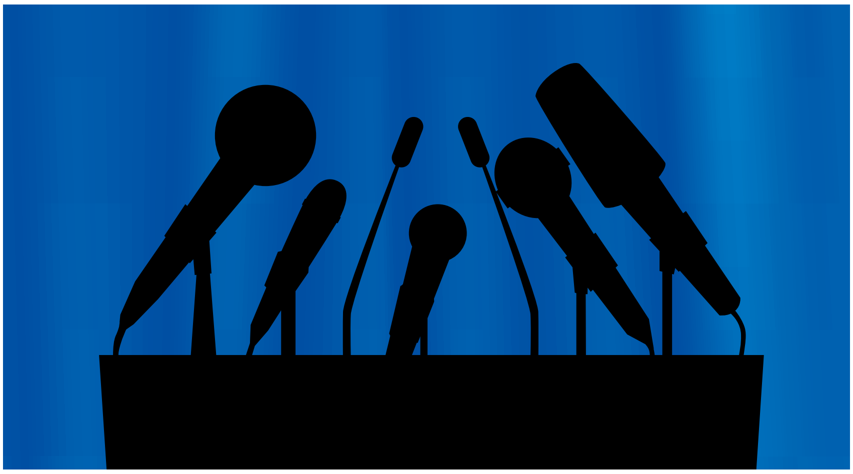
CSS Analyses in Security Policy
CSS ETH Zurich
No. 62 • October 2009

RISK COMMUNICATION IN SECURITY POLICY

Risk communication between political decision-makers, public authorities, experts, and the general public is considered a central component in the official handling of complex and networked risks. So far, however, the concept has been applied almost exclusively in the context of technical and environmental risks. Harnessing risk communication for specific issues in foreign and security policy can sensitize the public to specific problems, create legitimacy for the actions of government agencies, and thus enhance the strategic capabilities of political actors in the case of a crisis.



Risk communication has been neglected in security policy to date. *istockphoto.com*

Risk communication is a well-established concept in a number of areas. For instance, the danger of a global influenza pandemic has been communicated by national and international authorities for months via a range of channels. Such information campaigns aim to sensitize the public, to give timely guidance for individual responses to any potential outbreak, and to accelerate the return to normal after a pandemic.

Unlike in the field of health risks, risk communication is practically non-existent in the areas of Swiss foreign and security policy. This causes recurrent problems. Due to the absence of preventive communication that would allow the public to assess emerging issues and response options realistically, the broader population frequently views the apparently unprepared actions of decision-makers in case of crises with incomprehension.

In this, Switzerland is not an exceptional case. In practical application at the international level, strategies for risk communication are applied almost exclusively in the areas of technical and environmental risks, for example in the fields of genetic engineering, nuclear power, or hazardous areas (flooding, landslides, etc.). This is linked to the origins of the concept: While the term 'risk' was already being used in the environmental sciences and in connection with technical issues in the 1970s, it was not applied in security policy until the 1990s.

In the 1970s, risks were largely conceived as issues for regulatory experts. Governments negotiated directly with the industry on safety values and legal parameters without involving the affected population groups. Not least in response to industrial and environmental disasters, the public increasingly demanded to have a say in risk management. In this context, risk communication evolved into an established component of a participative discourse. Initially, this mainly affected so-called "individual risks", where the individual has the choice of whether or not to take the risk (e.g., building a house in an earthquake zone).

In security policy, too, public risk perceptions play a central role. Holding a dialog on foreign and security policy risks *before* the emergence of an actual crisis can raise the overall crisis resistance of an entire society. Furthermore, risk communication can legitimize the actions of public authorities during a crisis and enhance acceptance of them. Insufficient communication brings with it the danger that the public may fail to comprehend political decisions or perceive them as ill-conceived kneejerk reactions. This may result in withdrawal of public support, which decisively reduces the strategic capabilities of political actors.

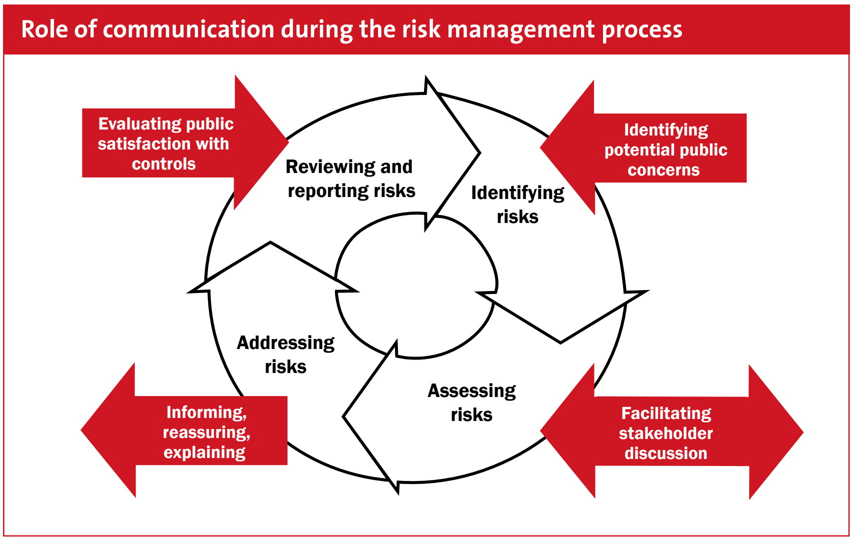
Risk communication: Concept and objectives

Risk communication includes all kinds of communication that serve to identify, assess, evaluate, and manage risks. Thus, risk communication is closely associated at the functional level with risk management. In private companies and public agencies, risk communication may include transparent conveyance of the internal risk management, in which case it becomes part of public relations. This approach should be distinguished from the communication of social and security policy risks and efforts to cope with them.

Risk communication is not the same as crisis communication, however. While risk communication encompasses the entire communication process across all phases of risk management (cf. illustration), crisis communication is limited to communication during an unusual and unexpected event, i.e., when a risk has materialized. Crisis communication aims to overcome this unusual state of affairs and to restore the normal state while trying to minimize lasting damage to the institutions involved. In contrast, risk communication aims to empower individuals through information, dialog, or active participation to arrive at personal assessments of the risks in question based on facts, thus increasing the risk literacy of laypeople. Furthermore, risk communication also serves to explain official precautionary measures.

We may distinguish two components of risk communication that usually appear in chronological succession: In *expert dialogs*, specialists communicate among themselves in order to arrive at joint risk assessments and thus create actual knowledge about the risk. *Public discourse* aims at mediating and debating this risk knowledge in the public arena. Ideally, risk communication amounts to an open matching-up of knowledge and arguments. It is important to take into account the differing risk perceptions of all parties involved. Frequently, there will be large discrepancies between the respective awareness levels of laypeople and experts. In public discourses, the circle of people involved is significantly larger that in expert dialogs. The groups involved are more likely to have heterogeneous knowledge bases, attitudes, and value judgments. Thus, public discourses are frequently more difficult affairs than expert dialogs.

Role of communication during the risk management process


Evaluating public satisfaction with controls
Reviewing and reporting risks
Identifying potential public concerns
Identifying risks
Addressing risks
Assessing risks
Informing, reassuring, explaining
Facilitating stakeholder discussion

Adapted from UK Cabinet Office, Communicating Risk Guidelines.

Risk communication and security policy

In an age of global risks with unexpected outcomes, a systematic application of risk communication to security policy would have certain advantages to offer. It is important to note, however, that most risks in the field of security policy are substantially different from those related to technology and the environment. Risk communication in security policy thus exhibits certain idiosyncratic characteristics: *First of all*, risks in security policy are usually not individual risks, but go beyond the scope of everyday politics, since they occur on a large scale and have both a high intensity and a very high damage potential. The *second* distinguishing trait of security policy risks is that they enhance the vulnerability of the entire social system (e.g., due to interdependencies in technical infrastructures). Complex (technical) systems enhance the probability of cascading effects, which is all the more problematic since responsibility for these systems usually resides outside of governmental authority.

Third, it is particularly difficult in the field of security policy to assess which of the identified risks are the most important ones and how these will continue to develop in the future. Once such risks have been identified, the problem is, *fourth*, that they are potentially incalculable due to high uncertainty. Scientific risk assessments are generally based on a more or less differentiated version of a risk concept borrowed from actuarial mathematics: "Risk = Damage x Probability". It is always assumed that secure knowledge can be gained as to the likelihood of occurrence and the extent of loss. However, in the case of many foreign and security policy risks (terrorist attacks, pandemic outbreaks, diplomatic crises, trade conflicts), such secure knowledge is not available.

These specific characteristics of security policy risks shape risk communication in the field of security policy and define certain limitations for the latter. *First of all*, the enhancement of individual risk literacy, which is usually the goal of risk communication strategies, is only of secondary importance in the case of collective and large-scale risks. In this context, risk communication must aim primarily at explaining and legitimizing public precautionary measures and influencing the behavior of the public in such a way as to raise the resilience (cf. CSS Analysis no. 60) of the social system (e.g., by purchasing protective masks or strengthening resistance to panic in the case of terrorist attacks).

Secondly, the large number of (state and non-state) actors involved, whose risk perceptions vary considerably, makes it difficult even at the level of expert dialogs to reach agreement on the messages to be communicated. Also, the state can often only act as a coordinating actor in such expert dialogs, because the state institutions frequently lack important expert knowledge. Since clear boundaries of jurisdiction are often absent, the distinction between expert dialog and public discourse may be largely blurred. *Third*, risk communication for security policy must be linked to a broader process of strategic early warning (*Horizon Scanning*, cf. CSS Analysis no. 52) if it is not only to react to events, but to prepare proactively for certain risks. *Fourth*, great uncertainty in terms of risk assessment may result in overreactions on the part of public authorities when it comes to governmental information policy. The behavior of public bodies is frequently predicated on the maxim “better safe than sorry”. For instance, the swine flu epidemic is currently progressing rather mildly. However, should the virus undergo a mutation, it could certainly become a starting point for a lethal super-virus, with the point in time of such a mutation being completely unpredictable. Such a risk is difficult to communicate. Therefore, the WHO is upholding the maximum alert level. A similar phenomenon was long seen in the case of US Homeland Security Advisory System, where the threat level was constantly at “orange”, or “high”.

These examples show that risk communication can be a delicate balancing act. If risk communication is omitted altogether, there is an increasing probability that official measures will not be accepted or the public will be caught unprepared by events. However, if excessively extended or urgent warnings are issued for an event that fails to materialize, there is a danger that credibility may be lost and the message may no longer be taken seriously. Additionally, it is almost impossible to measure the effectiveness of risk communication in overcoming a crisis, making it difficult to assess the concept’s usefulness or to improve communication strategies.

In a direct democracy, however, it is essential to hold a dialog on risks where so much is at stake. In order to deal with the problem of “false alarms”, it would make sense to have an open and frank discussion on the limits of knowledge in view of the multifaceted and complex nature of modern-day risks. Such a debate should center on the issue of “unknowability” as well as the potential and limitations of methodologies for identifying risks. Furthermore, it must include an impartial debate over adequate handling of knowledge gaps and the implications of incomplete knowledge backgrounds and decisionmaking rationales for governance.

Risk communication in Switzerland

In the Swiss federal administration, risk communication is generally assigned secondary priority. As in other countries, the focus is on crisis management and crisis communication. Should a crisis arise, organizations (crisis units) are available that have been prepared for foreseeable contingencies. In special cases, ad-hoc organizations (emergency task forces) may be activated. Crisis units undergo more or less regular training exercises, during which shortcomings in the area of crisis communication in particular have been noted time and again (e.g., during the strategic leadership exercise in January 2005 in preparation for a swine flu pandemic). No connection to potential antecedent risk communication has been noted so far.

There are, however, some rudimentary approaches to risk communication in Switzerland. For example, expert dialogs on security policy risks are already being held. Examples include the working groups on the Risks Switzerland project or in the area of Critical Infrastructure Protection under the aegis of the Federal Office for Civil Protection (FOCP). Most of these expert dialogs are currently conducted as internal administration activities. The next imperative step, however, will be to expand these expert dialogs to the private sector and other non-typical security policy actors. A structured public dialog in the framework of the Risks Switzerland project, which could be built up incrementally, would also be useful, given certain caveats. Since the project aims to cover practically all types of risks, multiple approaches will be required for different kinds of risks. Specifically, this involves a clear definition of responsibilities, goals, and tasks.

> ***“Risk communication could enhance Switzerland’s strategic capabilities.”***

In certain areas, public discourses are already underway. For instance, the PLANAT web portal “www.naturgefahren.ch” could be useful for the Risks Switzerland project. Initial experiences have also been gathered in the area of participative discourses: Examples include the work of the Brunner Commission ahead of the publication of Security Policy Report 2000 and the ETH Zurich web platform for the Security Policy Report 2009, an interactive webpage that made the transcripts of statements publicly available and facilitated public participation in the security policy debate (cf. SIPOL WEB). Furthermore, a similar semi-public process is planned for elaborating the “Challenges 2011–2015 in View of Upcoming Legislature Planning”, chaired by the Federal Chancellery.

All of these activities, however, are taking place in an environment in which there is only limited understanding of the necessity of risk communication, let alone efforts to contemplate options for an overarching risk communication strategy in foreign and security policy. However, today even a neutral small country is inextricably linked to its global environment and is directly or indirectly affected by global developments. This makes coherent strategizing in foreign and security policy – as well as ongoing dialog on international issues – indispensable. In order to debate existing risk fields, explain possible responses by the authorities, and enhance societal resilience towards such risks, such a strategy makes a risk communication concept mandatory.

Responsibilities for communication in the fields of technical, environmental, and health risks are usually defined and easily attributable. In foreign and security policy issues, which usually cut across multiple departments, responsibility for defining a strategic position would naturally fall to the entire Federal Council. Specialized units of the Department of Defence, Civil Protection and Sports and the Department of Foreign Affairs could be tasked with announcing these positions in the framework of expert dialogs and public discourses. The application of risk communication could enhance Switzerland’s strategic capabilities. This would make it easier to prepare international dealings, legitimize official measures, prevent loss of prestige by the authorities, and avoid insecure reactions among the general public.

Authors:
Myriam Dunn Cavelty, Jonas Hagmann
dunn@sipo.gess.ethz.ch
hagmann@sipo.gess.ethz.ch

Responsible editor:
Daniel Trachsler
analysen@sipo.gess.ethz.ch

Translated from German:
Christopher Findlay

Other CSS Analyses / Mailinglist:
www.isn.ethz.ch/isn/Current-Affairs/Policy-Briefs

German and French versions:
www.ssn.ethz.ch