Working Paper
Research Division EU Integration
Stiftung Wissenschaft und Politik
German Institute for International
and Security Affairs

Kathrin Ulmer

Cyber Risks and Cyber Security – Risk Communication and Regulation Strategies in the U.S. and Germany

Ludwigkirchplatz 3–4
10719 Berlin
Phone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

Working Paper FG 1, 2014/Nr. 02, June 2014
SWP Berlin

Introduction

Advancements in information and communication technologies and their widespread use have lead to an ever greater dependence on cyberspace and its infrastructure, which increases the vulnerabilities of societies and economies to disruptions. Policy-makers and civil society have become more and more aware of cyber risks such as cybercrime, cyber espionage and cyber terrorism, even acts of cyberwar have already been diagnosed.[1]

Many of the risks in and emanating from cyberspace[2] can be understood as potentially systemic risks,[3] which means that they are characterized by high uncertainty, complexity and ambiguity. In consequence, the probability and the possible damage of an event cannot be fully calculated. The sources of possible damages cannot be exactly identified and an event can have widespread effects across nations. Expert judgments of cyber risks and their possible damage differ widely. Since a strictly scientific assessment of the problem is not possible due to a lack of objective measurement, political interpretations of cyber risks weigh all the more. Actors participate in »discursively structured fights for reality definitions«[4] and those definitions play an important role for legitimizing political action. Notably in the emerging field of cyber policy, discourses play a crucial role and present a highly relevant area of research.

This paper presents the analytical framework I developed for my PhD project.[5] It argues for a two-level approach to analyzing cyber risk discourses understood as risk communication by political decision-makers. It takes into account what is termed the discursive and the regulatory level as well as the interaction between both. In the following, the main elements of the approach are presented as well as some reflections on preliminary research findings. The paper aims to make a contribution to the research debate in the field of cyber policy.

[1] For example with regard to the attacks on Estonia in 2007: <http://www.heise.de/newsticker/meldung/In-Estland-wurde-der-Cyber-Krieg-getestet-133482.html> (24 June 2014).

[2] For a taxonomy of cyber risks see James J. Cebula/Lisa R. Young, *A Taxonomy of Operational Cyber Security Risks*, Software Engineering Institute, Carnegie Mellon 2010, online: <http://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_15200.pdf> (24 June 2014).

[3] Marjolein B.A. van Asselt/Ortwin Renn, »Risk Governance«, in: *Journal of Risk Research* 14 (April 2011) 4, pp. 431–449.

[4] Reiner Keller, *Diskursforschung. Eine Einführung für SozialwissenschaftlerInnen*, Opladen 2004, p. 62, own translation.

[5] More precisely, the project looks at the most recent developments (2007-2013) in cyber policy in the U.S. and Germany in a comparative perspective with regard to the discursive and the regulatory level and the interaction between both.

Analytical Framework

The Sociology of Knowledge Approach to Discourse (SKAD) applied to Cyber Risk Communication

Approaching cyber risks from the perspective of risk research offers a very interesting perspective. In general, handling risks involves several tasks, among them communicating risks. According to Ortwin Renn, effective risk communication plays a central role in successful risk governance. He identifies four functions of risk communication. These are (1) to educate and inform the audience, (2) to support people in coping with risks (for example, by providing risk training and giving incentives to change one's behavior), (3) to create trust in risk handling institutions, and (4) to facilitate opportunities for stakeholder participation in decisions and in the resolution of conflicts with regard to the risk in question.[6] Official discourses by political decision-makers on cyber risks can be defined as risk communication. Relevant speakers with regard to risk communication are political decision-makers, notably government and parliament. Regarding the type of cyber risks, the focus in our context is on »deliberate...actions by people«,[7] a subclass of cyber risks composed of fraud, sabotage, theft and vandalism.

In its theoretical conceptualization, the approach presented in the following is based on Reiner Keller's Sociology of Knowledge Approach to Discourse (SKAD).[8] Through the integration of two more theoretical elements, namely frames in communication and regulatory properties, it proposes an innovative way of operationalizing the SKAD framework and applies it to a new empirical field.

SKAD is a »research programme embedded in the sociology of knowledge tradition in order to examine the discursive construction of symbolic orders which occurs in the form of conflicting social knowledge relationships and competing politics of knowledge«.[9] In Keller's approach, discourses are understood as manifest social practice that is realized in communication in diverse ways of sign usages, such as documents or the spoken word.[10] They are able to stabilize meanings, which is to »fix them in time and by so doing, institutionalize a binding context of meaning, values and actions/agency within social collectives«.[11]

One of SKAD's theoretical building blocks is Foucault's work. It inspires SKAD's double perspective on »the knowledge side and the 'power effects of discourse'«,[12] thus discourse and discourse effects. This twofold view is

[6] Ortwin Renn, *Risk Governance. Coping with Uncertainty in a Complex World*, London/Sterling, VA 2008, pp. 206–208.

[7] Cebula/Young, *A Taxonomy of Operational Cyber Security Risks* [see footnote 2], p. 4.

[8] Reiner Keller, »The Sociology of Knowledge Approach to Discourse (SKAD)«, in: *Human Studies* 34 (March 2011) 1, pp. 43–65.

[9] Ibid., p. 48, emphasis in original.

[10] Ibid., p. 53.

[11] Ibid., p. 51.

[12] Ibid., p. 63.

particularly interesting with regard to the empirical context of cyber policy and integrated in the analytical framework presented here by organizing it as a two-level approach: the knowledge side is referred to as »discursive level« and the power-effects side as »regulatory level«.

As to the operationalization of this two-level approach, the focus is on frames in communication with regard to the discursive level. This element is borrowed from social movements research. As to the second level, the idea of the »dispositif« is taken into account: Discourse effects can manifest themselves in various ways, among other things via what Keller, following Foucault, calls »dispositif«. A dispositif means »an installed infrastructure designed to 'solve a problem', for instance, consisting of a law, administrative regulations, staff, things like cars, computers and so on«.[13] More concretely, the focus of the regulatory level lies on regulatory properties, namely risk regulatory styles that have been developed in risk research and two more general features of regulatory structure. A short explanation to both elements integrated to SKAD follows.

Frames in Communication

A particularly relevant research question that emerges from the above considerations concerns the framing of cyber risks, i.e. how they are interpreted within the communication of policy-makers.[14] In general, frames are used to structure situations and to attribute meaning to them.[15] More precisely, a frame »refers to an interpretative schemata that simplifies and condenses the 'world out there' by selectively punctuating and encoding objects, situations, events, experiences, and sequences of actions within one's present or past environment«.[16]

Basically, frames in thought can be distinguished from frames in communication.[17] With regard to political and thus also cyber risk communication, the second category of frames in communication is relevant. James N. Druckman explains as follows: »The frame that the speaker chooses may reveal what the speaker sees as relevant to the topic at hand (...). For example, a politician who emphasizes economic issues when discussing

[13] Ibid., p. 49.

[14] There has been previous research on cyber »threat frames« and »threat representations«, however from the angle of security studies based on securitisation theory (see Myriam Dunn Cavelty, *Cyber-Security and Threat Politics. US Efforts to Secure the Information Age*, London/New York 2008; Myriam Dunn Cavelty, »From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse«, in: *International Studies Review* 15 (2013) 1, pp. 105–122). In my research, I choose a different theoretical framework that builds on Keller's Sociology of Knowledge Approach to Discourse (SKAD) (see also graphic on p. 5). Moreover, I seek to expand existing research through a comparative design and add to it with state of the art data.

[15] Erving Goffman, *Rahmen-Analyse. Ein Versuch über die Organisation von Alltagserfahrungen*, Frankurt am Main 1993.

[16] David A. Snow/Robert D. Benford, »Master Frames and Cycles of Protest«, in: Aldon D. Morris/Carol M. Mueller (Eds.): *Frontiers in Social Movement Theory*, New Haven/London 1992, pp. 133–155 (137).

[17] James N. Druckman, »The Implications of Framing Effects for Citizen Competence«, in: *Political Behavior* 23 (2001) 3, pp. 225–256 (227–228).

the campaign uses an 'economy frame' that suggests economic considerations are pertinent«.[18]

According to the definition of Entman (1993), frames have different functions: »Frames ... define problems – determine what a causal agent is doing with what costs and benefits, usually measured in terms of common cultural values; diagnose causes – identify the forces creating the problem; make moral judgments – evaluate causal agents and their effects; and suggest remedies – offer and justify treatments for the problems and predict their likely effects«.[19]

Regulatory Properties

Risk regulatory styles have been developed in the research on environmental, health and safety risk regulation.[20] They contain important elements of risk regulation such as the inclusion and status of scientific expertise, the openness of the political process to third parties or the inclusion of public perceptions.[21] Studies revealed different styles in the U.S. and Europe.[22] In particular, the U.S. was found to have an »adversarial« style of regulation, whereas a »corporatist« style was attributed to Germany.[23]

It is especially promising to use this typology in order to find out, whether these styles can be found in the field of cyber policy, thus if the typology is also valid in a new policy field that has not yet been taken into account by research. To obtain a more comprehensive picture of the regulatory level, two more features of regulatory structure are integrated into the approach: the type and direction of regulation (top-down vs. bottom-up) and the organization of risk-handling institutions (fragmentation vs. centralization).

In a summarizing manner, the graphic below shows the analytical framework laid out above: The SKAD framework with the integration of frames in communication and regulatory properties in order to operationalize the discursive and the regulatory level.

[18] Ibid., p. 227.

[19] Robert M. Entman, »Framing: Toward Clarification of a Fractured Paradigm«, in: *Journal of Communication* 43 (1993) 4, pp. 51–58 (52), emphasis in original.

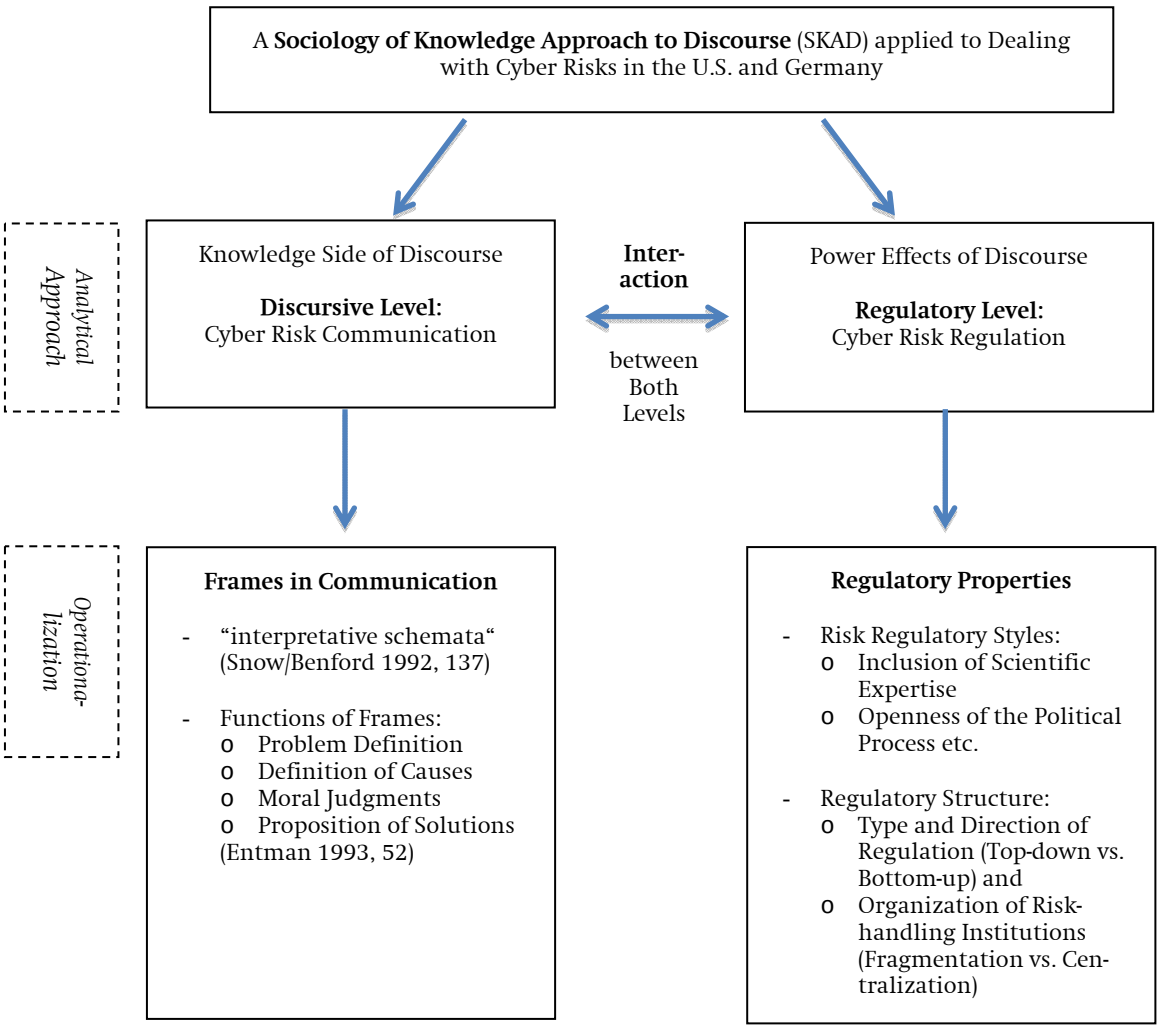
[20] Ortwin Renn, »The Changing Character of Regulation: A Comparison of Europe and the United States. Commentary«, in: *Risk Analysis*, 21 (2001) 3, pp. 406–410; T. O'Riordan/B. Wynne, »Regulating Environmental Risks: A Comparative Perspective«, in: Paul R. Kleindorfer/Howard C. Kunreuther (Eds.), *Insuring and Managing Hazardous Risks: From Seveso to Bhopal and Beyond*, Berlin/Heidelberg et al. 1987, pp. 389–410; David Vogel, *National Styles of Regulation. Environmental Policy in Great Britain and the United States*, Ithaca/London 1986; Ronald Brickman/Sheila Jasanoff/Thomas Ilgen, *Controlling Chemicals. The Politics of Regulation in Europe and the United States*, Ithaca/London 1985.

[21] Ortwin Renn, »The Changing Character of Regulation: A Comparison of Europe and the United States. Commentary«, in: *Risk Analysis*, 21 (2001 (3), pp. 406–410; T. O'Riordan/B. Wynne, »Regulating Environmental Risks: A Comparative Perspective«, in: Paul R. Kleindorfer/Howard C. Kunreuther (Eds.), *Insuring and Managing Hazardous Risks: From Seveso to Bhopal and Beyond*, Berlin/Heidelberg et al. 1987, pp. 389–410.

[22] See footnote 20.

[23] See footnote 21.

Graphic: Analytical Framework



Source: Own representation.

Preliminary Research Findings

Undoubtedly, cyber experts see the U.S. as the pioneer country in the cyber domain. It stands out in technological advancements with regard to cyberspace and its infrastructure. Whereas in the U.S., policy related to aspects of cyberspace dates back to the 1980s,[24] many European countries have begun only in recent years to establish a cyber policy. Germany issued its first cyber strategy in 2011, the cyber strategy of the EU dates back to 2013.

Cyber security has a clear European dimension because of the possible cross-national impact of cyber risks. Given the interdependence of the EU

[24] Dunn Cavelty, *Cyber-Security and Threat Politics. US Efforts to Secure the Information Age* [see footnote 14], p. 9.

member states (for example via common network structures), a cyber incident in one member state can lead to effects in one or more other member states. As to EU policies towards critical infrastructures, the EU initially concentrated on energy and traffic infrastructures in the wake of the bombings of Madrid (2004) and London (2005). Later, critical information and communication infrastructures gained in importance. On the one hand, the EU seeks to increase the level of protection in the member states; on the other hand, the EU identifies a need for supranational action because of the cross-border dimension of cyber risks. Central measures and projects are the digital agenda, the identification and protection of (European) critical infrastructures, the fight against cybercrime, the protection from attacks on information systems as well as the dialogue on cyberspace-related questions with international partners. The European Network and Information Security Agency (ENISA) provides technical expertise. Despite its European dimension, cyber policy is no Europeanized policy field in the narrow sense and the national states are the decisive players in most of the main aspects, at least for now. Against this background, this paper argues for an analysis of German cyber policy by including the relevant European developments as they provide the context in which German policy-making takes place.

Taking a look at the empirical context in Germany and the U.S. with regard to the discursive and the regulatory level,[25] one can state that overall, cyber issues are controversial in Germany as well as in the U.S. Political interpretations manifest themselves and are created in discourse. Observing the U.S. discourse, one notes an important security policy-related interpretation of cyber issues, for example, Leon Panetta's »cyber Pearl Harbor«.[26] In this frame, there is a strong national security link. The language is militarized and outlines the risk of one devastating event with terrible consequences. As is noted by Ian Wallace, such a militarized language—another example is »cyberwar«—can be »dangerous«, as »[t]he war analogy implies the requirement for military response to cyber intrusions«.[27] Another quite dominant frame in the U.S. discourse could be termed the »China threat«. These frames are also present in Germany, albeit on a much weaker scale, partially due to the lack of an event comparable to 9/11. However, going further back in Germany's past, the experience of two dictatorships explains the prominence of the data protection frame on this side of the Atlantic.

[25] In this section, some of my preliminary research findings are presented. They have first been published in an essay: Kathrin Ulmer, *Cyber Policy in Germany and the U.S.: Challenges in an Emerging Policy Field*, AICGS Transatlantic Perspectives, Washington, DC, December 2013, online: <http://www.aicgs.org/publication/cyber-policy-in-germany-and-the-u-s-challenges-in-an-emerging-policy-field/> (24 June 2014).

[26] Leon E. Panetta, *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security*, New York City, 11 October 2012, <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136> (24 June 2014).

[27] Ian Wallace, *Why The U.S. Is Not In A Cyber War*, The Daily Beast, 10 March 2013, <http://www.thedailybeast.com/articles/2013/03/10/why-the-u-s-is-not-in-a-cyber-war.html> (24 June 2014).

Regarding the regulatory level, the field of cyber policy is particularly complex given that a large part of critical (information) infrastructure is owned and operated by the private sector. Thus, top-down and bottom-up approaches are discussed in the U.S. and Germany.

The difficulty to regulate cyberspace issues in the U.S. can be illustrated by the House of Representative's Cyber Intelligence and Sharing Protection Act (CISPA) and the Senate's Cybersecurity Act (CSA), neither of which became law.[28] Following these legislative failures, Executive Order 13636[29] and Presidential Policy Directive 21[30] were issued in February 2013, tasking the Department of Commerce's National Institute of Standards and Technology (NIST) with developing a voluntary Cybersecurity Framework, the first version of which was released in February 2014.[31]

Interestingly, we can observe an inverse process – first a voluntary approach, then regulation – in Germany. Initiated by the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik), the »Alliance for Cyber Security« (»Allianz für Cybersicherheit«) sought a voluntary information-sharing on cyber security threats and incidents between federal agencies, companies, and other institutions.[32] As voluntary measures did not work out as intended, former Federal Minister of the Interior Hans-Peter Friedrich proposed an IT security law (IT-Sicherheitsgesetz) in March 2013.[33] His successor, current Federal Minister Thomas de Mazière will present a new version in autumn 2014.[34]

These insights illustrate some of the dynamics in cyber risk communication and regulation on both sides of the Atlantic. Further research will follow up on these developments in more detail. It will notably be interest-

[28] Steven P. Bucci et al., *A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace*, The Heritage Foundation, Backgrounder #2785 on National Security and Defense, 1 April 2013, <http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace> (24 June 2014).

[29] The White House, *Executive Order–Improving Critical Infrastructure Cybersecurity*, 12 February 2013, <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity> (24 June 2014).

[30] The White House, *Presidential Policy Directive–Critical Infrastructure Security and Resilience*, 12 February 2013, <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil> (24 June 2014).

[31] See the Website of the National Institute of Standards and Technology (NIST) < http://www.nist.gov/cyberframework/> (24 June 2014).

[32] Federal Office for Information Security, *Allianz für Cybersicherheit*, Website of the Federal Office for Information Security, <https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Strategie/Allianz_fuer_Cybersicherheit/Allianz_node.html> (24 June 2014).

[33] Federal Ministry of the Interior, *Friedrich stellt Wirtschaft IT-Sicherheitsgesetz vor*, Website of the Federal Ministry of the Interior, 12 March 2013, <http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2013/03/eco_mmr_itsicherheitsgesetz.html?nn=3446780> (24 June 2014)

[34] Federal Ministry of the Interior, *»Schutz, Sicherheit und Vertrauen« – Bundesinnenminister de Maizière spricht auf der Jahresfachkonferenz der DuD über die Aufgaben der Politik im digitalen Zeitalter*, Website of the Federal Ministry of the Interior, 23 June 2014, <http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/06/dud-fachkonferenz.html> (24 June 2014).

ing to find out which further commonalities and differences can be found in the U.S. and Germany, which overall strategies in risk communication and regulation are chosen, and whether effects of (discursive or regulatory) »spill-over« across the Atlantic can be identified.