David Gorr, Wolf J. Schünemann:

Creating a secure cyberspace – Securitization in Internet governance discourses and dispositives in Germany and Russia

Abstract:

This article deals with the phenomenon of securitization in the emerging policy field of Internet governance. In essence, it presents a combination of theoretical reflections preparing the grounds for a comparative analysis of respective discourses and so-called dispositives as well as preliminary findings from such a comparative project. In the following sections we firstly present some theoretical reflections on the structural conditions of Internet regulation in general and the role and relevance of securitization in particular. Secondly, we shed light on how securitization is constructed and how it might affect the build-up process of instruments of Internet regulation. How does securitization happen, how does it work in different societies/states? Which discursive elements can be identified in elites' discourses? And which politico-legal dispositives do emanate from discourse? In a third section we illustrate our reflections with some preliminary findings from a comparison of cybersecurity discourses and dispositives in Germany and Russia.

Agenda:

ISSN 1614-1687

Authors:

David Gorr, M.A.:

- Institute for Social Sciences, Dept. of Political Science, University of Koblenz-Landau, Kaufhausgasse 9, D-76829 Landau
- ☎ + 49 6341 280 38 400

Dr. Wolf J. Schünemann:

- Institute for Political Science, Heidelberg University, Bergheimer Str. 58, D-69115 Heidelberg
- ☎ +49 6221 542860, ✉ wolf.schuenemann@ipw.uni-heidelberg.de , 💻 http://www.uni-heidelberg.de/politikwissenschaften/
- Relevant publications:

  Schünemann, Wolf J.: E-Government und Netzpolitik - eine konzeptionelle Einführung. In: Schünemann, Wolf J./Weiler, Stefan (Hrsg.): E-Government und Netzpolitik im europäischen Vergleich. Baden-Baden, Nomos-Verlag 2012. 9-38.

  Schünemann, Wolf J./Zilles, Julia: Die Vermessung der Netzwerkgesellschaft - Internationale Statistiken und Evaluationen als empirische Grundlagen für die vergleichende Forschung. In: Schünemann, Wolf J./Weiler, Stefan (Hrsg.): E-Government und Netzpolitik im europäischen Vergleich. Baden-Baden, Nomos-Verlag 2012. 39-69.

In the course of the so-called information revolution that we experience for at least two decades the impact of the Internet on our daily lives has become immense and it has caused dramatic changes in the way we live and communicate. At the same time, the openness of the Internet seems to have an important downside. With regulation lagging behind, it seems to be a dangerous place. In the emerging net political debates, it is sometimes even depicted or perceived as a wild west[1] full of hackers, cybercrooks and sexual predators. As a consequence, political demand for more or less strict national or international regulations of the allegedly borderless space has increased in recent years. In order to fight cybercrime or cyber attacks or even to perform cyber operations themselves (e.g. cyber-espionage) authoritarian as well as democratic states have developed a variety of techniques and have implemented unilateral and/or multilateral strategies. The currently unfolding details on how and to what extent primarily US and British based intelligence services (NSA and GCHQ) monitor online communication all over the world have shown the strong determination of democratic regimes to secure cyberspace. But, however, how do political-administrative authorities in established and defective democracies react to changing patterns of public life? Which narratives and divergent interpretive schemes are observable in the respective elites' discourses that might serve as justifications for Internet regulation or even censorship? In the following sections, we want to deal with these questions, putting our main focus on the discussion and instruments of cybersecurity. Therefore, we firstly have to explain the structural difficulties of effective Internet regulation and we will deal with the question of what is a cyber threat. In our second section we will present the theoretical concept of securitization and give some general illustrations of how it 'works' in the particular context of cyberspace. In the third section we will present some illustrative findings from cybersecurity discourses and dispositives of Germany that is taken as an established and functioning democracy and Russia which is described as a defective democracy at best or even as an authoritarian state. Finally, our reflections will be summed up by a short conclusion.

Internet governance and cyber threats

The wired world and its fragmented socio-political structures

In this section, the basic condition under which the regulation of the Internet necessarily takes place has to be explained: The cyberspace is a global sphere.[2] The Internet as the 'network of networks' since its beginnings has been planned and designed in a global dimension. This becomes obvious in everyday experiences with the *World Wide Web*. Normally, Internet users do not know where the website they easily access from at home is really located, that means: where the server stands that is hosting the website.[3] Also when using *email* the normal user does not know which way through the Internet it takes, how many borders the data package transcends before reaching the mailbox of the recipient. So in essence, the Internet as a technical infrastructure has a transnational or global dimension. In contrast, political-administrative actors that would be responsible for its technical setup, its organization and regulation are stuck to fragmented institutional structures (mostly of the nation state), i.e. political and legal systems, markets, cultures and languages. This can be seen as the basic structural condition or tension under which the broader field of Internet regulation must be examined. When national governments try to regulate or even restrict online communication, they often act in vein because within the transnational system the owners of a website or the providers of server capacity may reside in another country, thus another jurisdiction and do not fall under domestic law.[4] Also, Internet users can easily

[1] The notion is indeed frequently used, see for instance: Andress, Jason/Winterfeld, Steve: Cyber warfare techniques. xx, 4; Lewis, James A./CSIS: Cybersecurity two years later. 4.

[2] Also „Virtual Public Space, VPS", see Schünemann, Wolf J.: E-Government und Netzpolitik – eine konzeptionelle Einführung.

[3] See Beckedahl, Markus/Lüke, Falk: Die digitale Gesellschaft. 67-68. Schünemann. Wolf J.: E-Government und Netzpolitik – eine konzeptionelle Einführung. 18.

[4] Cf. Möller, Jan: Rechtsfrei oder recht frei? 312-314; Nye, Joseph S.: Cyber Power. 6.

ISSN 1614-1687

circumvent national rules and restrictions what makes law enforcement potentially ineffective.[5] True, institutions of international governance (e.g. the Internet Governance Forum of the United Nations, IGF) have been established in order to deal with the transnational quality of cyberspace but as in other policy fields, the international governance of the Internet through organizations and regimes is marked by the same weaknesses of institutional complexity, a lack of cohesion, authority and compliance which basically can be traced back to the fundamental structural condition of fragmentation. Additionally, in the concrete field of Internet governance the international community is marked by a rather clear ideological schism between a group of autocratic states that seek to hold control of the Internet because they fear a de-stabilization of their political systems given the free transnational flows of information and on the other hand a group of liberal democracies that at least publicly support these very flows and thus the leading vision of a 'Web of the Free'[6] and criticize governmental control or censorship of Internet content.[7] This is not to say that democratic regimes would deliberately refrain from cyber espionage. The practices of leading intelligence services as NSA and GCHQ which exploited the technical structure of the internet as well as the dominance of US-based technology firms for their own purposes might serve as an illustration for the very opposite. Indeed, this can be seen as a good reason for questioning the alleged link between democratic order and a 'free' internet. However, given the features of world order listed above, we come to a differentiated assumption concerning the range of action nation states have when dealing with the Internet. While it is generally difficult for nation states to control the Internet because of its global dimensions, governments still have some leverage in Internet regulation and they are more or less able and willing to use or misuse this leverage if it fits to their political goals. And indeed, there always have been regimes that have sought – more or less successfully – to hold a control on their 'national Internet' (e.g. China's 'Great Firewall').

What is a cyber threat?

What is considered a cyber threat in the expanding cybersecurity discourses covers a broad range of quite different activities.[8] In order to analyze and understand how societies discuss and try to build a secure cyberspace it seems to be crucial to have a clear concept of what would be a threat to defend against. Scholars from different disciplines (security studies, political science, international law, etc.) have tried to bring some order into the categorical chaos. A fundamental dichotomy can be drawn between cyber exploitation and cyber attack.[9] As cases of exploitation of the network we can understand most incidents of cyber crime and cyber espionage (Internet fraud, identity theft, etc.) that indeed may cause a lot of damage (especially economic losses), but do not affect the functioning of a given network.[10] Also cyber exploitations do not necessarily serve political goals, they are more often committed for economic profit.

Cyber attacks, in contrast, often have political motives and the main objective is to alter or damage computer networks and create dysfunctions of some kind. According to Hathaway et al. as cyber attack can be understood "any action taken to undermine the functions of a computer network for a political or national security purpose".[11] Cyber attacks can take different forms. The most frequent variants are distributed denial of service attacks (DDOS), the defacement of websites, the planting of inaccurate information or the infiltration of a computer network (e.g. through worms and viruses). The incidents of cyber attacks that have increased in

[5] Cf. Schünemann. Wolf J.: E-Government und Netzpolitik – eine konzeptionelle Einführung. 26.

[6] The notion "Web of the Free" is borrowed from a New York Times article with this title written by the lawyer Mark A. Shiffrin and the computer scientist Avi Silberschatz. Therein the authors argue for a loose control of the Internet pointing to the technology's origin in the US.

[7] This schism even reflects in the discussion on how to define cyber attacks, see Hathaway, Oona A. et al.: The Law of Cyber-Attack. 824-825.

[8] Cf. Carr, Jeffrey: Inside cyber warfare. xiii, 5.

[9] See Nye, Joseph S.: Cyber Power. 11.

[10] Hathaway, Oona A. et al.: The Law of Cyber-Attack. 829.

[11] Ibid. 826.

number during the recent decade are often depicted as cyberwar or cyber terrorism by politicians, security experts and the media.[12] It is absolutely legitimate that many scholars warn of exaggerations and present more careful and objective definitions. Indeed, not many cyber attacks fulfil the criteria of war or terrorism.[13] When a group of individual hackers or script kiddies succeeds in defacing a governmental website or even shutting it down, this is clearly a cyber attack, but is this really a new type of warfare or terrorism? As important as clear answers to this question seem, especially from an international law perspective, given the far reaching consequences of such categorizations in this respect,[14] for the social reality of threat perception and its political effects which vary from one society to the next objective criteria of what is a threat and how it is to be called do not really matter. This latter reflection points to our constructivist perspective on the issue and leads to the main theoretical concept of securitization.

Securitization and cybersecurity

The concept of securitization

The concept of securitization stands central in an approach to international relations (IR) that originally has been developed by the so-called Copenhagen School (CS) and that should widen the focus of classical security studies from a military and state-centred view to a broader range of security issues. Therefore, security in an IR sense is not defined according to objective criteria, e.g. a military attack. In contrast, what makes an incident a threat is the outcome of an intersubjective process. As Buzan, Wæver and De Wilde define it, security "is when an issue is presented as posing an existential threat to a designated referent object".[15] Thus a security issue can be every issue that is perceived and/or successfully depicted as a security issue by societal actors in a given social setting. So, obviously, this is a constructivist approach to security. Its core concept of securitization has its roots in speech act theory (Austin/Searle) and is understood as a performative act: "The process of securitization is what in language theory is called a speech act. It is not interesting as a sign referring to something more real; it is the utterance itself that is the act."[16] Facing the difficulties in conceptualizing a cyber threat mentioned above this approach provides an elegant solution. As analysts of political processes we do not have to cope with the question whether an issue constitutes a real threat or not. A threat is a threat if there is a so-called securitizing actor that presents it as such and if this move is accepted by a legitimating audience. Or as Balzacq puts the fundamental insight of securitization theory: "no issue is essentially a menace. Something becomes a security problem through discursive politics."[17] The most important effect of a successful act of securitization is a justification for extraordinary measures. The issue is moved outside the normal political procedures into an emergency mode in which governmental action beyond given rules that would otherwise bind security actors is required and accepted. That is why the inventors of the concept put securitization in contrast to politicization, thus highlighting its de-politicizing effect.[18]

[12] For the German discussion Gaycken's book that does not belong into an academic context might serve as a good example: Gaycken, Sandro: Cyberwar.

[13] Cf. Lewis, James A./CSIS: Cybersecurity two years later. 2.

[14] The classification of an incidence as an act of war can have meaningful implications as for example the right to self-defense for a state that suffered from such an assault, see Hathaway, Oona A. et al.: The Law of Cyber-Attack. 820 u. 841.

[15] Buzan, Barry/Waever, Ole/De Wilde, Jaap: Security: A New Framework for Analysis. 21.

[16] Ibid. 26.

[17] Balzacq, Thierry: A theory of securitization. 1.

[18] Actually they say both: "Although in one sense securitization is a further intensification of politicization (thus usually making an even stronger role for the state), in another sense it is opposed to politicization." Buzan, Barry/Waever, Ole/De Wilde, Jaap: Security: A New Framework for Analysis. 29.

For the empirical study of securitization Buzan, Wæver and De Wilde themselves propose discourse analysis as favoured methodology without giving concrete indications how the analysis should be conducted. Before designing a more concrete method for our study it is important to note that not just discursive practices should be examined but also the more comprehensive *dispositif* which additionally includes non-discursive practices, institutions, tools etc.[19] The further development of securitization theory by Thierry Balzacq takes this direction. Balzacq regards the phenomenon from a sociological-pragmatic rather than a mere language philosophy perspective.[20] This reorientation has the advantage that the social context in which a securitizing move has to resonate is taken into account. Following Balzacq "the success of securitization is contingent upon a perceptive environment" and "the semantic repertoire of security is […] a combination of textual meaning and cultural meaning".[21] Finally, we affiliate to Balzacq's clarification that securitization should not be understood as a self-referential performative but in reality "takes the form of argumentative processes".[22] So our research essentially is a combination of discourse analysis taking arguments as the main interpretive categories and dispositif analysis examining practices and tools of cybersecurity (see section 3).

Cyberspace: A security issue?

The concept of securitization seems particularly suited to understand how cybersecurity agendas have been developed in different societies. Having said this, it makes no wonder that the concept has been applied to the new policy field in a number of works already.[23] A look into the broader conceptual framework of securitization might help to understand how this application is done. Firstly, according to the inventors of the concept a securitization act needs a referent object, thus any collective unit or principle that is said to be existentially threatened. In our case this might be the Internet as technical infrastructure itself or, via the vision of critical infrastructures disturbed or destructed by cyber attacks, it can be our economy, our social system, maybe, most alarmingly, our lives.[24] In a less dramatic vision, it also could be the idea of a *Web of the Free* that is heavily endangered. Secondly, there obviously is a need for a securitizing actor, someone or a group that might serve as legitimate speaker(s) in this field and is listened to by a legitimating audience. This can be politicians, of course, or cyber experts, be it activists or even representatives of firms that sell cybersecurity tools. Finally, in order to understand securitization in the field of cybersecurity it seems particularly important to look at what Buzan, Wæver and De Wilde call facilitating conditions. For, compared to other attacks in international relations, cyber attacks seem to be relatively harmless, judged by an overlook of the incidents known so far.[25] Assaults that would clearly justify classifications as terrorism or even war have been seldom or have not happened at all. On the other hand, in the field of cybersecurity, there are strong facilitating conditions which help explain why securitization is nonetheless successful. Firstly, the Internet is a relatively young phenomenon, which our industrial societies already heavily rely on. There is a particularly high vulnerability even of sovereign states as for example Stuxnet has shown in the case of Iran.[26] Secondly, the majority of users, including many politicians, does not know in detail how this technology works. Thus there is a fundamental combination of dependency and uncertainty that easily breeds diffuse anxieties. Thirdly, the Internet and many Internet applications have been developed for easy usage, while often enough ignoring security concerns which would have made costly

[19] The concept was originally coined by Foucault, see Foucault, Michel: L'ordre du discours.

[20] Cf. Balzacq, Thierry: A theory of securitization.

[21] Ibid. 13, 14.

[22] Ibid. 22.

[23] See for instance Guitton, Clement: Cyber insecurity as a national threat; Thiel, Thorsten: Unendliche Weiten...? Umkämpfte Grenzen im Internet.

[24] Cf. Billo, Charles G./Chang, Welton: Cyber Warfare. 13-14.

[25] Cf. Carr, Jeffrey: Inside cyber warfare. 8; Guitton, Clement: Cyber insecurity as a national threat. 25. For a regularly updated list of incidents see the respective reports of the US-based Center for Strategic & International Studies (CSIS), URL: http://csis.org/publication/cyber-events-2006 (09/14/2013).

[26] A case that is often referred to also by governmental actors in Western democracies in order to illustrate potential cyber threats, see Hathaway, Oona A. et al.: The Law of Cyber-Attack. 884.

upgrades or even the abdication of higher speed and convenience necessary.[27] Finally, in the field of IR, the cyberspace accelerates a development of power diffusion that is observable since the end of the cold war.[28] This is connected to the fact that attribution has become notoriously difficult in cyberspace which gives states and other actors that are engaged in cyber exploitations or attacks a permanent chance of anonymity or as Carr puts it "plausible deniability".[29] While in conventional conflicts, a state mostly could know by whom it has been attacked, this is not at all the case for cyber attacks the origin of which mostly remains unknown. Not knowing where an attack comes from is also likely to increase uncertainty among security actors because under this condition almost any conventional defence strategy seems hopeless.

Empirical findings from Russia and Germany

For the broader empirical research project that we can illustrate in this article only by exhibiting some preliminary findings, we basically use discourse and dispositive analysis, mainly according to the research program called *Sociology of Knowledge Approach to Discourse*, SKAD.[30] According to SKAD, discourse is to be understood as a material manifestation and circulation of knowledge.[31] SKAD is particularly suited to not just examine the global diffusion of concepts, norms and practices but to investigate more closely the fundamental processes of their reception, translation, and transformation in and through specific socio-cultural settings.

As regards the countries selected, we particularly expect instructive similarities and differences that become obvious through a comparative study of net political discourses and practices in a functioning democracy on the one hand – Germany is considered as belonging to this type – and a defective democracy on the other – here Russia can serve as a good example given its autocratic traits. This selection might be justified for the issue of cybersecurity by a look on the "Freedom of the Net Index", developed by the US-based NGO *Freedom House*. According to the collected data, Russia's 70 million Internet users endure only a "partly free" Internet in their country,[32] whereas Germany's 68 million Internet users face "free" conditions.[33] As democratization literature mostly suggests, public discourses on Internet governance and online communication converge around liberal ideas of civic freedoms, causing bottom-up pressure for democratic reforms in autocracies and defective democracies. Scholars of so-called eDemocracy largely tend to an optimistic outlook saying that new forms of online communication are likely to serve as democratization catalysts.[34] Yet, while Internet communication in Germany seems to be very free and the rather hesitant measures of regulation and control by the government have been responded to by open protests (see the domestic debate on "Netzsperren" in the year 2009), the Russian government is still controlling online communication to a much higher degree and protests for a free Internet are often repressed through state forces. Especially the Russian Internet restriction bill, which initially was created as a blacklist of Internet sites with content that is seen as harmful to children, is considered to be used for censorship of online content of a broader kind. Moreover, in international negotiations on Internet governance, Russia positions itself as the leading nation of an international coalition for new governmental powers of Internet regulation, e.g. within the organizational frame of the Shanghai Cooperation.

---

[27] Cf. Lewis, James A./CSIS: Cybersecurity two years later. 2; Nye, Joseph S.: Cyber Power. 5.

[28] Robert Nye has elucidated the phenomenon of power diffusion in cyberspace in a recent article: Nye, Joseph S.: Cyber Power.

[29] Carr, Jeffrey: Inside cyber warfare. 3.

[30] Keller, Reiner: Wissenssoziologische Diskursanalyse.

[31] Ibid. 97. Konersmann, Ralf: Der Philosoph mit der Maske. 80.

[32] Freedom House: Freedom of the Net 2012. Russia.

[33] Freedom House: Freedom of the Net 2012. Germany.

[34] One of the first books that argued in this direction and attracted a lot of attention is: Benkler, Yochai: The wealth of networks. See also: Abbott, Jason: Social media; Bruns, Axel: Blogs, Wikipedia, Second Life and Beyond; Diamond, Larry: The Coming Wave; Shirky, Clay: Here comes everybody; Shirky, Clay: The political power of social media. In: Foreign Affairs 1/2011. 28.

For the pre-studies to present in this article we only analyzed rather small data corpora of governmental documents, interviews of government officials etc. (Germany: 17, Russia: 15). All texts are open source documents. They were chosen according to the fact that they predominantly deal with the topic of cybersecurity. For this article, we concentrated on elite discourses. In the following sections, we present some preliminary findings from the case studies. For each case, we present the most important results of our interpretive work, i.e. the main recurrent elements we identified in the respective discourse. Taken together, they might serve as a prototype of a code book for a more comprehensive qualitative study (1). Then, we describe which institutions and practices, i.e. dispositives have been developed so far (2).

Germany

Germany's cybersecurity discourse – interpretive analysis

In the governmental documents analyzed so far the Internet technology is primarily perceived as a possibility to boost the economy. The elites consider the Internet as a chance in terms of job creation and ensuring further growth and prosperity (*Economic Argument*, EcoA). In addition, the Federal Foreign Office describes the Internet as a political tool leading to a democratization and to a strengthening of civil society (*Democratic Argument*, DemA). In both respects, it is said, Germany has fully benefitted from digital economy and the Internet so far. Yet, the whole society is perceived to be extremely dependent on a reliable and functioning Internet technology. So, not the cyberspace per se, but the technical infrastructure is seen as particularly vulnerable and insecure (*Risk Perception*, RP). Many officials state that the openness and the expansion of the Internet as well as its disorder or even anarchy would facilitate cyber attacks. The interdependence and global dimension of IT infrastructures would even increase the damage of those assaults. Exactly these two elements have been stressed for instance by Udo Helmbrecht, former president of the *Federal Office for Information Security* (BSI), in 2005 already when he concluded that IT security "must be understood as a national task"[35] and they were updated when he later explicitly demanded a security strategy tackling cyber criminality.[36]

Cyber attacks are perceived by the German Government as attacks coming most frequently from terrorists, professional fraudsters, and criminal organisations because those IT attacks are more attractive than conventional attacks.[37] As to concrete external threats, several cyber exploitations attributed to China and the computer worm Stuxnet discovered in 2010 are explicity addressed when it comes to illustrating risk assessment. Referring to Stuxnet the German Government argues that considerable action needs to be taken because "important industrial infrastructures are no longer exempted from targeted IT attacks" (*Complexity Argument*, CompA).[38] Companies, not to mention individual Internet users, are seen to be overstrained as regards their abilities of handling those cyber attacks alone (*Paternalistic Argument*, PatA). After all, it is said, that the dynamic development of the cyberspace poses new risks which can only be managed by a strong state with a flexible cybersecurity strategy in order to cope with new challenges. However, the necessary measures should only be taken under the condition of ensuring the balance of means and ends (*Proportionality Argument*, PropA). Moreover, the measures should not affect the possibilities of the Internet as an economic driver (*Economic Framework Argument*, EFA) and the protection of data privacy should be taken into account as well (*Data Protection Argument*, DPA).

[35] Federal Office for Information Security: The IT-Security Situation in Germany in 2005. 5.

[36] Federal Office for Information Security: Die Lage der IT-Sicherheit in Deutschland 2007. 5.

[37] Cf. Federal Office for Information Security: Nationales Cyber-Abwehrzentrum. 4.

[38] Federal Ministry of the Interior: Cyber Security Strategy for Germany. 3; see also Bundestag: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Petra Pau, Jan Korte, Dr. Petra Sitte, weiterer Abgeordneter und der Fraktion DIE LINKE.

Table 1: The building blocks/interpretive schemes of cybersecurity discourse in Germany:

Dimension	Category	Interpretive Scheme
Perception of the Cyberspace	Economic argument (EcoA)	Cyberspace as an economic driver
	Democratic argument (DemA)	Cyberspace as a political tool for liberation and democratisation
		Web of the Free
	Risk Perception (RP)	Internet (technical network) as a vulnerable/insecure structure
		Internet development as a dynamic process, governmental actors lagging behind
		States/societies as highly dependent on Internet technology and thus vulnerable
Challenges	Complexity Argument (CompA)	New quality and complexity of cyberattacks
	Paternalistic Argument (PatA)	State as provider of IT security for overstrained private IT users (companies, individuals, etc.)
Framework for action	Proportionality Argument (PropA)	Balance of means and ends within the securitization process
	Economic Framework Argument (EFA)	Opportunities of the Internet as an economic driver should not be affected
	Data Protection Argument (DPA)	Ensuring the protection of data privacy
Propositions for Action	New Authorities Proposition (NAP)	Establishing new authorities (National Cyber Response Centre, National Cyber Security Council), strengthen law enforcement agencies
	Coordination Proposition (CoP)	Closer coordination based on intensified information sharing at national and international level
	Standardisation Proposition (StP)	Establishing minimum standards, harmonise rules, introducing legal commitments for the business owners of critical infrastructures
	Awareness Promotion Proposition (APP)	Awareness promotion relating to IT security for private IT users

Germany's cybersecurity dispositif – tools, institutions, practices

As regards new tools, institutions and practices that have been established in the policy field, Germany recently adopted measures to secure cyberspace by a "National Cyber Response Centre" which was set up in April 2011 to "optimize operational cooperation between all state authorities and improve the coordination of protection".[39] Under the lead of the BSI, the centre will submit recommendations to the also newly established "National Cyber Security Council"[40] headed by the Federal Commissioner for Information Technology Rogall-Grothe (*New Authorities Proposition*, NAP). Since the main goal of the centre is information sharing, all important authorities

[39] Federal Ministry of the Interior: Cyber Security Strategy for Germany. 8.

[40] The body is composed of representatives from the Federal Chancellery, different federal ministries (Foreign Affairs, Interior, Defence, Economics and Technology, Justice, Finance, Education and Research) as well as representatives of the Federal States/Länder, see ibid. 9.

will be involved and cooperate both directly and indirectly. Apart from the installation of new authorities, the federal government generally seeks to portray itself as a role model as regards cybersecurity by the publication of guidelines and a general framework addressing cyber threats. State agencies shall establish minimum standards, harmonize rules, introduce legal commitments, strengthen law enforcement agencies and promote coordination at national and international level (EU, NATO, United Nations, OECD etc.; *Coordination Proposition*, CoP, *Standardisation Proposition*, StP). As to international relations, the Federal Foreign Office established the International Cyber Policy Coordination Staff in 2011 and announced this summer that it will appoint diplomat Dirk Brengelmann as a Commissioner for International Cyber Policy.[41] Furthermore, state authorities intensify research on IT security, promote further training for personnel and dedicate more resources in order to tackle cyber threats. Also, the Federal Ministry of Economics and Technology has set up a task force on "IT security in industry" in order to support small and medium sized businesses securing their infrastructures. Overall, the state agencies shall promote awareness among private users (businesses and citizens) and provide them with better information and education relating to IT security (*Awareness Promotion Proposition*, APP).

Russia

Russia's cybersecurity discourse – interpretive analysis

Firstly, compared to Germany, it is significant to note that none of the important Russian doctrines and strategy papers does contain the words "cyberspace", "cyber attacks" or "cyber warfare". All relevant documents[42] use instead the term "information security". In order to understand the mind set of the Russian leaders towards cybersecurity it is important to realize that for them information is per se a "valuable asset" which needs to be protected "in times of peace and war".[43] Consequently, cyber attacks are rather seen as a part of information warfare.[44] The same holistic approach is found in the Russian cyber security strategy published in December 2011.[45] According to this strategy, an information war is a conflict between states with the aim to destroy national information systems leading to a destabilization of the social and political situation in a country. As typical of Russian governmental documents it is held in a defensive tone,[46] trying to avoid any description of Russia's offensive capabilities and focussing only on control, prevention and solution of cyber conflicts.

Cyberspace is generally perceived by the Russian Government as something that the state has no control over yet. However, if a state wants to retain its sovereignty, it is argued, it should be also able to regulate and monitor the information sphere. In this sense, oversight over any phenomenon, in this case information technology, is seen as the most natural thing, no matter how difficult the implementation might be (*Sovereignty Argument*, SovA). Unlike German governmental speakers, Russian officials do not fear the economic but rather the political consequences of cyber attacks which might even lead to a potential regime change (*Revolution Argument*, RevA). In this context, officials stress that information manipulation by the West could evoke Orange Revolution-like events in Russia. For this reason they favour the idea that any interference in the internal affairs of a state via the Internet should be forbidden. The officials acknowledge that information technology is affecting all areas of life. Thus, the main concern of the Russian Government is the growing dependency on the

[41] Brengelmann shall act for Germany's interest on Internet governance at the international level. His appointment attracted attention because it was announced in the face of the NSA scandal, see Federal Foreign Office: Commissioner for International Cyber Policy.

[42] For a complete list of documents related to security issues, see http://www.scrf.gov.ru/documents/sections/3/ (09/12/2013). A brief review of the National Security Concept to 2020 is provided by Haas, Marcel de: Medvedev's Security Policy; Schröder, Henning: Russia's National Security Strategy to 2020; Liaropoulos, Adrew/Dimitrakopoulou, Sophia: Russia's National Security Strategy to 2020.

[43] Heickerö, Roland: Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations. 4.

[44] Cf. Giles, Keir: Russia and Cyber Security. 70-71.

[45] Ministry of Defence of the Russian Federation: Conceptional Views on the Activity of the Russian Federation Armed Forces in the Information Space.

[46] Cf. Giles, Keir: Russia and Cyber Security. 78.

Internet technology (*Risk Perception*, RP): "The national security of the Russian Federation substantially depends on the level of information security, and with technical progress this dependence is bound to increase."[47] But not dependency per se, but reliance on Western technology is seen as an even bigger threat to the national security (*Risk Perception*, RP). The Kremlin has recognised the need for action because it admits that the legal and regulatory framework dealing with information security is imperfect, the protection of state secrets and data privacy is deteriorating and the coordination among authorities is insufficient combined with poor budget financing. The fact that the Russian news agencies and mass media are not competitive and still lagging behind Western technology is also a reason why the Government demands immediate solutions (*Poor Conditions Argument*, PCA). However, also the Russian officials state that any measure will only be useful if the balance of interests among the individual, society and the state in the information sphere is respected (*Proportionality Argument*, PropA).

Table 2: Building blocks/interpretive schemes of cybersecurity discourse in Russia

Dimension	**Category**	**Interpretive Scheme**
Perception of the Cyberspace	Sovereignty Argument (SovA)	Cyberspace as a sphere which is not yet controlled by the state, thus endangering national sovereignty
	Risk Perception (RP)	Internet development as a dynamic process, governmental actors lagging behind
		States/societies as highly dependent on "western Internet technology" and thus vulnerable
Challenges	Poor Conditions Argument (PCA)	Failed attempts and poor legal, political and socioeconomic conditions dealing with cybersecurity
	Revolution Argument (RevA)	Cyberspace/online communication as facilitating conditions for insurrection and regime change
		Web of the Free in a negative sense
		Preventing Orange Revolution-like events in Russia
Framework for action	Proportionality Argument (PropA)	Balance of means and ends within the securitization process
Propositions for Action	New Authorities Proposition (NAP)	Establishing special departments and IT security units, strengthen law enforcement agencies
	Coordination Proposition (CoP)	Closer coordination among authorities
	Self-Reliance Proposition (SRP)	Building independent information systems and create Cyrillic Internet domain names
	Global Governance Proposition (GGP)	Establishing global rules of state behaviour in cyberspace
		Negotiating a cyberspace disarmament treaty

Russia's cybersecurity dispositif – tools, institutions, practices

Since 1997, the Russian Criminal Code includes a chapter tackling "Crimes in the Sphere of Computer Information" composed of three articles, "Illegal Accessing of Computer Information" (Art. 272), "Creation, Use, and Dissemination of Harmful Computer Viruses" (Art. 273) and "Violation of Rules for the Operation of Computers,

[47] Ministry of Foreign Affairs of the Russian Federation: Information Security Doctrine of the Russian Federation.

Computer Systems, or Their Networks" (Art. 274). Russia's Internet is generally regulated under the Law on Mass Media (No. 2124-1) because the authorities interpret the Internet as an extension of media space, with the consequence that bloggers and website owners are responsible for their websites' content. Russian politicians have often expressed their ambitions to have an overall control of the Russian cyberspace implementing a Chinese-style filtering method.[48] The government agency *Federal Service of Communications, Information Technology and Mass Media* (abbreviated: Roszomnadzor), established under the jurisdiction of the Ministry of Telecom and Mass Communications in 2008, is responsible for overseeing compliance with the Law on Personal Data (No. 152-FZ) and the Law on Information, Information Technologies and Protection of Information (No. 149-FZ), both passed in 2006. The agency is also currently maintaining the database of websites containing alleged child pornography, drug-related and extremist material. Another important authority is the *Federal Communication Agency* (abbreviated: Rossvyaz), formed in 2008. It deals with providing public services in the sphere of communication and information.

In matters concerning the implementation of security measures the Russian Government is seeking to increase the efficiency and coordination of government administration (*Coordination Proposition*, CoP), set up special departments and units for cybersecurity (*New Authorities Proposition*, NAP) and enhance law enforcement activities of federal executive bodies. Due to the wide dissemination of information technology in all spheres of life, the Russian Government had already initiated the federal program "Electronic Russia" in 2002 in order to establish an overall eGovernment concept.[49] In order to reduce dependency on technology the Kremlin wants to create independent information systems stemmed from Russian Western engineers and inventors (*Self-Reliance Proposition*, SRP). In this context, on several occasions, Medvedev, Putin and other high-rank officials announced plans to establish a Cyrillic Web of Russia parallel to the World Wide Web. Given its fear of interference into internal affairs via the Internet, at the international level the Russian government is a strong supporter of a universal cyber convention including global standards of state behaviour in cyberspace. Together with the members of the Shanghai Cooperation Group it endorsed the 2011 proposal for an International Code of Conduct for Information Security aiming at strengthening state sovereignty in cyberspace (*Global Governance Proposition*, GPP). Russian officials even claim that the absence of an international treaty would lead to a cyberwar arms race, which they seek to avoid by negotiating a cyberspace disarmament treaty as part of the UN framework.

Conclusion

The cyberspace constitutes a vast field of activities that can be perceived as threats by governmental actors. Facing this fact, the concept of securitization has proved to be particularly useful for examining the emergent cybersecurity discourses and dispositives in different countries. As the constructivist approach suggests: What is perceived as a threat is the outcome of an intersubjective process that normally takes place within a given society. Due to a wide range of powerful facilitating conditions explained above cyberspace is particularly prone to securitization despite the fact that the incidents of cyber attacks known so far have been relatively harmless compared to the effects traditional conflicts in international relations can have. In addition, as especially the sociological-pragmatic version of securitization theory chosen for this article leads one to expect: Whether and how an issue is securitized depends on the social context, but therein also on the established institutions and practices within a given security sub-system.

The preliminary findings of our empirical study of cybersecurity discourses and dispositives in Germany and Russia have shown similarities as well as differences. Securitization is evidently present in both cases. Even some arguments for government action are quite similar (see tables 1 and 2). Nevertheless, the fundamental perceptions of the cyberspace and the risks of Internet technology differ significantly, especially regarding the

[48] Cf. Deibert, Ronald/Palfrey, John/Rohozinski, Rafal/Zittrain, Jonathan: Russia. 215, 218.

[49] It has been replaced by the program "On the Information Society State Programme of the Russian Federation (2011-2020)" (Executive Order No. 1815-r) in 2010. Moreover, the overall "Strategy of the Development of the Information Society in the Russian Federation" from the year 2008 will address the issue in further detail (cf. Security Council of the Russian Federation 2008).

focus either on the stability of the economy (Germany) or the stability of the political system (Russia). This variation is also expressed in the measures that have been taken and institutions that have been established to create a secure cyberspace in each of the cases. It also reflects the fundamental schism mentioned above that regularly comes up in international negotiations on Internet governance. While Russia pursues a state-centrist regulatory approach to combat and overcome cyber threats which are interpreted in a broad sense of information security, seeking to avoid any interference in internal affairs as an expression of national sovereignty, Germany on the other side has adopted "a mediating role" (Bendiek 2012, p. 15), supporting a global codex for government actions in cyberspace but supporting the idea of a *Web of the Free* and thus not showing any fear of free flows of information. Furthermore, Germany seems particularly eager to promote and protect its economy against cyber threats rather than its political regime.

To finally conclude, it is almost needless to say that a lot of further research on the issue needs to be done. This should include an extension of case studies as well as a more in-depth analysis of discourses and dispositives for each case. This article, nonetheless, might serve as an explorative work preparing the path for future studies in this direction.

References

Abbott, Jason: Social media. In: Kersting, Norbert (ed.): Electronic democracy. Leverkusen [u.a.], Barbara Budrich 2012. 77-102.

Andress, Jason/Winterfeld, Steve: Cyber warfare techniques. Tactics and tools for security practitioners. Amsterdam [u.a.], Elsevier Syngress 2011.

Balzacq, Thierry: A theory of securitization. Origins, core assumptions, and variants. In: Balzacq, Thierry (ed.): Securitization Theory. How security problems emerge and dissolve. London [u.a.], Routledge 2011. 1-30.

Beckedahl, Markus/Lüke, Falk: Die digitale Gesellschaft. Netzpolitik, Bürgerrechte und die Machtfrage, München, Deutscher Taschenbuch Verlag 2012.

Benkler, Yochai: The wealth of networks. How social production transforms markets and freedom. New Haven, Conn. [u.a.], Yale University Press 2006.

Billo, Charles G./Chang, Welton: Cyber Warfare. An Analysis of the means and motivations of selected nation states. Dartmouth, ISTS 2004.

Brenner, Susan W.: Cyberthreats. The emerging fault lines of the nation state. New York [u.a.], Oxford University Press 2009.

Bruns, Axel: Blogs, Wikipedia, Second Life and Beyond: From Production to Produsage. New York, Peter Lang 2009.

Bundestag: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Petra Pau, Jan Korte, Dr. Petra Sitte, weiterer Abgeordneter und der Fraktion DIE LINKE. Drucksache 17/5694. 02.05.2011. URL: http://dip21.bundestag.de/dip21/btd/17/056/1705694.pdf (08/08/2013).

Buzan, Barry/Waever, Ole/De Wilde, Jaap: Security: A New Framework for Analysis. Boulder, Lynne Rienner Publishers 1998.

Carr, Jeffrey: Inside cyber warfare. Mapping the cyber underworld. Beijing [u.a.], O'Reilly 2009.

Deibert, Ronald/Palfrey, John/Rohozinski, Rafal/Zittrain, Jonathan: Russia. In: Deibert, Ronald/Palfrey, John/Rohozinski, Rafal/Zittrain, Jonathan (eds.): Access Controlled. The Shaping of Power, Rights, and Rule in Cyberspace. Cambridge, MIT Press 2010. 209-226.

Diamond, Larry: The Coming Wave. In: Journal of Democracy 1/2012. 5-13.

Federal Foreign Office: Commissioner for International Cyber Policy. 2013. URL: http://www.auswaertiges-amt.de/EN/AAmt/Koordinatoren/Cyber-AP/Uebersicht.html (08/16/2013).

Federal Ministry of the Interior: Cyber Security Strategy for Germany. Berlin 2011. URL: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber_eng.pdf?__blob=publicationFile (07/25/2013).

Federal Office for Information Security: Nationales Cyber-Abwehrzentrum. Cybersicherheit in Deutschland. Präsentation von Hartmut Isselhorst, Bonn 2011. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Presse/Cybersicherheit-in-Deutschland.pdf?__blob=publicationFile (08/08/2013).

Federal Office for Information Security: Die Lage der IT-Sicherheit in Deutschland 2007. Bonn 2007. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/lagebericht2007_pdf.pdf?__blob=publicationFile (08/10/2013).

Federal Office for Information Security: The IT-Security Situation in Germany in 2005. Bonn 2005. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2005_pdf.pdf?__blob=publicationFile (08/10/2013).

Foucault, Michel: L'ordre du discours. Paris, Gallimard 1971.

Freedom House: Freedom of the Net 2012. Russia – Country Report. 2012. URL: http://www.freedomhouse.org/sites/default/files/Russia%202012.pdf (06/30/2013).

Freedom House: Freedom of the Net 2012. Germany – Country Report. 2012. URL: http://www.freedomhouse.org/sites/default/files/Germany%202012.pdf (06/30/2013).

Gaycken, Sandro: Cyberwar. Das Wettrüsten hat längst begonnen. Vom digitalen Angriff zum realen Ausnahmezustand. München, Goldmann 2012.

Giles, Keir: Russia and Cyber Security. In: Nação e defesa 133/2012. 69-88.

Guitton, Clement: Cyber insecurity as a national threat: overreaction from Germany, France and the UK? In: European Security 1/2013 (Vol. 20). 21-35.

Haas, Marcel de: Medvedev's Security Policy: A Provisional Assessment. In: russian analytical digest 62/2009. 2-5.

Hathaway, Oona A. et al.: The Law of Cyber-Attack. In: California Law Review 4/2012. 817-885.

Heickerö, Roland: Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations. Stockholm, Swedish Defence Research Agency 2010.

Hindman, Matthew Scott: The myth of digital democracy. Princeton, NJ [u.a.], Princeton University Press 2009.

Keller, Reiner: Wissenssoziologische Diskursanalyse. Grundlegung eines Forschungsprogramms. Wiesbaden, VS-Verlag 2008.

Keller, Reiner: Analysing Discourse. An Approach from the Sociology of Knowledge. In: Forum: Qualitative Social Research (FQS) 3/2005, Art. 32.

Konersmann, Ralf: Der Philosoph mit der Maske. Michel Foucaults L'ordre du discours. In: Foucault, Michel; Konersmann, Ralf (ed.): Die Ordnung des Diskurses. Frankfurt am Main, Fischer Taschenbuch Verlag 2007. 51-94.

Lewis, James A./CSIS: Cybersecurity two years later. A report of the CSIS Commission on cybersecurity for the 44th presidency. In: Studies, Center for Strategic & International, Washington, DC 2011.

Lessing, Lawrence: Code: And Other Laws of Cyperspace. New York, Basic Books 1999.

Liaropoulos, Adrew/Dimitrakopoulou, Sophia: Russia's National Security Strategy to 2020: A Great Power in the Making? In: Caucasian Review of International Affairs, 1/2010 (Vol. 4). 35-42.

Ministry of Defence of the Russian Federation: Conceptional Views on the Activity of the Russian Federation Armed Forces in the Information Space. 2011. URL: http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle (08/20/2013).

Ministry of Foreign Affairs of the Russian Federation: Information Security Doctrine of the Russian Federation. Approved on September 9 2000. URL: http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument (08/16/2013).

Möller, Jan: Rechtsfrei oder recht frei? Zur Vereinbarung, Anwendung und Durchsetzung von gesellschaftlichen Konventionen im Internet. In: Schünemann, Wolf J./Weiler, Stefan (eds.): E-Government und Netzpolitik im europäischen Vergleich. Baden-Baden, Nomos 2012. 309-320.

Morozov, Evgeny: The Net Delusion: The Dark Side of Internet Freedom. New York, Public Affairs 2011.

Norris, Pippa: Political mobilization and social networks. The example of the Arab spring. In: Kersting, Norbert (ed.): Electronic democracy. Leverkusen [u.a.], Barbara Budrich 2012. 55-76.

Nye, Joseph S.: Cyber Power. In: Nye, Joseph S. (ed.): The Future of Power. New York, Public Affairs 2011.

Schröder, Henning: Russia's National Security Strategy to 2020. In: russian analytical digest 62/2009. 6-10.

Schünemann. Wolf J.: E-Government und Netzpolitik – eine konzeptionelle Einführung. In: Schünemann, Wolf J./Weiler, Stefan (eds.): E-Government und Netzpolitik im europäischen Vergleich. Baden-Baden, Nomos. 9-38.

Shiffrin, Mark A./Silberschatz, Avi: Web of the Free. In: New York Times, Oct. 23, 2005.

Shirky, Clay: Here comes everybody: the power of organizing without organizations, New York, NY [u.a.], Penguin 2008.

Shirky, Clay: The political power of social media. In: Foreign Affairs 1/2011. 28.

Thiel, Thorsten: Unendliche Weiten...? Umkämpfte Grenzen im Internet. In: INDES 4/2012. 61-67.

Wu, Tim: The Master Switch: The Rise and Fall of Information Empires. New York, Knopf 2010.

Zittrain, Jonathan: The Future of the Internet And How to Stop it. New Haven, Yale University Press 2008.