universität wien

# DIPLOMARBEIT

## Cyber Security: DNS-CERT as a Case for Securitization in Internet Governance

Verfasser

Philipp Mirtl

angestrebter akademischer Grad

Magister der Philosophie (Mag. phil.)

Wien, 2012

| | |
|---|---|
| Studienkennzahl lt. Studienblatt: | A 300 |
| Studienrichtung lt. Studienblatt: | Politikwissenschaft |
| Betreuerin / Betreuer: | Ao. Univ.- Prof. Dr. Otmar Höll |

*To my mother, Marion*

# Contents

# Introduction[1, 2]

The Internet started as a research project between computer engineers during the 1960s. When it became commercialized during the 1990s, both civil society and private sector actors not only started to make use of it, but also influenced its governance. Although the Internet is but the most recent technology in a long series of different communication technologies (such as telephone, teleprinters, or the radio), today Internet technology is nearly all-embracing. This is especially due to the fact that global communication is increasingly heading towards the *Internet Protocol* (IP) as being the main technical standard in communications (e.g., Voice-over IP, or VoIP).[3]

This engagement of a whole range of diverse actors made it necessary to experiment with new means of governance. In this respect, the most prominent example is multi-stakeholder collaboration, which can be characterized as the involvement of all different actors who affect or who are affected by certain policies. However, as a governance model, multi-stakeholder collaboration is still very vaguely defined and does not provide any answers about *who* is in the power to do *what* and *when*.

One of the most prominent examples for a multi-stakeholder model is the nonprofit *Internet Corporation for Assigned Names and Numbers* (ICANN), the global coordinator for the *domain name system* (DNS). Essentially, ICANN is a collection of multiple stakeholders coming from governments, the private sector and civil society. Each of these different groups has its own set of interests, values and power constellations. However, not every group holds the same amount of power. This has important implications for the organization as a whole.

Since its inception in 1998, ICANN has struggled for legitimacy. It has applied a series of different strategies to overcome this problem, but, to date, has not succeeded. For Andrew Hurrell, this is not surprising. For him, "questions of legitimacy emerge whenever power is exercised in the context of competing interests and conflicting values."[4] In the case of ICANN, throughout its history, power has shifted from one stakeholder to the other, constantly. Nevertheless, is there anything that can be considered to be a constant characteristic for

[1] I want to thank Prof Otmar Höll for his trust and his patience. Also, I would like to thank Alexander Klimburg for his support and his vision!

[2] N.B. In order to optimize the quality of the results of this thesis, minor parts have preliminarily been published in a joint publication: Klimburg, Alexander and Mirtl, Philipp, 'Cyberspace and Governance—A Primer', *oiip policy paper*, September 2011, http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Newsletter/Cyberspace_and_Governance-A_primer.pdf.

[3] Kurbalija, Jovan, *An Introduction to Internet Governance*, Genève, DiploFoundation, 2010, p. 6.

[4] Hurrell, Andrew, *On Global Order. Power, Values, and the Constitution of International Society*, Oxford, Oxford University Press, 2007, p. 116.

multi-stakeholder collaboration?

By looking through a security lens, we will try to tackle this question. By asking who can speak security in a multi-stakeholder collaboration such as ICANN, we hope to uncover some of the specific characteristics of this governance model.

Essentially, this study consists of three main parts. The first one provides an in-depth introduction to the concept of security, viewed through the theoretical lens of the *Copenhagen school*. Here, we will look at the school's most influential origins and provide an overview of both its concept of security sectors and its theory of securitization. Furthermore, we will introduce yet another sector to the Copenhagen school's magnificent five. Along with the military, environmental, economic, societal and political sectors, we will also argue in favor of a so called cyber sector. In fact, this idea is not new. The concept of a distinct cyber sector was originally introduced by Lene Hansen and Helen Nissenbaum.[5] They argued that cyber security had its own distinct form, which would warrant a theoretical widening. This study supports their concept in that it not only applies their ideas about sector-specific security grammars, but also tries to develop it further. While the authors claimed that technical referent objects (such as computer networks) only gained legitimacy through their linkage to a social referent object (such as the state), they remained unclear about what these computer networks actually included. Was it an entire network (e.g., the Internet) that was linked to a social referent object or was it single components of that network (e.g., cables, protocols or content)? We will answer this question by introducing a four-layer model of cyberspace with a physical layer at the bottom, both a logical and a content layer above as well as social layer on top.

The second major part of this study is aimed at setting the scene for the final case study. In doing so it not only provides a basic understanding for some technical issues around the Internet, but also contextualizes them with history and ongoing discussions as to whether the global network of networks is being securitized or not. We also give an overview of the key protocols upon which the Internet is built today and define the domain name system (DNS) as one of the most critical services on the Net. With this in mind, we will define the concept of Internet governance and its main political constellation: multi-stakeholder collaboration. Multi-stakeholder collaboration got a great deal of attention in context of Internet governance. However, it is still a rather new concept, which is why we close the second part of this study with a presentation about one of the most controversially discussed

[5] Hansen, Lene and Nissenbaum, Helen, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53, 2009, pp. 1155-75, p. 1163.

multi-stakeholder platforms worldwide: the *Internet Corporation for Assigned Names and Numbers* (ICANN).

Ultimately, we will apply our acquired theoretical and technical skills in a final case study. Most of the data gathering was already accomplished by the *Berkman Center for Internet & Society at Harvard University*. Thus, we can directly build upon the already published results and put them in context of our own cyber security framework. Through applying the Copenhagen school's concept of securitization, we will try to answer the question whether the CEO and President of ICANN has the voice to speak security in the name of networks and states.

In our final conclusion we will deliver (at least some) answers to the questions that were posed initially and try to derive from them some inspirations for future research in our field.

# 1. The Copenhagen School

## 1.1. The Concept of Security

The *Copenhagen school* emerged in the 1980s around Barry Buzan and Ole Wæver who, at that time, worked together at the *Copenhagen Peace Research Institute* (COPRI).[6] The name of the school was originally coined by Bill McSweeney who found the publications by Buzan, Wæver and their collaborators "sufficiently interrelated to warrant the collective shorthand, the 'Copenhagen school' of security studies."[7]

For the Copenhagen school, the *concept of security* follows a straightforward security form, or logic. In essence, "[s]ecurity means survival in the face of existential threats."[8] More precisely, security

> "is when an issue is presented as posing an existential threat to a designated referent object (traditionally, but not necessarily, the state, incorporating government, territory, and society). The special nature of security justifies the use of extraordinary measures to handle them."[9]

This definition heavily builds upon traditional security analysis[10] where actors (mostly states) strife to ensure their constantly threatened existence in absence of a central authority (anarchy). However, while traditionalists'[11] argue in favor of *objectively* identifiable threats (e.g., the threat arising from the devastating combination of superpower rivalry and nuclear weapons), the Copenhagen school takes up a radically different position, claiming that there is no such thing as an objective measure for so called "real" threats:

> "Even if one wanted to take a more objectivist approach, it is unclear how this could be done except in cases in which the threat is unambiguous and immediate. (An example would be hostile tanks crossing the border; even here, 'hostile' is an attribute not of the vehicle but of the socially constituted relationship. A foreign tank

[6] In 2003 COPRI was merged into the *Danish Institute for International Studies* (DIIS).
[7] McSweeney, Bill, 'Identity and security: Buzan and the Copenhagen school', in *Review of International Studies* 22, 1, 1996, pp.81-94.
[8] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 27.
[9] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 21.
[10] See, for instance, Waltz, Kenneth, *Theory of International Politics*, New York, Random House, 1979.
[11] See Hansen, Lene and Buzan, Barry, *The Evolution of International Security Studies*, Cambridge et al., Cambridge University Press, 2009, pp. 156-86.

> could be part of a peacekeeping force.)"[12]

Therefore, instead of holding that security threats could be approached objectively (as do traditionalists), the Copenhagen school suggests that threats are constructed in an *inter-subjective* discourse where someone in the position of power points at a specific issue and claims:

> "this is an existential threat with a point of no return; if we do not handle this in time, if we do not give it full priority, then we will not be here to tackle the other more mundane matters."[13]

More to the point, for the Copenhagen school "'security' *is* what actors make it:"[14] a process by which a powerful actor discursively constructs an issue as a threat to a specific referent object. Consequently,

> "'[s]ecurity' is [. . .] a self-referential practice, because it is in this practice that the issue becomes a security issue—not necessarily because a real existential threat exists but because the issue is presented as such a threat."[15]

Traditionally, the state has been the only referent object within international security studies. However, as will become clear in the following sections, this narrow view has been widened considerably since the end of the Cold War. Just to name a few, today referent objects can include states and nations as well as rain forests and political ideologies. Nevertheless, this does not imply that referent objects can be appointed randomly:

> "Referent objects must establish security legitimacy in terms of a claim to survival. Bureaucracies, political regimes, and firms seldom hold this sense of guaranteed survival and thus are not usually classed as referent objects. Logically, they could try to establish a claim to survival and thus to security legitimacy, but empirically this is not usually possible."[16]

The reason why a referent object must hold enough security legitimacy is to mobilize sufficient support from the audience that is addressed to accept the security claim. Yet, if

[12] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 30.

[13] Wæver, Ole, 'European Security Identities', *Journal of Common Market Studies*, 34, 1, pp. 2120-132, p. 108.

[14] Buzan, Barry and Wæver, Ole, *Regions and Powers. The Structure of International Security*, Cambridge, Cambridge University Press, 2003, p. 48.

[15] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 24.

[16] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 39.

this audience does not back an object's claim to survival, eventually taken extraordinary measures (e.g., a higher level of secrecy and a resulting lack of transparency, levying taxes, limiting otherwise inviolable rights, a limiting focus on just one single issue, etc.[17]) cannot be sufficiently justified. We will come back to this when explaining the *concept of securitization*.

Having defined the concept of security as a discursive practice, we can now proceed in introducing the framework that was built around these basic assumptions. Traditionally, the Copenhagen school is made up of "three main ideas:"[18] *securitization*,[19] *security sectors*,[20] and *regional security complexes*.[21] More recently, however, the concepts of *macrosecuritization*[22] and *security constellations*[23] have been added. For the purpose of this study, however, we will only consider the first two concepts.

Among the Copenhagen school's main ideas, "securitisation is what defines most distinctly the school in a meta-theoretical sense."[24] Thus, the first subsection to follow will set out the theoretical roots that underpin Wæver's securitization theory. In a second move, the concepts of security sectors and securitization will be presented.

### 1.1.1. Theoretical Origins

The theoretical foundation for securitization theory is constituted by three distinct approaches. The first one was developed by linguist John L. Austin and is widely known as *speech act theory*. The second one refers to parts of *Carl Schmitt's political theory* which includes both his concept of the political and his decisionist theory of sovereignty. Ultimately, the third one concerns *traditionalist security debates* culminating around

[17] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 247.

[18] Wæver, Ole, 'Aberystwyth, Paris, Copenhagen: New Schools in Security Theory and the Origins between Core and Periphery', *unpublished paper*, presented at the International Studies Association's 45th Annual Convention in Montreal, Canada, 2004, p. 7.

[19] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, chapter 2, pp. 21-47.

[20] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998.

[21] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998; pp. 9-20; Buzan, Barry and Wæver, Ole, *Regions and Powers. The Structure of International Security*, Cambridge, Cambridge University Press, 2003.

[22] See Barry and Wæver, Ole, 'Macrosecuritization and security constellations: reconsidering scale in securitization theory', *Review of International Studies*, 35, pp. 253-76, 2009.

[23] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998 , pp. 201-2; Buzan, Barry and Wæver, Ole, 'Macrosecuritization and security constellations: reconsidering scale in securitization theory', *Review of International Studies*, 35, pp. 253-76, 2009.

[24] See, Wæver, Ole, 'Aberystwyth, Paris, Copenhagen: New Schools in Security Theory and the Origins between Core and Periphery', *unpublished paper*, presented at the International Studies Association's 45th Annual Convention in Montreal, Canada, 2004, p. 7.

Kenneth Waltz.[25] Each of them shall be presented here briefly.[26]

#### 1.1.1.1. John L. Austin and John Searle

*Speech act theory* was first introduced by John L. Austin and further developed by John Searle. Drawing on Ludwig Wittgenstein's *language games*, Austin suggests that, apart from the *semantic meaning*, a statement also has a *pragmatic meaning*.[27] As opposed to the latter, the pragmatic meaning of a statement is not inherent in the words or phrases themselves, but results from the particular setting in which it is used (context). Yet, a *speech act* "is normally not thought of as just saying something,"[28] but as an utterance "where by saying something, something is being done."[29] For instance, in the context of a wedding, when a priest is saying "I now pronounce you man and wife," a marriage is being done. This process of creating social reality is what Austin calls a *performative utterance* or *performative speech act* where "the uttering of the sentence is, or is part of, the doing of an action."[30]

Basically, speech acts can be broken down into three different levels. The most basic one is the *locutionary act*, which refers to the literal meaning of an utterance: "He said to me 'Shoot her!', meaning by 'shoot', shoot and referring by 'her' to her."[31] The second level is the *illocutionary act*, which is about the pragmatic meaning of the utterance: "He urged (or advised, ordered, &c.) me to shoot her."[32] Finally, the *perlocutionary act* means the action that is actually induced by an utterance: "He persuaded me to shoot her."[33] For the Copenhagen school of security studies, however, only the illocutionary act plays a role.[34]

By taking into account that during a speech act, "things [. . .] can be or go wrong", Austin identifies *six felicity conditions* which are required for performative speech acts to be successful:

> "first, the speech act must be in line with the 'accepted conventional procedure'

[25] Hansen, Lene and Buzan, Barry, *The Evolution of International Security Studies*, Cambridge et al., Cambridge University Press, 2009, p. 213; Floyd, Rita, *Security and the Environment. Securitisation Theory and US Environmental Security Policy*, Cambridge et al., Cambridge University Press, 2010, pp. 9-23.

[26] This overview heavily builds upon Floyd, Rita, *Security and the Environment. Securitisation Theory and US Environmental Security Policy*, Cambridge et al., Cambridge University Press, 2010, pp. 9-42.

[27] Thanks to Natalia Egorova for that point.

[28] Austin, John L., *How to Do Things with Words*, New York, Oxford University Press, 1965, p. 7.

[29] Floyd, Rita, *Security and the Environment. Securitisation Theory and US Environmental Security Policy*, Cambridge et al., Cambridge University Press, 2010, p. 11.

[30] Austin, John L., *How to Do Things with Words*, New York, Oxford University Press, 1965, p. 5.

[31] Austin, John L., *How to Do Things with Words*, New York, Oxford University Press, 1965, p. 101.

[32] Austin, John L., *How to Do Things with Words*, New York, Oxford University Press, 1965, p. 101.

[33] Austin, John L., *How to Do Things with Words*, New York, Oxford University Press, 1965, p. 101.

[34] See Wæver, Ole, 'Securitization and Desecuritization', in Lipschutz, Ronnie D., *On Security*, New York, Columbia University Press, 1995, p. 49.

> referring to the utterance itself.[. . .] Second, 'the particular persons and circumstances in a given case must be appropriate for the invocation of the particular procedure invoked'.[. . .] Third, '[t]he procedure must be executed by all participants both correctly and [fourth] completely'.[. . .] Fifth, a person participating in a speech act must be sincere in her utterance. And sixth, the enunciator of the speech act must live in accordance with the utterance subsequently."[35]

The first four felicity conditions are more powerful than the last two, which is why a breach of felicity conditions five and six has less compromising consequences than the breach of conditions one to four. In fact, if the first four conditions are reneged, one can talk about the "misfiring" of the speech act as a whole.[36] This becomes clearer by looking at Austin's own explanation:

> "a bigamist doesn't get married a second time, he only 'goes through the form' of a second marriage; I can't name the ship if I am not the person properly authorized to name it; and I can't quite bring off the baptism of penguins, those creatures being scarcely susceptible of that exploit.'"[37]

However, Jacques Derrida objects that, in speech act theory, Austin presupposes context as a fixed given. Stressing that the conditions for speech acts are continuously changing, Derrida argues that context will never be exhaustively determinable and could therefore not be theorized sufficiently.[38] He suggests that instead of studying *con*text, the analyst of speech acts should solely focus on publicly available texts. This type of discourse analysis necessarily blinds out questions about an actor's motivation for a certain speech act. Wæver supports this approach, which in his securitization theory leads to an exclusive focus on questions such as "who securitises, on what issue, under what circumstances and to what effect."[39] As Wæver put it in his own words:

> "security thinking does not mean how the actors think, which would be rather difficult to uncover—and not all that interesting. What is up for discussion here is how and what they think aloud. That is, the thinking they contribute to the public debate/political process; 'public logic'. What we investigate is the political process—

[35] Floyd, Rita, *Security and the Environment. Securitisation Theory and US Environmental Security Policy*, Cambridge et al., Cambridge University Press, 2010, p. 12.
[36] Austin, John L., *How to Do Things with Words*, New York, Oxford University Press, 1965, p. 16.
[37] Austin, John L., 'Speech Acts and Convention: Performative and Constative', in Nuccetelli, Susana and Seay, Gary (eds.), *Philosophy of Language: The Central Topics*, Lanham, Rowman & Littlefield Publishers, 2008, p. 330.
[38] See Derrida, Jacques, Signature event context, in Idem, *Limited Inc*, Illinois, Northwestern University Press, 1988, pp. 1-23.
[39] Floyd, Rita, *Security and the Environment. Securitisation Theory and US Environmental Security Policy*, Cambridge et al., Cambridge University Press, 2010, p. 16.

> not the isolated, individual formation of ideas that are afterwards put into the political interplay."[40]

### 1.1.1.2. Carl Schmitt

Another theoretical root of securitization theory has been exposed by Michael C. Williams.[41] In pointing at both Carl Schmitt's *concept of the political* and his *decisionist theory of sovereignty*,[42] Williams was among the first to argue "that in the Copenhagen School the concept of 'security' plays a role almost identical to that which Schmitt defined as his concept of 'the political.'"[43] However, one should keep in mind that, while formulating his securitization theory back in 1988, Ole Wæver was aware of, but not directly inspired by Carl Schmitt's political theory.[44]

Acknowledging that parts of Schmitt's thinking are still influential today, it is also important to point out that his work remains controversial today.[45] This is especially due to the fact that, as one of the most prominent jurists and political theorists in the third Reich, Schmitt fell prey to National Socialism.[46] In this context, Williams claimed:

> "I certainly do not want to imply that it [the Copenhagen school] is implicated in the authoritarian politics with which Schmitt (sometimes called the 'crown jurist of the Nazi Party') is often associated. [. . .] However, I do want to argue that the specificity of 'security' as a particular kind of speech-act in the work of the Copenhagen School is underpinned by an understanding of the politics of enmity, decision, and emergency which has deep roots in Schmitt's understanding of political order."[47]

Within Schmitt's broader political theory, "the concept of the state presupposes the concept of the political." In this regard, the *concept of the political* can typically be characterized as the distinction between friend and enemy—the antagonism between those who are

[40] Wæver, Ole, *Concepts of Security*, Copenhagen, Institute of Political Science, University of Copenhagen, 1997.

[41] See Williams, Michael C., 'Words, Images, Enemies: Securitization and International Politics', *International Studies Quarterly*, 47, 2003, pp. 511-31.

[42] See Schmitt, Carl, *The Concept of the Political*, Chicago, The University of Chicago Press, 2007 [1932].

[43] See Williams, Michael C., 'Words, Images, Enemies: Securitization and International Politics', *International Studies Quarterly*, 47, 2003, pp. 511-31, p. 515.

[44] See Wæver, Ole, 'The Ten Works', *Tidsskriftet Politik*, 4, 7, 2004.

[45] See, for instance, Müller, Jan-Werner, *A Dangerous Mind: Carl Schmitt in Post-War European Thought*, New Haven and London, Yale University Press, 2003.

[46] See, for instance, Gross, Raphael, *Carl Schmitt und die Juden: Eine deutsche Rechtslehre*, Frankfurt am Main, Suhrkamp Taschenbuch Verlag, 2000.

[47] Williams, Michael C., 'Words, Images, Enemies: Securitization and International Politics', *International Studies Quarterly*, 47, 2003, pp. 511-31, p. 515.

existentially threatened and those who are actually threatening.[48] This implies that a state can only endure if there is an enemy. For Schmitt, however, an enemy is not just a private adversary whom one hates (lat. *inimicus*), but rather a collective public opponent (lat. *hostis*):

> "An enemy exists only when, at least potentially, one fighting collectivity of people confronts a similar collectivity. The enemy is solely the public enemy, because everything that has a relationship to such a collectivity of men, particularly to a whole nation, becomes public by virtue of such a relationship."

This friend/enemy polarity can be found in all areas of society. Every "religious, moral, economic, ethical, or other antithesis transforms itself into a political one if it is sufficiently strong to group human beings according to friend and enemy."[49] But who has the authority to decide when a certain friend/enemy polarity has reached a sufficiently high tension (emergency situation) that would justify to take exceptional measures?

As opposed to legal positivists, Schmitt did not believe that a state could be regulated by law alone—especially not in emergency situations that have not been anticipated in advance. In his *decisionist theory of sovereignty* he thus made clear that a sovereign was needed who was above law and constitution, and who would have the power to publicly decide upon the exception in order to subsequently take emergency measures. In the Weimar Republic, such a strong role was assigned to the President of the Reich, who—through article 48 of the Weimar Constitution—held the authority to execute sole power in situations of national emergency:

> "If a state does not fulfill the obligations laid upon it by the Reich constitution or the Reich laws, the Reich President may use armed force to cause it to oblige."[50]

Convinced that the provisions of article 48 could help to relax the political tensions internal to the Weimar Republic, "Schmitt was among those who sought to strengthen the Weimar regime by trying to persuade Hindenburg to invoke the temporary dictatorial powers of article 48 against the extremes on the Right and the Left."[51]

[48] "The specific political distinction to which political actions and motives can be reduced is that between friend and enemy."

[49] See Schmitt, Carl, *The Concept of the Political*, Chicago, The University of Chicago Press, 1996, p. 37.

[50] *Constitution of the German Reich* (Weimar Constitution), art. 48, para. 1.

[51] Strong, Tracy B., 'Foreword: Dimensions of the New Debate around Carl Schmitt', in Schmitt, Carl, *The Concept of the Political*, Chicago, The University of Chicago Press, 1996, p. xv.

### 1.1.1.3. Kenneth Waltz

The third approach that sets out the foundation for securitization theory concerns International Relations scholar Kenneth Waltz. Following Floyd,[52] Kenneth Waltz matters for three reasons: his preference for *parsimonious theory*, his *understanding of security* and his *concept of capabilities*.

The first reason is meta-theoretical by nature and does not say much about what Waltz theorized in respect to International Relations (IR). More generally, it is about his understanding of economizing theory. For Waltz, theory must have clear boundaries, otherwise it gets watered down. One must be careful in what needs to be involved and strict in what is by definition outside of a theory. As Waltz points out:

> "The construction of theory is a primary task. One must decide which things to concentrate on in order to have a good chance of devising some explanations of the international patterns and events that interest us. To believe that we can proceed otherwise is to take the profoundly unscientific view that everything that varies is a variable."[53]

Recalling the discussion on either including context in speech act theory (as suggested by Austin) or excluding it (as objected by Derrida), it should be clear now, why Wæver—in support for Derrida's approach—ultimately kept context outside of his securitization theory:

> "the inclusion of context (though perhaps drawing a clearer picture of the world than securitisation theory currently can) would change the theory beyond recognition, moving the focus away from the act that is securitisation, towards a causal theory of securitisation instead."[54]

The second reason why Waltz matters for securitization theory derives from his understanding of *security*. In his seminal work *Theory of International Politics* Waltz suggested anarchy to be the ordering principle of the international system. Without a Leviathan, actors live in constant fear of each other and struggle to survive (*homo homini lupus*). As long as a state cannot secure its own existence in face of anarchy, it will ultimately stop to exist.[55] This understanding also gained support in securitization theory. The fact that security is ultimately about survival implies here that speaking security not only means that

[52] Floyd, Rita, *Security and the Environment. Securitisation Theory and US Environmental Security Policy*, Cambridge et al., Cambridge University Press, 2010, p. 19-23.

[53] Waltz, Kenneth, *Theory of International Politics*, New York, Random House, 1979, p. 16.

[54] Wæver in Floyd, Rita, *Security and the Environment. Securitisation Theory and US Environmental Security Policy*, Cambridge et al., Cambridge University Press, 2010, p. 21.

[55] See Waltz, Kenneth, *Theory of International Politics*, New York, Random House, 1979, p. 126.

something is threatened, but—more urgently—something is threatened *existentially*. Only by referring to an *existential threat*, extraordinary measures can eventually be legitimately taken:

> "The special nature of security threats justifies the use of extraordinary measures to handle them. The invocation of security has been the key to legitimizing the use of force, but more generally it has opened the way for the state to mobilize, or to take special powers, to handle existential threats. Traditionally, by saying 'security', a state representative declares an emergency condition, thus claiming a right to use whatever means are necessary to block a threatening development"[56]

Lastly, Waltz is important here because of his concept of capabilities. In anarchy, a state best secures its survival by increasing its power. It essentially does so by extending its capabilities. For Waltz these include material factors such as the size of population and territory, resource endowment, economic capability, military strength, political stability and competence.[57] The more capabilities a state has at its disposal, the more powerful it is and the less likely it can be brought down by other states.

While supplementing Waltz's concept of capabilities with *social* (social networks of relationships) and *cultural factors* (e.g., knowledge, skills or education),[58] also securitization theory makes use of this idea. Similar to Waltz' theory of international politics (where not everyone has the capability to *survive*) in securitization theory not everyone has the capability to *perform a successful speech act*:

> "The more capabilities a securitizing actor has, the more likely will this actor be to succeed in an attempted securitization. In other words, who can or cannot securitize is already inscribed into the position of the actor within the social hierarchy of the system."[59]

### 1.1.2. Main Ideas

After this short side note on the Copenhagen school's theoretical origins, we can now proceed by concentrating on those ideas that seem to be relevant for the purpose of this study: *security sectors* and *securitization theory*. For a better understanding, each of them

[56] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 27.

[57] See Waltz, Kenneth, *Theory of International Politics*, New York, Random House, 1979, p. 131.

[58] See Bourdieu, Pierre, 'The forms of capital', in Richardson, John G. (ed.), *Handbook of Theory and Research for the Sociology of Education*, New York, Greenwood, 1986, pp. 241-258.

[59] Floyd, Rita, *Security and the Environment. Securitisation Theory and US Environmental Security Policy*, Cambridge et al., Cambridge University Press, 2010, p. 22.

shall be presented here roughly.

#### 1.1.2.1. Security Sectors

Through applying a constructivist view of security as a discursive construct—*where by saying something, something is being done*—the Copenhagen school does not only challenge the traditionalists' concept of "real" and "objectively" existing threats, but also goes beyond their exclusive focus on military security. As mentioned above, the two schools agree that the main form (or logic) of security is *survival in the face of an existential threat*. However, instead of equating this overarching security form with military security, the Copenhagen school argues that military security is but one possible sub-form within a wider security spectrum:

> "Security is a generic term that has a distinct meaning but varies in form. Security means survival in the face of existential threats, but what constitutes an existential threat is not the same across different sectors."[60]

The desire to conceptualize security across multiple sectors must be understood in light of the widespread dissatisfaction during the 1980s to view international security almost exclusively through the traditionalists' military lens. Members of the Copenhagen school and proponents of other widening debates (including *constructivism*, *post-colonialism*, *human security*, *critical security studies* and *poststructuralism*[61]) claimed that nonmilitary aspects such as international economics, energy and resources, climate and ecology, as well as transnational drug trade and demography also had some relevance for the field of international security studies. However, it was not before the end of the Cold War—when the threat of *Mutually Assured Destruction* (MAD) was perceived to be contained—that the analytical widening of the field was generally accepted.[62] Along with the *military sector*, in the 1990s the Copenhagen school thus identified four more sectors that could be applied by security analysts. Originally, these included an *environmental*, *economic*, *societal* and *political sector*. However, as will be mentioned in one of the later sections, this set has recently been extended by both a *humanitarian*[63] and a *cyber sector*.[64]

[60] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 27.

[61] See Hansen, Lene and Buzan, Barry, *The Evolution of International Security Studies*, Cambridge et al., Cambridge University Press, 2009, pp. 187-225.

[62] See, for instance, Buzan, Barry, 'Rethinking Security after the Cold War', *Cooperation and Conflict*, 32, 1, pp. 5-28, 1997.

[63] See Watson, Scott, 'The 'human' as referent object? Humanitarianism as securitization', *Security Dialogue*, 42, 1, 2011, pp. 3-20.

Understanding security along different sectors is not to say that these sectors should be perceived as totally detached from each other. They should rather be seen as "analytical lenses" through which one can focus on world affairs.[65] For instance, if, in a given conflict, war were "a mere continuation of politics by other means,"[66] exclusively applying the *military* lens for looking at the conflict would potentially blind out the underlying *political* logic.[67] For analysts it is therefore necessary to apply the most suitable lens through which to scrutinize specific issues.

Dividing international security into multiple security discourses has proved to be a useful analytical device to facilitate security analysis.[68] However, speaking in terms of philosophy of science, their theoretical roots and ontological standing have long remained rather vague. In an attempt to push sectors beyond their analytical quality and put them onto more solid ground, Albert and Buzan have recently[69] suggested to link them to the sociological framing of "functional differentiation."[70]

Since each of the five originally defined sectors differ in their respective *security agenda*, *units of analysis*, and *sub-forms of security*, it is useful to look at them in more depth. In doing so, the following subsections will provide an introduction to each of the sector-specific *security agenda*. For illustrative purposes, the characteristic *units of analysis* and *sub-forms of security* are set out in the context of the section on securitization. In order to deliver a clear overview, however, these observations are drawn together in a table attached to the closing synthesis.

[64] See Hansen, Lene and Nissenbaum, Helen, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53, 2009, pp. 1155-75.

[65] See Buzan, Barry et al., *The Logic of Anarchy: Neorealism to Structural Realism*, New York, Columbia University Press, 1993, p. 31.

[66] Clausewitz, Carl von, *On War*, London, Penguin Books, 1982 [1832], p. 119.

[67] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 166f.

[68] See, for instance, Collins, Alan, *Contemporary Security Studies*, New York, Oxford University Press, 2010, pp. 167-217.

[69] See Buzan, Barry and Albert, Mathias, 'Differentiation: A sociological approach to international relations theory' *European Journal of International Relations*, 16, 3, 2010, pp. 315-337; Albert, Mathias and Buzan, Barry, 'Securitization, sectors and functional differentiation', *Security Dialogue*, 2011, 42, 4-5, pp. 413-25.

[70] According to the *theory of differentiation*, society can be segmented into a set of relatively autonomous realms that operate according to their own logic (e.g., politics, economics, law, art, science,…). Depending on the theoretical approach of functional differentiation (*communication*- vs. *agent-based*), these realms can either be defined by the specific basal code in which communication is conducted (e.g., "legal/illegal" in the legal system, "having power/not having power" in the political system, "believing/non-believing" in the religious system, "true/false" in the scientific system,…) or by the specific milieus in which people perceive themselves (e.g., whether they regard themselves as primarily operating in an economic, political or military setting).

### 1.1.2.1.1. Military Sector

The military sector is traditionally considered to be a state domain which is shaped by the instruments of force a state has at its disposal. However, the security agenda can be split into a domestic (or *internal*) dimension on the one hand, and an interstate (or *external*) dimension on the other one.

At the *internal level*, the military sector touches upon the maintenance of civil order and peace. These properties can be threatened by a variety of different actors, such as militant separatists, rebels, terrorists and other actors opposed to the respective state authority:

> "When the perceived threat is internal, military security is primarily about the ability of the ruling elite to maintain civil peace, territorial integrity, and, more controversially, the machinery of government in the face of challenges from its citizens."[71]

At the *external level*, the military sector is about the state's territorial integrity towards other actors within the international system. Here, the security agenda is primarily concerned about how states equip themselves to use force, and how this "arms race" is perceived by other states:

> "When securitization is focused on external threats, military security is primarily about the two-level interplay between the actual armed offensive and defensive capabilities of states on the one hand and their perceptions of each other's capabilities and intentions on the other."[72]

### 1.1.2.1.2. Environmental Sector

In the environmental sector the difference between the *scientific agenda* on the one hand, and the *political agenda* on the other, has been defined as a distinctive feature:

> "The scientific agenda is about the authoritative assessment of threat for securitizing or desecuritizing moves, whereas the political agenda deals with the formation of concern in the public sphere about these moves and the allocation of collective means by which to deal with these issues raised."[73]

[71] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 50.

[72] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 51.

[73] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 72.

Although this division can also be found in other security sectors, the exceptional complexity of environmental issues as well as their far-reaching linkages and potential consequences intensify the need for political actors to rely on the expertise of an environmental scientific community:

> “The particular difficulty in dealing with the cumulative global effects of local developments, as well as in many cases threat assessment within a time frame beyond present generations, causes this specific form of dependence upon scientific authority.”[74]

The *scientific agenda* is embedded in scientific discourse and constructed outside the core of politics.[75] It is formulated by a transgovernmental and transnational “network of professionals with recognized expertise and competence in a particular domain and an authoritative claim to policy-relevant knowledge within that domain or issue-area.”[76] While the professionals of such a network can have different disciplinary backgrounds, epistemically speaking, they must share a common set of established academic standards (e.g., shared causal beliefs or notions of validity). This is why in international relations theory these networks have been referred to as “epistemic communities.”[77] In this respect, the environmental epistemic community sets out a wide spectrum of issues and communicates them to the press as well as to political elites. Such issues can range from the disruption of ecosystems and civil strife to energy, population, food, and economic problems.[78]

The *political agenda*, on the other hand, is embedded in the wider public discourse and constructed by “governmental, media, and public standards which are influenced much more by short-term events.”[79] It can be formulated by a governmental and intergovernmental community, and includes public policies addressing the issues that have already been set out in the scientific agenda. In this regard, the political agenda is about three areas:

[74] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 72.

[75] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 71f.

[76] See Haas, Peter M., ‘Introduction: Epistemic Communities and International Policy Coordination’, *International Organization*, 46, 1, 1992, pp. 1-35, p. 3.

[77] See Haas, Peter M., ‘Introduction: Epistemic Communities and International Policy Coordination’, *International Organization*, 46, 1, 1992, pp. 1-35.

[78] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 74f.

[79] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 73.

> “(1) state and public awareness of issues on the scientific agenda (how much of the scientific agenda is recognized by policymakers, their electorates, and their intermediaries—the press); (2) the acceptance of political responsibility for dealing with these issues; and (3) the political management questions that arise: problems of international cooperation and institutionalization—in particular regime formation, the effectiveness of unilateral national initiatives, distribution of costs and benefits, free-rider dilemmas, problems of enforcement, and so forth.”[80]

Despite their characteristic distinction, both are highly interdependent and often overlap in public discourse.[81] Moreover, it is important to note that in the early phases of regime building, scientific actors play a crucial role in political agenda-setting. When a new topic arises at the political horizon, uncertainty about the potential outcomes of political action is relatively high. This increases the chances for epistemic communities to get involved in politics and enhances their power to put their own issues on the political agenda:

> “These actors are often involved in both science and politics: for example, scientists who are attentive to political logic—for instance, who are aware of the necessity to develop scientific consensus positions—but who are also obliged to avoid being stabbed in the back scientifically. Typically, these actors will link up with political actors who have specialized in relating to the field of science; thus, a chain forms from science to politics without the two having to meet in their pure forms [. . .].”[82]

### 1.1.2.1.3. Economic Sector

The economic sector offers a wide range of highly politicized debates. These are deeply rooted in the controversies among a diverse set of ideological positions, with each stressing its specific agenda of preferred issues:

> “The main contending positions reflect different views about whether states and societies or markets should have priority and whether private economic actors have security claims of their own that must be weighed against the verdict of the market.”[83]

[80] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 72.

[81] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 72.

[82] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 73.

[83] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 95.

Referring to the discipline of *international political economy* (IPE)—which examines both states *and* markets—the Copenhagen school identifies *(neo-)mercantilist*, *liberal*, and *socialist doctrines* as the three most defining ideological positions within the economic sector:[84]

The *(neo-)mercantilist doctrine* gives state intervention priority over the free play of market forces. It is based on the assumption that the international economic system can be described as a *zero-sum game*: the benefit of one state equals the loss of another one. Thus, in terms of international trade, government intervention had to encourage exports while, at the same time, restricting imports as much as possible. By having exports exceeding imports, the resulting trade surplus guaranteed economic security insofar as the generated wealth could be used for national purposes (such as war and conquest).

As opposed to the (neo-)mercantilist ideology, the *liberal doctrine* argued in favour of the free play of market forces. Economic relations are seen as a *non-zero-sum game* in which every merchandizing party potentially benefits. Instead of regulating trade, the state should provide basic institutions (such as the military, police and courts) that enable individuals to move safely between national economies.

The *socialist doctrine* lies somewhat in between the two previously mentioned ideological positions. It basically agrees that the economy is an essential part of the social system. Nonetheless, considered by itself, the free play of market forces does not guarantee a beneficial outcome for everyone. Therefore, the state needs to control the economy up to the point where justice and equity can sufficiently be assured.

Having identified the three most eminent economic ideologies, it is important to add that in the aftermath of the Cold War, the discourse on economic security was pre-eminently shaped by a liberal agenda including security issues such as the ability of states to sustain military capabilities independently from the global market, the economic dependence of states on foreign (scarce) resources, the worries that the global market would generate inequalities, the illegal trade in drugs and weapons (especially those of mass destruction), and the fears that systematic crisis could trigger government intervention.[85]

[84] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 95f.

[85] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 98.

### 1.1.2.1.4. Societal Sector

The societal or socio-cultural[86] sector is about the security of a collective "we" identity. It is about the subjective feeling of together constituting an entity; be it a small group of people (such as a family, friends, or sports teams), a community (such as "we artists"), a nation (such as "we Austrians"), or a civilizational and religious identity (such as "we Europeans," or "we Muslims").[87] However, the societal sector is neither about social security (which is basically about individuals and their economic status), nor is it about the population of a specific state (which only applies to the people who physically live within a relevant territory). Likewise, the notion of "nation" does not always refer to the same concept of collective identity. Sometimes a nation can be defined by language, other times by blood or culture.[88] Therefore,

> "[f]or international security analysis, the key to society is those ideas and practices that identify individuals as members of a social group. Society is about identity, the self-conception of communities and of individuals identifying themselves as members of a community. [. . .] Definitional, societal security is about large, self-sustaining identity groups; what these are empirically varies in both time and place."[89]

With the collective identity, also the security agenda changes through different eras and regions. However, the most common issues that have often posed threats to societal security can be summarized as *migration* (identity is changing due to a shift in the composition of members of a community), *horizontal competition* (identity is changing due to the *unintended* effects posed by another identity), *vertical competition* (identity is changing due to the *intended* effects posed by another identity), and *depopulation* (identity is changing due to plague, war, famine or natural catastrophe).[90]

### 1.1.2.1.5. Political Sector

The political sector is the widest of all sectors: "In some sense, all security is political."[91]

[86] See Buzan, Barry and Little, Richard, *International Systems in World History*. Oxford, Oxford University Press, 2000, p. 73.

[87] Wæver, Ole et al., *Identity, Migration and the New Security Agenda in Europe*, Pinter Publishers Ltd., London, 1993, p. 17f.

[88] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 120.

[89] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 119.

[90] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 121.

[91] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 141.

Thus, it is crucial to be clear about what exactly is meant by the terms *politics* and *political security*. Broadly speaking, politics can be defined as "the shaping of human behavior for the purpose of governing large groups of people."[92] In reference to Machiavelli, this process of *shaping* can be characterized as "a continuous struggle to establish the quasi-permanence of an ordered public realm within a sea of change."[93] For the Copenhagen school, such a *quasi-permanent* (or stable) order can imply any kind of *political unit*, described as "collectivity that has gained a separate existence distinct from its subjects"[94] (such as tribes, firms, churches, states or empires), and any form of *political patterns* (such as structures, processes, and (interunit) institutions like the international society[95] or international law).[96]

In this context, the political security agenda is basically about *ensuring* organizational stability. It is about *framing* politics through both internal and external recognition:

> "the critical variables are obviously the recognition of such an arrangement from within and without that lends it legitimacy and thereby the stability needed for political activities to be framed by it rather than to be about it."[97]

Similar to the military sector, one can distinguish between internal and external issues. While internal issues might include the constitutive ideas defining a political unit or pattern, external issues can contain questions about the recognition or non-recognition of quasi-states such as the Palestine Liberation Organization.[98]

### 1.1.2.2. Securitization

It is worthwhile recalling what we already know from the above mentioned: Instead of focussing on objective threats that exclusively arise within the narrow scope of the military sector, the Copenhagen school looks at security as an inter-subjective process by which a

[92] Buzan, Barry et al., *The Logic of Anarchy: Neorealism to Structural Realism*, New York, Columbia University Press, 1993, p. 35.

[93] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 144.

[94] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 143.

[95] As defined by Buzan, Barry, *From International to World Society? English School Theory and the Social Structure of Globalisation*, Cambridge, Cambridge University Press, 2004, p. xvii: "situations in which the basic political and legal frame of international social structure is set by the states-system, with individuals and TNAs [transnational actors] being given rights by states within the order defined by interstate society."

[96] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 143f.

[97] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 144.

[98] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 144f.

powerful actor discursively constructs an issue as an existential threat to a referent object within a specific security sector in order to legitimately employ extraordinary measures. As the shorthand for this description, Ole Wæver came up with the term *securitization*, which he defined as follows:

> "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. By saying the words, something is done (like betting, giving a promise, naming a ship). What we can study is this practice: Who can 'do' or 'speak' security successfully, on what issues, under what conditions, and with what effects?"[99]

However, by definition, a performative speech act alone does not create an instance of successful or "complete securitization."[100] The mere utterance whereby a securitizing actor identifies a referent object as being existentially threatened just constitutes a *securitizing move*. Only if this attempted securitization is also accepted by a relevant audience, securitization is complete:

> "We do not push the demand so high as to say that an emergency measure has to be adopted, only that the existential threat has to be argued and just gain enough resonance for a platform to be made from which it is possible to legitimize emergency measures or other steps that would not have been possible had the discourse not taken the form of existential threats, point of no return, and necessity. If no signs of such acceptance exist, we can talk only of a securitizing move, not of an object actually being securitized."[101]

Once an issue is successfully securitized it is elevated from the normal run of political practice to a level of existential immediacy. The reason for an actor to perform a securitization is to break free from procedures and rules he would otherwise be bound to. Once an issue is successfully moved to the realm of emergency politics, the securitizing actor can legitimately employ extraordinary measures to deal with it. In this way,

> "[s]ecurity is the move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics.

[99] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 26.

[100] Floyd, Rita, *Security and the Environment. Securitisation Theory and US Environmental Security Policy*, Cambridge et al., Cambridge University Press, 2010, p. 1.

[101] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 25.

Securitization can thus be seen as a more extreme version of politicization."[102]

In order to distinguish securitized issues from non-securitized issues, the Copenhagen school provides a spectrum along which one can find different issue categories: If security issues "do not command political and/or media attention and [. . .] are regulated through consensual and technical measures,"[103] they can be categorized as *non-politicized*.[104] If, at some point, issues "are devoted to close media and political scrutiny, generating debate and usually multiple policy approaches, while not commanding the threat-urgency modality of securitization,"[105] one can refer to them as being *politicized*.[106] Moreover, if an issue "is presented as an existential threat, requiring emergency measures and justifying actions outside the normal bounds of political procedure"[107] it is considered to be *securitized*.

This resulting spectrum does not presuppose a mandatory sequence where an issue can only be securitized after first having been successfully elevated from the non-politicized to the politicized level. In environmental security, for instance, issues can immediately be securitized coming from outside any political or media attention. Moreover, it is important to add that, for an issue to be either politicized or securitized, it does not necessitate a state to do so. In fact, both "politicization as well as securitization can be enacted in other fora as well."[108]

Whether an issue becomes securitized or not is a matter of politics. Recalling one of the definitions delivered in the opening section, *security is what states make it*. Essentially, this means that actors have a choice about what they do with a certain issue: They can ignore it, deal with it as part of political routine or present it as an existential threat. For the Copenhagen school, however, securitization is not a desirable condition—quite the contrary.

[102] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 24.

[103] Hansen, Lene and Nissenbaum, Helen, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53, 2009, pp. 1155-75, p. 1159.

[104] This definition departs from the original one, "meaning the state does not deal with it and it is not in any other way made an issue of public debate and decision", in Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 23.

[105] Hansen, Lene and Nissenbaum, Helen, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53, 2009, pp. 1155-75, p. 1159.

[106] This definition departs from the original one, "meaning the issue is part of public policy, requiring government decision and resource allocation or, more rarely, some other form of communal governance", in Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 23.

[107] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 23f.

[108] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 24.

Wæver demands “Less security, more politics!”,[109] and claims:

> “Our belief [. . .] is not ‘the more security the better.’ Basically, security should be seen as negative, as a failure to deal with issues as normal politics. Ideally, politics should be able to unfold according to routine procedures without this extraordinary elevation of specific ‘threats’ to a prepolitical immediacy.”[110]

Nonetheless, sometimes it might be useful to securitize an issue for tactical reasons. Again, this is especially true for the environmental sector, where securitization is often conceived as the only way how an issue could publicly receive the attention needed to deal with it at all. However, in the long-run it is more desirable to politicize issues and thus remove them from emergency politics to public discourse. This is why the Copenhagen school introduces a fourth category of issues referred to as *desecuritized issues*, meaning issues that are removed from the emergency status into political discourse.[111]

The size or significance of an instance of securitization can vary. A way to measure and thus distinguish important cases of securitization from unimportant ones is to look at the cascading effects a securitization has on other security issues and securitizations. The more chain reactions a securitization provokes within and across sectors, the more important it can be considered to be.[112]

For the Copenhagen school, security analysis is mostly interested in successful instances of (de)securitization. However, it also acknowledges unsuccessful and partially successful cases of (de)securitization. These instances are interesting

> “primarily for the insights they offer into the stability of social attitudes toward security legitimacy, the process by which those attitudes are maintained or changed, and the possible future direction of security politics.”[113]

Lastly, securitization can either occur *ad hoc* or *institutionalized*.[114] Since many

[109] Wæver, Ole, “Securitization and Desecuritization”, in Lipschutz, Ronnie D. (ed.), *On Security*, pp. 46-86. New York: Columbia University Press, 1995.

[110] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 29.

[111] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 29.

[112] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 25-6.

[113] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 25.

[114] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 27.

environmental issues are still relatively new and controversially discussed, they are securitized if needed and have not yet become a conventional practice. If, by contrast, a threat is perceived to be persistent and recurrent, they become institutionalized. This is most obvious in the military sector "where states have long endured threats of armed coercion or invasion and in response have built up standing bureaucracies, procedures, and military establishments to deal with those threats."[115] In the case of institutionalized securitizations, threats have lost both their surprising effect and their dramatic flavor. However, as opposed to desecuritization, institutionalized securitizations still operate in the threat/urgency mode.

### 1.1.2.2.1. Facilitating Conditions

Based on Austin's *felicity conditions*, Wæver identifies three *facilitating conditions*[116] which he defines as "conditions under which the speech act works, in contrast to cases in which the act misfires or is abused."[117] However, as opposed to the felicity conditions set out by Austin, Wæver's facilitating conditions cannot be subdivided into conditions that facilitate a speech act more powerfully than others. Instead, the Copenhagen school implicitly assumes the unexceptional fulfillment of all three conditions.[118]

The first condition relates to the "logical, rhetorical or semiotic structure"[119] of the speech act. This does not imply that the securitizing actor needs to use the word "security" correctly, but that he has to follow the main form of security and "construct a plot that includes existential threat, point of no return, and a possible way out."[120] However, since the security form can vary across different security sectors, the securitizing actor needs to apply the sector-specific sub-form or *grammar of security*. If this requirement is not met, the relevant audience will have trouble to understand the attempted securitization correctly and the speech act will consequently misfire. The different plots or narratives within the specific security sectors can be summed up as follows:

1. In the *military sector*, the characteristic plot is mainly focused on sovereignty and has

[115] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 27f.

[116] See Wæver, Ole, 'Securitisation: Taking Stock of a Research Programme in Security Studies', *unpublished manuscript*, 2003, pp. 14-15; and Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 32f.

[117] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 32.

[118] See Floyd, Rita, *Security and the Environment. Securitisation Theory and US Environmental Security Policy*, Cambridge et al., Cambridge University Press, 2010, p. 14.

[119] See Waever, Ole, 'European Security Identities,' *Journal of Common Market Studies*, 34, 1, 1996, pp. 2120-132, p. 106.

[120] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 33.

traditionally been constructed around military force (e.g., the opponent's army), geography (e.g., closeness[121] and terrain[122]), history (e.g., past experiences and present perceptions) and politics (e.g., contradicting ideologies, recognition and status).[123]

2. In the *environmental sector*, the characteristic plot is mainly focused on sustainability and built around nature-caused threats (e.g., earthquakes), human-caused threats that seem to cause existential damage to civilization (e.g., CFCs[124]), and human-caused threats that do not seem to cause existential damage to civilization (e.g., the depletion of minerals that can be replaced by alternative substances, such as copper by silicon, or metal by ceramics).[125]
3. In the *economic sector*, the plot has traditionally been focused on the sovereign economy and constructed around different actors: For individuals, the security logic can be constructed around basic human needs (e.g., adequate food, water, clothing, shelter, education). When speaking about firms, one can refer to risks of boycotts and risks of investment. When enquiring into the economic security of states, an analyst might be interested in state bankruptcy.[126] Traditionally, however, security policy in the economic sector can mainly be found in relation to state sovereignty. As already mentioned, a firm, for instance, rarely has a legitimate right to survive through itself, but only through its link to the state's claim to survive as a sovereign economy (e.g., a company employing a critical mass of citizens).[127]
4. In the *societal sector*, the plot is mainly focused on identity: "If a society is no longer itself, it has not survived."[128] The narrative can be constructed in manifold ways. If the social identity is based on separateness, for instance, foreigners can potentially be seen as threatening. If, by contrast, identity is tied to specific cultural habits, foreign cultural habits (e.g., McDonald's) can be perceived as threatening. Furthermore, if identity is constructed around a certain language (e.g., French),

[121] The closer, the more dangerous.

[122] Flat land can be occupied more easily than mountains.

[123] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 57-61.

[124] Chlorofluorocarbon.

[125] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 79-84.

[126] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 103-9.

[127] See Waever, Ole, European Security Identities, Journal of Common Market Studies, 34, 1, 1996, pp. 2120-132, p. 109.

[128] See Waever, Ole, European Security Identities, Journal of Common Market Studies, 34, 1, 1996, pp. 2120-132, p. 109.

English as the contemporary *lingua franca* can possibly pose a societal threat.[129]

5. In the *political sector*, the security plot is focused on sovereignty and has traditionally been built around the idea of the state (including organizing ideologies such as democracy, capitalism or communism), its governing institutions (containing the legislative, administrative and judicial bodies, as well as the laws, procedures and norms by which they operate), and the physical base at its disposal (implying both the population and the territory).[130]

The second facilitating condition is connected to the *authority of the securitizing actor*. The ability of a securitizing actor to conduct a successful securitization depends upon the social position he holds.[131] His position in the social hierarchy defines his relationship to the relevant audience. This relationship is shaped by the capabilities of the enunciator. As was mentioned earlier, *the more capabilities a securitizing actor has, the more likely will this actor be to succeed in an attempted securitization. In other words, who can or cannot securitize is already inscribed into the position of the actor within the social hierarchy of the system*.

Finally, the third condition is *threat* related. It is more likely for a security threat to be invoked if the issues that are referred to as threatening are commonly conceived as such (e.g., tanks, hostile sentiments, or polluted waters); although, inter-subjectively speaking, such objects "never make for necessary securitization"[132] themselves.

### 1.1.2.2.2. Levels of Analysis

Securitizations can essentially be examined along the traditional IR spectrum of different levels of analysis including the *micro* (individual), *meso* or *middle* (unit), and *macro level* (system). However, as opposed to the traditionalists' state centrism in international security studies—emphasizing *statesmen* (at the micro level), the *state* (at the meso level), and the *interstate system* (at the macro level)[133]—, the Copenhagen school argues in favor of a more comprehensive framework that accounts for both state and non-state actors. It holds that

[129] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 124-26.

[130] Buzan, Barry, *People, States and Fear: An Agenda for International Security Studies In the Post-Cold War Era*, Harvester Wheatsheaf, 1992, pp. 36-65.

[131] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 33.

[132] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 33.

[133] See, most prominently, Waltz, Kenneth Neal, *Man, the State and the War. A Theoretical Analysis*, New York, Columbia University Press, 1954.

"[t]here is no necessity for levels to privilege states"[134] and concedes:

> "We have designed our theory so that it can accommodate nonstate actors, and even allow them to be dominant."[135]

However, even though the Copenhagen school rules out the idea that states are the only significant actors in international security analysis, it does not go so far as to argue in favor of a concept of *individual security*. Rather, it "still privileges collective security concepts"[136] where one collective entity differentiates itself from a collective Other. As will become clear in the six-tiered categorization presented below, this theoretical preference reaches its limits both at the bottom (with the individual lacking the "collective" component) and at the top end (with the total collective Self of humankind lacking the opposition of an "Other"). With this in mind, the Copenhagen school sets out the following six levels of analysis:[137]

1. Individual level: Individual actors are at the very bottom end of any security analysis.[138] However, the Copenhagen school maintains that "the individual himself is in no position to provide for his own security."[139] They will seldom claim security legitimacy in their own right because they "do not appear in political discourse as free-standing entities, but with gendered, racial, religious, class, and other collective identities."[140]
2. Subunit level: Similar to individuals, small groups at the subunit level seldom hold a legitimate claim to survival. Here, one can find bureaucracies, and political regimes as well as firms and lobbies. As mentioned in the opening section, these groups *could try to establish a claim to survival and thus to security legitimacy, but empirically this is not usually possible*. However, they can unfold the power to affect the (de)securitizations of their superior unit level.
3. Unit level: At the unit level individual collectivities engage in interdependent

[134] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 7.

[135] Buzan, Barry and Wæver, Ole, *Regions and Powers. The Structure of International Security*, Cambridge, Cambridge University Press, 2003, p. 12.

[136] Hansen, Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53, 2009, pp. 1155-75, p. 1159.

[137] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 5-7; Barry and Wæver, Ole, 'Macrosecuritization and security constellations: reconsidering scale in securitization theory', *Review of International Studies*, 35, 2009, p. 259.

[138] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 36.

[139] Floyd, Rita, 'Human Security and the Copenhagen School's Securitization Approach: Conceptualizing Human Security as a Securitizing Move', *Human Security Journal*, 5, 2007, pp. 38-49.

[140] Hansen, Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53, 2009, pp. 1155-75, p. 1160.

securitizations with each other. Here, the audiences have been coherent, and the processes of differentiation powerful enough to establish strong interpretive communities that are able to construct their own Self/Other, or friends/enemies perceptions ("we" feeling). Traditionally, the unit level was limited to states and nations, but can also include transnational actors (TNAs) such as multinational corporations, international non-governmental organizations (INGOs), mafias and terrorist groups as well as anti-nuclear and anti-globalization groups.[141] This level has long been the focal point for mainstream IR analysis. However, due to advancing regional and international dynamics, higher levels of analysis have also gained attention.

4. Subsystem level: The subsystem level is mainly about different groups of units interacting with each other within the international system. It accounts for different groups of units that can either be territorially coherent (e.g., regional security complexes) or not (e.g., OECD or AOSIS).
5. System level: The system level is about the interplay between units, subsystemic groups of units and great-powers building their respective Self/Other perceptions. "Currently, this level encompasses the entire planet, but in earlier times several more or less disconnected international systems existed simultaneously,"[142] such as the relatively free-standing international systems of the "warring states" period in China (ca. 403-221 BC) or the Ganges valley civilization between the seventh and the fourth centuries BC.[143] Since before 1500 "the global level was not strong enough to generate a global world system",[144] these "separate systems were not regions (subsystems) but really *worlds*."[145]
6. Global level: The global level is the top end of any (contemporary) security analysis. It is the overarching level "where the absence of an Other makes it difficult to securitize the total collective Self of humankind."[146] It is about the physical fate of humankind as a whole, and can incorporate concerns about nuclear weapons as well as global warming.

[141] See, for instance, Buzan, Barry, *From International to World Society? English School Theory and the Social Structure of Globalisation*, Cambridge, Cambridge University Press, 2004, pp. 118-38.

[142] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 5f.

[143] See Buzan, Barry and Little, Richard, 'The Idea of 'International System': Theory Meets History', *International Political Science Review*, 15, 3, 1994, pp. 231-255.

[144] Buzan, Barry and Wæver, Ole, *Regions and Powers. The Structure of International Security*, Cambridge, Cambridge University Press, 2003, p. 14.

[145] Buzan, Barry and Wæver, Ole, *Regions and Powers. The Structure of International Security*, Cambridge, Cambridge University Press, 2003, p. 14.

[146] Barry and Wæver, Ole, 'Macrosecuritization and security constellations: reconsidering scale in securitization theory', *Review of International Studies*, 35, p. 256.

If, at some point, the collective Self of humankind happens to perceive "unknown unknowns"[147] such as "Alien Others" (perhaps even similar to those depicted in *Star Trek*), "Robot Others" (like those anticipated in *Battlestar Galactica*)[148] or zombies (famously appearing in movies such as *Night of the Living Dead*)[149] as threats to its very existence, this six-tiered categorization might be further expanded. However, even though UFOs already appear to threaten "anthropomorphic sovereignty,"[150] for the purpose of this study, the world provides a sufficient framework to analytically distinguish between *micro* (individual and subunit), *middle* (unit) and *macro level* (subsystem, system and global).

### 1.1.2.2.3. Units of Analysis

In securitization theory, one distinguishes between three different units of analysis: *referent objects*, *securitizing actors*, and *functional actors*.[151] These will be presented here briefly. For a better illustration, the unit's theoretical characteristics shall be complemented by examples from the respective sectors.

Historically, international security studies have mainly focused on the state as the one and only unit of analysis. However, by acknowledging that the state still occupies a privileged standing within the discipline, the Copenhagen school intentionally sets out a very broad definition of what they understand a referent object should be defined as. In this context, *referent objects* have been characterized as

> "things that are seen to be existentially threatened and that have a legitimate claim to survive. [. . .] The referent object is that to which one can point and say, 'It has to survive, therefore it is necessary to…'."[152]

Referent objects can be found at the *micro level* (individuals and small groups speaking for themselves), the *middle level* (collectivities such as states, nations, or civilizations), and the

[147] Rumsfeld, Donald, *DoD News Briefing—Secretary Rumsfeld and Gen. Myers*, February 12, 2002, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2636.

[148] For a discussion on *Star Trek* and *Battlestar Galactica* being pre-9/11 expressions of an optimistic and outgoing America searching for the "last frontiers" see Buzan, Barry, 'America in Space: The International Relations of Star Trek and Battlestar Galactica', *Millennium: Journal of International Studies*, 39, 1, 2010, pp. 175-180.

[149] See, for instance, Drezner, Daniel W., *Theories of International Politics and Zombies*, New Jersey, Princeton University Press, 2011.

[150] For a discussion on UFOs posing a threat to anthropomorphic sovereignty see Wendt, Alexander and Duvall, Raymond, 'Sovereignty and the UFO', *Political Theory*, 36, 4, 2008.

[151] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 35-42.

[152] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 36.

*macro level* (such as the nature, humankind, international working class, liberal world economy or free trade). At the micro and macro level it is very difficult to legitimately establish a right for protection. Individuals and small groups rarely have the necessary legitimacy to speak security effectively. Similarly, at the global level it is still a challenge to securitize issues across nations:

> "Somehow the system-level candidates are still too subtle and indirect to trigger the levels of mass identity necessary for securitization."[153]

However, over the last centuries actors at the middle level have been most successful in securitizing issues. Directly referring to Michel Foucault's idea about a "site of judgment,"[154] for the Copenhagen school this is especially due to the fact that each unit at the middle level can successfully form a "we" that serves as an interpretive community which can clearly identify itself as opposed to others. The most prominent referent objects proposed by the Copenhagen school can be read as follows:

1. In the *military sector*, the most important referent object is the state which is narrowly defined as the single holder of military power. Also, would-be states claiming a status as actors at the unit level can fall within this category. The same is true for actors at the subsystem or system levels (e.g., WEU/EU, NATO).[155]
2. In the *environmental sector*, the ultimate referent object is not the nature or "Mother Earth" itself, but human enterprise that would perish without it. Therefore, it is not crucial to maintain the global ecosystem as such, but to do so because mankind is dependent upon it: "The earth has been in its place for billions of years, and what has been happening on its crust since, say, the Industrial revolution is rather unimportant.[156] [. . .] Thus, in the environmental sector two different kinds of referent objects represent two wings within the environmental movement: the environment itself and the nexus of civilization and environment."[157]
3. In the *economic sector*, referent objects can include individuals, classes, states, firms, and the liberal international economic order. The most important ones, however, are

[153] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 37.

[154] See Foucault, Michel, *Discipline and Punish: The Birth of Prison*, New York, Vintage Books, 1979.

[155] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 52-5.

[156] This includes nuclear winter, global warming, a hole in the ozone layer as well as the disappearance of dinosaurs.

[157] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 76-7.

firms that search protection through states and the liberal economic order.[158]

4. In the *societal sector*, the referent object is the collective identity of a certain group that is threatened; the "we" loyalties of a clan, a tribe, a region, a religion a race or a nation that are defined in contrast to other communities.[159]
5. In the *political sector*, the territorial state is the most prominent referent object. However, other state-like organizations such as quasi-superstates (e.g., the EU), self-organized, but stateless societal groups with strong institutions (e.g., tribes or minorities), and transnational movements (e.g., the Catholic Church, the Muslims or the communists) can also reach this status—even if they are not formally recognized by the interstate society.[160]

Alongside a whole range of possible referent objects at the micro, middle, and system level, a second unit of analysis is defined as *securitizing actors*. Securitizing actors can be characterized as

> "actors who securitize issues by declaring something—a referent object—existentially threatened. [. . .] [S]omeone, or a group, who performs the security speech act. Common players in this role are political leaders, bureaucracies, governments, lobbyists, and pressure groups."[161]

In face of such a broad definition, every individual could arbitrarily be said to be a securitizing actor. However, for the Copenhagen school the decisive qualification for an actor to be able to execute a speech act is the position he holds within a social community (concept of capabilities). This position can either be assigned by formal rules, or the trust and confidence a community places in certain individuals or groups. The government, for instance, can be assumed to have the legal authority to speak "on behalf" of a certain state. In this respect, the prime minister is most likely to securitize a threat to the state. However, he can also fail. Moreover, the government's representatives are not the only ones who could successfully conduct a speech act. Other political parties or pressure groups can potentially gain enough attention to do so too. The most prominent securitizing actors highlighted by the Copenhagen school are the following:

[158] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 100-3.

[159] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 123f.

[160] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 145f.

[161] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 36 and p. 40.

1. In the *military sector*, securitizing actors are typically state representatives and other officials, the United Nations General Secretary, intelligence services, mafias, gangs, clans, tribes or rebels.[162]
2. In the *environmental sector*, securitizing actors can be divided in lead actors who have a strong commitment to global action (such as states and non-governmental organizations, or NGOs, like Greenpeace and the World Wildlife Fund), support actors who do not have the resources to be in a lead position (especially most parts of the developing world), and both veto actors (such as emerging economies and parts of industries), as well as veto coalitions (such as the US-based Global Climate Coalition) that try to downgrade environmental issues.[163]
3. In the *economic sector*, securitizing actors can be found at two different levels. At the local level a firm might be protected by individuals, trade unions, city governments, or local political representatives. At the national level possible securitizing actors are trade unions and the state government in pursuit of economic security.[164]
4. In the *societal sector*, there are many different actors who potentially can securitize an issue. These actors include official and semiofficial leaders who claim to speak on behalf of a certain group. For a nation it is most likely the state government that securitizes an issue.[165]
5. In the *political sector*, securitizing actors are comparatively well defined. Thanks to established institutions, the authority to frame an issue as a security question is clearer here than in other sectors. For a state it is usually the authorized leaders who can speak security. The same is true for the EU and most institutionalized organizations and movements.[166]

After having characterized both referent objects and securitizing actors, *functional actors* can ultimately be defined as

> "actors who affect the dynamics of a sector. Without being the referent object or the actor calling for security on behalf of the referent object, this is an actor who

[162] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 55f.

[163] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 77-9.

[164] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 100f.

[165] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 123f.

[166] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 145f.

> significantly influences decisions in the field of security."[167]

This category encompasses all those actors who have a significant influence on security making in general. With respect to securitization, this includes the processes *before*, *during*, and *after* securitization. However, these actors do not intend to be referent objects and do not securitize issues as existential threats. Some of the most prominent functional actors can be highlighted as follows:

1. In the *military sector*, functional actors can be different agencies of force such as assassins, mercenary companies, armies, defense bureaucracies, the arms industry, or defense, finance and foreign ministries.[168]
2. In the *environmental sector*, functional actors can be seen as those who are actually causing the problem. It is the actors whose behavior affects the ecosystem but who neither politicize nor securitize themselves. Examples are economic actors (such as transnational corporations, state firms, agricultural, chemical, and nuclear industries, fishing, mining etc.), governments and Intergovernmental organizations (such as the United Nations Environmental Program or the Food and Agriculture Organization).[169]
3. In the *economic sector*, the firm affects the security dynamics within the sector most notably. However, it is also governments and Intergovernmental organizations (such as the World Trade Organization or the World Bank) that play a role here.[170]
4. In the *societal sector*, especially the media plays an important role. Without actually securitizing an issue, the media interprets the dynamics and can, therefore, affect the processes of framing the "us" on the one hand and the "them" on the other.[171]
5. In the *political sector*, one can imagine a broad variety of different functional actors ranging from the (international) media, to governments and (I)NGOs.[172]

### 1.1.2.2.4. Methodology

Studying securitization means to tackle questions about "who securitizes, on what issues (threats), for whom (referent objects), why, with what results, and, not least, under what

[167] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 36.

[168] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 56f.

[169] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 79.

[170] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 103.

[171] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 122.

[172] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 151.

conditions (i.e., what explains when securitization is successful)."[173] To answer these questions comprehensively, the Copenhagen school suggests studying both *discourse* and *political constellations*.[174]

In terms of *discourse analysis*, Wæver supports Jacques Derrida's approach to blind out context and exclusively focus on publicly available text:

> "*The analysis should be conducted on texts that are central* in the sense that if security discourse is operative in this community, it should be expected to materialize in this text because this occasion is sufficiently important."[175]

Against this backdrop, an analyst of securitization should not be expected to reveal "underlying motives, hidden agenda, or such."[176] For Wæver "[d]iscourse analysis can [only] uncover one thing: discourse."[177] Thus, instead of using "sophisticated linguistic or quantitative techniques"[178] to uncover secret subtext, the analyst should rather listen closely to what actors think aloud in public debate:

> "The technique is simple: Read, looking for arguments that take the rhetorical and logical form defined here as security."[179]

In addition to discourse, the analyst should also pay attention to the *political constellations* and processes that accompany the securitization. This makes it necessary to not only concentrate on text, but also to look closer at the interacting units and facilitating conditions.[180]

## 1.2. Cyber Sector

The sectoral approach of the Copenhagen school originally contained a set of five distinct

[173] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 32.

[174] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 25.

[175] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 177.

[176] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 176.

[177] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 177.

[178] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 176.

[179] Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998 , p. 177.

[180] See Buzan, Barry et al., *Security: A New Framework for Analysis,* London, Lynne Rienner Publishers, Inc., 1998, p. 177.

sectors. Each of them was identified by their characteristic *security agenda*, *units of analysis*, and *sub-forms or grammars of security*. In recent years, however, proponents of the Copenhagen school have suggested to add additional sectors.[181] One of them is the cyber sector.[182]

Most basically, *cyberspace* can be defined as the "world behind your screen."[183] However, today there is a broad variety of different definitions of cyberspace.[184] One of the first to be used in politics was put forward in the aftermath of 9/11. As part of the 2003 *US National Strategy to Secure Cyberspace*, cyberspace has been described as a national "nervous system" that controls the country's critical infrastructure. While highlighting the role of public-private engagement, the strategy stated:

> "Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security."[185]

Five years later, in 2008, a similar definition was put forward in US President George W. Bush's *National Security Presidential Directive 54*, also known as *Homeland Security Presidential Directive 23* (NSPD-54/HSPD-23).[186] This document established the Comprehensive National Cybersecurity Initiative (CNCI); [187] a still partially classified[188] USD 17 billion program designed to protect Federal Government systems against intrusion attempts.[189] In this context, the directive defines cyberspace as

[181] One of them was Scott Watson who argued in favor of a *humanitarian sector*. See, for instance, Watson, Scott, 'The 'human' as referent object? Humanitarianism as securitization', *Security Dialogue*, 42, 1, 2011, pp. 3-20.

[182] See Hansen, Lene and Nissenbaum, Helen, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53, 2009, pp. 1155-75.

[183] Naughton, John, *A brief History of the Future. The Origins of the Internet*, London, Phoenix, 1999, p. 311.

[184] For a first overview see Kuehl, Daniel T., 'From Cyberspace to Cyberpower: Defining the Problem,' in Kramer, Franklin D. et al., eds., *Cyberpower and National Security*, Washington, D.C., National Defense UP, 2009, pp. 26-7.

[185] White House, *The National Strategy to Secure Cyberspace,* 2003, http://georgewbush-whitehouse.archives.gov/pcipb/.

[186] FAS, *National Security Presidential Directives (NSPD) George W. Bush Administration*, 2001-2009, http://www.fas.org/irp/offdocs/nspd/.

[187] White House, *The Comprehensive National Cybersecurity Initiative*, 2 March 2011, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

[188] United States District Court for the District of Columbia, *Complaint for Injunctive release*, 2009, http://epic.org/foia/NSPD54_complaint.pdf.

[189] Samson, Victoria, 'The Murky Waters of the White House's Cybersecurity Plan', *CDI*, 23 July 2008, http://www.cdi.org/program/document.cfm?DocumentID=4345&from_page=../index.cfm.

> “the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.”[190]

### 1.2.1. Security Agenda

The cyber sector does not offer a univocal discourse dominated by a single ideological position (as is the case in the economic sector). Rather, it has been argued that it is characterized by multiple discourses and competing articulations of constellations of linked (rather than discrete) referent objects within and across geographical and political boundaries:[191]

> “[p]rivacy advocates and cyberlibertarians point to governmental violations of personal security [. . .], and authoritarian (and not so authoritarian) regimes securitize transborder information flows as threats to regime/state security and national (societal) identity.”[192]

In the following section it is argued that this multi-discursivity can be explained by different ideological positions that are (more or less) equally in play with each other. This seems familiar from the economic sector, where the mercantilist, liberal and socialist doctrines were identified as the most defining ideological views, with each stressing its own specific security agenda. However, while the economic sector is mostly dominated by a liberal agenda, it is not fully clear yet what agenda will dominate the cyber sector. The following section can therefore only provide a rough and very theoretical overview.

#### 1.2.1.1. Structuring Cyber Discourse

Drawing on Milton Mueller, one can identify four pure forms of ideological positions within the cyber sector: *cyberconservatism/-reactionaries*, *networked nationalism*, *global governmentality* and *denationalized liberalism*.[193] The main differences between them are their answers to questions about whether state sovereignty and societies or the free (cross-border) interplay of networks and information should have priority, and whether self-

[190] FCC, *Tech Topic 20: Cyber Security and Communications*, http://transition.fcc.gov/pshs/techtopics/techtopics20.html.

[191] See Hansen, Lene and Nissenbaum, Helen, ‘Digital Disaster, Cyber Security, and the Copenhagen School’, *International Studies Quarterly*, 53, 2009, pp. 1155-75.

[192] Hansen, Lene and Nissenbaum, Helen, ‘Digital Disaster, Cyber Security, and the Copenhagen School’, *International Studies Quarterly*, 53, 2009, pp. 1155-75, p. 1162.

[193] See Mueller, Milton, *Networks and States. The Global Politics of Internet Governance*, MIT Press, Cambridge et al., 2010, pp. 253-71.

organized social aggregates have security claims of their own that must be weighed against the malpractices within cyberspace.

Each of these ideologies can be located in one of the four quadrants partitioned by two mutually perpendicular axes, both representing a particular spectrum between two extremes. The first axis describes "the status of the territorial nation-state"[194] and can range from nation-state dominance (with state actors setting the basic political and legal frame around linguistic, religious and ethnic communities[195]) to transnational dominance (with non-state actors setting the basic institutional frame around flexible and shifting social aggregates). However, Mueller notes:

> "There are, of course, various spots in between these extremes: from right to left there are bilateral agreements and clubs among states, formal international organizations, multistakeholder governance arrangements, delegation private actors, etc."[196]

The second axis indicates "the level of hierarchy one is willing to countenance."[197] It runs from hierarchical governance (emerging from adherence to institutions held in place by *coercion*, *calculation* or *belief*,[198] and enforced by an authority) towards networked governance (emerging from optional adherence to institutions that can be freely communicated, concluded and even broken). As Mueller points out:

> "Of course, between these two extremes there are many points. A base of private contract law can support a superstructure of more or less free networking; or we can recognize free networking as the primary mechanism of governance but opt for hierarchical intervention when network externalities convey too much power to a private group, or when bottlenecks form around essential facilities."[199]

[194] Mueller, Milton, *Networks and States. The Global Politics of Internet Governance*, MIT Press, Cambridge et al., 2010, p. 255.

[195] This also includes cases in which one nation-state, or hegemon (e.g., the United States) successfully imposes its jurisdiction upon other international actors.

[196] Mueller, Milton, *Networks and States. The Global Politics of Internet Governance*, MIT Press, Cambridge et al., 2010, p. 255f.

[197] Mueller, Milton, *Networks and States. The Global Politics of Internet Governance*, MIT Press, Cambridge et al., 2010, p. 255.

[198] For an IR discussion on different modes of institutional obedience (Hobbesian coercion, Lockean self-interest, and Kantian belief) see, for instance, Wendt, Alexander, *Social Theory of International Politics*, Cambridge University Press, New York, 1999, p. 247-50; and Hurd, Ian, 'Legitimacy and Authority in International Politics', *International Organization* 53, 2, 1999, pp. 379-408.

[199] Mueller, Milton, *Networks and States. The Global Politics of Internet Governance*, MIT Press, Cambridge et al., 2010, p. 257.

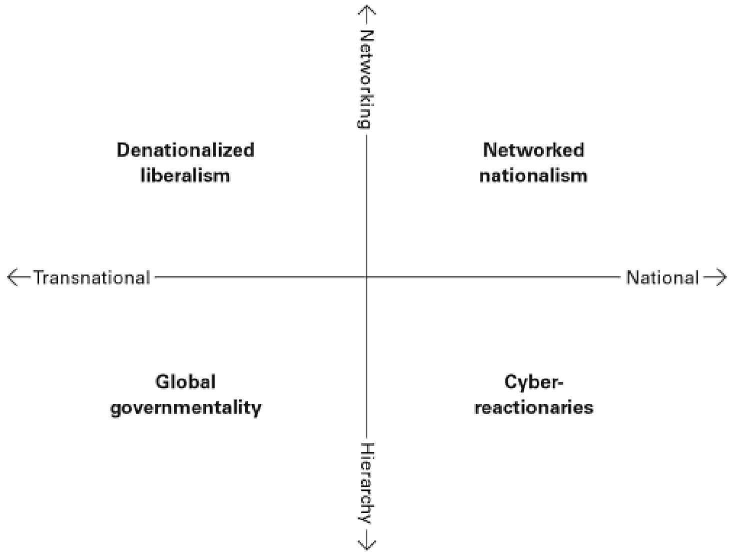

**Figure 1:** Structuring Cyber Discourse[200]

Against this backdrop, the first one of the four just mentioned ideologies of the cyber sector is located in the lower-right quadrant. It is referred to as *cyberreactionism* or *-conservatism* and can be defined "as something that favours retaining the status quo, something resistant to change."[201] Here, territorial jurisdiction is given priority over the free[202] and cross-border interplay of networks and information. Citizens must adhere to domestic and international institutions and are protected through the sovereign state, no matter whether it is democratic or non-democratic, authoritarian or non-authoritarian.

In the upper-right quadrant one finds *networked nationalism*. Similar to cyberconservatism, for networked nationalists the nation-state is the dominant entity authorized to establish political institutions, both domestic and international. However, as opposed to cyberconservatism, judicial loopholes and escape valves leave enough room for networked actors to "escape" the basic political and legal frame. On the one hand, this allows for a largely free (though not necessarily cross-border) interplay of networks and information. On the other one, however, constantly avoiding a state's institutions can ultimately lead to the erosion of its sovereignty and, consequently, of its ability to protect its citizens. Therefore, networked nationalism can be considered an unstable candidate for ideological longevity.

[200] Mueller, Milton, *Networks and States. The Global Politics of Internet Governance*, MIT Press, Cambridge et al., 2010, p. 256.
[201] Mueller, Milton, 'The New Cyber-Conservatism: Goldsmith/Wu and the Premature Triumphalism of the Territorial Nation-State. A review of Goldsmith and Wu's 'Who Controls the Internet? Illusions of a Borderless World'', *Internet Governance Project Paper*, 2006, http://www.internetgovernance.org/pdf/MM-goldsmithWu.pdf.
[202] Defined as "able to act or be done as one wishes; not under the control of another" (OED).

The lower left quadrant is occupied by *global governmentality*. Here, non-state jurisdiction allows for a cross-border interplay of networks and information. However, even though the social aggregates concerned must not adhere to territorial jurisdiction, they are bound to the political and legal frame they have chosen to be protected by. Thus, transnational jurisdiction is given priority over the free interplay of networks and information. Historically speaking, it might be difficult to imagine sufficient security capabilities centered within an institution other than the state. However, this does not necessarily mean that it is impossible.

Lastly, *denationalized liberalism* (with *cyberlibertarianism* being its visionary precursor[203]) is about transnational actors defining the political institutions that can be freely communicated, concluded and even broken by flexible and shifting social aggregates. The free and cross-border interplay of networks and information is considered to leverage peer production processes regardless of any frontiers (such as peer-to-peer file sharing or email lists[204]). "Political institutions should seek to build upon, not undermine or reverse, the limitless possibilities for forming new social aggregations around global communications. [. . .] Governance should emerge primarily as a byproduct of many unilateral and bilateral decisions by its members to exchange or negotiate with other members (or to refuse to do so)."[205]

### 1.2.1.2. Security Issues

As should have become clear in the previous section, the discourse in the cyber sector is highly fragmented. Consequently, issues on the security agenda are widely scattered and can—as suggested by Alexander Klimburg—contain such diverse topics as cyberwarfare (e.g., an arms race between actors for cyber weapons of mass destruction), cybercrime/-terrorism (e.g., identity theft and the production of computer viruses for ideological or purely disruptive reasons), cyberespionage (e.g., disclosing company and government secrets), critical infrastructure protection (e.g., disruption of interdependent physical and virtual facilities that are vital to a country's people) as well as Internet Governance (e.g., threats to the global domain name system).[206]

[203] See, for instance, Barlow, John Perry, *A Cyberspace Independence Declaration*, 9 February 1996, http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration.
[204] Mueller, Milton, *Networks and States. The Global Politics of Internet Governance*, MIT Press, Cambridge et al., 2010, pp. 35-8.
[205] Mueller, Milton, *Networks and States. The Global Politics of Internet Governance*, MIT Press, Cambridge et al., 2010, p. 269.
[206] See Klimburg, Alexander and Mirtl, Philipp, 'Cyberspace and Governance—A primer', *oiip Policy Paper*, September 2011, pp. 9-14, http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Newsletter/Cyberspace_and_Governance-A_primer.pdf.

Suffice it to say that all of these issues are highly interconnected with each other. This is especially true for cybercrime/-terrorism and cyberespionage which often makes it difficult to rigorously keep them apart.

### 1.2.2. Units of Analysis

The cyber sector is comprised of a broad variety of significant referent objects. One way to think about them is to arrange them along distinct layers of activity. In the literature one finds different numbers and names of layers.[207] However, this study argues in favor of the following four-level model:[208]

1. The *physical layer* contains all the *hardware devices* which include routers, switches, storage media, satellites, sensors, and other technical conduits, both wired and wireless. The physical infrastructure can be located geographically[209] in "real space" and is thus subject to different policies and jurisdictions.

2. The *logical layer* generally refers to the *code*,[210] which contains both the software as well as the protocols that can be incorporated within that software.[211] This layer does not only include benign logic but also malicious one, referred to as *malware* which includes a variety of different sorts of *Trojans*, *viruses* and *worms*.[212] For our context it is important to note that most of the Internet infrastructure (e.g., the Domain Name System) is concentrated on this layer.

3. The *content layer* describes all the *information* that is created, captured, stored and processed within cyberspace. Inter alia, it contains all the messages that are delivered by social media websites or email; the content of articles and books that are stored on memory sticks and virtual databases; the news that are broadcasted via blogs and websites as well as the music, movies and pictures that are consumed online.

[207] See, for instance, Libicki, Martin C., *Conquest in Cyberspace, National Security and Information Warfare*, Cambridge et al., Cambridge University Press, 2007, chapter 10; and Kramer, Franklin D. et al., eds., *Cyberpower and National Security*, Washington, D.C., National Defense UP, 2009, chapter 2.

[208] See Clark, David, 'Characterizing cyberspace: past, present and future', *Working Paper MIT/Harvard*, http://web.mit.edu/ecir/pdf/clark-cyberspace.pdf.

[209] See, for instance, TeleGeography, *Map Gallery*, 2010, http://www.telegeography.com/telecom-resources/map-gallery/index.html.

[210] See, for instance, Lessig, Lawrence, *The Future of Ideas. The Fate of the Commons in a Connected World*, New York, Random House, p. 23, http://www.the-future-of-ideas.com/download/lessig_FOI.pdf; and Lessig, Lawrence, *Code v2*, New York, Basic Books, 2006, http://codev2.cc/download+remix/Lessig-Codev2.pdf; I also want to thank Thomas Schinagl for technical advice.

[211] Thanks to Thomas Schinagl for that point.

[212] Beal, Vangie, 'The Difference Between a Computer Virus, Worm and Trojan Horse', *Webopedia*, 29 June 2011, http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp.

4. The *social layer* is made up of all the *people* who are using and shaping the character of cyberspace. It is the actual interaction of people, rather than the implied interaction of hardware and software. Essentially, the social layer includes governments as well as private sector, civil society and technical community actors.

Mapping these four layers hierarchically into a four-tiered pyramid is not just due to aesthetical reasons, but it aptly highlights that the referent objects at the *physical*, *logical*, and *content layer* ultimately converge in an overall triangle: the *social layer* on top.[213]

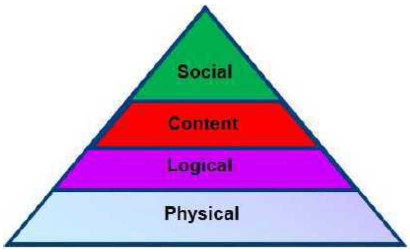

**Figure 2:** Four-Level Cyber Layer[214]

In order to mobilize sufficient support for a securitizing move, referent objects must hold enough security legitimacy in terms of a claim to survival; a feature objects like bureaucracies, political regimes and firms rarely possess. However, by linking them to a higher entity's security legitimacy (e.g., linking a firm to national economy), they potentially become fully securitized. In this context, it is argued that hardware devices, code and information can only hold a legitimate claim to survive by their direct link to the social layer. A quite similar argument has been brought forward by Hansen and Nissenbaum. For them, the security of computer networks as such is in fact a significant referent object, but it is only through its connection to referent objects invoking a social collectivity that it becomes politically important:

> "a securitization of the network cannot, and does not, stop at the network itself: it is the implications of network break-downs for other referent objects, 'society,' 'the regime,' or 'the economy' (which is, again, in turn linked to 'state' and 'society') that makes cyber securitization a plausible candidate for political and media attention."[215]

In this context, the two authors identify governments, private organizations, businesses and experts as examples of potential securitizing actors. Going a step further, one could also identify black and white hat hackers as well as owners of critical infrastructures as being

[213] Thanks to Alexander Klimburg for that point.

[214] Thanks to Alexander Klimburg for that point.

[215] Hansen, Lene and Nissenbaum, Helen, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53, 2009, pp. 1155-75, p. 1163.

what earlier has been referred to as functional actors.[216]

### 1.2.3. Security Grammar

As was mentioned earlier, security grammars refer to the sector-specific constructions of a plot in which existential threats are tied together adequately. For the cyber sector, Hansen and Nissenbaum defined three distinct security grammars: *hypersecuritization*, *everyday security practice*, and *technification*.[217] While all of these three security sub-forms can potentially be found in other security sectors as well, their prominence is particularly striking within the cyber sector.

#### 1.2.3.1. Hypersecuritization

As opposed to Buzan, *hypersecuritization* in the cyber sector does not refer to "the tendency both to exaggerate threats and to resort to excessive countermeasures."[218] Rather it is defined as

> "the striking manner in which cyber security discourse hinges on multi-dimensional cyber disaster scenarios that pack a long list of severe threats into a monumental cascading sequence and the fact that neither of these scenarios has so far taken place."[219]

The first part of this definition touches upon the "instantaneity and inter-locking effects"[220] of potential cyber attacks on a national or global network of information and communication technologies. The significance, however, does not arise from the network itself, but from the immediate and far-reaching cascading effects on the referent objects in the military, economic, societal and political sectors.

The second part of the definition refers to the fact that a catastrophic cyber event has not yet occurred. This makes it impossible to perform an instance of securitization on the grounds of historic experience, as was the case during the Cold War, when the devastations of Hiroshima and Nagasaki were used as a yardstick for what nuclear war could look like.

[216] Also see Dunn Cavelty, Myriam, *Cyber-security and threat politics: US efforts to secure the information age*, Routledge, New York 2008.

[217] See Hansen, Lene and Nissenbaum, Helen, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53, 2009, pp. 1155-75, pp. 1163-68.

[218] See Buzan, Barry, *The United States and the Great Powers: World Politics in the Twenty-First Century*, Cambridge, Polity, 2004, p. 172.

[219] Hansen, Lene and Nissenbaum, Helen, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53, 2009, pp. 1155-75, p. 1164.

[220] Hansen, Lene and Nissenbaum, Helen, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53, 2009, pp. 1155-75, p. 1164.

Thus, lacking historic experience, securitizing actors in the cyber sector often use historic analogies of disasters such as the "Cyber Pearl Harbor."

Additionally, it is often difficult to visualize potential cyber threats or communicate them to a wider public. As for the environmental sector, one can imagine the devastating effects of acid rain, the extinction of numerous animal and plant species as well as melting polar icecaps and glaciers. But the lack of experience in the cyber sector makes it difficult for a securitizing actor to mobilize a wider audience to support his securitizing move.

#### 1.2.3.2. Everyday Security Practice

The second modality in the security grammar within the cyber sector refers to *everyday security practice* which "points to the way in which securitizing actors, including private organizations and businesses, mobilize 'normal' individuals' experiences"[221] to get their message through. In order to make hypersecuritization scenarios more plausible for the wider public, the securitizing actor needs to link them to experiences familiar from everyday life. By directly referring to individual dangers such as credit card fraud, identity theft, and email spamming, the securitizing actor can raise the awareness of his relevant audience.

Moreover, since the networks of information and communication technologies are ultimately made up by individual actors, the securitizing actor also needs to ensure that the individual acts as a partner and complies in protecting network security. Similar to the discourse of epidemics and contagion, individuals in the cyber sector are often urged to behave responsibly in order to not endanger the "health" of the whole.

#### 1.2.3.3. Technification

The third security modality considers *technification*. To successfully securitize an issue, the securitizing actor can draw on scientific argument which gives his move additional authority. Through claiming "objectivity" he clearly distinguishes himself from the "politicking" of politicians. In that way, technifications

> "construct an issue as reliant upon technical, expert knowledge, but they also simultaneously presuppose a politically and normatively neutral agenda that technology serves."[222]

Technification can also serve to prevent an issue from being/becoming subject to a wider

[221] Hansen, Lene and Nissenbaum, Helen, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53, 2009, pp. 1155-75, p. 1165.

[222] Hansen, Lene and Nissenbaum, Helen, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53, 2009, pp. 1155-75, p. 1167.

public. By constructing it as primarily technical—requiring expertise that the public and most politicians do not have—underlying intentions can be hidden behind scientific "objectivity" and easily kept/taken out of any public discourse.

Technifications can also be found in other sectors such as the environmental sector, where technifications deal with the scientific reliability of predictions about global warming, resource depletion, and population growth. Yet, while the audience in the environmental sector "is expected to know more and the repeated contestation of environmental 'evidence' makes for a public view of (some) environmental actors as political ones rather than apolitical, 'objective' experts,"[223] in the cyber sector "the knowledge required to master the field of computer security is daunting and often not available to the broader public."[224] This hampers public discourse and empowers those who have the necessary knowledge to substantially influence the discourse (in their own interest).

## 1.3. Synthesis

As promised at the outset of this part, this synthesis shall provide a quick overview of the Copenhagen school's security sectors that were just mentioned; each with its specific security agenda, units of analysis and sub-forms or grammars of security.

| | **Security Agenda** | **Units of Analysis** | **Sub-Forms of Security** |
|---|---|---|---|
| **Military Sector** | → Mainly about the instruments of force a state has at its disposal. However, one has to distinguish between an internal dimension (ability of the ruling elite to maintain civil order and peace), and an external dimension (how states equip themselves and how this is perceived by other states).<br>→ Internally, issues on the agenda might include militant separatists, rebels, terrorists and other actors opposed to the respective | → Referent objects can be states (as single holders of military power), would-be states (claiming a status as actors at the unit level), and actors at the subsystem or system level (e.g., WEU/EU, NATO).<br>→ Securitizing actors can be state representatives and other officials, the United Nations General Secretary, intelligence services, mafias, gangs, clans, tribes or rebels.<br>→ Functional actors can be | → The plot is mainly focused on sovereignty and has traditionally been constructed around military force (e.g., the opponent's army), geography (e.g., closeness and terrain), history (e.g., past experiences and present perceptions) and politics (e.g., contradicting ideologies, recognition and status). |

[223] Hansen, Lene and Nissenbaum, Helen, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53, 2009, pp. 1155-75, p. 1168.
[224] Hansen, Lene and Nissenbaum, Helen, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53, 2009, pp. 1155-75, p. 1166.

| | | | |
|---|---|---|---|
| | state authority. Externally, issues might include the state’s territorial integrity towards other actors. | different agencies of force (e.g., assassins, mercenary companies, armies, defense bureaucracies, the arms industry, or federal ministries). | |
| **Environmental Sector** | → Difference between the scientific agenda (about defining a reliable set of issues) and the political agenda (about addressing the issues already set out in the scientific agenda by raising awareness, taking political responsibility, and managing them politically).<br>→ Issues on the scientific agenda include the disruption of ecosystems and civil strife as well as energy, population, food, and economic problems. | → The ultimate referent object is not nature itself, but human enterprise that would perish without it.<br>→ Securitizing actors can be divided in lead actors (such as states and NGOs like Greenpeace and the World Wildlife Fund), support actors (especially most parts of the developing world), veto actors (such as emerging economies and parts of industries), and veto coalitions (such as the US-based Global Climate Coalition).<br>→ Functional actors can be economic actors (such as transnational corporations, state firms, agricultural, chemical, and nuclear industries, fishing, mining etc.), governments and Intergovernmental organizations (such as the United Nations Environmental Program or the Food and Agriculture Organization). | → The plot is mainly focused on sustainability and constructed around nature-caused threats (e.g., earthquakes), human-caused threats that seem to cause existential damage to civilization (e.g., CFCs), and human-caused threats that do not seem to cause existential damage to civilization (e.g., the depletion of minerals that can be replaced by alternative substances, such as copper by silicon, or metal by ceramics). |
| **Economic Sector** | → Mainly shaped by the liberal agenda (less by the mercantilist or socialist agenda).<br>→ Issues on the (liberal) agenda include the ability of states to sustain military capabilities independently from the global market, the economic dependence of states on foreign (scarce) | → Referent objects can include individuals, classes, states, firms, and the liberal international economic order. The most important ones, however, are firms that search protection from states and the liberal economic order.<br>→ Securitizing actors are found on two different | → The plot has traditionally been focused on the sovereign economy and can be constructed around individuals (e.g., basic human needs), firms (e.g., risks of boycotts and risks of investment), or states (e.g., state bankruptcy). |

| | | | |
|---|---|---|---|
| | resources, the worries that the global market would generate inequalities, the illegal trade in drugs and weapons (especially those of mass destruction), and the fears that systematic crisis could trigger government intervention. | levels: At the local level (e.g., individuals, trade unions, city governments, or local political representatives), and at the national level (e.g., trade unions and the state government).<br>→ Functional actors are firms as well as governments and Intergovernmental organizations (such as the World Trade Organization or the World Bank). | |
| **Societal Sector** | → Agenda are dependent upon self-defined identity groups which can vary severely through time and place.<br>→ The issues on most agenda, however, include migration, horizontal identity competition, and vertical identity competition. | → The ultimate referent object is the collective identity (or "we" feeling) of a certain group (e.g., a clan, a tribe, a region, a religion a race or a nation).<br>→ There is a broad variety of securitizing actors including both official and semiofficial leaders claiming to speak on behalf of a certain group.<br>→ By framing the "us" and the "them", the media can influence dynamics as the functional actor. | → The plot is mainly focused on identity and can be constructed in manifold ways. |
| **Political Sector** | → Mainly about ensuring organizational stability. However, one has to distinguish between an internal dimension (recognition from within), and an external dimension (recognition from without).<br>→ Internally, issues might include the constitutive ideas defining a political unit or pattern. Externally, issues might include the recognition or non-recognition of political units | → The territorial state can be a referent object as well as quasi-superstates (e.g., the EU), self-organized, but stateless societal groups with strong institutions (e.g., tribes or minorities), and transnational movements (e.g., the Catholic Church, the Muslims or the communists).<br>→ Securitizing actors are comparatively well defined here and include the | → The plot is mainly focused on sovereignty and has traditionally been built around the idea of the state (e.g., democracy, capitalism or communism), its governing institutions (e.g., the legislative, administrative and judicial bodies, and laws), and the physical base at its disposal (such as population and territory). |

| | | | |
|---|---|---|---|
| | and pattern. | institutionally authorized leaders who can speak security.<br>→ Functional actors include the media as well as governments and (I)NGOs. | |

Additionally to the five classical security sectors, the following table shall give an overview of the details discussed in the cyber section.

| | **Security Agenda** | **Units of Analysis** | **Security Grammar** |
|---|---|---|---|
| **Cyber Sector** | → There is no single agenda in the cyber sector. Rather, it is characterized by multiple discourses, including denationalized liberalism, networked nationalism, global governmentality and cyberreactinaries.<br>→ Taken together, issues on the different agenda can include cyberwarfare, cybercrime/-terrorism, cyberespionage, Critical Infrastructure Protection (CIP) and Information Assurance (IA) as well as Internet Governance. | → The analytical significance of referent objects at the physical, logical and informational cyber layers (e.g., confidentiality, integrity and availability, CIA) only arises from their connection to the social top layer which refers to all possible levels of security analysis (micro, middle and macro levels).<br>→ Securitizing actors include governments, private organizations, businesses and experts.<br>→ Functional actors can include (both black and white hat) hackers, Intelligence communities, owners of critical infrastructures, Internet Service Provider,… | → The plot is mainly constructed around multidimensional cascading disasters (e.g., the opponent's army), everyday security practice (e.g., closeness and terrain), and technical and expert knowledge (e.g., contradicting ideologies, recognition and status). |

# 2. Internet Governance

## 2.1. Internet Governance and the Copenhagen Cchool

In the previous part, Internet governance has been identified as an issue area within the wider cyber agenda. However, before we can move on and investigate area specific instances of *securitization*,[225] we first need to set the characteristic scene in which the securitizing actor can feasibly apply the *sector-specific sub-form* or *grammar of security*.[226] Consequently, the primary task of the following sections is to identify a critical element of the Internet whose breakdown could possibly have important implications for one or more social layer *referent objects*.[227] In doing so, we will also pay due attention to the historic *processes* that finally led to the creation of the Internet as we know it today. Moreover, we will provide an understanding of the main *political constellation* in Internet governance. Finally, we offer a set of possible *securitizing actors*[228] with the *capabilities*[229] to potentially succeed in an attempted securitization.

### 2.1.1. The Internet

Cyberspace has been characterized as *the world behind your screen*. However, when computers were enabled to talk to each other, that world started to expand. The Internet (or Net) has played a decisive, yet not exclusive role for the expansion of cyberspace. Referring to the previous part, the Internet is mainly located at the logical cyber layer. By using a combination of different data transmission mechanisms—such as the *Transmission Control Protocol* (TCP) and the *Internet Protocol* (IP) as the two most important protocols within the *Internet Protocol Suite* (TCP/IP)—an increasing number of Internet users (defined as persons who have available access to an Internet connection point,[230] and the basic knowledge required to use web technology[231]) was empowered by receiving unprecedented access to information. Especially over the last 16 years, the total number of Internet users has risen

[225] Defined as an inter-subjective process by which a powerful actor discursively constructs an issue as a threat to a specific referent object.

[226] In the case of the cyber sector, the sub-form of security is mainly focused on integrity/availability/confidentiality and constructed around multidimensional cascading disasters, everyday security practice, technical and expert knowledge as well as metaphors.

[227] Referred to as things that are seen to be existentially threatened and that have a legitimate claim to survive. The referent object is that to which one can point and say, “It has to survive, therefore it is necessary to….”

[228] Defined as actors who securitize issues by declaring something—a referent object—existentially threatened; someone, or a group, who performs the security speech act. Common players in this role are political leaders, bureaucracies, governments, lobbyists, and pressure groups.

[229] Including both Waltzian *material capabilities* as well as Bourdieuan *socio-cultural capabilities*.

[230] Internet connection points are usually provided by Internet service providers (ISPs) against payment.

[231] See Internet World Stats, *Surfing and Site Guide*, 2011, http://www.internetworldstats.com/surfing.htm#1.

from 16 million in 1995 to more than 2.1 billion in 2011.[232] This is an outstanding increase of +13,000%.

While the Internet was largely an American creation,[233] today most Internet users come from other parts of the world. In 2011, 44% came from Asia, 22.7% from Europe, and only 13% from North America.[234] In this context, the Internet has been defined as

> "the global data communication capability realized by the interconnection of public and private telecommunication networks using Internet Protocol (IP), Transmission Control Protocol (TCP), and the other protocols required to implement IP internetworking on a global scale, such as DNS and packet routing protocols."[235]

The strong technical emphasize of this definition will be more accessible after looking in more depth at the history of the Internet. However, prior to that it is important to point at the basic difference between generic computer networks and the Internet as the one and only network of networks with a global reach.

#### 2.1.1.1. The Internet as the Global Network of Computer Networks

Most basically, an *internetwork*, or simply *internet* (with a lowercase "i"), is established by interconnecting computer networks through routers, switches, satellites, sensors, and other conduits, both wired and wireless. These *generic networks of networks* can vary in scale. One of the smallest networks is the *personal area network* (PAN). In essence, a PAN is a network that does not exceed the scale of a conventional desk or office and that only covers small computers and devices (such as a notebook, a printer and a PDA[236]). However, if PANs are connected with other PANs within areas such as office buildings, universities or power plants, one usually speaks about *local area networks* (LANs). Moreover, if the level of interconnection exceeds the size of a LAN in that it covers a terrain such as a city or a state,

[232] See Internet World Stats, *Internet Growth Statistics*, 2011, http://www.internetworldstats.com/emarketing.htm.

[233] See, for instance, Naughton, John, *A brief History of the Future. The Origins of the Internet*, London, Phoenix, 1999, p. 119.

[234] See Internet World Stats, *Internet Users in the World. Distribution by World Region*, 2011, http://www.internetworldstats.com/stats.htm; also see NewScientist, *Exploring the exploding Internet*, 2009, http://www.newscientist.com/gallery/mg20227061900-exploring-the-exploding-internet/5.

[235] Mueller, Milton et al., 'The Internet and Global Governance: Principles and Norms for a New Regime', *Global Governance*, 13/2, 2007, p. 244. For more definitions of the "Internet" see, for instance, Lindsay, David, *International domain name law: ICANN and the UDRP*, Oxford, Hart Publishing, 2007, p. 1; IETF, *FYI on Questions and Answers. Answers to Commonly asked 'New Internet User' Questions (RFC 1206)*, 1991, http://tools.ietf.org/html/rfc1206; FNC, *FNC Resolution: Definition of "Internet"*, 24 October 1995, http://nitrd.gov/fnc/Internet_res.html; Mueller, Milton et al., 'The Internet and Global Governance: Principles and Norms for a New Regime', *Global Governance*, 13/2, 2007, p. 244.

[236] Personal Digital Assistant.

one can speak about *wide area networks* (WANs).

By contrast, the *Internet* (with an uppercase “I”) can be described as the worldwide collection of all existing PANs, LANs and WANs. It is the unique “global network of computer networks,”[237] the one and only network of networks that concerns the total collective Self of all Internet users on a planetary (or even “intergalactic”[238]) scale.

### 2.1.1.2. Decisive Moments in Internet History

After having characterized the Internet as the *global network of computer networks*, we are now ready to look in more depth at its history. By sketching the Internet’s gradual development, we will not only try to provide some basic technical explanations, but also pay due attention to the political constellations and processes that accompanied the progressive advancement of the Net.

#### 2.1.1.2.1. From Sputnik to ARPA

The Internet was not created in one single unexpected “Eureka!” moment, but evolved over time. If one wanted to finger point at a specific event that triggered this evolution, he can safely be referred to the Soviet Union’s launch of *Sputnik 1* on 4 October 1957. With the size of a basketball, Sputnik was the world’s first ever seen earth-orbiting satellite, capable only of relaying radio signals back to earth.[239] From today’s perspective, this does not sound particularly alarming. However, the language of reaction that was eventually employed by the US press created a general atmosphere of hysteria and self-doubt.[240] Thus, without posing an objectively identifiable (“real”) threat, Sputnik nevertheless prompted the employment of radical measures that were far beyond the adoption of conventional policy approaches.

Most importantly, Sputnik facilitated a shift from traditional to modern-day US science policy.[241] This meant an increased budget for advanced research and development (R&D) as well as organizational changes. Probably one of the utmost important organizational innovations included the establishment of the *Advanced Research Projects Agency* (ARPA), a federal body located in the US *Department of Defense* (DoD) and with the central control

[237] Naughton, John, *A brief History of the Future. The Origins of the Internet*, London, Phoenix, 1999, p. 314.
[238] See Licklider, J.C.R., Memorandum for: Members and Affiliates of the Intergalactic Computer Network, Advanced Research Projects Agency, 23 April 1963, http://www.chick.net/wizards/memo.html.
[239] For more information on *Sputnik* and the early days of space reconnaissance, see, for instance, Dickson, Paul, *Sputnik: The Shock of the Century*, New York, Walker Publishing Company, Inc., 2001.
[240] For further discussions see, for instance, Lule, Jack, ‘Roots of the Space Race: Sputnik and the Language of U.S. News in 1957’, *Journalism Quarterly*, 68, 1-2, 1991, pp. 76-86.
[241] See, for instance, Neal, Homer A. et al., *Beyond Sputnik: U.S. science policy in the twenty-first century*, Ann Arbor, University of Michigan Press, 2008.

over advanced science and technology.[242] In 1972 the agency was renamed into *Defense Advanced Research Projects Agency* (DARPA).[243]

As a relatively small and independent organization with a lean and non-bureaucratic structure, ARPA "was designed to be an agent for change in the Department of Defense."[244] It was not only authorized to direct R&D projects within the DoD, but also to work in relation with other government agencies, and "to enter into contracts and agreements with individuals, private business entities, educational, research or scientific institutions including federal or state institutions."[245] In its role as an "instigator of radical innovation," ARPA committed itself to a multi-disciplinary "high-risk—high-payoff" agenda that should "Create surprise", "Build communities of 'change-state advocates'", as well as "Define challenges, develop solution concepts, and demonstrate them."[246]

Originally, ARPA focused on three key areas: *space*, *missile defense*, and *nuclear-test detection*. However, after the *National Aeronautics and Space Administration* (NASA) became operational in October 1958, ARPA's aerospace competences and large parts of its budget were transferred over to NASA.[247] Nonetheless, as the Defense Department's premiere research arm, ARPA was soon assigned responsibility for alternative military and non-military research areas. Among others, these included the engagement in building weapons as well as the development of advanced computers and communications for the DoD's command and control systems. While the initial aim of the previous (and less successful) task was to help South Vietnamese troops to defend themselves against the North and Viet Cong guerillas, the latter one was the actual facilitator for what is now known as the Internet.[248]

### 2.1.1.2.2. ARPANET and Packet-Switching

During the 1960s and 70s, ARPA's engineers gave birth to ARPANET, a distributed computer network that used *packet-switching* technology to make computers speak with each other.

[242] See, for instance, Hafner, Katie and Lyon, Matthew, *Where Wizards Stay Up Late: The Origins Of The Internet*, New York, Touchstone, 1996, pp. 11-42.
[243] Today, DARPA has six program offices that work in areas such as *Information, Innovation & Cyber*; *Sensors, Communications & Energy*; and *Weapons, Platforms & Space* (see http://www.darpa.mil/our_work/).
[244] Herzfeld, Charles, 'How the change agent has changed', *Nature*, 451, 24 January 2008, pp. 403-4.
[245] US Department of Defense, *DoD Directive 5105.15 establishing the Advanced Research Projects Agency (ARPA)*, signed on February 7, 1958, http://www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2473.
[246] Atta, Richard Van, 'Fifty Years of Innovation and Discovery', in DARPA, *50 Years of Bridging the Gap*, Defense Advanced Research Projects Agency, April 2008, pp. 20-9, p. 25, http://www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2553.
[247] See, for instance, Hafner, Katie and Lyon, Matthew, *Where Wizards Stay Up Late: The Origins Of The Internet*, New York, Touchstone, 1996, p. 22.
[248] See Herzfeld, Charles, 'How the change agent has changed', *Nature*, 451, 24 January 2008, pp. 403-4.

One of the biggest advantages of packet switching is that a line between two communicating nodes can be used by third users as well. While in traditional telephony (using *circuit-switching* technology) the engaged line between two interconnected subscribers cannot be used to carry other calls at the same time (even if the subscribers remain silent), in packet-switching systems there is no need for a permanent pathway between the subscribers. This is made possible only because everything that can effectively be digitized (or translated into zeros and ones) is cut into data packets with an average size of 512 bytes. In order to use communications channels effectively, these chunks of information can subsequently be transmitted simultaneously across a variety of different circuits. Once the packets have arrived at their intended destination (no matter in what sequence) the respective data packets can be reassembled.[249] For the first time, this technology was tested in 1969, when the Universities of California (UCLA) and Stanford (SRI)—the first two nodes of ARPANET—exchanged their first host-to-host message.[250]

### 2.1.1.2.3. Transmission Control Protocol and Internet Protocol (TCP/IP)

After making *computers* speak with each other within their respective networks, one of the following steps was to find a way how these relatively heterogeneous *computer networks* could speak with each other too. The underlying problem was that networks were relatively autonomous in that they used their own distinct communication conventions or *network protocols*[251] to interconnect their respective computers. Therefore, the aim was to find a protocol that would recognize and support heterogeneity between different networks. The protocol that made that possible was the so called *Transmission Control Protocol* (TCP), which was first tested in 1977 when ARPANET was successfully connected with a radio and a satellite network.[252]

Soon, TCP was supplemented by the so called *Internet Protocol* (IP), which is essentially responsible for passing packets from one node to another. This process of passing and delivering packets can only be successfully implemented if the attached IP addresses are unique across the Internet. An IP address is a complex string of values that identifies the

[249] Copeland, Lee, 'QickStudy: Packet-Switched vs. Circuit-Switched Networks', *Computerworld*, 20 March 2000, http://www.computerworld.com/s/article/41904/Packet_Switched_vs._Circuit_Switched_Networks; and Mathiason, John R. and Kuhlmann, Charles C., 'An International Communication Policy: The Internet, international regulation & new policy structures', *New York University*, http://www.un.org/esa/socdev/enable/access2000/ITSpaper.html.

[250] See, for instance, Leiner, Barry M. et al., 'A brief history of the Internet', *ISOC*, 1997, http://www.isoc.org/internet/history/brief.shtml.

[251] Protocols are not to be confused with software which is the computer program that actually implements these protocols.

[252] Abbate, Janet, *Inventing the Internet*, Cambridge (MA), MIT Press, 1999, pp. 113-145.

physical location of a computer that is connected to the Internet (e.g., PCs, servers, smartphones). In this way, an IP address is the binary equivalent to license plate numbers which uniquely identify any form of vehicle in the streets. In the early 1980s, a total number of 4.3 billion (4.3x10^9) IP addresses (referred to as *IPv4*)[253] was considered to be enough for the foreseeable future.[254] However, the explosive demand for IP address blocks over the last thirty years, as well as the vision of an *Internet of Things* (IoT)—where everyday objects (such as home appliances or clothing) are made accessible over the Internet—have proven that the original quantity of IP addresses was inadequate. This is why, in the 1990s IP version 6 (referred to as *IPv6*)[255] had been developed. IPv6 would provide enough addresses space for around 340 undecillion (3.4x10^38) Internet connection points. With an estimated world population of 6.8 billion living human beings,[256] the potential number of IPv6 addresses would enable each individual to connect around 1.2 billion devices to the Net; or, metaphorically speaking: "if all the IPv4 addresses could fit within a Blackberry, it would take something the size of Earth to contain IPv6."[257]

TCP/IP lies at the core of today's Internet. But, in fact, there are far more protocols that directly depend upon TCP/IP. Instead of using a single universal protocol to handle all transmission tasks, a set of cooperating protocols has been (and still is being) developed. Altogether, these network protocols can be segmented by their function along the four layer stack of the so called *Internet Protocol Suite*,[258] which is—due to the importance of its two central protocols—also known as *TCP/IP*.[259] Referring to the four-layer model of cyberspace that was set out in the units of analysis section of the previous part, the TCP/IP protocol stake can be located on the logical (or code) cyber layer containing both the software as well as the protocols that can be incorporated within that software.

[253] For a better overview, IPv4 addresses are usually not displayed in a long line of zeros and ones, but in four groups of decimal numbers, separated by dots and ranging from 0 to 255 (e.g., 208.80.152.2).

[254] See, for instance, ICANN, *To 4,294,967,296 and Beyond – Under 10% of IPv4 Space Remains: Adoption of IPv6 Is Essential*, 29 January 2010, http://www.icann.org/en/announcements/announcement-29jan10-en.htm.

[255] Similar to IPv4 addresses, IPv6 addresses are usually not written in long lines of zeros and ones, but in eight groups of four-digit, case insensitive hexadecimal values (0-9 and A-F/a-f), separated by colons (e.g., 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A).

[256] The World Bank, *World Development Indicators*, September 2011, p. 36, http://data.worldbank.org/data-catalog/world-development-indicators?cid=GPD_WDI.

[257] ICANN, *IPv6 Factsheet*, 26 October 2007, p.3, http://www.icann.org/en/announcements/announcement-26oct07.htm.

[258] IETF, *Requirements for Internet Hosts—Communication Layers (RFC 1122)*, http://tools.ietf.org/html/rfc1122.

[259] Alternatively, network protocols can also be mapped into the seven layers of the *Open Systems Interconnection Model*, also called OSI Model (ISO/IEC, Standard 7498-1:1994).

### 2.1.1.2.4. The Global Domain Name System (DNS)

Building upon TCP/IP, one of the most critical elements of the Internet is its *Domain Name System* (DNS). The DNS is a global addressing system that—through a process called DNS resolution—converts unique machine-readable IP addresses into human-readable domain names (e.g., wikipedia.org). Typically, domain names are used to make content accessible through Internet services such as email or the *World Wide Web* (WWW). Today, almost all Internet activity relies upon a properly functioning DNS. If, for some reason, DNS resolution cannot be ensured, any Internet service will be affected. In this way, a breakdown of the DNS can potentially have significant implications for social layer referent objects such as "society," "the regime," or "the economy" (which is, again, in turn linked to "state" and "society").

When the DNS was created in the 1980s, a single database file called "hosts.txt" was sufficiently enough to map host names to their respective IP addresses.[260] However, especially after Mosaic—the first major graphics supporting browser—was released in 1993, the amount of Web content started to increase exponentially. In August 1995 there were around 18,000 Websites (including sub pages) with domain names and content on the Net,[261] compared to more than 463 million in August 2011.[262] This is a total increase of more than 2.5 million percent over the last 16 years; even though a significant share of this increase was only generated over the last two years.[263]

Due to the growing number of Web content it soon became clear that storing domain names and corresponding IP addresses in one all-encompassing directory was not feasibly manageable. Consequently, the global DNS directory was hierarchically distributed over different name server levels, with 13 *root server locations* on top (10 in the US, and one each in Japan, Holland and Sweden),[264] a considerable contingent of *top-level domain* (TLD) *servers* underneath, and a large number of authoritative *DNS servers* at the very bottom end.[265]

The hierarchic apex of the DNS is the root zone file which is published by the 13 root server

[260] See, for instance, Alfred, Randy, 'June 23, 1983, DNS Test Sets Stage for Internet Growth,' *Wired*, 23 June 2008, http://www.wired.com/science/discoveries/news/2008/06/dayintech_0623#.

[261] Walton, Marsha, 'Web reaches new milestone: 100 million sites', *CNN*, 1 November 2006, http://edition.cnn.com/2006/TECH/internet/11/01/100millionwebsites/

[262] Netcraft, *August 2011 Web Server Survey*, 2011, http://news.netcraft.com/archives/2011/08/05/august-2011-web-server-survey-3.html.

[263] Netcraft, *August 2011 Web Server Survey*, 2011, http://news.netcraft.com/archives/2011/08/05/august-2011-web-server-survey-3.html.

[264] http://root-servers.org/.

[265] See, Kurbalija, Jovan, *An Introduction to Internet Governance*, Malta, DiploFoundation, p. 41.

locations. However, instead of listing all existing server locations in the world, the root zone file only contains information about the TLD servers immediately below it. This means that the authority of the TLD zone only lies with the operator of the respective TLD servers. Once a higher name server level delegates authority for a subordinate zone (or namespace) to a lower level, this lower level has sole responsibility over the zone.

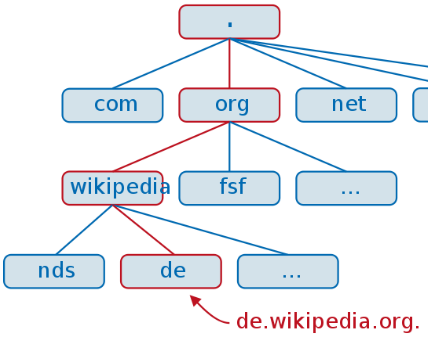

**Figure 3:** DNS Hierarchy[266]

Reading from right to left, this hierarchic organization is reflected in domain names, where dots separate higher level domains at the right side from lower level domains at the left (see graph). In domain names, the root is basically displayed at the rightmost end. In a conventional Web browser, however, the root is usually invisible and separated by an equally invisible dot from the rest of the domain name (de.wikipedia.org" ").

The (visible) top end of domain names is referred to as top-level domain or TLD (de.wikipedia."org"). Currently, there are 312 different TLDs.[267] Most prominently, these can be segmented into *generic TLDs* or *gTLDs* (such as "org", "com" or "info") and *country code*[268] *TLDs* or *ccTLDs* (such as "at", "tv" or "to"). Also, this number includes both a small contingent of different TLDs that are exclusively reserved for the US (such as "gov", "mil" or "edu") and couple of *Internationalized Domain Names* or *IDNs* that have recently been introduced to the DNS (such as "рф" for Russia).[269] Due to a continuing expansion of *Internationalized Domain Names* or *IDNs* (such as the upcoming introduction of "ελ" for Greece) and an expected rollout estimate of 315-40 new gTLDs per year[270] (such as "radio", "car" or "gay"), the current number of TLDs can soon be expected to increase.[271]

Typically, the lower a domain name is located within the DNS hierarchy, the closer it is to the

[266] http://de.wikipedia.org/w/index.php?title=Datei:Dns-raum.svg&filetimestamp=20060206004402
[267] http://www.iana.org/domains/root/db/.
[268] As defined by ISO 3166-1 alpha-2.
[269] http://www.icann.org/en/topics/idn/.
[270] http://www.icann.org/en/topics/new-gtlds/summary-analysis-proposed-final-guidebook-21feb11-en.pdf.
[271] For more information on the ongoing gTLD process see http://newgtlds.icann.org/en/.

individual end-user machine. In our example, the second-level domain (de."wikipedia".org) referred to an organization, the third-level domain ("de".wikipedia.org) indicated the language in which this organization provides Web content. However, even though second level domains often stand for the name or type of a specific institution, this classification does not always hold true and can vary significantly (e.g., in "sex".com, "beer".com or "business".com).[272]

The logic of a hierarchical distributed DNS can best be described by looking at a very simplified example (see graph). For instance, if someone—everything else being equal—wanted to access a website on the Internet (e.g., google.com), his computer would first need to query one of the 13 root server location on top about where to find the relevant TLD server (in this case the "com" server). With this information, the particular TLD server can be located and eventually queried about how to find the DNS server hosting the desired Web site (in this case the "google" server). If, in this very simplified example, the information in the root zone file is suddenly not available anymore, DNS queries would not be resolved sufficiently and the Web site could not be accessed.

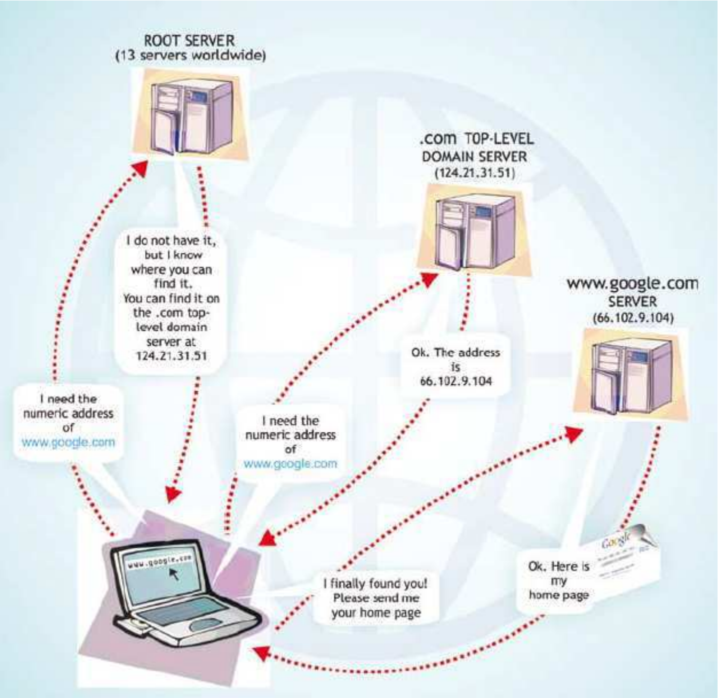
ROOT SERVER
(13 servers worldwide)
.com TOP-LEVEL DOMAIN SERVER (124.21.31.51)
www.google.com SERVER (66.102.9.104)
I do not have it, but I know where you can find it. You can find it on the .com top-level domain server at 124.21.31.51
I need the numeric address of www.google.com
I need the numeric address of www.google.com
Ok. The address is 66.102.9.104
www.google.com
I finally found you! Please send me your home page
Ok. Here is my home page
Google

**Figure 4:** How does the DNS work?[273]

[272] See, for instance, Irvine, Chris, 'Top Ten Most Expensive Domain Names', *The Telegraph*, 10 March 2010, http://www.telegraph.co.uk/technology/news/7412544/Top-10-most-expensive-domain-names.html.

[273] Kurbalija, Jovan, *An Introduction to Internet Governance*, Malta, DiploFoundation, 2010.

However, to give this example a more realistic flavor, root servers are usually not queried every time anew. In most cases the lower level servers will memorize or cache the location of previously searched sites and can directly provide the information needed. As Karrenberg puts it:

> “A well behaved DNS server needs to query the root name servers only once every 48 hours for each particular TLD. In the meantime it can resolve names for that TLD without involvement of the root name servers. Because of this caching almost all DNS queries are answered without involvement of the root name servers.”[274]

One of the biggest advantages of DNS caching is not only the increased query performance achieved by bypassing root servers, but also the redundancy it adds to the DNS. If queries can be resolved (more or less) independently from the root servers, the Internet keeps working even if all 13 root server locations simultaneously disappear.

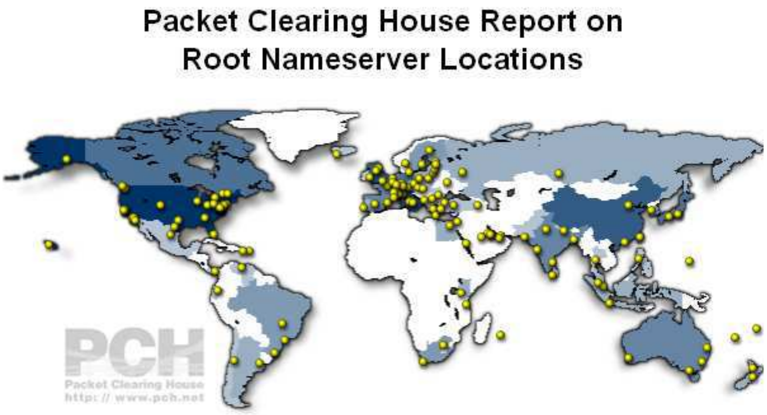

**Figure 5:** Root Name Server Locations[275]

A similar effect is achieved by virtually adding more root server locations to the DNS. Increasing the number of root server locations not only allows for better redundancy, but also for closer proximity, which potentially leads to a quicker response to the users’ query. Increasing the total number of root server locations would also make it necessary to equally increase the corresponding number of IP addresses. For technical reasons, however, this is not possible.[276] Therefore, a technology called *anycast* was developed. Without equally

[274] Karrenberg, Daniel, ‘DNS Root Name Servers Frequently Asked Questions’, *ISOC*, 27 January 2005, ’http://www.isoc.org/briefings/020_v1/.

[275] Packet Clearing House, *Packet Clearing House Report on Root Nameserver Locations*, 8 June 2008, https://prefix.pch.net/applications/ixpdir/summary/root-servers/.

[276] See, for instance, Mitchell, Bradley, ‘Why there are only 13 DNS Root Name Servers,’ *About.com,* 19 November 2008, http://compnetworking.about.com/b/2008/11/19/why-there-are-only-13-dns-root-name-servers.htm.

increasing the total number of 13 IP addresses, anycast allowed for additional server locations all across the world. Today, 9 root server operators make use of anycast which is why, as of June 2011, root servers were operated in more than 239 locations in 69 countries—most of them outside the US (see map).[277]

### 2.1.1.3. Do DNS Disruptions have any Relevance for the Social Layer?

Due to the fact that today almost all Internet activity relies upon properly functioning DNS resolution, in the previous section it has been argued that a breakdown of the DNS can possibly lead to significant implications for social layer referent objects. To look at this argument in more depth, the following section will discuss an (attempted) national-level politicization[278] of DNS risks that was conducted by the US *Department of Homeland Security* (DHS).[279]

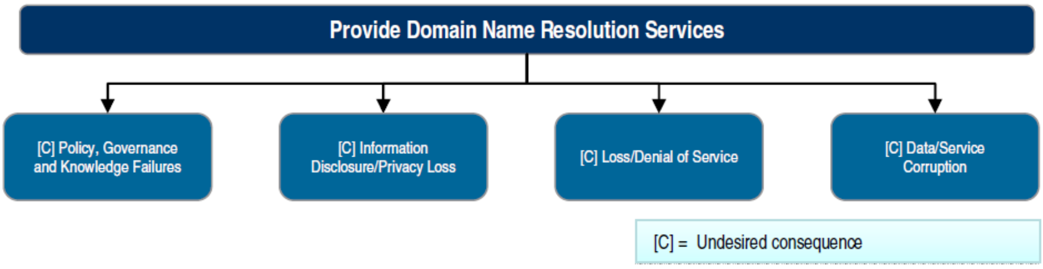
Provide Domain Name Resolution Services
[C] Policy, Governance and Knowledge Failures
[C] Information Disclosure/Privacy Loss
[C] Loss/Denial of Service
[C] Data/Service Corruption
[C] = Undesired consequence

**Figure 6:** Undesired Consequences for the National DNS Infrastructure[280]

In its 2009 *Information Technology Sector Baseline Risk Assessment* (ITSBRA),[281] the DHS together with participating subject-matter experts evaluated national-level risks across six critical IT sector functions,[282] with the provision of DNS resolution being one of them.[283] In an attempt to engage all relevant public and private actors in national risk management, the ITSBRA intended to serve as a "foundation for ongoing national-level collaboration to

[277] Packet Clearing House, *Packet Clearing House Report on Root Nameserver Locations*, 8 June 2008, https://prefix.pch.net/applications/ixpdir/summary/root-servers/.

[278] Politicization refers to the process by which security issues *are devoted to close media and political scrutiny, generating debate and usually multiple policy approaches, while not commanding the threat-urgency modality of securitization*.

[279] Thanks to Prof Milton Mueller for that point.

[280] See DHS, *Information Technology Sector Baseline Risk Assessment*, 2009, pp. 30-9, http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf.

[281] See DHS, *Information Technology Sector Baseline Risk Assessment*, 2009, pp. 30-9, http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf.

[282] The other five critical IT sector functions included the provision of: *IT products and services*; *incident management capabilities*; *identity management and associated trust support services*; *Internet-based content, information, and communications services*; as well as *Internet routing, access, and connection services*)

[283] See DHS, *Information Technology Sector Baseline Risk Assessment*, 2009, pp. 30-9, http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf.

enhance the security and resiliency of the critical IT Sector functions."[284] As regards the provision of DNS resolution, the report distinguished between four "undesired consequences" that could potentially have a negative effect on the national DNS infrastructure (see graph).

1. Policy, governance and knowledge failures refer to the fragmentation of the single interoperable and global Internet into disconnected, separate root systems. Policy failures can be caused for various reasons. The report identifies four principal objectives:
    a. politically-motivated attempts to influence or disrupt DNS operations,
    b. desire for financial gain,
    c. demonstration of technical superiority, and
    d. gratuitous defacement or damage.[285]

   Once the Internet is fragmented, the resultant lack of interoperability between alternate root systems as well as technical confusion over different standards can have "significant economic and national security impacts to the DNS critical function, and [. . .] could result in political and diplomatic tensions between the U.S. and nation-state threat actors."[286] Policy approaches to mitigate these economic and political implications can include further implementation of IDNs, increasing information sharing to build confidence and awareness across the DNS community or conducting exercises to test DNS services.
2. Information Disclosure and Privacy Loss can be caused by mismanagement of cached data files (e.g., through USB drives), bad code (e.g., software vulnerabilities), phishing attacks (e.g., acquiring passwords for bank accounts), insecure wireless networks (e.g., in hotels). There can be various reasons for information disclosure and privacy loss. However, often they are politically or economically motivated. Policy approaches to mitigate risks can include education and training as well as adopting standards and best practices.
3. Loss and Denial of Service can be caused by attacks against DNS infrastructure (e.g., against root servers), inadequately implemented new technologies (e.g., IPv6 or

[284] See DHS, *Information Technology Sector Baseline Risk Assessment*, 2009, p. 4, http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf.
[285] See DHS, *Information Technology Sector Baseline Risk Assessment*, 2009, p. 32, http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf.
[286] DHS, *Information Technology Sector Baseline Risk Assessment*, 2009, p. 32, http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf.

DNSSEC[287]) or bad code (e.g., software vulnerabilities). Such attacks "could include denial or loss of service of electronic education and tracking systems, supply chain issues, disrupted or degraded electronic banking, shipment tracking, and Voice-over-Internet Protocol (VoIP) technologies, and credit trading."[288] Policy approaches to mitigate these implications can include diplomatic and law enforcement responses or improving emergency communications.

4. Data and Service Corruption can be caused by man-in-the-middle or eavesdropping attacks against high-access system administrators of name servers as well as by (malicious) data injection through hacked user accounts or social engineering attacks. By coercing, co-opting or convincing[289] "an employee, the attack could be as simple as shutting down specific network hardware or software components."[290]

In fact, there was no obvious media scrutiny on ITSBRA in the US. However, the collaboration of all relevant public and private actors in the report's preparatory process generated enough debate and policy approaches that one can indeed speak of an (at least attempted) politicization of DNS risks posing an (economic and political) threat to the state as the legitimate social layer referent object. Therefore, to conclude this section, we can maintain our argument that a breakdown of the DNS can potentially have significant implications for social layer referent objects such as "society," "the regime," or "the economy" (which is, again, in turn linked to "state" and "society").

### 2.1.2. Internet Governance

Discussions related to Internet governance issues date at least back to the early 1990s, when the *Harvard Information Infrastructure Project* (HIIP)[291] drew together experts from government, industry, and academia, to elaborate on emerging policy issues related to the development, use and growth of the global information infrastructure (most notably the Internet).[292] The HIIP was intended to serve as an interdisciplinary forum for economists,

[287] For a discussion on obstacles to IPv6 and DNSSEC implementation see Klimburg, Alexander, 'Ruling the domain', *oiip policy paper*, 2011, http://www.oiip.ac.at/publikationen/publikationen-detail/article/104/ruling-the-domain-self-regulation-and-the-security-of-the-internet-1.html.

[288] DHS, *Information Technology Sector Baseline Risk Assessment*, 2009, p. 33, http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf.

[289] For a discussion on coercing, co-opting and convincing private actors in cybersecurity see Klimburg, Alexander, 'The Whole of Nation in Cyberpower', *Georgetown Journal of International Affairs*, Special Edition, 2011, http://www.oiip.ac.at/publikationen/publikationen-detail/article/105/the-whole-of-nation-in-cyberpower.html.

[290] DHS, *Information Technology Sector Baseline Risk Assessment*, 2009, p. 35f, http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf.

[291] http://ksgnotes1.harvard.edu/IIP/HIIP_PG.nsf.

[292] Thanks to Prof Wolfgang Kleinwächter for this point.

lawyers, political scientists and technologists, and culminated in a series of different publications. Their basic assumption was that the Internet had an unprecedented impact on our existing world order. As HIIP key researcher Brian Kahin and Charles Nesson put it:

> "Our experience of geographic space has been transformed by the information revolution, as it was by the railroad and air travel. But the transformation now underway on the Internet is not only greater and qualitatively different. It has collapsed the world, transcending and blurring political boundaries in the process. It gives individuals instant, affordable access to other individuals, wherever they may be, and it enables each to publish to the world."[293]

However, transcending national borders does not simultaneously imply the dissolution of the state. With physical power over people and infrastructure, states will remain important actors. However, what will change is the way how this power is exercised. In an environment where the (trans-border) interaction between people can hardly be confined to the sole jurisdiction of a single state actor, overlapping responsibilities will make it necessary for governments to collaborate with private sector and civil society actors.[294]

In the course of the 1990s, the rather academic debates over Internet governance reached a broader public. When it became clear that the global DNS was not only a single point of technical failure, but also a single point for policy decisions about surveillance and control of access to cyberspace, questions about the difference between technical management on the one hand, and regulatory control on the other were posed. For instance, was the decision to enter a TLD into the root zone file a mere technical issue or is it a public policy issue? For Milton Mueller, "[t]he uncomfortable fact is that the two meanings of 'Internet governance' are inseparably linked."[295]

Increasingly, state actors became aware of the fact that they did not really understand the concrete subject matter of Internet governance. Therefore, in the final document to the 2003 *United Nation's* (UN) *World Summit on the Information Society* (WSIS-I),[296] "the representatives of the peoples of the world"[297] called for setting up a collaborative *Working*

[293] Kahin, Brian and Nesson Charles (eds.), *Borders in cyberspace: information policy and the global information infrastructure*, Cambridge, MIT Press, 1997.

[294] See Reidenberg, Joel, 'Governing Networks and Rule-Making in Cyberspace', in: Kahin, Brian and Nesson Charles (eds.), *Borders in cyberspace: information policy and the global information infrastructure*, Cambridge, MIT Press, 1997, pp. 84-105.

[295] Mueller, Milton, *Ruling the Root: Internet Governance and the Taming of Cyberspace*, Cambridge, MIT Press 2002, p. 10.

[296] http://www.itu.int/wsis/geneva/index.html.

[297] Note that, similar to the 2002 *UN Johannesburg Declaration on Sustainable Development* of the *World Summit on Sustainable Development* (WSSD), the *Geneva Declaration of Principles* does not open with a direct

*Group on Internet Governance* (WGIG). The WGIG should be composed of states as well as the private sector and civil society actors. It had the aim to "investigate and make proposals for action, as appropriate, on the governance of [the] Internet by 2005."[298] After four meetings and with full and active participation of multiple stakeholders—including governments (44%), the private sector (28%) and non-governmental actors (28%)[299] from both developing (59%) and developed countries (41%)[300]—the WGIG delivered a report[301] (and an accompanying background report[302]) that served as an input for the 2005 WSIS in Tunis (WSIS-II).[303] The main recommendation of the WGIG was the creation of a forum that

> "could address [. . .] issues, that are cross-cutting and multidimensional and that either affect more than one institution, are not dealt with by any institution, or are not addressed in a coordinated manner."[304]

This recommendation fundamentally inspired WSIS-II and led to the creation of a multi-stakeholder *Internet Governance Forum* (IGF) which should "identify emerging issues, bring them to the attention of the relevant bodies and the general public, and, where appropriate, make recommendations."[305]

However, WGIG did not only recommend the creation of an Internet-related forum, but also provided a working definition of *Internet governance* that was eventually adopted by WSIS-II. By clearly reflecting the multi-stakeholder spirit behind WGIG and the IGF the definition reads as follows:

> "Internet governance is the development and application by governments, the

reference to "states", "governments" or "nations" (such as "We, heads of states and governments…"), but rather prefers a diction (saying "We, the representatives of the peoples of the world") that potentially leaves enough room for non-state actors to be involved as well. See, for instance, Mestrum, Francine, 'Poverty reduction and sustainable development', in: Hens, Luc and Nath, Bhaskar (eds.), *The World Summit on Sustainable Development. The Johannesburg Conference*, Dordrecht, Springer, 2005, pp. 35-56, p. 40f.

[298] Geneva Declaration of Principles, para. 50 (WSIS-03/GENEVA/DOC/0004), http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160.

[299] Mathiason, John, *Internet Governance. The new frontier of global institutions*, Routledge, New York, 2009, p. 118.

[300] Mathiason, John, *Internet Governance. The new frontier of global institutions*, Routledge, New York, 2009, p. 118.

[301] Report from the Working Group on Internet Governance (WSIS-II/PC-3/DOC/05), p. 3, http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1695|0.

[302] WGIG, *Background Report from the Working Group on Internet Governance*, 2005, http://www.wgig.org/docs/BackgroundReport.doc.

[303] For the website of WSIS-II see: http://www.itu.int/wsis/tunis/index.html.

[304] Report from the Working Group on Internet Governance (WSIS-II/PC-3/DOC/05), pp. 10f, http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1695|0.

[305] Tunis Agenda for the Information Society, para. 72-82 (WSIS-05/TUNIS/DOC/6(Rev. 1)-E), http://www.itu.int/wsis/documents/doc_multi.asp?id=2267|0.

> private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."[306]

This definition is intentionally broad in scope and touches upon a myriad of different issue areas[307] and actors. This is also why, in Internet governance, one cannot speak of one single Internet governance regime, but of multiple regimes (including the DNS regime, intellectual property regime, etc.).[308]

### 2.1.2.1. Multi-Stakeholder Collaboration

Multi-stakeholder collaboration is the main mode of Internet governance. It is the basic pattern or political constellation of interaction. Freedman provided the following definition:

> "A stakeholder in an organization is (by definition) any group or individual who can affect or is affected by the achievement of the organization's objectives."[309]

While the term "stakeholder" only refers to one actor, the expression "multi-stakeholder" refers to at least two of them. Most recently, multi-stakeholder collaboration has been defined as follows:

> "The development and implementation of Internet governance arrangements should ensure, in an open, transparent and accountable manner, the full participation of governments, the private sector, civil society and the technical community, taking into account their specific roles and responsibilities. The development of international Internet-related public policies and Internet governance arrangements should enable full and equal participation of all countries."[310]

The concept of multi-stakeholder collaboration is still in its infancy. To provide a better understanding, we refer to the next section that comprehensively tries to describe probably one of the most prominent examples of multi-stakeholder corporation: the *Internet Corporation for Assigned Names and Numbers* (ICANN).

[306] Tunis Agenda for the Information Society, para. 34 (WSIS-05/TUNIS/DOC/6(Rev. 1)-E), http://www.itu.int/wsis/documents/doc_multi.asp?id=2267|0.

[307] See, for instance, Dutton, William H. and Peltub, Malcolm, 'The emerging Internet governance mosaic: connecting the pieces', *Information Polity*, 12, 2007, pp. 63-81.

[308] Thanks to Prof William Dutton for this point.

[309] Freeman, R. Edward, *Strategic Management: A stakeholder approach*, Toronto, Pitman, 1984m p. 46.

[310] Council of Europe, *Internet Governance Principles*, Strasbourg 18-19 April 2011, http://www.coe.int/t/dghl/standardsetting/media-dataprotection/conf-internet-freedom/Internet%20Governance%20Principles.pdf.

### 2.1.3. The Internet Corporation for Assigned Names and Numbers (ICANN)

After having identified the DNS worth to be linked to a social layer referent object, and multi-stakeholder collaboration as the most characteristic political constellation in Internet governance, we can now move on and uncover a set of potential securitizing actors that are relevant in context of the overall coordination of the global DNS.

Securitizing actors have been defined as those *actors who have enough capabilities*[311] *to potentially succeed in declaring something—a referent object—as existentially threatened; someone, or a group, who performs the security speech act.* In context of the overall coordination of the global DNS, all relevant stakeholders are concentrated in one multi-stakeholder organization called *Internet Corporation for Assigned Names and Numbers* (ICANN).

ICANN is a private-sector nonprofit public benefit corporation organized under the *California Nonprofit Public Benefit Corporation Law* (NPBCL).[312] As one of the few globally centralized points of control and surveillance over the Internet, ICANN is "the main Internet governance institution."[313] To ensure "the stable and secure operation of the Internet's unique identifier systems,"[314] ICANN does essentially three things:

1. coordinate the allocation and assignment of domain names, IP addresses, autonomous system numbers (ASNs)[315] as well as protocol and parameter numbers;[316]
2. coordinate the operation and evolution of the DNS root name server system; and
3. coordinate policy development reasonably and appropriately related to these technical functions.[317]

The strong emphasize on "technical coordination"[318] obfuscates ICANN's public policy functions. In this respect, it is crucial to note that ICANN not only serves a technical function, but also plays a *regulatory role*.[319] Allocating and assigning domain names also implies

[311] Including both Waltzian *material capabilities* as well as Bourdieuan *socio-cultural capabilities*.

[312] http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=corp

[313] Kurbalija, Jovan, *An Introduction to Internet Governance*, Malta, DiploFoundation, p. 171.

[314] http://www.icann.org/en/general/bylaws.htm#I

[315] An *autonomous system* (AS) is defined as a domain of IP networks using a particular *Interior Gateway Protocol* (IGP) that determines how data packets are forwarded within the system. These independent domains are interconnected through *Exterior Gateway Protocols* (EGP), most prominently the *Border Gateway Protocol* (BGP). In this context, an ASN is a mere indicator for a specific domain with the size of an ISP or end user entity.

[316] For the purpose of this study, however, it is especially domain names and IP addresses that are relevant.

[317] http://www.icann.org/en/general/bylaws.htm#I

[318] http://www.icann.org/en/faq/.

[319] See Mueller, Milton, 'Dancing the Quango: ICANN and the Privatization of International Governance'

important policy decisions about the market supply of new TLDs. These can either be driven by trademark interests or different concerns about the appropriateness of specific TLDs. More recently, however, ICANN has also tried to strengthen its *security role*.[320] In this way it increasingly started to commit itself to questions about the deployment of security measures in the DNS and about how to make its stakeholders comply with cost-intensive solutions. Consequently, the management of the DNS is not only about technical issue, but also about public policy issues.

From this perspective, it is interesting why global DNS policy making is carried out by a newly established Californian private-sector corporation, and not—as was the case with telegraphy, telephony and radio communication—by a venerable intergovernmental Geneva-based organization such as the *International Telecommunication Union* (ITU). In fact, the choice to establish ICANN must be understood in context of the strong desire to liberalize US telecommunications after the 1984 breakdown of the AT&T monopoly. After the US had successfully managed to quickly change to an open-competitive market, it was feared that other countries, which followed a slower path of privatization (such as most countries in Europe), could have a negative impact on prizes in the US telecommunication market.[321] This general spirit reached its peak with the publication of the Clinton administration's *Framework for Global Electronic Commerce* (FGEC), which set forth principles of private sector leadership and industry self-regulation.[322]

Having emphasized US concerns about restrictions to competition as being the driving force behind ICANN's creation, we can now look in more depth at the historic processes around ICANN's formation.

### 2.1.3.1. From Postel to ICANN

In its early days DNS administration was solely handled by one particular person: Jon Postel, a computer scientist and Internet pioneer working at the *University of California* (UCLA).[323] Under contract with DARPA, Postel held exclusive policy authority over the name and address space and was responsible that all the assigned names and numbers were unique throughout the Internet. In this role, he has lovingly been referred to as a "[b]eared and

[320] See Klimburg, Alexander, 'Ruling the Domain: (Self) Regulation and the Security of the Internet', *oiip policy paper, 2011*, http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/Ruling_the_Domain_Klimburg.pdf.

[321] See, for instance, Noll, Michael, 'Telecommunication privatisation: mixed progress', *info*, 2, 1, 2000, pp. 21-3, http://www.emeraldinsight.com/journals.htm?articleid=873852&show=pdf

[322] http://clinton4.nara.gov/WH/New/Commerce/.

[323] http://www.postel.org/postel.html

sandaled [. . .] resident hippie-patriarch"[324] and the "'benevolent dictator' of the network."[325] In 1990, Postel's function became to be known as the *Internet Assigned Numbers Authority* (IANA).

However, after the *World Wide Web* was successfully introduced as an application on the Internet, the number of domain name registrations started to grow exponentially, "from 300 per month in 1992 to 45,000 per month by late 1995."[326] The sudden rush for unique domain names during the 1990s quickly led to a legal conflict between trademark owners and Jon Postel as IANA, who did not sufficiently provide private property protection procedures against misuse and speculation with trademarked names.

Looking for a better legal and financial framework, Postel suggested moving the IANA function from DARPA into the newly created private non-profit *Internet Society* (ISOC). This proposal was immediately challenged by the US government who viewed this move as "a privatization of the root without any formal legal authority."[327] But also the *International Telecommunication Union* (ITU) and several private actors raise doubts about ISOC's political legitimacy and legal authority to adequately handle the administration of the root.

As a result, in 1996, ISOC forged ahead and pulled together its most influential critics (including the *International Trademark Association* (INTA) and the *World Intellectual Property Organization* (WIPO)) in an *International Ad Hoc Committee* (IAHC) that ultimately resulted in the creation of a *Memorandum of Understanding* (MoU)[328] under the ITU. In effect, the MoU called for the establishment of an international self-regulatory framework for the administration and management of the DNS.

The newly established international framework, however, triggered governmental resentment. As Mueller reports:

> "In late April 1997 US Secretary of State Madeline Albright wrote a memo criticizing the ITU Secretariat for acting 'without authorization of member governments' to hold [. . .] 'a global meeting involving an unauthorized expenditure of resources and

[324] Cerf, Vint, 'RFC 2468 I Remember IANA', 1998, http://tools.ietf.org/html/rfc2468

[325] Goldsmith, Jack and Wu, Tim, *Who controls the Internet, Illusions of a Borderless World*, Oxford, Oxford University Press, 2006, p. 34.

[326] Mueller, Milton, 'ICANN and Internet governance. Sorting through the debris of self-regulation', *info*, 1, 6, 1999, p. 500.

[327] Mueller, Milton, 'ICANN and Internet governance. Sorting through the debris of self-regulation', *info*, 1, 6, 1999, p. 501.

[328] ITU, *gTLD-MoU*, 28 Februar 1997, http://www.itu.int/net-itu/gtld-mou/gTLD-MoU.htm.

> concluding with a quote international agreement unquote."[329]

But also the *European Commission* (EC) chimed in on the chorus of criticism over the MoU and claimed "it was 'too US-centric' and demanding more EC representation and 'further public debate.'"[330] Lacking the necessary recognition, the MoU was consequently taken from the political agenda and replaced by a US Green Paper.[331] The Green Paper was submitted for public comment in February 1998 by the *Department of Commerce* (DoC) that, through the *Presidential Directive on Electronic Commerce*, has been officially authorized

> "to support efforts to make the governance of the domain name system private and competitive and to create a contractually based self-regulatory regime that deals with potential conflicts between domain name usage and trademark laws on a global basis."[332]

In this context, the Green Paper essentially suggested the establishment of a newly created US-based, private not-for-profit corporation that would promote international participation in the DNS and displace DARPA's role as the legal home for IANA. Unsurprisingly, the Green Paper was mainly criticized for its US-centric orientation:[333]

> "The E.U. criticized U.S. dominance over the Internet and called for an international representative body for future Internet governance. 'The European Union and its Member States would wish to emphasis [sic] our concern that the future management of the Internet should reflect the fact that it is already a global communications medium and the subject of valid international interest."[334]

In response to the public concerns about potential US government control over the new corporation, the US DoC made important changes that in June 1998 finally led to the release

[329] Mueller, Milton, 'ICANN and Internet governance. Sorting through the debris of self-regulation', *info*, 1, 6, 1999, p. 502.

[330] Mueller, Milton, 'ICANN and Internet governance. Sorting through the debris of self-regulation', *info*, 1, 6, 1999, p. 502.

[331] NTIA, *Improvement of Technical Management of Internet Names and Addresses; Proposed Rule*, 20 February 1998, http://www.ntia.doc.gov/federal-register-notice/1998/improvement-technical-management-internet-names-and-addresses-proposed-

[332] Presidential Directive on Electronic Commerce, *Memorandum for the Heads of Executive Department and Agencies*, 1 July 1997, http://www.thecre.com/fedlaw/legal25e/presiden.htm.

[333] See Mathiason, John, *Internet Governance. The New Frontier of Global Institutions*, Oxford, Routledge, p. 55.

[334] Kleinwächter, Wolfgang, 'From self-governance to public-private partnership: The changing role of governments in the management of the Internet's core resources', *Loyola of Los Angeles Law Review*, 36, 2003, pp. 1103-1122, p. 1111.

of a White Paper.[335] Therein, the DoC confirmed that it would

> "recognize the need for and fully support mechanisms that would ensure international input into the management of the domain name system. In withdrawing the U.S. Government from DNS management and promoting the establishment of a new, non-governmental entity to manage Internet names and addresses, a key U.S. Government objective has been to ensure that the increasingly global Internet user community has a voice in decisions affecting the Internet's technical management."[336]

The DoC's commitment to a process of self-regulation in the establishment of an international non-governmental DNS entity was hopefully picked up and widely taken at face value. This was especially true for large parts of the Internet community who were effectively calling for an *International Forum on the White Paper* (IFWP). In the time between June and August 1998, the IFWP included a series of open multi-stakeholder discussions, electronic mailing lists and workshops with participants from all around the world. In order "to prepare for the transition from government to private management,"[337] the self-imposed aim of the forum's participants was to draft a legal framework for the new DNS corporation.[338]

Meanwhile, IANA and ISOC started a separate initiative outside the IFWP process. Although "IANA participated in every one of the IFWP meetings,"[339] Postel, together with a corporate lawyer,[340] produced his own set of draft articles and bylaws, posted them online and tried to incorporate the comments he received into a revised version.[341] This procedure was similar to the procedures usually applied by IETF members for developing Internet standards

[335] See NTIA, *Statement of Policy on the Management of Internet Names and Addresses*, 5 June 1998, http://ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses.

[336] US DoC, *Management of Internet Names and Addresses*, 5 June 1998, http://www.icann.org/en/general/white-paper-05jun98.htm.

[337] http://www.ifwp.org/press.html

[338] See Kleinwächter, Wolfgang, 'From self-governance to public-private partnership: The changing role of governments in the management of the Internet's core resources', *Loyola of Los Angeles Law Review*, 36, 2003, pp. 1103-1122, p. 1113.

[339] Postel, Jon quoted in: Kleinwächter, Wolfgang, 'From self-governance to public-private partnership: The changing role of governments in the management of the Internet's core resources', *Loyola of Los Angeles Law Review*, 36, 2003, pp. 1103-1122, p. 1114.

[340] See Mueller, Milton, 'ICANN and Internet governance. Sorting through the debris of self-regulation', *info*, 1, 6, 1999, p. 506

[341] See Postel, Jon, *Testimony of Jon Postel*, Congressional Hearing 7 October 1998, http://news.dot-nxt.com/1998/10/07/postel-testimony.

through RFCs.[342] However, as Jeremy Malcolm put it,

> "[t]he IFWP participants [. . .] were not the same body of broadly like-minded engineers with which the IETF was accustomed to deal, and they proved not nearly so compliant. They rejected IANA's invitation to use its draft bylaws as a basis for discussion, on the ground that it pre-empted the achievement of consensus that the discussion was designed to forge."[343]

In a final meeting that was scheduled around September 1998, the members of the IFWP intended to assemble their points of consensus[344] in a set of proposals in order to submit them to the DoC. They invited IANA to join the meeting and to provide some final input. However, this time, IANA stroke back and rejected to appear. It announced that it had already obtained agreement on its own revised bylaws purporting to reflect the IFWP consensus."[345] But it got even worse: "IANA's supporters on the IFWP steering committee, most notably Mike Roberts [one of ISOC's founders], pushed to disband the IFWP instead of holding a wrap-up meeting."[346] As a result, the IFWP was dissolved.

In October 1998, IANA submitted its proposal to the DoC in which it was calling for the creation of the *Internet Corporation for Assigned Names and Numbers* (ICANN). Unexpectedly, a small group of undiscouraged IFWP members returned, referring to themselves as the Boston Group. By putting together what they regarded to be the real consensus of the IFWP process, they also made a competing submission to the DoC.[347] However, in the end the DoC only recognized IANA's proposal, notwithstanding the strong recommendation to consult with other groups and review the submitted proposal in order "to broaden the consensus."[348]

[342] Malcolm, Jeromy, *Multi-Stakeholder Governance and the Internet Governance Forum*, Perth, Terminus Press, 2008, p. 36.

[342] http://cyber.law.harvard.edu/ifwp/consensuslist.asp.

[343] Malcolm, Jeromy, *Multi-Stakeholder Governance and the Internet Governance Forum*, Perth, Terminus Press, 2008, p. 36.

[344] http://cyber.law.harvard.edu/ifwp/consensuslist.asp.

[345] Malcolm, Jeromy, *Multi-Stakeholder Governance and the Internet Governance Forum*, Perth, Terminus Press, 2008, p. 36.

[346] Mueller, Milton, 'ICANN and Internet governance. Sorting through the debris of self-regulation', *info*, 1, 6, 1999, p. 507.

[347] Boston Working Group, *Management of Internet Names and Addresses*, 28 September 1998, http://www.ntia.doc.gov/legacy/ntiahome/domainname/proposals/bosgrp/submission-letter.html.

[348] US DoC, *Internet Corporation for Assigned Names and Numbers*, 20 October 1998, http://ntia.doc.gov/legacy/ntiahome/press/icann102098.htm.

### 2.1.3.2. Struggle for Legitimacy

The widespread discontent over ICANN's formation laid the basis for its deep-seated legitimacy problem. As holds Andrew Hurrell, "questions of legitimacy emerge whenever power is exercised in the context of competing interests and conflicting values."[349] This was most obvious during the history of ICANN's formation. However, after its inception substantive doubts about ICANN's legitimacy remained. While state actors (first and foremost the EC) criticized the US administration's unilateral engagement during ICANN's formation, IFWP members were highly dissatisfied about the dismissal of their community consensus. This frustration was aggravated when it became clear that many of John Postel's self-selected board members were unfamiliar with technical issues concerning the Internet and only slowly adapted to both the community's mores and its open approach to communication.

As if this were not enough, the DoC did not keep its promise to transfer the management of the DNS to a new, non-governmental entity. Instead, it retained leverage over ICANN through a set of different contracts.[350] Most importantly, it signed a *Memorandum of Understanding* (MoU) with ICANN, specifying a list of objectives for ICANN to accomplish before the DoC would release it from official oversight as a fully non-governmental entity. From 1999 to 2003 this document was amended six times and ultimately replaced by a *Joint Project Agreement* (JPA) in 2007. In essence, the JPA has been perceived as yet another amendment to the MoU[351] and effectively squeezed the "outstanding" modifications to ICANN's policy making in a biblical series of ten key responsibilities. In 2008, ICANN's board claimed that these requirements were already met and proposed that the JPA was no longer necessary.[352] In 2009, the JPA expired without being extended. Instead, the DoC and ICANN entered into an *Affirmation of Commitment* (AoC).[353] Under the AoC, ICANN commits itself to "remain a not for profit corporation, headquartered in the United States of America with offices around the world to meet the needs of a global community"[354] and to establish review panels that would regularly make recommendations.

[349] Hurrell, Andrew, *On Global Order. Power, Values, and the Constitution of International Society*, Oxford, Oxford University Press, 2007, p. 116.

[350] See ICANN, *ICANN's Major Agreements and Related Reports*, http://www.icann.org/en/general/agreements.htm

[351] See Mueller, Milton, 'What is the JPA?', *Internet Governance Project*, 8 February 2008, http://blog.internetgovernance.org/blog/_archives/2008/2/8/3512862.html .

[352] See ICANN, *ICANN's Response to the JPA Midterm Review*, http://www.icann.org/en/jpa/.

[353] See ICANN, *Affirmation of Commitment*, http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm

[354] See ICANN, *Affirmation of Commitment*, http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm

A second important instrument for the US to conduct oversight over ICANN is through the *IANA functions contract*. Most importantly, these functions contain the allocation of IP address blocks and the editing of the root zone file. However, any changes in the root zone file must be approved by the DoC.[355]

In a multi-stakeholder environment such as Internet governance, a lack of stakeholder support for an organization's control over a key infrastructure has been considered to be problematic. As Weinberg points out:

> "To the extent that its legitimacy was less secure, ICANN would be forced to concede greater autonomy to other actors. If its legitimacy collapsed entirely, it might see large segments of the community defecting to alternative root systems."[356]

In this context, it is interesting to observe how ICANN mobilized a whole series of different tactics to tackle its legitimacy problem. [357] For instance, soon after its incorporation, ICANN tried to calm tempers by positioning itself as a primarily technical body. One of the most prominent examples in constructing ICANN as a politically and normatively neutral body was brought forward by Esther Dyson, the first chair on ICANN's board. In 1999, she claimed:

> "ICANN does not 'aspire to address' any Internet governance issues; in effect, it governs the plumbing, not the people. It has a very limited mandate to administer certain (largely technical) aspects of the Internet infrastructure in general and the Domain Name System in particular."[358]

A second strategy to bolster its legitimacy was ICANN's attempt to conduct global online elections. In 2000, the board decided that five of its then nineteen members should be elected for two years by Internet users[359] all around the world ("at-large"); each representing one of the five ICANN regions (including Africa, Asia/Australia/Pacific, Europe, Latin America/Caribbean, and North America).[360] Funding was provided by the US *Markle*

[355] See Mueller, Milton, *Networks and States. The Global Politics of Internet Governance*, Cambridge, MIT Press, 2010, p. 62.

[356] Weinberg, Jonathan, 'ICANN and the Problem of Legitimacy', *Duke Law Journal*, 50, 1, 2000, pp. 187-260, p. 215.

[357] For a discussion on ICANN's struggle to handle its legitimacy problem see: Weinberg, Jonathan, 'ICANN and the Problem of Legitimacy', *Duke Law Journal*, 50, 1, 2000, pp. 187-260, pp. 225-57; and Weinberg, Jonathan, 'Non-State Actors and Global Informal Governance—The Case of ICANN', International Handbook on Informal Governance, 7 June 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1621862.

[358] Nader, Ralph, *Esther Dyson's Response to Ralph Nader's Questions*, 15 Juni 1999, http://www.icann.org/en/correspondence/dyson-response-to-nader-15jun99.htm.

[359] In this case, an Internet user is someone with an email address.

[360] http://www.icann.org/en/announcements/icann-pr21sep00.htm

*Foundation*[361] and online voting was outsourced to a global Internet election company (election.com). In total, 158,593 people registered to vote. After having received their *personal identification number* (PIN), 76,183 also activated their membership, and 34,035 actually voted.[362] It was especially in North America and Europe, where most of the public discussions came from, where ICANN's candidates were all defeated by established critics. While Andy Müller-Maghun, the European winner of the election, was described as an "anarchist hacker" and member of the Computer Chaos Club, Karl Auerbach, the North American victor, was affiliated with the Boston Group.[363] As a board member, together with the *Electronic Frontier Foundation* (EFF), Auerbach ultimately sued ICANN for denying access to corporate documents.[364] As a result, the at-large election was effectively abolished. As Mueller points out:

> "The 'Internet community consensus' that ICANN had been claiming since its inception seemed not to exist. Following its decisive defeat in the elections, the ICANN management and board acted to contain the elected board members and minimize their impact. The bylaws were altered to keep the newly elected directors out of the selection process for new TLDs. A new executive committee of the board was formed that excluded the maverick members."[365]

However, for Weinberg, ICANN's key strategy for gaining legitimacy was not the establishment of broad community consensus. Rather, it was its "institutional isomorphism;"[366] the move to adapt the mores and structures of those entities it ultimately depended upon: state actors, big ISPs and root server operators. Neither of them had much experience with the Internet community's anarchic tradition of "rough consensus." They had their particular interests, and the best way to materialize them was "a structure that was elite-oriented, bureaucratized, and corporate-modelled, with privileged roles reserved for

[361] See http://www.markle.org/.

[362] For a comprehensive report on ICANN's elections see Aizu, Izumi, The NGO and Academic ICANN Study (NAIS), August 2001http://kambing.ui.ac.id/onnopurbo/library/library-ref-eng/ref-eng-1/application/policy/statistics/naisreportA4.pdf.

[363] See Mueller, Milton, *Ruling the Root. Internet Governance and the Taming of Cyberspace*, Cambridge, MIT Press, 2002, p. 200.

[364] See Bowman, Lisa, 'EFF sues ICANN over corporate records', *CNET News*, 18 March 2002, http://news.cnet.com/EFF-sues-ICANN-over-corporate-records/2110-1023_3-862461.html

[365] See Mueller, Milton, *Ruling the Root. Internet Governance and the Taming of Cyberspace*, Cambridge, MIT Press, 2002, p. 200f.

[366] Powell, Walter W. and Paul J. DiMaggio, *The New Institutionalism in Organizational Analysis*, Chicago: University of Chicago Press, 1991.

governments and representatives of specific industry segments."[367] In this respect, one of most important beneficiaries was ICANN's staff. As Weinberg writes:

> "ICANN staff, for their part, sought to maximize their own autonomy and to increase their own empires. In that connection, a role as neutral facilitator of the consensus emerging from an IETF-modelled process was less appealing to them than was a role steering a self-sufficient, self-perpetuating, staff-dominated, ever-growing organization."[368]

It is important to add that this process of institutional isomorphism was additionally bolstered by the immense increase in revenues over the last six years (see next section). Since ICANN is chartered as a nonprofit corporation, it simultaneously had to spend all of these additional revenues each year. As a result, ICANN started to bureaucratize itself. Just one example for this is the increasing number of multilingual documents that are simultaneously published on the ICANN Web site.

However, even though ICANN was heavily engaged in finding a way to overcome its legitimacy problem over the years since its inception, this struggle is an ongoing project and has not been solved yet.

### 2.1.3.3. Board of directors

As was shown in the previous section, the creation of ICANN was the result of a complex process between a myriad of different actors. Unsurprisingly, this complexity is clearly reflected in ICANN's organizational structure. Since its inception, ICANN's bylaws have been amended 31 times.[369] However, the board has consistently been the central decision-making body of the organization—even though the number of board members has changed frequently.

Currently, there are 21 members on the board: 16 voting, and 5 non-voting members. All board members represent a specific group of constituencies that all have a stake in the overall coordination of the global DNS. Thus, the selection of the board shall ensure that at all times each of the five geographic regions[370] shall have at least one voting member (not

[367] Weinberg, Jonathan, 'Non-State Actors and Global Informal Governance—The Case of ICANN', *International Handbook on Informal Governance*, 7 June 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1621862, p. 25.

[368] Weinberg, Jonathan, 'Non-State Actors and Global Informal Governance—The Case of ICANN', *International Handbook on Informal Governance*, 7 June 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1621862, p. 25f.

[369] See http://www.icann.org/en/general/archive-bylaws/.

[370] Europe; Asia/Australia/Pacific; Latin America/Caribbean islands; Africa; and North America

including the President).[371]

The *Nominating Committee* (NomCom) delegates eight voting members to the board. NomCom acts on behalf of the broad interests of the global Internet community as a whole. Therefore, it is composed of all other board member stakeholder groups. NomCom is responsible for the selection of all ICANN board members, except the President and the supporting organizations.

The *Address Supporting Organization* (ASO) delegates two voting members to the board. ASO members act on behalf of the five existing *Regional Internet Registries* (RIRs), consisting of the *African Network Information Centre* (AfriNIC), the *Asia Pacific Network Information Centre* (APNIC), the *American Registry for Internet Numbers* (ARIN), *Latin American and Caribbean IP Address Regional Registry* (LACNIC), *RIPE Network Coordination Centre* (RIPE NCC). RIRs receive Internet number resources (IP address blocks and AS numbers) from IANA and manage, distribute, and register them within their respective regions.

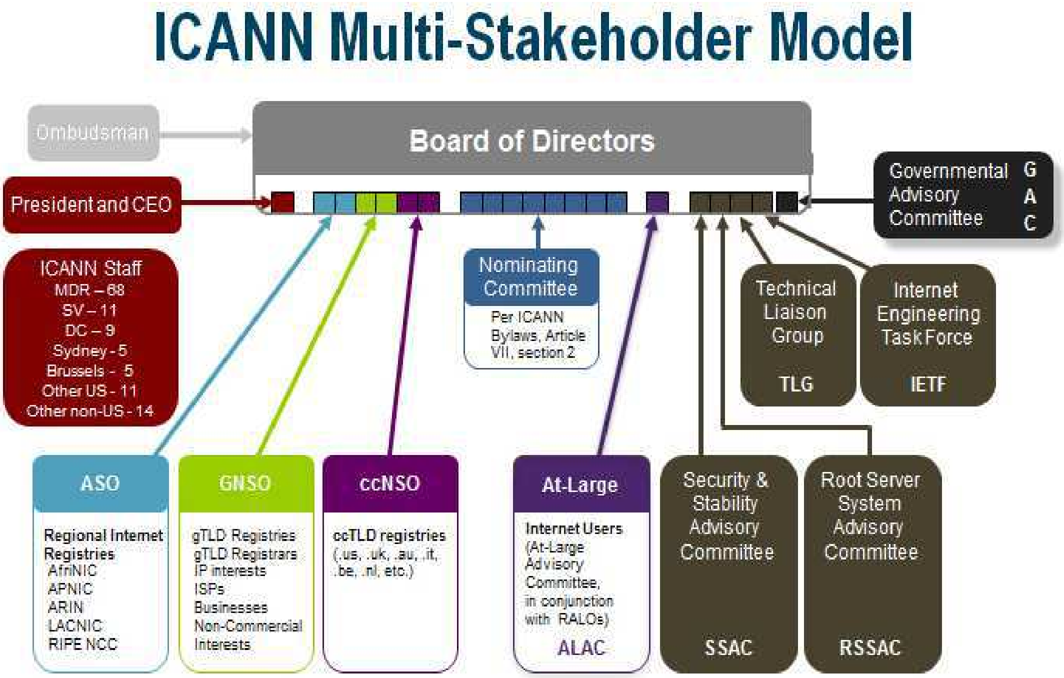

**Figure 7:** ICANN Board of Directors[372]

The *Country-Code Names Supporting Organization* (ccNSO) delegates two voting members to the board. The ccNSO represents ccTLD managers (managing the registration of domain

[371] This overview heavily builds upon the ICANN bylaws (as of 8 December 2011).

[372] See http://www.icann.org/en/about/.

names under their respective ccTLD) who have agreed to be members of the ccNSO. However, a ccNSO member may resign from membership at any time. The ccNSO is responsible for global policies relating to ccTLDs.

The *Generic Names Supporting Organization* (GNSO) delegates two voting members to the board. The GNSO represents the entirety of all gTLD registries (managing the registration of domain names under their respective gTLD), registrars (selling domain names under their accredited gTLD and/or ccTLD) and commercial stakeholders such as *Internet Service Provider* (ISPs). GNSO is responsible for developing and recommending to the ICANN Board substantive policies relating to gTLDs.

The *At-Large Advisory Committee* (ALAC) delegates one voting members to the board. ALAC represents the individual Internet users within their *Regional At-Large Organizations* (RALO) and shall advice ICANN on issues that are of any interest for individual Internet users.

The *President* serves as the *Chief Executive Officer* (CEO) of ICANN and has one vote (ex officio). The President and CEO is in charge of all of ICANN's activities and business. All other officers and staff have to report to him. (For a more in depth analysis of how ICANN's previous Presidents and CEOs shaped the organization, see the following section).

The *Governmental Advisory Committee* (GAC) delegates one non-voting member to the board. In principle, the GAC is open to all national governments and distinct economies as recognized in international fora. On invitation of the GAC, also multinational governmental organizations and treaty organizations may participate. The GAC advices ICANN on activities that relate to concerns of governments, particularly where ICANN's policies interact with various laws and international agreements or where they may affect public policy issues.

The *Root Server System Advisory Committee* (RSSAC) delegates one non-voting member to the board. Membership to the RSSAC is open to each operator of a root name server.[373] RSSAC provides advice to the board about operational requirements of root name servers, including host hardware capacities, operating systems and name server software versions, network connectivity and physical environment. The RSSAC also gives advice on security aspects of the root name server system and reviews the number, location, and distribution of root name servers considering the total system performance, robustness, and reliability.

The *Security and Stability Advisory Committee* (SSAC) delegates one non-voting member to the board. Chair and members are appointed by the board for a three-year term. The SSAC advises the ICANN community and board on matters relating to the security and integrity of

[373] As listed on ftp://ftp.internic.net/domain/named.root.

the DNS. In doing so, the SSAC is responsible to communicate on security matters with the Internet technical community, the operators and managers of critical DNS infrastructure services, the root name server operator community, the TLD registries and registrars and others as events and developments dictate. Furthermore, SSAC shall conduct threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie. The committee shall also communicate with those who have direct responsibility for DNS security matters (IETF, RSSAC, RIRs, name registries, etc.), publish periodical reports and make policy recommendations to the board.

The *Technical Liaison Group* (TLG) delegates one non-voting member to the board. The TLG shall consist of the *European Telecommunications Standards Institute* (ETSI), the *International Telecommunications Union's Telecommunication Standardization Sector* (ITU-T), the *World Wide Web Consortium* (W3C), and the *Internet Architecture Board* (IAB). The TLG shall connect the board with technical advice on specific matters adequate to ICANN's activities.

The *Internet Engineering Task Force* (IETF) delegates 1 non-voting member to the board. There is no more information about the specific responsibilities of IETF in ICANN's bylaws.

#### 2.1.3.4. Previous Presidents and CEOs

To date, all of ICANN's Presidents and CEOs have left their characteristic mark on the organization.[374] This becomes obvious when looking at their overall accomplishments while being in office.

Appointed by the interim board chaired under Esther Dyson, the first President and CEO of ICANN was Mike Roberts (1998-2001).[375] Roberts had an academic background in information technology and a sound understanding of the Internet community's mores. His tenure was characterized by a strong commitment to broad community consensus which is clearly expressed in his warning farewell remarks as interim President and CEO:

> "Frequently, as is the case with several of the agenda items for today, we must seek that broad middle ground which represents consensus. The Board must strip away the fevered advocacy, the impure exhortations, the arguments from limited knowledge and find the essence of the contending views on which it may make a

[374] Thanks to Désirée Miloshevic for that point.

[375] For a biographical note see http://www.icann.org/en/biog/roberts.htm.

> reasoned decision."[376]

Roberts was followed by Stuart Lynn (2001-2003).[377] Similar to his predecessor, Lynn was closely related to the Internet community's open approach to communication. During his time in office, Lynn not only reformed considerable parts of ICANN's structures, but also tried to give every stakeholder a voice in this process.[378] Unsurprisingly, it was also during Lynn's term as President and CEO that ICANN successfully conducted global online elections for five of the then nineteen board members. However, it was also under Lynn that Karl Auerbach, the North American winner of the elections, sued ICANN for denying access to corporate documents.

ICANN's third President and CEO was Paul Twomey (2003-2009).[379] As opposed to his predecessors, Twomey had both a business and governmental background. He had previously served as a member of ICANN's *Governmental Advisory Committee* (GAC) (see below). He represented ICANN in international fora such as the Tunis WSIS, and played an important role in strengthening ICANN's GAC. After Twomey announced his departure, Peter Dengate Thrush, then chairman of the board, assessed Twomey's time as President and CEO as follows:

> "He was involved in its set up, helped establish the role of governments in his term as founding chair of the GAC, and then was its longest serving CEO. He guided the organization through the World Summit on the Information Society in 2005 and has been one of the strongest and most persuasive advocates for the multi-stakeholder model of Internet governance."[380]

Probably one of ICANN's most controversially discussed Presidents and CEOs was Rod Beckstrom.[381] Previously being a Silicon Valley entrepreneur and author, in 2008 Beckstrom became director of the US *National Cybersecurity Center* (NCSC) at the *Department of Homeland Security* (DHS). After less than a year, Beckstrom stepped down, complaining that the intelligence community not only dominated most national cyber efforts, but also made it difficult for the DHS to do their job and work together with stakeholders at all possible levels of federal, state and local government, and the private sector.[382] In 2009, Beckstrom became

[376] http://www.icann.org/en/meetings/melbourne/roberts-remarks-12mar01.htm.
[377] For a biographical note see http://www.icann.org/en/biog/lynn.htm.
[378] See Mathiason, John, *Internet Governance. The New Frontier of Global Institutions*, London, Routledge, 2009, p. 82f.
[379] For a biographical note see http://www.icann.org/en/biog/twomey.htm.
[380] http://www.icann.org/en/announcements/announcement-02mar09-en.htm
[381] For a biographical note see http://www.icann.org/en/biog/beckstrom.htm.
[382] See http://www.washingtontimes.com/news/2009/mar/12/cyber-security-chief-resigns-in-protest/.

President and CEO of ICANN. The expectations were high, not least due to a book he had co-authored, in which he compared leaderless starfish models of organization on the one hand with leader-orientated spider models on the other.[383] Notwithstanding, soon voices were being raised that Beckstrom seemed more like a spider that was concentrating more and more power on top.[384] However, even though it is difficult to charge Beckstrom's achievements while he is still in office, Klimburg holds that ICANN under Beckstrom characteristically started to extent its role as an international security actor.[385]

### 2.1.3.5. Economic capabilities

Additionally to looking at votes, membership, responsibilities and individual persons, we also need to get an awareness of the different stakeholders' economic capabilities. While acknowledging that socio-cultural capabilities (such as individual knowledge, skills or education)[386] also play an important role in securitization theory, in the following section, we will primarily focus on material capabilities.

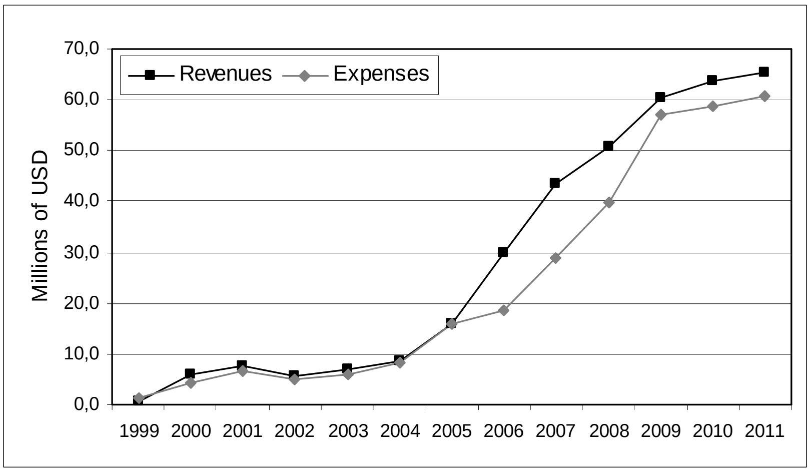

**Figure 8:** ICANN Revenues vs. Expenses (1999-2011)[387]

[383] See Brafman, Ori and Beckstrom, Rod A., *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*, Penguin Group, New York, 2006.

[384] See, for instance, McCarthy, Kieren, 'ICANN Fires it CEO,' *.nxt*, 16 August 2011, http://news.dot-nxt.com/2011/08/16/icann-fires-ceo.

[385] Klimburg, Alexander, 'Ruling the Domain: (Self) Regulation and the Security of the Internet', *oiip policy paper*, 2011, http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/Ruling_the_Domain_Klimburg.pdf.

[386] See Bourdieu, Pierre, 'The forms of capital', in Richardson, John G. (ed.), *Handbook of Theory and Research for the Sociology of Education*, New York, Greenwood, 1986, pp. 241-258.

[387] Data derived from http://www.icann.org/en/financials/historical.htm; a similar table has been published in Mueller, Milton, *Networks and States. The Global Politics of Internet Governance*, Cambridge, MIT Press, 2010, p. 219.

To get an impression of the different stakeholder's economic capabilities, we look at their financial contributions to ICANN's total revenue (as exposed in ICANN's current operating plan and budget).[388] ICANN's operating activities are almost entirely financed by generic registries and registrars. Due to an increased demand for domain names over the last couple of years, ICANN's revenues have increased by a factor of about ten every year since 2006. Due to the fact that ICANN is a nonprofit corporation under the California NPBCL, it simultaneously had to increase its expenditures. This not least

From the expected 2012 total revenue of $69.8 million, a share of $34.8 million are expected to be transferred from gTLD registries, and $30.9 million from registrars that have been accredited by ICANN and the respective gTLD and ccTLD registries. The remaining $4.1 million are acquired from ccTLD registries ($1.6 million), sponsorships ($900,000), RIRs ($823,000), and IDN ccTLDs ($780,000).[389]

While RIRs and ccTLD contribute annually, gTLD registries hold individual temporary contracts in which different types of fees are determined. Essentially, there are *fixed* and *transaction-based fee* contracts. Fixed fees are paid annually by eight gTLDs. However, from an estimated total amount of $18 million, only $90,500 can be expected to come from TLDs other than .com—which is run by Verisign. Similarly, as regards transaction-based fees, from an estimate of $16.7 million, a share of $10.5 million can be expected to be transferred from the .net registry—which is also run by Verisign.[390]

Along with gTLDs, registrars provide the second biggest source for ICANN's revenues. Currently there are over 960 registrars that are accredited by both ICANN and the respective g/ccTLD registries. Most of these relationships are governed by a uniform *Registrar Accreditation Agreement* (RAA), with transaction-based fees representing the bulk of all registrar contributions.[391]

With gTLD registries and registrars contributing the lions share to ICANN's total revenue, it could be argued that both ASO and GNSO also have the most capabilities to conduct a successful securitization. However, before this hypothesis can be confirmed, we first need to proceed to our final case study and investigate an area specific instance of *securitization*.

[388] See http://www.icann.org/en/general/financial.html.
[389] See http://www.icann.org/en/financials/adopted-opplan-budget-fy12-09sep11-en.pdf
[390] See p. 37 http://www.icann.org/en/financials/adopted-opplan-budget-fy12-09sep11-en.pdf
[391] See p. 38-40 http://www.icann.org/en/financials/adopted-opplan-budget-fy12-09sep11-en.pdf

## 2.2. Synthesis

The aim of this part was to set the scene for the following case study. In doing so, we first gave a short overview of the historic processes around the Internet in general, and ICANN in particular. We argued that a breakdown of the DNS can potentially have significant implications for social layer referent objects such as “society,” “the regime,” or “the economy” (which is, again, in turn linked to “state” and “society”). Moreover, the board of ICANN’s directors was defined and characterized as a platform for potential securitizing actors. Ultimately, we gave an impression of the stakeholder’s (primarily economic) capabilities.

# 3. DNS-CERT as a Case for Securitization in Internet Governance

In the previous part we argued that a breakdown of the DNS can potentially have significant implications for social layer referent objects such as “society,” “the regime,” or “the economy” (which is, again, in turn linked to “state” and “society”). We defined multi-stakeholder collaboration as the main political constellation in Internet governance and held that the ICANN board consists of all relevant stakeholders who could potentially conduct a securitizing move. The aim of this part is to apply the theoretical concepts that were set out above and ask, how the Copenhagen school would explain a case of cyber securitization in the field of Internet governance.

## 3.1. Data

Sticking to the Copenhagen school’s methodological approach, our analysis was mostly conducted on *texts that are central in the sense that if security discourse is operative in this community, it should be expected to materialize in this text because this occasion is sufficiently important*. In this context, most of the data we are using here is publicly available and accessible via the Internet. Additionally, we conducted a series of qualitative interviews with experts working in the field of Internet governance.

Also, the *Berkman Center for Internet & Society* at *Harvard University* has produced a very valuable and comprehensive review of ICANN’s accountability and transparency.[392] The following part will therefore make heavy use of the review’s appendix on the DNS-CERT proposal.[393] Building upon the results delivered through both the Berkman study and our own primary research, we finally apply the Copenhagen school’s securitization theory.

## 3.2. What’s in a CERT

Before running a case study on DNS-CERT, it is worth to pause for a moment and explain what this acronym actually stands for. As should be clear by now, DNS refers to the *Domain Name System*. A CERT, however, is the short-hand for an organization called *Computer Emergency Response Team*.[394] The first CERT was created in response to the 1988 Morris worm incident. This worm caused around 10% of all then connected US computers to disconnect from the Net. Since most of the network security experts used the Net as their

[392] Berkman Center, *Accountability and Transparency at ICANN. An Independent Review*, August 2010, http://cyber.law.harvard.edu/pubrelease/icann/.

[393] Berkman Center, *Accountability and Transparency at ICANN. An Independent Review, Appendix E: The DNS-CERT Proposal*, August 2010, http://cyber.law.harvard.edu/pubrelease/icann/pdfs/AppendixE_DNS-CERT.pdf.

[394] Sometimes also referred to as *Computer Security Incident Response Team* (CSIRT).

main means of communication, the breakdown of large parts of their infrastructure made it difficult for them to conduct a coordinated response.[395] Consequently, DARPA called for a single point of contact for Internet security issues and funded a CERT coordination center (CERT/CC) at Carnegie Mellon University.

In essence, a CERT can be described as an information hub that transfers information about security incidences to the right people.[396] In 1998, a CERT has been defined as

> "a team that coordinates and supports the response to *security incidents* [any adverse event which compromises some aspect of computer or network security] that involve sites within a defined *constituency* [the group of users, sites, networks or organizations served by the team]."[397]

Today CERT/CC has links to all other CERTs worldwide. Even though many countries have their own national CERTs,[398] the size of a CERT is not restricted to states. In fact, CERTs can also be found at other levels as well (e.g., at the sub-unit or regional level). CERTs work closely together with the Internet community and take important steps to prevent future incidences. The mission of a CERT can be defined in five distinct categories:

1. Provide a reliable, trusted, 24-hour, single point of contact for emergencies.
2. Facilitate communication among experts working to solve security problems.
3. Serve as a central point for identifying and correcting vulnerabilities in computer systems.
4. Maintain close ties with research activities and conduct research to improve the security of existing systems.
5. Initiate proactive measures to increase awareness and understanding of information security and computer security issues throughout the community of network users and service providers.[399]

## 3.3. Basic Documents

ICANN's role in global DNS security is specified in its bylaws and agreements. As was mentioned in the previous part, ICANN has the mission to "ensure the stable and secure operation of the Internet's unique identifier systems."[400] In this respect, the first core

[395] See, for instance, http://www.cert.org/encyc_article/tocencyc.html#History
[396] Thanks to Robert Schischka for that point.
[397] http://tools.ietf.org/html/rfc2350
[398] http://www.cert.org/csirts/national/contact.html
[399] http://www.cert.org/meet_cert/.
[400] ICANN, *Bylaws*, http://www.icann.org/en/general/bylaws.htm.

principle by which ICANN's decisions and actions should be guided is:

> "Preserving and enhancing the operational stability, reliability, security, and global interoperability of the Internet."[401]

Through the 2009 AoC with the DoC, ICANN commits itself to preserving security, stability and resiliency. In doing so, it agrees to pay particular attention to:

> "(a) security, stability and resiliency matters, both physical and network, relating to the secure and stable coordination of the Internet DNS; (b) ensuring appropriate contingency planning; and (c) maintaining clear processes."[402]

In this context, ICANN published its first draft *Plan for Enhanced Internet Security, Stability and Resiliency* in May 2009.[403] The plan clarified ICANN's competencies in respect to other Internet security actors and was intended to serve as a foundation for establishing future security programs and activities such as improving the root zone management and building upon existing Internet security community efforts to effectively respond to DNS threats.

In February 2010, ICANN released its final draft *July 2010-June 2013 Strategic Plan*.[404] The plan set out four strategic focus areas, with *DNS stability and security* being one of them. On the strategic projects layer under this item, the establishment of a DNS-CERT was mentioned. Later on, it is stated in the document:

> "ICANN will work in partnership with other organizations to develop an approach to the establishment of a DNS CERT in order to address one of the broader issues of Internet security. This system would enable a more coordinated and effective response to incidents and attacks on the DNS. In addition, ICANN will be working with the Internet community to enhance contingency planning and exercises to address risks and threats to the DNS."[405]

Around the same time, two more security-focused policy documents were issued: The *Proposed Strategic Initiatives for Improved DNS Security, Stability and Resiliency*[406] as well as the *Global*

[401] ICANN, *Bylaws*, http://www.icann.org/en/general/bylaws.htm.

[402] ICANN, *Affirmation of Commitment*, http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm.

[403] ICANN, *Plan for Enhanced Internet Security, Stability and Resiliency*, 21 May 2009, http://www.icann.org/en/announcements/announcement-2-21may09-en.htm.

[404] ICANN, *July 2010 — June 2013 Strategic Plan Posted*, http://www.icann.org/en/announcements/announcement-2-22feb10-en.htm.

[405] ICANN, *Strategic Plan July 2010-June2010*, http://www.icann.org/en/strategic-plan/strategic-plan-2010-2013-19feb10-en.pdf.

[406] ICANN, *Proposed Strategic Initiatives for Improved DNS Security, Stability and Resiliency (SSR)*, http://www.icann.org/en/public-comment/strat-ini-ssr-12feb10-en.htm.

*DNS-CERT Business Case*.[407] These two documents can be said to form the core of ICANN's DNS-CERT proposal.

### 3.3.1. Proposed Strategic Initiative

ICANN's *Proposed Strategic Initiatives*[408] paper starts out by arguing that the global DNS is increasingly threatened. It claims that "the DNS exists in an environment of increasing threats and risks."[409] By referring to three press releases—two from the *European Network and Information Security Agency* (ENISA), and one from the US *Information Technology Sector Coordinating Council* (ITSCC)—the document points out that, over the past view years, "[s]everal calls to action on addressing and mitigating systemic DNS risks have been made."[410]

By referring to its bylaws and commitments, ICANN asserts that it has to respond to these calls by undertaking efforts to preserve the security, stability and resiliency of the DNS. In this respect, the paper first identifies three major types of current security risks to the DNS:

1. Malicious activity risks such as *Denial-of-Service attacks* (DoS attacks) that usually lead to root and TLD server overload, or *cache poisoning* whereby Internet users are misdirected to Web sites with fraudulent code.
2. Technical risks including vulnerabilities in the DNS protocol or problems that might arise from changes to the root level of the DNS, for instance during the transition from IPv4 to IPv6 or the implementation of *DNS Security Extensions* (DNSSEC).
3. Organizational failures include the potential disruptions of DNS operations that are caused if key organizations for the DNS (such as ICANN, root server operators, TLD registries and registrars) no longer perform their function. Therefore, system level provisions must be made for contingencies.

After having grouped the existing risks, the paper moves on and proposes two strategic initiatives in response to these threats. The first refers to the necessity for community-wide DNS risk assessment, contingency planning and the establishment of response capabilities and system-wide DNS exercise programs. This shall be facilitated by a specialized expert advisory group.

[407] 407 ICANN, *Proposed Strategic Initiatives for Improved DNS Security, Stability and Resiliency (SSR)*, http://www.icann.org/en/public-comment/strat-ini-ssr-12feb10-en.htm.

[408] 408 ICANN, *Proposed Strategic Initiatives for Improved DNS Security, Stability and Resiliency (SSR)*, http://www.icann.org/en/public-comment/strat-ini-ssr-12feb10-en.htm.

[409] 409 ICANN, *Proposed Strategic Initiatives for Improved DNS Security, Stability and Resiliency (SSR)*, http://www.icann.org/en/public-comment/strat-ini-ssr-12feb10-en.htm, p. 2.

[410] 410 ICANN, *Proposed Strategic Initiatives for Improved DNS Security, Stability and Resiliency (SSR)*, http://www.icann.org/en/public-comment/strat-ini-ssr-12feb10-en.htm p. 2

In its second initiative, ICANN calls for the creation of a DNS-CERT; a central point of contact for all key stakeholders, including DNS operators and users, vendors, security researchers, and incident responders. The details to this initiative are presented in the *Global DNS-CERT Business Case*.[411]

### 3.3.2. DNS-CERT Business Case

In the introduction to the *Global DNS-CERT Business Case*,[412] special attention is paid to the Internet's role as a global means of communication and its impact on a broad variety of different actors, ranging from the individual to companies and public institutions:

> "Relied upon not only by individuals, the Internet provides services necessary to the functioning of governments, corporations and financial institutions, not to mention schools, medical facilities and merchants small and large."[413]

Wide-scale coordinated attacks against the DNS, it is held, could potentially cause "significant economic and political fallout."[414] If these attacks cannot be rapidly detected by a central point of technical and policy coordination, this may result in "lasting economic consequences."[415] However, referring to the 2009 *Global DNS Security, Stability, and Resiliency Symposium*,[416] "[i]nformation sharing within the DNS community is sorely lacking."[417] This "lack of situational awareness among incident responders could leave critical assets, systems, networks and functions vulnerable."[418]

Therefore, in order to overcome the problem of insufficient coordination, two constraints must be removed. The first one refers to resource constraints, especially those in lesser-developed regions of the world. This was also pointed out at the *Global DNS Security, Stability, and Resiliency Symposium*:

[411] ICANN, *Global DNS-CERT Business Case*, 2010, http://www.icann.org/en/public-comment/dns-cert-12feb10-en.htm.
[412] ICANN, *Global DNS-CERT Business Case*, 2010, http://www.icann.org/en/public-comment/dns-cert-12feb10-en.htm.
[413] ICANN, *Global DNS-CERT Business Case*, 2010, http://www.icann.org/en/public-comment/dns-cert-12feb10-en.htm, p. 4.
[414] ICANN, *Global DNS-CERT Business Case*, 2010, http://www.icann.org/en/public-comment/dns-cert-12feb10-en.htm, p. 5.
[415] ICANN, *Global DNS-CERT Business Case*, 2010, http://www.icann.org/en/public-comment/dns-cert-12feb10-en.htm, p. 6.
[416] GTISC, *Global DNS Security, Stability, and Resiliency Symposium*, 3-4 February 2009, http://www.gtisc.gatech.edu/icann09.
[417] ICANN, *Global DNS-CERT Business Case*, 2010, http://www.icann.org/en/public-comment/dns-cert-12feb10-en.htm, p. 6.
[418] ICANN, *Global DNS-CERT Business Case*, 2010, http://www.icann.org/en/public-comment/dns-cert-12feb10-en.htm, p. 6

> *"resource constrained organizations have difficulty establishing networks of professionals to reach out and solicit information from. An organization will instinctively turn to its professional network, either in reaction to an event/incident or for proactive assistance. It is imperative that organizations know where to begin establishing their networks."*[419]

The second constraint refers to geographically limited efforts to share information on a global level:

> "An effective CERT capability for the DNS should not be limited [by] geography because of the dispersed nature of operations. In this sense, what might ordinarily be considered to be *critical national infrastructure* may have impacts far beyond a national border."[420]

By drawing its lessons from previous cyber attacks in which the DNS was involved (including cache poisoning and cases of botnet attacks),[421] the paper finally calls for the need of a "DNS security response capability, as well as the wide range of contingencies and stakeholders that may be involved."[422] This need could be sufficiently met by creating a global DNS-CERT capability.

The foundational idea or vision statement of the DNS-CERT would be to "enhance the security, stability and resiliency of the Global DNS."[423] The corresponding mission statement of the organization would be to:

> *"Ensure DNS operators and supporting organizations have a security coordination center with sufficient expertise and resources to enable timely and efficient response to threats to the security, stability and resiliency of the DNS."*[424]

In carrying out this mission, the DNS-CERT would essentially be dedicated to three main goals and objectives:

[419] ICANN, *Global DNS-CERT Business Case*, 2010, http://www.icann.org/en/public-comment/dns-cert-12feb10-en.htm, p. 6-7

[420] ICANN, *Global DNS-CERT Business Case*, 2010, http://www.icann.org/en/public-comment/dns-cert-12feb10-en.htm, p. 7

[421] ICANN, *Global DNS-CERT Business Case*, 2010, http://www.icann.org/en/public-comment/dns-cert-12feb10-en.htm, p. 7-9

[422] ICANN, *Global DNS-CERT Business Case*, 2010, http://www.icann.org/en/public-comment/dns-cert-12feb10-en.htm, p. 9

[423] ICANN, *Global DNS-CERT Business Case*, 2010, http://www.icann.org/en/public-comment/dns-cert-12feb10-en.htm, p. 11

[424] ICANN, *Global DNS-CERT Business Case*, 2010, http://www.icann.org/en/public-comment/dns-cert-12feb10-en.htm, p. 11

1. Goal: Gain situational awareness and share information.
   Objective: Establish communications means and procedures to maximum number of players; exercise regularly.
2. Goal: Improve coordination within the DNS operational community.
   Objective: Enable measurement and facilitate information sharing about the health, stability and resiliency of the DNS. Engage in appropriate situations: support contingency planning and exercises; undertake After Action Reporting (AAR). Engage with DNS-OARC and RISG, among others collaborators, to leverage expertise and existing operational response capabilities related to information sharing and analysis.
3. Goal: Improve coordination with the broader security community.
   Objective: Establish relationships with key partners (CERTs, security researchers, key security lists, vendors, antivirus companies, law enforcement and governments); participate in contingency planning and exercises; engage in appropriate situations; undertake After Action Reporting (AAR).[425]

The organization's operations should be reviewed regularly and can be adapted according to "constituency needs, funding, exigencies, policy drivers and technical capability of the CERT itself."[426] In essence, the DNS-CERT team will provide both reactive (e.g., 365x24x7 point of contact, incident handling coordination or direct assistance) and proactive services (e.g., watch and warning services or education and training)[427] and will act as a central point of coordination (see graph) for

1. Root server operators and supporting organization
2. Registries and registrars
3. DNS vendors
4. Other interested and qualified parties, as identified by the DNS-CERT management.[428]

Based on the CSIRT development guidelines suggested by the CERT/CC, in the remaining section of the proposal, ICANN sets out the details about how to establish the DNS-CERT. ICANN would provide initial funding (annually $4.2 million), "until the organization can stand

[425] ICANN, *Global DNS-CERT Business Case*, 2010, http://www.icann.org/en/public-comment/dns-cert-12feb10-en.htm, pp. 11f.
[426] ICANN, *Global DNS-CERT Business Case*, 2010, http://www.icann.org/en/public-comment/dns-cert-12feb10-en.htm, pp. 12.
[427] ICANN, *Global DNS-CERT Business Case*, 2010, http://www.icann.org/en/public-comment/dns-cert-12feb10-en.htm, p. 12.
[428] ICANN, *Global DNS-CERT Business Case*, 2010, http://www.icann.org/en/public-comment/dns-cert-12feb10-en.htm, p. 14.

on its own."[429] Certainly, the proposed annual amount would fit with ICANN's need to spend considerable amounts of its annual revenues obtained from gTLD registries and registrars.

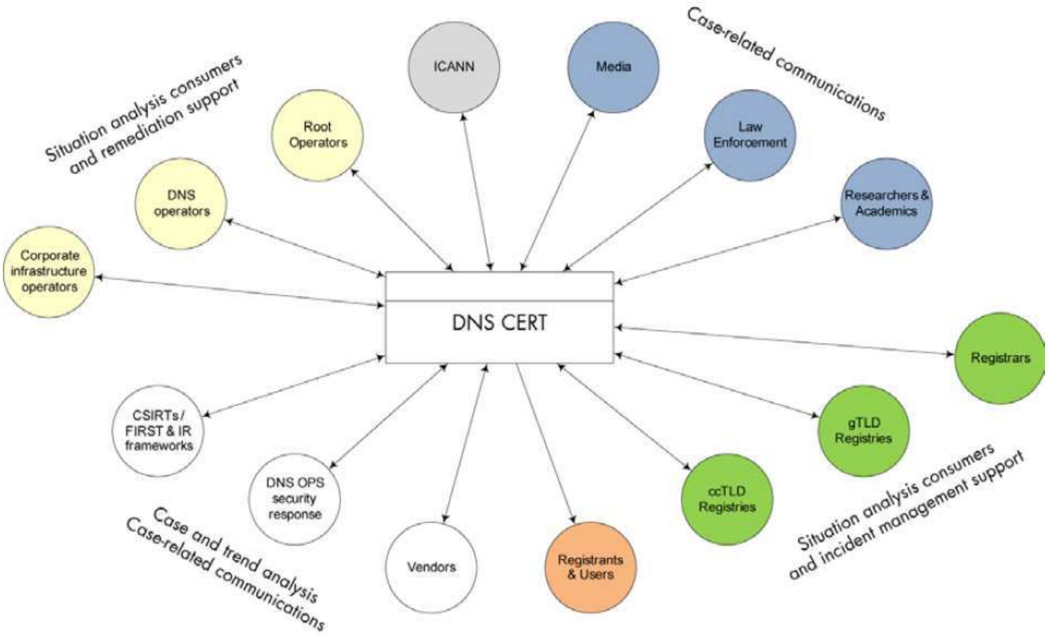
Situation analysis consumers and remediation support
ICANN
Media
Case-related communications
Root Operators
Law Enforcement
DNS operators
Researchers & Academics
Corporate infrastructure operators
DNS CERT
Registrars
CSIRTs/ FIRST & IR frameworks
gTLD Registries
DNS OPS security response
ccTLD Registries
Situation analysis consumers and incident management support
Case and trend analysis
Case-related communications
Vendors
Registrants & Users

**Figure 9:** DNS-CERT proposed structure[430]

## 3.4. DNS-CERT viewed through the Cyber Lens

Public comment for the draft *2010-2013 Proposed Strategic Initiative* was open between 1 December 2009 and 21 January 2010.[431] As the Berkman report states, during this period, interest for the DNS-CERT proposal was relatively low. However, most of the comments received were predominantly supportive.[432] Between 12 February and 25 March 2010 both the *Proposed Strategic Initiatives* and the *DNS-Business Case* were released for public comment,[433] with only one comment related to DNS-CERT. The Berkman report highlights

[429] ICANN, *Global DNS-CERT Business Case*, 2010, http://www.icann.org/en/public-comment/dns-cert-12feb10-en.htm, p. 16.
[430] ICANN, *Global DNS-CERT Business Case*, 2010, http://www.icann.org/en/public-comment/dns-cert-12feb10-en.htm, p. 14.
[431] ICANN, *2010-2013 Strategic Plan*, 2009, http://www.icann.org/en/public-comment/strat-plan-2010-01dec09-en.htm.
[432] Berkman Center, *Accountability and Transparency at ICANN. An Independent Review, Appendix E: The DNS-CERT Proposal*, August 2010, http://cyber.law.harvard.edu/pubrelease/icann/pdfs/AppendixE_DNS-CERT.pdf, p. 8
[433] ICANN, *Invitation for Public Comment: Proposed Strategic Initiatives for Improved DNS SSR and Global DNS-CERT Business Case*, http://www.icann.org/en/announcements/announcement-2-12feb10-en.htm.

that “the DNS-CERT proposal remained largely uncontroversial until ICANN’s meeting in Nairobi in March 2010.”[434]

### 3.4.1. Nairobi Speech Act

The peace around the DNS-CERT proposal was suddenly interrupted when ICANN’s CEO and President Rod Beckstrom gave his state of the DNS address in front of the *Governmental Advisory Committee* (GAC) on 9 March 2010.[435] It is important to emphasize here that this very speech constitutes the centrepiece of our study. In order to provide a comprehensive overview, we will therefore deliver the quote at full length:

> “I want to share one last piece of information with you, an observation I feel obligated to share as the CEO of ICANN, particularly under the Affirmations of Commitments, paragraphs 3 and 9.2, which refer to the security of a domain name system.
>
> Paragraph 3 refers to ICANN’s role and requirement to preserve the security of a domain name system globally. What I want to share with you as a representative of many countries of the world is that the domain name system is under attack today as it has never been before. I have personally consulted with over 20 CEO’s of the top Registries and top Registrars globally, all of whom are seeing increasing attacks and complexity of attacks and who are extremely concerned.
>
> The domain name system is more fragile and vulnerable today than it has ever been. It could stop at any given point in time literally. It has never stopped, it has been slowed down through attacks and the Kominsky [sic] exploit that was disclosed only 18 months or so ago could have been used to fundamentally cripple the domain name system. That system is used 1 trillion times per day and your economies depend upon it. It can stop or it can materially be damaged and harmed. It is under attack.
>
> Parts of that system are only in your countries and I’m going to be writing you a letter and asking you for what is happening in the domain name system in your countries because we’re seeing new levels of wild carding that is occurring at the telecom service provider level, synthesis of domain name system providers interrupting DNS requests and providing false data and information for commercial or other purposes.

[434] Berkman Center, *Accountability and Transparency at ICANN. An Independent Review, Appendix E: The DNS-CERT Proposal*, August 2010, http://cyber.law.harvard.edu/pubrelease/icann/pdfs/AppendixE_DNS-CERT.pdf, p. 9.

[435] GAC, *GAC Meeting with ICANN Board*, 9 March 2010, Transcript, http://nbo.icann.org/node/8943.

> But the system is under full scale attack and I am extremely concerned as the CEO of ICANN I want to let you know that.
>
> We're all in this together and I have met with the heads of cyber security or technical infrastructure of 3 of the largest counties on earth who are concerned as well. I'm sharing this because I'm gravely concerned and we need your help. So we're going to be asking you for your advice on domain name security and on the DNS SERT [sic] and what can be done and particularly to learn the lessons from you as well. What has been accomplished in your countries?
>
> I have experience with SERTS [sic] in several countries but we need to learn more. So that will be coming and I just want to express my concern to this group because I don't want to wait until Brussels. Thank you."[436]

To cut a long story short, what Beckstrom is really saying here is that, as the appointed CEO and President of the global preserver of the DNS (ICANN), he is *officially obliged to urgently inform the countries* he represents about the fact *that the DNS* is more threatened today than it was ever before. Even worse, it *could stop at any given point in time literally*. Since *the countries' economies* are *using the system 1 trillion times per day*, a breakdown of the DNS would have significant implications *for all humankind*. Beckstrom adds additional authority to his argument by claiming that he *has not only talked to over 20 CEO's of the top Registries and top Registrars worldwide, but that his concerns are equally shared by the heads of cyber security or technical infrastructure of 3 of the largest counties on earth*.

The urgency in Beckstrom's words calls for immediate action: threats against the global DNS have reached a point of no return; if we do not handle them in time, the states' economies will necessarily break down soon.

### 3.4.2. Reactions

Beckstrom's speech was widely perceived and provoked strong reactions ranging from support to skepticism.[437] The public comment period for both the *Proposed Strategic Initiative* and the *DNS-CERT Business Case* was extended. While the *Strategic Initiative* now only received 13 comments, a total of 25 comments were brought forward just for the *Business Case*:

[436] GAC, *GAC Meeting with ICANN Board*, 9 March 2010, Transcript, http://nbo.icann.org/node/8943.

[437] See Berkman Center, *Accountability and Transparency at ICANN. An Independent Review, Appendix E: The DNS-CERT Proposal*, August 2010, http://cyber.law.harvard.edu/pubrelease/icann/pdfs/AppendixE_DNS-CERT.pdf, p. 12

> "Three of ICANN's advisory committees and supporting organizations submitted comments: ALAC, ccNSO, and gNSO. Five commercial stakeholders submitted comments: AT&T, Net Choicer, PayPal, PRESENSE Technologies GmbH, and USCIB. Governments, national CERTs, registry operators, TLD associations, and other Internet organizations submitted the remainder of the comments."[438]

Without going into much detail about the whole range of different reactions that followed Nairobi, we will take a shortcut and build on already existing material. Most prominently, this study will draw on the results generated by the Berkman institute. After analyzing existing online material and conducting high-level expert interviews, the Berkman team usefully grouped the reactions into three overall categories. Consequently, these categories read as follows:[439]

1. Substantive Issues referred to (1) questions about whether a DNS-CERT was needed at all, "given the current landscape of DNS security risks."[440] To answer this question sufficiently makes it necessary not only to *access* a whole wealth of incidence information, but also to *assess* it correctly. (2) Also, this point touches upon questions about whether, "given the existing knowledge about the threats to DNS,"[441] a DNS-CERT should actually be established.
2. The issue about ICANN's DNS security mandate mainly concerned its role in the proposed organization. It was feared that, (1) through sponsoring the creation of a new security actor, ICANN could broaden its competencies beyond being a mere coordinating and non-operating body. In this context, (2) further concerns were raised as to whether ICANN has the right to dispose of considerable parts of its revenues ($4.2 million) independently from the stakeholders who actually contribute them.[442]
3. The procedural issues that were addressed involved (1) complaints about the lacking

[438] Berkman Center, *Accountability and Transparency at ICANN. An Independent Review, Appendix E: The DNS-CERT Proposal*, August 2010, http://cyber.law.harvard.edu/pubrelease/icann/pdfs/AppendixE_DNS-CERT.pdf, p. 10

[439] Berkman Center, *Accountability and Transparency at ICANN. An Independent Review, Appendix E: The DNS-CERT Proposal*, August 2010, http://cyber.law.harvard.edu/pubrelease/icann/pdfs/AppendixE_DNS-CERT.pdf, pp. 11-7

[440] Berkman Center, *Accountability and Transparency at ICANN. An Independent Review, Appendix E: The DNS-CERT Proposal*, August 2010, http://cyber.law.harvard.edu/pubrelease/icann/pdfs/AppendixE_DNS-CERT.pdf, p. 12

[441] Berkman Center, *Accountability and Transparency at ICANN. An Independent Review, Appendix E: The DNS-CERT Proposal*, August 2010, http://cyber.law.harvard.edu/pubrelease/icann/pdfs/AppendixE_DNS-CERT.pdf, p. 12

[442] See CIRA, *Comments on ICANN's Global DNS-CERT Business Case*, 14 April 2010, p. 2, http://forum.icann.org/lists/dns-cert-proposal/pdfFxQAZdha2U.pdf.

openness and transparency. Beckstrom did neither inform other stakeholders about his intention to speak about a DNS-CERT, nor did he disclose the names of the registries and registrars he was referring to in this speech. Moreover, (2) community members reacted disturbed about the lack of stakeholder participation and open dialogue during the development of the proposals. It was objected that Beckstrom did not sufficiently consult with the community through a bottom-up, knowledge- and consensus-based multi-stakeholder approach. This point was also confirmed by one of the interviewees to this study, who indicated that it was a rush to a solution without really reaching an agreement before.

### 3.4.3. Analysis

How does the Copenhagen school deal with Beckstrom's attempted securitization? Before we can answer this question, we first need to clarify whether Beckstrom's speech act qualified as a case for securitization in the cyber sector. In fact, Beckstrom not only identified the DNS as an existentially threatened (technical) referent object, but also linked it to the state and its economy. It could also be argued that this linkage is even stronger by Beckstrom calling himself a "representative of many countries of the world." However, one must keep in mind here that Beckstrom is not talking to *all* ICANN stakeholders, but only to a little fraction: namely states and intergovernmental organizations as assembled in the *Governmental Advisory Committee* (GAC). We do not know whether ICANN's President and CEO also calls himself a *representative of many gTLDs* when speaking to the GNSO, or *of all individual Internet users in the world* when consulting with ALAC. Thus, while we can indeed confirm that Beckstrom's Nairobi speech linked the logical with the social layer of cyberspace, we cannot be certain about whether this link was additionally strengthened through Beckstrom calling himself the representative of a certain stakeholder group.

Having clarified that Beckstrom's speech act indeed qualifies as a case for securitization in the cyber sector, we can now contextualize the results from the Berkman study with securitization theory and try to explain why Beckstrom's securitizing move ultimately misfired. This is done by recalling the Copenhagen school's *three facilitating conditions* for a successful securitization.

For a securitization to be successful, it is necessary to fulfill three unconditional criteria: (1) the sector-specific *security grammar* has to be applied,[443] (2) the necessary *capabilities* must

[443] In order to make the relevant audience understand the speech act correctly, the securitizing actor needs to apply the sector-specific sub-form or grammars of security.

be held,[444] and (3) the *security threat* must be commonly perceived as such.[445] If these conditions are not entirely met, the securitizing move necessarily misfires.

### 3.4.3.1. Security Grammar

As regards the sector-specific security grammar, for the cyber sector we distinguished between (a) *hypersecuritization*, (b) *everyday security practice*, and (c) *technification*. As Hansen and Nissenbaum pointed out, not all of them must be met. However, in order to fulfill the first criteria, at least one of these three sub-grammars must be applied.

Recalling the concept of (a) hypersecuritization, we need to look at *the striking manner in which cyber security discourse hinges on multi-dimensional cyber disaster scenarios that pack a long list of severe threats into a monumental cascading sequence and the fact that neither of these scenarios has so far taken place*. This concept was opposed to *the tendency both to exaggerate threats and to resort to excessive countermeasures*. In the case of Beckstrom's Nairobi speech we find no clear indication for a hypersecuritization. One could point at Beckstrom's claim that the DNS "is used 1 trillion times per day" and that our "economies depend upon it." However, there is no real reference to any multi-dimensional cyber disaster scenarios. If there is no instance of hypersecuritization, is there some sort of exaggeration in Beckstrom's speech? Obviously, there is one. As was observed by the Berkman report, Beckstrom's claim the DNS "could stop at any given point in time literally" was widely perceived as "inflammatory" and "alarming." It was stated that

> "the tone of the message could be considered somewhat inflammatory [. . .] Many people in the room felt that Beckstrom was speaking out of turn and disregarding the work the community is already undertaking to ensure the stability and the security of the DNS."[446]

If Beckstrom really exaggerated in his speech act, why did he do that and what were his intentions? Were there any intentions at all? Securitization theory does not provide any answers to these questions. It discards hypersecuritization on grounds that Beckstrom's speech was an exaggeration, but it does not try to explain why he actually exaggerated.

[444] The securitizing actor must be in the authority to conduct a speech act. His position in the social hierarchy defines his relationship to the relevant audience. This relationship is shaped by the capabilities of the enunciator. The more capabilities he holds, the more likely he will succeed in his attempted securitization.

[445] The identified security threat must be commonly perceived as such. For the Copenhagen school, a threat is not objective but an inter-subjectively constructed.

[446] Berkman Center, *Accountability and Transparency at ICANN. An Independent Review, Appendix E: The DNS-CERT Proposal*, August 2010, http://cyber.law.harvard.edu/pubrelease/icann/pdfs/AppendixE_DNS-CERT.pdf, p. 11

As regards (b) technification, one could argue that Beckstrom tried to add authority to his argument by claiming that he had not only talked to “over 20 CEO’s of the top Registries and top Registrars globally,” but that he had also “met with the heads of cyber security or technical infrastructure of 3 of the largest counties on earth who are concerned as well.” By claiming that experts would share his opinion, Beckstrom tried to give his utterance the appearance of objectivity. However, in the case of Nairobi, this tactic failed. The multiple stakeholders in ICANN started to doubt and asked Beckstrom to be clear about who he was actually referring to. However, as was set out in the Berkman study,

> “Beckstrom [. . .] refused to disclose the names of the registry and registrar members with whom he consulted.”[447]

This triggers interesting questions. Why did he refuse to provide the names? Was it a secret or just a bluff? Unfortunately, the Copenhagen school does not deliver a satisfying answer here. Since there was doubt among the multiple stakeholders about Beckstrom’s technification, he obviously failed to apply this sub-form correctly.

As was mentioned above, an analyst of securitization should not be expected to reveal underlying motives, hidden agenda, or such, discourse analysis can only uncover one thing: discourse. But what if there is no open discourse? The Copenhagen school does not give an answer to this question.

Ultimately, we did not find any reference to (c) everyday security practice. Claiming that the DNS “is used 1 trillion times per day and that our economies depend upon it” does not really have a direct link to “normal” individuals’ experiences as would be necessary for a case of everyday security practice.

### 3.4.3.2. Capabilities

After having identified the sector-specific grammars of security, we can now look at the authority of Beckstrom as a securitizing actor. We argue that he derives his authority only through the stakeholders on the board. If one—everything else being equal—defined capabilities narrowly in terms of economic capabilities, these stakeholders would almost all be concentrated in GNSO (contributing the highest amount of money to ICANN’s revenues). This is most obvious in the Nairobi reactions challenging ICANN’s right to dispose of considerable parts of its revenues ($4.2 million) independently from the stakeholders who

[447] Berkman Center, *Accountability and Transparency at ICANN. An Independent Review, Appendix E: The DNS-CERT Proposal*, August 2010, http://cyber.law.harvard.edu/pubrelease/icann/pdfs/AppendixE_DNS-CERT.pdf, p. 15

actually contribute them. This becomes clear when looking at the statement posted by the Canadian ccTLD registry:

> "There are concerns as well with respect to the manner in which ICANN has allocated the budget for the DNS-CERT, which is estimated at $ 4.2 million USD. This is a considerable financial commitment to undertake without a thorough examination of existing organisations and community consultation to determine if the money could be better spent supporting other initiatives. Given that ICANN's revenue is nearly entirely generated from community stakeholders, it concerns us that ICANN would attempt to undertake such a substantial financial commitment without proper prior consultation with those who will ultimately be responsible for funding the initiative. We also question whether the community should be paying for something which would be better or preferably managed by another organisation."[448]

Therefore, we argue that, without the support of the most capable stakeholders in play, Beckstrom's unilateral securitizing move was predestinated to misfire.

### 3.4.3.3. Security Threat

The last facilitating condition in securitization theory was the necessity that the identified security threat must be commonly perceived as such. A threat does not exist independently from the actors involved in the securitizing move, but is inter-subjectively constructed by them. In the case of the DNS-CERT proposal, the threat was not clearly defined. Beckstrom claimed that the DNS were "under attack today as it has never been before." However, he did not deliver any details. When asked to provide the information that would be necessary to assess this high level of threats sufficiently, Beckstrom replied

> "that many registries have experienced increases in botnet attacks; but none have, so far, been willing to come forth and share their data [. . .] It would be very helpful if we could work together to gather additional data on attacks on registries, and on how that information is being shared and measured on a global basis. It would greatly contribute to our joint efforts to evaluate the seriousness of the threat and coordinate our forces more effectively to meet it."[449]

[448] Canadian Internet Registration Authority, *Comments on ICANN's Global DNS-CERT Business Case*, April 14, 2010, http://forum.icann.org/lists/dns-cert-proposal/pdfFxQAZdha2U.pdf.

[449] Berkman Center, *Accountability and Transparency at ICANN. An Independent Review, Appendix E: The DNS-CERT Proposal*, August 2010, http://cyber.law.harvard.edu/pubrelease/icann/pdfs/AppendixE_DNS-CERT.pdf, p. 11

# 4. Conclusion

In the first part of this thesis we set out a framework to tackle questions about cyber security. In the second part, we tried to provide the background against which we could conduct our final case study. After applying the Copenhagen school's concept of securitization to our cyber case, we can conclude that Beckstrom's speech act on the DNS-CERT proposal misfired entirely. In fact, none of the three facilitating conditions was met. Beckstrom did neither succeed in applying the sector-specific security grammar (hypersecuritization, technification or everyday security practice), nor did he hold sufficient capabilities to unilaterally act. Furthermore, he did not provide any information that would have convinced his audience of an existential threat to DNS security.

As a result, DNS-CERT was soon removed from the agenda. However, it did not disappear altogether. It rather seems that the idea has taken on a new form.[450] In January 2011, the *DNS Security and Stability Analysis Working Group* (DSSA) was established by ALAC, ccNSO, GNSO and NRO. Its aim is to examine the severity and frequency of threats, to review ongoing processes to mitigate these threats and to identify possible gaps in response to them.[451] Additionally, in April 2011, ICANN appointed Jeff Moss, the founder of DEFCON (the world's largest hacker conference), as its Vice-President and Chief Security Officer. Beckstrom characterized Moss as someone who "has the in-depth insider's knowledge that can only come from fighting in the trenches of the on-going war against cyber threats."[452]

What does that tell us about the general question posed in the introduction to this study: *Who can speak security in a multi-stakeholder collaboration such as ICANN?* The disappointing answer is: not much. We have indeed identified a couple of continuities in the case of ICANN. We were able to point at continuing efforts to fight inbuilt legitimacy problems (through technification of core competences, global elections and institutional isomorphism). We also saw that previously serving Presidents and CEO's of ICANN had the chance to leave their characteristic mark on the organization. Moreover, we have shown that some actors (not states!) contribute more to the overall budget than others. Through our case study, we have ultimately found that ICANN's President and CEO was not able to present the DNS as legitimately threatened, even though he linked it to the economy being

[450] See Mueller, Milton, 'ICANN's New 'Chief Security Officer',' *Internet Governance Project*, 28 April 2011 http://blog.internetgovernance.org/blog/_archives/2011/4/28/4805590.html.

[451] See ICANN Community, *DSSA Working Group – Call for At-Large Members*, 12 January 2011. https://community.icann.org/display/atlarge/DSSA+Working+Group+-+Call+for+At-Large+Members.

[452] See ICANN, *Jeff Moss Appointed ICANN Chief Security Officer*, 28 April 2011, http://www.icann.org/en/news/releases/release-28apr11-en.pdf.

the legitimate referent at the social top end of our cyberspace pyramid. But do these observations qualify as specific features of multi-stakeholder collaboration? No, they do not.

Therefore, future work needs to be done on other multi-stakeholder collaborations not only outside ICANN, but also outside Internet governance. Thus, one of the crucial questions for our future research is to identify areas with other multi-stakeholder model and compare them across (security) sectors.

## References

Abbate, Janet, *Inventing the Internet*, Cambridge (MA), MIT Press, 1999.

Aizu, Izumi, *The NGO and Academic ICANN Study (NAIS)*, August 2001, http://kambing.ui.ac.id/onnopurbo/library/library-ref-eng/ref-eng-1/application/policy/statistics/naisreportA4.pdf.

Albert, Mathias and Buzan, Barry, 'Securitization, sectors and functional differentiation', *Security Dialogue*, 2011, 42.

Alfred, Randy, 'June 23, 1983, DNS Test Sets Stage for Internet Growth,' *Wired*, 23 June 2008, http://www.wired.com/science/discoveries/news/2008/06/dayintech_0623#.

Atta, Richard Van, 'Fifty Years of Innovation and Discovery', in DARPA, *50 Years of Bridging the Gap, Defense Advanced Research Projects Agency*, April 2008, pp. 20-9, p. 25, http://www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2553.

Austin, John L., 'Speech Acts and Convention: Performative and Constative', in Nuccetelli, Susana and Seay, Gary (eds.), *Philosophy of Language: The Central Topics*, Lanham, Rowman & Littlefield Publishers, 2008.

Austin, John L., *How to Do Things with Words*, New York, Oxford University Press, 1965.

Barlow, John Perry, *A Cyberspace Independence Declaration*, 9 February 1996, http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration.

Beal, Vangie, 'The Difference Between a Computer Virus, Worm and Trojan Horse', *Webopedia*, 29 June 2011, http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp.

Berkman Center, *Accountability and Transparency at ICANN. An Independent Review, Appendix E: The DNS-CERT Proposal*, August 2010, http://cyber.law.harvard.edu/pubrelease/icann/pdfs/AppendixE_DNS-CERT.pdf.

Boston Working Group, *Management of Internet Names and Addresses*, 28 September 1998, http://www.ntia.doc.gov/legacy/ntiahome/domainname/proposals/bosgrp/submission-letter.html.

Bourdieu, Pierre, 'The forms of capital', in Richardson, John G. (ed.), *Handbook of Theory and Research for the Sociology of Education*, New York, Greenwood, 1986.

Bowman, Lisa, 'EFF sues ICANN over corporate records', *CNET News*, 18 March 2002, http://news.cnet.com/EFF-sues-ICANN-over-corporate-records/2110-1023_3-862461.html.

Brafman, Ori and Beckstrom, Rod A., *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*, Penguin Group, New York, 2006.

Buzan, Barry and Albert, Mathias, ‘Differentiation: A sociological approach to international relations theory’, *European Journal of International Relations*, 16, 3, 2010.

Buzan, Barry and Little, Richard, ‘The Idea of ‘International System’: Theory Meets History’, *International Political Science Review*, 15, 3, 1994.

Buzan, Barry and Little, Richard, *International Systems in World History,* Oxford, Oxford University Press, 2000.

Buzan, Barry and Wæver, Ole, ‘Macrosecuritization and security constellations: reconsidering scale in securitization theory’, *Review of International Studies*, 35, pp. 253-76, 2009.

Buzan, Barry and Wæver, Ole, *Regions and Powers. The Structure of International Security*, Cambridge, Cambridge University Press, 2003.

Buzan, Barry et al., *Security: A New Framework for Analysis*, London, Lynne Rienner Publishers, Inc., 1998.

Buzan, Barry et al., *The Logic of Anarchy: Neorealism to Structural Realism*, New York, Columbia University Press, 1993.

Buzan, Barry, ‘America in Space: The International Relations of Star Trek and Battlestar Galactica’, *Millennium: Journal of International Studies*, 39, 1, 2010.

Buzan, Barry, ‘Rethinking Security after the Cold War’, *Cooperation and Conflict*, 32, 1, pp. 5-28, 1997.

Buzan, Barry, *From International to World Society? English School Theory and the Social Structure of Globalisation*, Cambridge, Cambridge University Press, 2004.

Buzan, Barry, *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, Harvester Wheatsheaf, 1992.

Buzan, Barry, *The United States and the Great Powers: World Politics in the Twenty-First Century*, Cambridge, Polity, 2004.

Canadian Internet Registration Authority, *Comments on ICANN’s Global DNS-CERT Business Case*, April 14, 2010, http://forum.icann.org/lists/dns-cert-proposal/pdfFxQAZdha2U.pdf.

Cerf, Vint, *RFC 2468 I Remember IANA*, 1998, http://tools.ietf.org/html/rfc2468.

CERT, *About Us*, http://www.cert.org/meet_cert/.

CERT, *Security of the Internet*, first published in The Froehlich/Kent Encyclopedia of Telecommunications vol. 15. Marcel Dekker, New York, 1997, http://www.cert.org/encyc_article/tocencyc.html#History.

Clark, David, 'Characterizing cyberspace: past, present and future', *Working Paper MIT/Harvard*, http://web.mit.edu/ecir/pdf/clark-cyberspace.pdf.

Clausewitz, Carl von, *On War*, London, Penguin Books, 1982 [1832].

Collins, Alan, *Contemporary Security Studies*, New York, Oxford University Press, 2010.

Copeland, Lee, 'QickStudy: Packet-Switched vs. Circuit-Switched Networks', *Computerworld*, 20 March 2000, http://www.computerworld.com/s/article/41904/Packet_Switched_vs._Circuit_Switched_Networks.

Mathiason, John R. and Kuhlmann, Charles C., 'An International Communication Policy: The Internet, international regulation & new policy structures', *New York University*, http://www.un.org/esa/socdev/enable/access2000/ITSpaper.html.

Council of Europe, *Internet Governance Principles*, Strasbourg 18-19 April 2011, http://www.coe.int/t/dghl/standardsetting/media-dataprotection/conf-internet-freedom/Internet%20Governance%20Principles.pdf.

Derrida, Jacques, 'Signature event context,' in Idem, *Limited Inc*, Illinois, Northwestern University Press, 1988.

DHS, *Information Technology Sector Baseline Risk Assessment*, 2009, http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf.

Dickson, Paul, *Sputnik: The Shock of the Century*, New York, Walker Publishing Company, Inc., 2001.

Drezner, Daniel W., *Theories of International Politics and Zombies*, New Jersey, Princeton University Press, 2011.

Dunn Cavelty, Myriam, *Cyber-security and threat politics: US efforts to secure the information age*, Routledge, New York 2008.

Dutton, William H. and Peltub, Malcolm, 'The emerging Internet governance mosaic: connecting the pieces', *Information Polity*, 12, 2007.

FAS, *National Security Presidential Directives (NSPD) George W. Bush Administration*, 2001-2009.

Floyd, Rita, 'Human Security and the Copenhagen School's Securitization Approach: Conceptualizing Human Security as a Securitizing Move', *Human Security Journal*, 5, 2007.

Floyd, Rita, *Security and the Environment. Securitisation Theory and US Environmental Security Policy*, Cambridge et al., Cambridge University Press, 2010.

FNC, *FNC Resolution: Definition of "Internet"*, 24 October 1995, http://nitrd.gov/fnc/Internet_res.html.

Foucault, Michel, *Discipline and Punish: The Birth of Prison*, New York, Vintage Books, 1979.

Freeman, R. Edward, *Strategic Management: A stakeholder approach*, Toronto, Pitman, 1984.

GAC, *GAC Meeting with ICANN Board*, 9 March 2010, Transcript, http://nbo.icann.org/node/8943.

Geneva Declaration of Principles, para. 50 (WSIS-03/GENEVA/DOC/0004), http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160.

Goldsmith, Jack and Wu, Tim, *Who controls the Internet? Illusions of a Borderless World*, Oxford, Oxford University Press, 2006.

Gross, Raphael, *Carl Schmitt und die Juden: Eine deutsche Rechtslehre*, Frankfurt am Main, Suhrkamp Taschenbuch Verlag, 2000.

GTISC, *Global DNS Security, Stability, and Resiliency Symposium*, 3-4 February 2009, http://www.gtisc.gatech.edu/icann09.

Haas, Peter M., 'Introduction: Epistemic Communities and International Policy Coordination', *International Organization*, 46, 1, 1992.

Hafner, Katie and Lyon, Matthew, *Where Wizards Stay Up Late: The Origins Of The Internet*, New York, Touchstone, 1996.

Hansen, Lene and Buzan, Barry, *The Evolution of International Security Studies*, Cambridge et al., Cambridge University Press, 2009.

Hansen, Lene and Nissenbaum, Helen, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53, 2009.

Herzfeld, Charles, 'How the change agent has changed', *Nature*, 451, 24 January 2008.

Hurd, Ian, 'Legitimacy and Authority in International Politics', *International Organization,* 53, 2, 1999.

Hurrell, Andrew, *On Global Order. Power, Values, and the Constitution of International Society*, Oxford, Oxford University Press, 2007.

ICANN, *2010-2013 Strategic Plan*, 2009, http://www.icann.org/en/public-comment/strat-plan-2010-01dec09-en.htm.

ICANN, *Adopted Opplan Budget*, http://www.icann.org/en/financials/adopted-opplan-budget-fy12-09sep11-en.pdf.

ICANN, *Affirmation of Commitment*, http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm.

ICANN, *Biography Beckstrom*, http://www.icann.org/en/biog/beckstrom.htm.

ICANN, *Biography Lynn*, http://www.icann.org/en/biog/lynn.htm.

ICANN, *Biography Roberts*, http://www.icann.org/en/biog/roberts.htm.

ICANN, *Biography Twomey*, http://www.icann.org/en/biog/twomey.htm.

ICANN, *Bylaws*, http://www.icann.org/en/general/bylaws.htm.

ICANN, *DNS CERT Proposal*, http://forum.icann.org/lists/dns-cert-proposal/pdfFxQAZdha2U.pdf.

ICANN, *DSSA Working Group - Call for At-Large Members*, https://community.icann.org/display/atlarge/DSSA+Working+Group+-+Call+for+At-Large+Members.

ICANN, *Finances 1999-2011*, http://www.icann.org/en/financials/historical.htm.

ICANN, *Financial*, http://www.icann.org/en/general/financial.html.

ICANN, *Global DNS-CERT Business Case*, 2010, http://www.icann.org/en/public-comment/dns-cert-12feb10-en.htm.

ICANN, *ICANN's Response to the JPA Midterm Review*, http://www.icann.org/en/jpa/.

ICANN, *ICANN's Major Agreements and Related Reports*, http://www.icann.org/en/general/agreements.htm.

ICANN, *Invitation for Public Comment: Proposed Strategic Initiatives for Improved DNS SSR and Global DNS-CERT Business Case*, http://www.icann.org/en/announcements/announcement-2-12feb10-en.htm.

ICANN, *IPv6 Factsheet*, 26 October 2007, p.3, http://www.icann.org/en/announcements/announcement-26oct07.htm.

ICANN, *July 2010 — June 2013 Strategic Plan Posted*, http://www.icann.org/en/announcements/announcement-2-22feb10-en.htm.

ICANN, *New Generic Top-Level Domains*, http://newgtlds.icann.org/en/.

ICANN, *News*, http://www.icann.org/en/news/releases/release-28apr11-en.pdf.

ICANN, *Plan for Enhanced Internet Security, Stability and Resiliency*, 21 May 2009, http://www.icann.org/en/announcements/announcement-2-21may09-en.htm.

ICANN, *Proposed Strategic Initiatives for Improved DNS Security, Stability and Resiliency (SSR)*, http://www.icann.org/en/public-comment/strat-ini-ssr-12feb10-en.htm.

ICANN, *Strategic Plan July 2010-June2010*, http://www.icann.org/en/strategic-plan/strategic-plan-2010-2013-19feb10-en.pdf.

ICANN, *To 4,294,967,296 and Beyond – Under 10% of IPv4 Space Remains: Adoption of IPv6 Is Essential*, 29 January 2010, http://www.icann.org/en/announcements/announcement-29jan10-en.htm.

IETF, *FYI on Questions and Answers. Answers to Commonly asked 'New Internet User' Questions (RFC 1206)*, 1991, http://tools.ietf.org/html/rfc1206.

IETF, *Requirements for Internet Hosts—Communication Layers (RFC 1122)*, http://tools.ietf.org/html/rfc1122.

International Organization for Standardization, *ISO 3166-1 decoding table ISO 3166-1 alpha-2*, http://www.iso.org/iso/iso-3166-1_decoding_table.

Internet World Stats, *Internet Growth Statistics*, 2011, http://www.internetworldstats.com/emarketing.htm.

Internet World Stats, *Internet Users in the World. Distribution by World Region*, 2011, http://www.internetworldstats.com/stats.htm.

Internet World Stats, *Surfing and Site Guide*, 2011, http://www.internetworldstats.com/surfing.htm#1.

Irvine, Chris, 'Top Ten Most Expensive Domain Names', *The Telegraph*, 10 March 2010, http://www.telegraph.co.uk/technology/news/7412544/Top-10-most-expensive-domain-names.html.

ITU, gTLD-MoU, 28 Februar 1997, http://www.itu.int/net-itu/gtld-mou/gTLD-MoU.htm.

Kahin, Brian and Nesson Charles (eds.), *Borders in cyberspace: information policy and the global information infrastructure*, Cambridge, MIT Press, 1997.

Karrenberg, Daniel, 'DNS Root Name Servers Frequently Asked Questions', ISOC, 27 January 2005, http://www.isoc.org/briefings/020/.

Kleinwächter, Wolfgang, 'From self-governance to public-private partnership: The changing role of governments in the management of the Internet's core resources', *Loyola of Los Angeles Law Review*, 36, 2003.

Klimburg, Alexander and Mirtl, Philipp, 'Cyberspace and Governance—A primer', *oiip Policy Paper*, September 2011, pp. 9-14, http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Newsletter/Cyberspace_and_Governance-A_primer.pdf.

Klimburg, Alexander, ‘Ruling the Domain: (Self) Regulation and the Security of the Internet’, *oiip policy paper*, 2011, http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/Ruling_the_Domain_Klimburg.pdf.

Klimburg, Alexander, ‘The Whole of Nation in Cyberpower’, *Georgetown Journal of International Affairs*, Special Edition, 2011, http://www.oiip.ac.at/publikationen/publikationen-detail/article/105/the-whole-of-nation-in-cyberpower.html.

Kramer, Franklin D. et al., eds., *Cyberpower and National Security*, Washington, D.C., National Defense UP, 2009.

Kuehl, Daniel T., ‘From Cyberspace to Cyberpower: Defining the Problem,’ in Kramer, Franklin D. et al., eds., *Cyberpower and National Security*, Washington, D.C., National Defense UP, 2009, pp. 26-7.

Kurbalija, Jovan, *An Introduction to Internet Governance*, Malta, DiploFoundation

Leiner, Barry M. et al., ‘A brief history of the Internet’, *ISOC*, 1997, http://www.isoc.org/internet/history/brief.shtml.

Lessig, Lawrence, *Code v2*, New York, Basic Books, 2006, http://codev2.cc/download+remix/Lessig-Codev2.pdf.

Lessig, Lawrence, *The Future of Ideas. The Fate of the Commons in a Connected World*, New York, Random House, p. 23, http://www.the-future-of-ideas.com/download/lessig_FOI.pdf.

Libicki, Martin C., *Conquest in Cyberspace, National Security and Information Warfare*, Cambridge et al., Cambridge University Press, 2007.

Licklider, J.C.R., *Memorandum for: Members and Affiliates of the Intergalactic Computer Network, Advanced Research Projects Agency*, 23 April 1963, http://www.chick.net/wizards/memo.html.

Lindsay, David, *International domain name law: ICANN and the UDRP*, Oxford, Hart Publishing, 2007.

Lule, Jack, ‘Roots of the Space Race: Sputnik and the Language of U.S. News in 1957’, *Journalism Quarterly*, 68, 1-2, 1991.

Malcolm, Jeromy, *Multi-Stakeholder Governance and the Internet Governance Forum*, Perth, Terminus Press, 2008.

Mathiason, John, *Internet Governance. The New Frontier of Global Institutions*, London, Routledge, 2009.

McCarthy, Kieren, ‘ICANN Fires it CEO,’ *.nxt*, 16 August 2011, http://news.dot-nxt.com/2011/08/16/icann-fires-ceo.

McSweeney, Bill, ‘Identity and security: Buzan and the Copenhagen school’, *Review of International Studies*, 22, 1, 1996.

Mitchell, Bradley, ‘Why there are only 13 DNS Root Name Servers,’ *About.com*, 19 November 2008, http://compnetworking.about.com/b/2008/11/19/why-there-are-only-13-dns-root-name-servers.htm.

Mueller, Milton et al., ‘The Internet and Global Governance: Principles and Norms for a New Regime’, *Global Governance*, 13/2, 2007.

Mueller, Milton, ‘Dancing the Quango: ICANN and the Privatization of International Governance’.

Mueller, Milton, ‘ICANN and Internet governance. Sorting through the debris of self-regulation’, info, 1, 6, 1999.

Mueller, Milton, ‘The New Cyber-Conservatism: Goldsmith/Wu and the Premature Triumphalism of the Territorial Nation-State. A review of Goldsmith and Wu’s ’Who Controls the Internet? Illusions of a Borderless World’’, Internet Governance Project Paper, 2006, http://www.internetgovernance.org/pdf/MM-goldsmithWu.pdf. Mueller, Milton, ‘What is the JPA?’, Internet Governance Project, 8 February 2008, http://blog.internetgovernance.org/blog/_archives/2008/2/8/3512862.html.

Mueller, Milton, *Networks and States. The Global Politics of Internet Governance*, Cambridge, MIT Press, 2010.

Mueller, Milton, *Ruling the Root. Internet Governance and the Taming of Cyberspace*, Cambridge, MIT Press, 2002.

Müller, Jan-Werner, *A Dangerous Mind: Carl Schmitt in Post-War European Thought*, New Haven and London, Yale University Press, 2003.

Nader, Ralph, *Esther Dyson’s Response to Ralph Nader’s Questions*, 15 Juni 1999, http://www.icann.org/en/correspondence/dyson-response-to-nader-15jun99.htm.

Naughton, John, *A brief History of the Future*. The Origins of the Internet, London, Phoenix, 1999.

Neal, Homer A. et al., *Beyond Sputnik: U.S. science policy in the twenty-first century*, Ann Arbor, University of Michigan Press, 2008.

Netcraft, *August 2011 Web Server Survey*, 2011, http://news.netcraft.com/archives/2011/08/05/august-2011-web-server-survey-3.html.

New Scientist, *Exploring the exploding Internet*, 2009, http://www.newscientist.com/gallery/mg20227061900-exploring-the-exploding-internet/5.

Noll, Michael, 'Telecommunication privatisation: mixed progress', *info*, 2, 1, 2000, pp. 21-3, http://www.emeraldinsight.com/journals.htm?articleid=873852&show=pdf.

NTIA, *Improvement of Technical Management of Internet Names and Addresses; Proposed Rule*, 20 February 1998, http://www.ntia.doc.gov/federal-register-notice/1998/improvement-technical-management-internet-names-and-addresses-proposed-.

NTIA, *Statement of Policy on the Management of Internet Names and Addresses*, 5 June 1998, http://ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses.

Packet Clearing House, *Packet Clearing House Report on Root Nameserver Locations*, 8 June 2008.

Postel, Jon, *Testimony of Jon Postel*, Congressional Hearing 7 October 1998, http://news.dot-nxt.com/1998/10/07/postel-testimony.

Powell, Walter W. and Paul J. DiMaggio, *The New Institutionalism in Organizational Analysis*, Chicago: University of Chicago Press, 1991.

Presidential Directive on Electronic Commerce, *Memorandum for the Heads of Executive Department and Agencies*, 1 July 1997, http://www.thecre.com/fedlaw/legal25e/presiden.htm.

Reidenberg, Joel, 'Governing Networks and Rule-Making in Cyberspace', in: Kahin, Brian and Nesson Charles (eds.), *Borders in cyberspace: information policy and the global information infrastructure*, Cambridge, MIT Press, 1997.

Rumsfeld, Donald, *DoD News Briefing—Secretary Rumsfeld and Gen. Myers*, February 12, 2002, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2636.

Samson, Victoria, 'The Murky Waters of the White House's Cybersecurity Plan', *CDI*, 23 July 2008, http://www.cdi.org/program/document.cfm?DocumentID=4345&from_page=../index.cfm.

Schmitt, Carl, *The Concept of the Political*, Chicago, The University of Chicago Press, 1996.

Schmitt, Carl, *The Concept of the Political*, Chicago, The University of Chicago Press, 2007 [1932].

Strong, Tracy B., 'Foreword: Dimensions of the New Debate around Carl Schmitt', in Schmitt, Carl, *The Concept of the Political*, Chicago, The University of Chicago Press, 1996.

TeleGeography, *Map Gallery*, 2010, http://www.telegeography.com/telecom-resources/map-gallery/index.html.

The World Bank, *World Development Indicators*, September 2011, p. 36, http://data.worldbank.org/data-catalog/world-development-indicators?cid=GPD_WDI.

Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6(Rev. 1)-E, http://www.itu.int/wsis/documents/doc_multi.asp?id=2267|0.

United States District Court for the District of Columbia, *Complaint for Injunctive release*, 2009, http://epic.org/foia/NSPD54_complaint.pdf.

US Department of Defense, *DoD Directive 5105.15 establishing the Advanced Research Projects Agency (ARPA)*, signed on February 7, 1958, http://www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2473.

US DoC, *Internet Corporation for Assigned Names and Numbers*, 20 October 1998, http://ntia.doc.gov/legacy/ntiahome/press/icann102098.htm.

US DoC, *Management of Internet Names and Addresses*, 5 June 1998, http://www.icann.org/en/general/white-paper-05jun98.htm.

Wæver, Ole et al., *Identity, Migration and the New Security Agenda in Europe*, Pinter Publishers Ltd., London, 1993.

Wæver, Ole, Aberystwyth, Paris, Copenhagen: New Schools in Security Theory and the Origins between Core and Periphery, *unpublished paper*, presented at the International Studies Association's 45th Annual Convention in Montreal, Canada, 2004.

Wæver, Ole, *Concepts of Security, Copenhagen*, Institute of Political Science, University of Copenhagen, 1997.

Waever, Ole, European Security Identities, *Journal of Common Market Studies*, 34, 1, 1996.

Wæver, Ole, Securitisation: Taking Stock of a Research Programme in Security Studies, *unpublished manuscript*, 2003.

Wæver, Ole, Securitization and Desecuritization, in Lipschutz, Ronnie D. (ed.), *On Security*, pp. 46-86. New York: Columbia University Press, 1995.

Wæver, Ole, The Ten Works, *Tidsskriftet Politik*, 4, 7, 2004.

Walton, Marsha, Web reaches new milestone: 100 million sites, *CNN*, 1 November 2006, http://edition.cnn.com/2006/TECH/internet/11/01/100millionwebsites/.

Waltz, Kenneth Neal, *Man, the State and the War*. A Theoretical Analysis, New York, Columbia University Press, 1954.

Waltz, Kenneth, *Theory of International Politics*, New York, Random House, 1979.

Watson, Scott, 'The 'human' as referent object? Humanitarianism as securitization', *Security Dialogue*, 42, 1, 2011.

Weinberg, Jonathan, 'ICANN and the Problem of Legitimacy', *Duke Law Journal*, 50, 1, 2000.

Weinberg, Jonathan, 'Non-State Actors and Global Informal Governance—The Case of ICANN', *International Handbook on Informal Governance*, 7 June 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1621862.

Wendt, Alexander and Duvall, Raymond, 'Sovereignty and the UFO', *Political Theory*, 36, 4, 2008.

Wendt, Alexander, *Social Theory of International Politics*, Cambridge University Press, New York, 1999.

WGIG, *Background Report from the Working Group on Internet Governance*, 2005, http://www.wgig.org/docs/BackgroundReport.doc.

White House, The Comprehensive National Cybersecurity Initiative, 2 March 2011.

White House, *The National Strategy to Secure Cyberspace*, 2003, http://georgewbush-whitehouse.archives.gov/pcipb/.

Williams, Michael C., 'Words, Images, Enemies: Securitization and International Politics', International Studies Quarterly, 47, 2003.

Abstract:

*Das grundlegende Ziel dieser Studie ist es, charakteristische Eigenschaften für Multi-Stakeholder Collaborations ausfindig zu machen. Am Beispiel von Internet Governance (genauer gesagt von Domain Name System Governance) soll dies unter Anwendung des Securitization-Konzeptes der Kopenhagener Schule erfolgen. Unter Anwendung der Theorie im Fall von DNS-CERT wird gehofft, dass bestimmte Merkmale festgemacht werden, die anschließend auch in anderen Zusammenhängen untersucht werden können. Darüber hinaus versucht diese Studie den Blick auf das Kopenhagener Konzept von Cyber Securitization zu schärfen, indem es ein Vier-Schichten Modell für den Cyberspace spezifiziert, mit je einer physischen, logischen, informationellen und sozialen Schicht.*

*The overall aim of this study is to detect some specific characteristics for multi-stakeholder collaboration. This shall be achieved by applying the Copenhagen school's concept of cyber securitization to the area of Internet governance (more precisely Domain Name System governance). By looking at DNS-CERT as a case for securitization in Internet governance, it is hoped to find some specific features that could eventually be detected in other areas as well. Also, this study tries to sharpen the Copenhagen school's concept of cyber securitization in that it specifies a four-layer model for cyberspace, including a physical, logical, content, and social layer.*

# Europass Curriculum Vitae

## Personal information

| | |
|---|---|
| First name(s) / Surname(s) | **Philipp MIRTL** |
| Address | Berggasse 7, 1090 Vienna (Austria) |
| E-mail(s) | philipp.mirtl@oiip.ac.at |
| Nationality | Austrian |
| Date of birth | 20 February 1984 |
| Gender | Male |

## Work experience

| | |
|---|---|
| Dates | September 2011 → |
| Occupation or position held | Affiliated Researcher / Adviser |
| Main activities and responsibilities | - Cybersecurity<br>- Internet Governance<br>- Critical Infrastructure Protection (CIP) |
| Name and address of employer | Austrian Institute for International Affairs (oiip)<br>Berggasse 7, 1090 Vienna (Austria) |
| Type of business or sector | Think Tank |
| Dates | October 2010 - June 2012 |
| Occupation or position held | Study Assistant for History of Political Thought |
| Main activities and responsibilities | - Text research<br>- Mentoring<br>- Program design |
| Name and address of employer | University of Vienna, Institute for International Development Studies<br>Sensengasse 3/2/2, 1090 Vienna (Austria) |
| Type of business or sector | University |
| Dates | Oktober 2010 - August 2011 |
| Occupation or position held | Research Assistant |
| Main activities and responsibilities | - Cybersecurity<br>- Internet Governance<br>- Critical Infrastructure Protection (CIP) |
| Name and address of employer | Austrian Institute for International Affairs (oiip)<br>Berggasse 7, 1090 Vienna (Austria) |
| Type of business or sector | Think Tank |
| Dates | September 2008 - March 2009 |
| Occupation or position held | Internship |
| Main activities and responsibilities | - Assistance in the monitoring of and cooperation with field offices<br>- General assistance in current projects<br>- Training and guidance of new interns |
| Name and address of employer | United Nations Organization, UNODC<br>Vienna International Centre, P.O. Box 500, 1400 Vienna (Austria) |
| Type of business or sector | International Organization |

## Education and training

| | |
|---|---|
| Dates | October 2004 → |
| Title of qualification awarded | Magister-Diplomstudium, comparable with Bachelor+Master |
| Principal subjects / occupational skills covered | Political Science |
| Name and type of organisation providing education and training | University of Vienna<br>Dr.-Karl-Lueger-Ring 1, 1010 Vienna (Austria) |
| Dates | October 2004 → |
| Title of qualification awarded | Magister-Diplomstudium, comparable with Bachelor+Master |
| Principal subjects / occupational skills covered | Economics |
| Name and type of organisation providing education and training | Vienna University of Economics and Business Administration<br>Augasse 2-6, 1090 Vienna (Austria) |
| Dates | July 2011 - July 2011 |
| Principal subjects / occupational skills covered | Internet Governance |
| Name and type of organisation providing education and training | European Summer School on Internet Governance 2011<br>Haferring 24, 04158 Leipzig (Germany) |
| Dates | June 2008 - August 2008 |
| Principal subjects / occupational skills covered | International Relations |
| Name and type of organisation providing education and training | University of Oslo<br>P.O. Box 1082 Blindern, 0317 Oslo Oslo (Norway) |
| Dates | October 2007 - June 2008 |
| Title of qualification awarded | LLP/ERASMUS-Program |
| Principal subjects / occupational skills covered | Political Science |
| Name and type of organisation providing education and training | University of Pavia<br>Strada Nuova 65, 17100 Pavia (Italy) |

## Personal skills and competences

| | |
|---|---|
| Mother tongue(s) | **German** |
| Other language(s) | |

| Self-assessment | **Understanding** | | | | **Speaking** | | | | **Writing** | |
|---|---|---|---|---|---|---|---|---|---|---|
| *European level (*)* | Listening | | Reading | | Spoken interaction | | Spoken production | | | |
| **English** | - | - | - | - | - | - | - | - | - | - |
| **Italian** | - | - | - | - | - | - | - | - | - | - |
| **French** | - | - | - | - | - | - | - | - | - | - |

(*) Common European Framework of Reference (CEF) level