CSS Analyses in Security Policy

CSS ETH Zurich

Vol. 3 • No. 30 • March 2008

RISK MANAGEMENT IN SECURITY POLICY

Risk management has been developed into an important tool for security policy in recent years. It has several advantages making it suitable for handling current dangers and threats, but it is also prone to some difficulties in practical implementation. Some challenges of effective risk management are identical for public and private actors alike, while others must be considered separately in the context of politics and public administration.

istockphoto.com

The state, the economy, and society are more closely linked today than ever before, and form a complex system of global interdependency. New risks such as pandemics, organized crime, or climate change are propagating rapidly across all national boundaries. Cascading effects further obstruct efficient damage limitation. At the same time, there is a large degree of uncertainty as to which risks are significant and what their concrete effects may be. This implies serious challenges for experts and decisionmakers who must adapt their strategies and methods to emerging challenges.

The concepts of risk and risk management have given a new impetus to the discipline of security policy. Risk may be defined as an uncertain future event with (negative) effects on the aims of individuals and organizations. Such a future event is not simply predestined; rather, risk implies that humans may direct the course of events in the desired direction by means of the choices they make. Furthermore, the meaning of the word "risk" is ambiguous: It can refer to a threat that must be warded off, or to an opportunity that should be exploited. Both of the above elements – the ambivalence of threat and opportunity as well as the self-determined shaping of the future – have contributed to making risk management a popular and widespread instrument, particularly in the economic sphere.

However, politics and administration have also taken up the concept, based on the paradigms set by private business. Experience has shown, though, that efficient risk management especially in the area of security policy is a highly challenging task, due to the specific characteristics of the public sector. Not everything that has been proven and tested in the corporate environment can be directly transferred to politics.

Anchored in business and politics

At its core, risk management refers to the analysis, planning, and direction of future events under conditions of uncertainty. Risks must be identified, assessed appropriately, and prioritized accordingly at an early stage in order to offer political actors an optimal basis for their decision-making. The core strength of risk management is its ability to survey the entire "risk landscape" permanently and comprehensively, to discover trend disruptions at an early stage, and thus to increase the range of entrepreneurial or political options. The concept is also significant because it serves as a caution against the illusion that risks can be fully eliminated: There is never "zero risk", since full control of future events is ultimately impossible to achieve, if for no other reason than due to limited resources.

Corporations have always investigated risks in order to ward off threats and exploit new market opportunities. The entrepreneurial nature of risk management can be seen in a wide range of contexts, from the maritime voyages of the early modern age to current debates over the optimal form of Enterprise Risk Management and the appointment of

Chief Risk Officers. Companies aim to use these instruments to cover the entire expanse of their risk landscape and to move beyond financial, credit, or market risks to incorporate social, political, or ecological risks into their business strategies.

In connection with the consequences of large-scale technical risks, the concept of risk management has entered the collective social consciousness in recent years. In contemporary security policy, the nexus with risk management is evident: On the one hand, the risk spectrum has become much broader; a narrow focus on classic military threat scenarios is no longer commensurate with the strategic picture. On the other hand, security policy is always geared towards a long-term perspective, and therefore its strategies must be explicitly formulated for conditions of uncertainty. Furthermore, in the specific context of security policy, it is important to emphasize that risks are not per se negative phenomena, but constitute important driving forces for innovation and progress. Therefore, maximizing security at (almost) any price and minimizing risk is ultimately more harmful than practical, since such an approach does not sufficiently take into account either the productivity of risk or the dangers of universal security.

The challenge of political legitimacy

Risk management is mainly developed in a process-oriented manner – ranging from the identification and assessment of risks to their mitigation. However, a systematic, "correct" navigation of the individual steps of the process without including "flexible elements" will not necessarily lead to the optimal result. Such a technocratic approach would be unsuitable for companies and even less appropriate for the political context, where mechanistic risk management without a feedback loop to the political decisionmakers will have no effect. Strategic leadership always retains the option of immediate intervention in the operative process and of rejecting, on political grounds, the solution preferred by the administrative level on grounds of efficiency.

Concrete questions such as "which risk is relevant?" or "how can it be contained?" can only be answered if there is agreement on the goals to be pursued. For companies, the matter is clear-cut: They are pursuing a fairly specific goal, namely an increase of the company's value. Furthermore, they have tight and lean decision-making structures. In the political realm, the starting point is a different one: On the one hand, the risk management of states often suffers from a deficit of strategic leadership. On the other, in view of highly divergent assessments and interests, there is rarely a consensus on overarching goals beyond very general ones, such as security and welfare. It is accordingly very difficult to prioritize risks and corresponding measures for mitigating them, since the core task of politics is not to overcome conflicts over targets, but to secure the legitimacy of public action. This legitimacy is primarily measured not in terms of whether the most efficient solution is produced, but in terms of whether citizens and people's representatives are able to influence the decision-making process and attribute more importance to other criteria, as the case may be.

Important platforms for risk dialog

Name	Purpose
Stiftung Risiko-Dialog (1989) www.risiko-dialog.ch	Discussion of technical innovation and social transformation; enhancing social risk competence
Crisis and Risk Network (CRN) (1999) www.crn.ethz.ch	Risk dialog of experts drawn from public administration, academia, and business
OECD Risk Management Policies (2003) www.oecd.org	Support for state risk management structures in the 21st century
International Risk Governance Council (2003) www.irgc.org	Anticipation and control of systemic risks affecting health, the environment, the economy, and society
WEF Global Risk Network (2004) www.weforum.org	Support for the global economy in dealing appropriately with the changing risk landscape

Unpopular risk management

Successful security policy only pays off in the long term, while the business of day-to-day politics is often dominated by short-term considerations. The pressure (e.g., from the media) to produce perceptible results rapidly is often not commensurate to the long-term nature of risks in security policy. Furthermore, it is politically unattractive to spend funds in order to stave off a hypothetical future danger – all the more so since it is difficult to show that inaction would have led to different outcomes. If the 11 September 2001 attacks in the US had been prevented, it is likely that the public as well as many politicians would never have been told about the success of intelligence and defense efforts. Since failures tend to come to light, but successes often remain covert, security policy and risk management are thankless and often unpopular measures.

Successful risk management therefore requires consistent political and financial support from those bearing political responsibility – and not only in case of crises. If important issues are neglected only because they are unpopular, the wrong priorities are set. In order for risk management to remain credible, it is indispensable that its insights be taken seriously and not discredited prematurely if they are prima facie in contrast to conventional thinking.

Side effects

Many risks are concomitant phenomena of conscious behavioral choices. Any advocate of minimizing risk should therefore demand changes in behavior. This requirement is difficult to accept for many companies as well as for actors in state and society. Furthermore, a number of contemporary risks are near-impossible to fight because they develop stealthily and are difficult to identify, both by appearance and in terms of the resulting consequences, until a (too) late stage. In a tightly networked world, risks frequently occur in several places simultaneously and are mutually reinforcing in such a way that not even the best precautions are effective. Generally speaking, there is always a danger that combating risks may lead to new risks: Unintended consequences may in many cases be worse than the risk itself, and risks that have already been eliminated may suddenly reappear elsewhere. Even if the results then affect someone else, global interdependence means that the risk can again fall back on the actor who originally set out to combat it.

Coordination and risk dialog

A core requirement for efficient risk management is coordination, which is needed at three levels. First of all, internal coordination within the company or administration is a prerequisite for preventing

individual departments or groups from advancing their particular interests ahead of the overall mission. Often, individual bodies regard the risks for which they are responsible as the most important ones. They argue over responsibilities, insulate themselves from the outside world, and refuse to divulge information, which makes integrated risk management across departmental boundaries impossible. Institutional barriers must therefore be reduced and incentives offered to combat risk-averse behavior and to strengthen the willingness to pass on information. In the case of risk management in the context of security policy, it is worth considering the establishment of a body that bundles all activities in this area. This should be a high-ranking entity, in order to ensure that it has the necessary political backing that ultimately results in more transparency and clear responsibilities. A possible model is the Civil Contingencies Secretariat in the UK, which is directly subordinate to the Cabinet Office.

Furthermore, coordination must be ensured between the public and private sectors. The outsourcing and privatization of former state services, such as in the areas of telecommunications or energy provision, means that many risks can only be reduced by public-private partnerships. However, the necessary dialog often fails to materialize on its own because the actors in question do not know one another, cannot grasp their shared interests, or are prejudiced. Therefore, initiatives promoting an exchange of ideas and knowledge transfer between experts from the state, business, academic, and civil society sectors must be purposefully fostered.

Thirdly, international coordination is becoming increasingly important, at least as far as state actors are concerned. The transnational nature of security policy risks means that purely national protection mechanisms are frequently ineffective. Both at the inter-state level and in the cross-sectoral context, some important platforms have been created that support creative and innovative risk dialog (see table).

A look at Switzerland

Risk management is also part of Swiss security policy. Among the measures in this field are projects undertaken by the Armed Forces Planning and Joint Staffs, the activities of the intelligence services, or – in a broader sense – the work of the Forward Planning Staff of the Federal Administration. One particularly important project is the "Comprehensive Risk Analysis Switzerland" (Umfassende Risikoanalyse Schweiz), launched at the beginning of the 1990s. This program, located under the auspices of the Federal Office for Civil Protection (FOCP) since 2005, has suffered some setbacks and has not been very active in the past few years. The history of its development reveals not only the general difficulties associated with risk management in security policy, but also the challenges that are specific to the Swiss context.

An important milestone was the "Risikoprofil Schweiz" (Risk Profile Switzerland) report of 1999, which predicted probabilities and damage potentials for a number of risks. This report with its focus on non-military risks was never officially published because the timing of its publication, ahead of a popular referendum on halving military expenditures, was perceived as not being politically expedient. This example shows how risk analyses can be extremely sensitive politically if they are taken seriously and implemented at the political level. Ultimately, risk management is only effective if the results are introduced into the strategy for security policy, if the jurisdictions of the political actors are adapted, and if the respective funding is made available.

The experience of the "Risk Profile Switzerland" report underlines that risk management in Switzerland must enjoy broad political support, and must be perceived as such. In Switzerland more than elsewhere, political legitimacy is derived from the opportunity for (direct) democratic participation and immediate influence on the work of the public administration. Therefore, a technocratic approach that is biased towards quantifiable factors and neglects integration with the political decision-making level does not stand a chance within the Swiss system.

The "Comprehensive Risk Analysis Switzerland" also illustrates the difficulties associated with a cross-cutting project within the federal administration, which tends towards compartmentalization. While a number of federal authorities conduct risk analyses on "their own" specific risks, there is no coordination of results across the entire administration. There is an observable lack of coordination not only between departments, but also within individual departments. This results in duplication of efforts, extra work, quarrels over jurisdiction, and ultimately, neglect of efficient risk policy.

In order to exploit the potential for risk management better on the basis of the "Comprehensive Risk Analysis Switzerland" in the future, a clear definition is required as to which products are to be generated by which bodies for which recipients and how the results can ultimately be integrated into the security policy process. Such decisions must be made at the highest political level; their implementation must subsequently be coordinated across official and departmental boundaries. At the same time, the internal exchange of information and knowledge within the federal administration as well as cooperation with business and academic partners must be strengthened.

Project "Comprehensive Risk Analysis Switzerland"

- 1992: In response to parliamentary enquiries, the Federal Council commissions a "Comprehensive Risk Analysis Switzerland".
- From 1993: Dialog of experts from administration, politics, academia, and the business sector under the auspices of the Central Defense Office ("Zentralstelle für Gesamtverteidigung", ZGV) for collecting and assessing existential risks that affect Switzerland.
- Summer 1999: Completion of the "Risk Profile Switzerland" study.
- Autumn 1999: The Defense Ministry decides to transfer the project to the Center for Security Studies of ETH Zurich so as to align it better academically with the methodology of a comprehensive risk analysis and integrate it better at the international level.
- Since 2000, the Crisis and Risk Network, in cooperation with international partner organizations and maintaining a strong practical focus, has conducted a number of conferences and seminars on issues of risk analysis.

- Author:
  Beat Habegger
  habegger@sipo.gess.ethz.ch
- Responsible editor:
  Daniel Möckli
  analysen@sipo.gess.ethz.ch
- Translated from German:
  Christopher Findlay
- Other CSS Analyses / Mailinglist:
  www.isn.ethz.ch
- German and French versions:
  www.ssn.ethz.ch