open. It is therefore hard to train effectively and systematically. Ultimately, resilience training must catch up to, and keep pace with, the already rapid political deployment of resilience approaches. GMU's attempt to develop syllabus around the topic of HS/CIP and resilience represents one of first attempts to put the pieces together and bring it to the classroom in a systematic manner. Yet this effort is still at its infancy, and thus its effectiveness will remain uncertain until proven. At this stage it is still experimental and will likely change or be adapted as it is evaluated. All other efforts are disparate, less

comprehensive, and also difficult to evaluate without carrying out a more extensive analysis. With that in mind, not only does this factsheet inspire ideas to conduct more in-depth research on these training programs, but it also presents a space for creativity – to develop training modules that can add to this growing educational pool. Naturally over time, more systematic approaches to training will emerge as risk managers gain a stronger grasp of resilience, evaluate training and educational programs, and test new approaches.

#### 3.1 Implications for Switzerland

Within Switzerland the concept of resilience is a key pillar in the CIP strategy. However, as Bara and Brönnimann noted, the 2011 study “the integral disaster management approach (see Fig. 8), promoted by the Swiss Federal Office for Civil Protection (FOCP), is inspired by resilience thinking: While prevention and preparation in this cycle correspond to risk management (by definition *before* an event occurs), intervention corresponds to traditional crisis management. Recondition and reconstruction, then, correspond to continuity management and as such are part of a resilience approach that encourages contingency plans in case a disaster cannot be averted.”



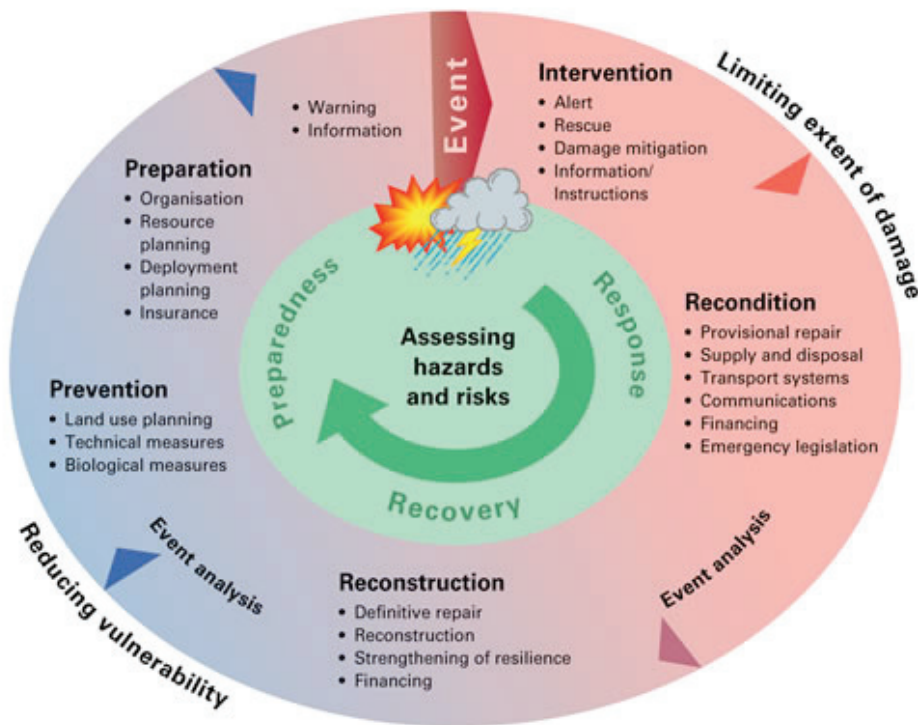


Fig. 8: Disaster management cycle used by the FOCP.<sup>32</sup>

These two areas, CIP and disaster management, provide domains where resilience education and training can be further developed and offered in Switzerland. Another factor to consider is the domestic context and its relationship to resilience in general. Discussions on building resilience oftentimes note the importance of decentralization and ‘network governance’ approaches. From this perspective, Switzerland fits quite well within a resilience framework due to the highly decentralized federal system in which responsibilities for disaster management are distributed vertically (between the local, cantonal, and federal administrative levels) and horizontally (between a multiplicity of actors on the same administrative level). This is a positive characteristic as it contributes to enhanced flexibility as resources and knowledge

can be distributed throughout the system rather than centralized. Of course, this also enhances the need for coordination between agencies and actors.

In terms of bringing the concept of resilience to the classroom, the Federal Office for Civil Protection (FOCP) could play a sponsoring and coordinating role in working with partners to develop training modules that specifically examine the role of resilience. These could be deployed not only in CIP, but also within the context of the integral disaster management approach referenced in Figure 8. Given that there is an interest in the concept of resilience, subject-matter expertise, and experience implementing it into policy (via the CIP strategy), the FOCP in particular could support the organization of training with local and state authorities and the private sector. Such training can be positioned within the joint training activities it already carries out with partner organizations, the

<sup>32</sup> Federal Office for Civil Protection (2003). Disasters and Emergencies in Switzerland: Risk Assessment from a Civil Protection Perspective. Berne: August 2003, p. 29.



army and cantons,<sup>33</sup> or simply inserted into existing training programs – for instance as an add-on to risk management courses. Overall, given FOCP’s relationship with university and academic partners, it has the necessary partnerships and resources to develop training modules and syllabi – similar to the partnership between GMU and DHS – that could tie CIP and resilience research and concepts to domestic policy needs.

Outside of official training, the FOCP could also be part of seminar development with partner organizations that provide additional outlets for resilience education. This could include developing cases studies based on past crises/disasters in Switzerland that highlight key questions, case narrative, recommended reading, and exercises that might include conducting full assessments and identifying vulnerabilities. In addition, they could draw from existing frameworks in order to teach resilience but, again, given the infancy of this field it would require developing pilot seminars to test approaches and evaluate effectiveness.

For instance, a seminar that looks at how organizations might need to change to enhance resilience could draw from the three guiding principles, possibly along the lines of those developed by Snowden<sup>34</sup>:

- ◆ Unravel hierarchy and strengthen networks to enhance governance – the logic being that in order to become more adaptable, organizations need to decentralize and increase the connectivity between relevant actors.

- ◆ Improve info sharing and exchange pathways and connectivity. Snowden refers to this as ‘distributed cognition’, whereby intelligence within a network is distributed so to encourage more ‘minds on the problem’.
- ◆ Strengthen ‘disintermediation’, or in other words, bring actors that operate at the top closer to those on the bottom and *vice versa*.<sup>35</sup>

Of course, those principles can be matched to the Swiss context to show its strong relationship to resilience systems as well as be used as discussion points to examine potential areas of improvement. It is clear that by getting ahead of the curve, the FOCP could be part of the effort to teach resilience within the Swiss HS/CIP domain, whether it is through incorporating it into existing training modules or developing a separate resilience education track.

33 [http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/das\\_babs/gb\\_ausb.html](http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/das_babs/gb_ausb.html)

34 See: Snowden, David. Everything is fragmented—Complex Adaptive Systems at Play. 2008 December. <http://www.kmworld.com/Articles/News/News-Analysis/Everything-is-fragmented%E2%80%94Complex-adaptive-systems-at-play--51363.aspx>; Snowden, David, and Mary Boone. “A Leader’s Framework for Decision Making.” Harvard Business Review, 2007: <http://hbr.org/2007/11/a-leaders-framework-for-decision-making/ar/1>.

35 This ties into the first point concerning hierarchy.

## 4 BIBLIOGRAPHY

- Bara, C. and Brönnimann, G. (2011), Resilience: Trends in Policy and Research, *Focal Report 6 – Risk Analysis*, Center for Security Studies, ETH Zurich.
- Bolton, M.J. and Stolcis, G.B. (2008), Overcoming Failure of Imagination in Crisis Management: The complex Adaptive System, in *The Innovation Journal: The Public Sector Innovation Journal*, 13 (3).
- Boone, W. E., & Hart, S. D. (2012). Full Spectrum Resilience. *CI Symposium* (pp. 1–10). Arlington : The Infrastructure Security Partnership.
- Buckle, P., G. Marsh, et al. (2001). Assessing Resilience & Vulnerability: Principles, Strategies & Actions. Guidelines prepared for Emergency Management Australia. 2001, [http://www.proventi-onconsortium.org/themes/default/pdfs/CRA/EMA\\_2001\\_meth.pdf](http://www.proventi-onconsortium.org/themes/default/pdfs/CRA/EMA_2001_meth.pdf)
- Brunner, Elgin and Jennifer Giroux (2009). Factsheet: Examining resilience – A concept to improve societal security and technical safety. Zurich: Center for Security Studies (CSS), ETH Zurich.
- Cascio, J. (2009), Uncertainty and Resilience, in *People and Place* 1(2).
- Chemical, Biological, Radiological, Nuclear and Explosives Resilience Strategy for Canada, 2011. [http://www.publicsafety.gc.ca/prg/em/\\_fl/cbrne-res-strt-eng.pdf](http://www.publicsafety.gc.ca/prg/em/_fl/cbrne-res-strt-eng.pdf).
- Evans, A and D Steven (2009), The Resilience Doctrine, in *World Politics Review*.
- Germany, Bundesministerium des Innern (2009). Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). <http://www.bmi.bund.de/cae/servlet/contentblob/544770/publicationFile/27031/kritis.pdf>
- George Mason University (GMU), Collapse A Case Study of the Minneapolis I-35W Bridge Disaster with Exercises. [http://cip.gmu.edu/archive/Case-Study\\_LearnerVersion.pdf](http://cip.gmu.edu/archive/Case-Study_LearnerVersion.pdf)
- George Mason University Courses:
- Introduction to Critical Infrastructure Protection and Resilience. [http://cip.gmu.edu/archive/CIPHS\\_Graduate\\_Course\\_1\\_Introduction\\_to\\_Critical\\_Infrastructure\\_Protection\\_and\\_Resilience.pdf](http://cip.gmu.edu/archive/CIPHS_Graduate_Course_1_Introduction_to_Critical_Infrastructure_Protection_and_Resilience.pdf)
  - Partnership and info sharing for CIP and resilience [http://cip.gmu.edu/archive/CIPHS\\_Graduate\\_Course\\_2\\_Critical\\_Infrastructure\\_Protection\\_and\\_Information\\_Sharing.pdf](http://cip.gmu.edu/archive/CIPHS_Graduate_Course_2_Critical_Infrastructure_Protection_and_Information_Sharing.pdf).
  - CIP, Resilience, and cybersecurity <http://cip.gmu.edu/archive/CertificateCourse4CriticalInfrastructureProtectionResilienceandCybersecurity.pdf>
- Germany, Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), 2009. [http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf?\\_\\_blob=publicationFile](http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf?__blob=publicationFile).
- Hardy, D. (2010, August). Joint George Mason University and Department of Homeland Security Initiative on Critical Infrastructure Higher Education Programs. *George Mason University CIP Report*, pp. 12–18.

- Opstal, D. v. (2012, December ). The Resilience Imperative. *George Mason University CIP Report*, pp. 2–10.
- Scalingi, Paula. “Moving Beyond Critical Infrastructure Protection to Disaster Resilience.” In *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*, by John A. McCarthy, 49–72. Washington: George Mason University, 2007.
- Snowden, David. *Everything is fragmented—Complex Adaptive Systems at Play*. 2008 December. <http://www.kmworld.com/Articles/News/News-Analysis/Everything-is-fragmented%E2%80%94Complex-adaptive-systems-at-play--51363.aspx>.
- Snowden, David, and Mary Boone. “A Leader’s Framework for Decision Making.” *Harvard Business Review*, 2007: <http://hbr.org/2007/11/a-leaders-framework-for-decision-making/ar/1>.
- Switzerland, Federal Office for Civil Protection (2003, August). *Disasters and Emergencies in Switzerland: Risk Assessment from a Civil Protection Perspective*. Berne.
- Switzerland, Federal Council (2009). [\*The Federal Council’s Basic Strategy for Critical Infrastructure Protection\*](#) – Basis for the national critical infrastructure protection strategy. Berne: 18 May 2009.
- Switzerland, Federal Council (2012). *National Strategy for the Protection of Critical Infrastructures*. Berne: 27 June 2012.
- United Kingdom, Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards, Cabinet Office, 2010, “<http://www.cabinetoffice.gov.uk/sites/default/files/resources/strategic-framework.pdf>.”
- United States, National Infrastructure Advisory Council (NIAC), 2009. URL: [http://www.dhs.gov/xlibrary/assets/niac/niac\\_critical\\_infrastructure\\_resilience.pdf](http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf).
- United States, National Infrastructure Protection Plan (NIPP): Partnering to enhance protection and resiliency, DHS, 2009. [http://www.dhs.gov/xlibrary/assets/NIPP\\_Plan.pdf](http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf).
- Walker, Jeremy and Melinda Cooper (2011), *Genealogies of Resilience From Systems Ecology to the Political Economy of Crisis Adaptation*, in *Security Dialogue* 14(2)





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.