UNIVERSITY OF AGDER

Confidence Building Measures as soft power?

A contribution to the study of international cybersecurity.

Jacob Daniel Schmidt

Supervisors

Oddgeir Tveiten, University of Agder (UiA)

Karl Ivar Jahr, Norwegian National Security Authority (NSM)

This master's thesis is carried out as a part of the education at the University of Agder and is therefore approved as a part of this education. However, this does not imply that the University answers for the methods that are used or the conclusions that are drawn.

University of Agder, 2013

Faculty of Humanities and Education

Department of Nordic and Media Studies

Abstract

The topic of this thesis is “CBMs and international cooperation within cybersecurity”.
The central research question it examines is: How can the use of CBMs in diplomacy enhance international cooperation within cybersecurity? In order to investigate this issue, I decided to conduct a number of in-depth interviews with experts within this field; these two groups of experts primarily consist of diplomats and researchers. My findings can be divided in two parts; the first concerns consequences of the emergence of the network society for diplomacy; the second part regards possibilities and limits of CBMs within international cybersecurity. Issues related to transparency, terminology and image constitute the core of these findings.

The study demonstrates that communication is a fundamental part of confidence building. While agreeing on specific multilateral CBMs within cybersecurity appears to be a difficult task at this early stage of international discussions, efforts at reaching agreement on cyber CBMs can be a type of CBM in itself. CBMs create mutual understanding, build relations and ultimately reduce the risk of misunderstanding and misperceptions which could lead to wrong decisions and the escalation of conflicts. Soft power represents a useful way to approach these issues as soft power and CBMs can be mutually reinforcing.

Preface

This thesis is written as the final section of the Master's Programme in Social Communication at the University of Agder in Kristiansand, Norway. It was postponed one semester due to a 6-month internship with the Norwegian Embassy/ Permanent UN-mission in Vienna during the spring of 2013.

The topic of this thesis is a result of the internship in Vienna. It was inspired by recent multilateral processes in the United Nations Office on Drugs and Crime (UNODC), in particular the 22nd Commission on Crime Prevention and Criminal Justice which was held 22-26 April in Vienna. I originally set out to write about the issue of cybercrime, but after some preliminary research and subsequent consultations I decided to focus instead on cybersecurity and CBMs. Part of the argument in this study is that CBMs fundamentally concern communication, making this topic highly relevant for social communication.

I would like to thank all of the 16 informants who kindly agreed to participate in this study and who generously shared their thoughts and experiences in this context. Without your generosity, this thesis would not have been possible. Furthermore, I would like to express my sincere appreciation for the support given by my family and friends; Mom, Dad, you know how grateful I am for your support. Cole, Håkon, Jeanette, Leah, Petter and Silje; thank you for your constructive feedback and valuable comments.

Finally, I would like to extend my deepest gratitude to my supervisors, Oddgeir Tveiten and Karl Ivar Jahr, for your insightful guidance and encouraging support throughout this research process. You have both been instrumental in helping me reach the end point of this thesis, and I will be forever thankful for your support throughout this thesis.

Daniel Schmidt

University of Agder

December 12, 2013

Table of contents

1.0 Introduction

1.1 Theme and background

In today's complex, globalized world, countries can no longer rely exclusively on military force or economic strength in order to succeed with their geopolitical ambitions. States and their citizens have never been as interconnected and as interdependent as they are now, in part thanks to the ICT revolutions and the emergence of the network society (Castells, 2010).

Thus, to reach their governments' national security and foreign policy goals, government representatives to a larger extent than ever before need to take into account their state's image in the international system and the way that their actions might be interpreted and judged by others. They need a conscious strategy for how to attain influence, for what Joseph Nye terms 'soft power'; that is, the ability to shape the preferences of others and achieve desired outcomes through attraction, rather than coercion (Nye, 2004, p. x). *Trust* is crucial in this context.

Hence, the theme for this thesis is Confidence Building Measures (CBMs) within international cybersecurity. CBMs are initiatives aimed at securing peace and predictability among states. They originated during the Cold War and have repeatedly been used in the past in various contexts as means to create trust and reduce the risk of misunderstanding and conflict escalation (Neuneck, 2013c, pp. 121-122). Concretely, CBMs can assume many different shapes including information exchange, open ended consultations, joint simulation exercises and capacity building, just to mention a few (OSCE, 2012, pp. 9-11).

Recently, trust and mistrust have come to the forefront in public debates internationally due to Edward Snowden's revelations concerning extended surveillance conducted by US intelligent services (Luce, 2013). In the cyberspace environment, trust becomes a scarce resource and a necessary foundation for international cooperation. There is currently widespread support internationally that trust building through CBMs within the cyber domain represents a promising way forward to enhance international cybersecurity (Stauffacher & Kavanagh, 2013a, p. 3).

In this thesis I will elaborate on the complexities and challenges related to the processes of agreeing on "cyber CBMs". I will investigate in what ways CBMs can be used in order to strengthen international cybersecurity. The role of soft power in this context will be discussed.

As an additional outcome, this analysis contributes to a broader understanding of the concept "cyberdiplomacy".

1.2 Research question

In order to clarify the intended goal of this thesis, I will approach the following research question:

How can the use of CBMs in diplomacy enhance international cooperation within cybersecurity?

For the purpose of finding answers to my research question, I will use an open, explorative research design drawing on principles from a qualitative research approach inspired by grounded theory. I have chosen to conduct a total of 16 in-depth interviews with experts within the field of diplomacy and/or cybersecurity. About half of the informants for this thesis are experienced diplomats, whereas the other half primarily consists of researchers. The main reason for this approach lies in the complexity and inter-disciplinary character of the topic and research question. This requires both detailed knowledge of the concrete subject matters as well as the ability to view CBMs in the greater context of international cybersecurity.

In addition, and as a way of operationalizing this question, I will look at the following two sub-questions:

1) What are the main consequences of the emergence of the network society for international cybersecurity?
2) What are the possibilities and limits of CBMs in terms of enhancing international cybersecurity, and how does soft power relate to CBMs in this context?

To shed some light on these questions, I will draw on various theoretical tools from communication theory, political science and sociology. Combined they provide a broad conceptual framework for our understanding of CBMs, diplomacy and power in and through the cyber domain. In particular, I will look to Castell's notion of the network society as a theoretical backdrop for discussing these issues. I will furthermore examine to what extent Joseph Nye's concept of soft power can provide a useful tool for analyzing and understanding CBMs within the context of international cybersecurity.

1.3 Limitations and justification

An important preliminary distinction in this context has to be made between cyberwarfare and cybercrime; cybersecurity in this thesis relates to the prevention of cyberwarfare, understood as "state-sponsored, offensive cyber activities directed towards another state, its infrastructure or population" (Baseley-Walker, 2011, p. 31). It does not focus on cybercrime, which relates to actions by non-state actors deemed illegal according to national or international law. In reality, however, clear-cut lines between different types of destructive behavior in cyberspace is difficult to achieve, for instance in grey areas such as espionage and illegal surveillance.

This thesis neither deals specifically with technical issues related to cybersecurity, for instance defending against various forms of network attacks, nor with the legal dimension regarding, inter alia, the applicability of existing legal frameworks such as International Humanitarian Law (IHL) or the Law of Armed Conflict (LOAC) to cyberspace. Furthermore, I will not elaborate on the role of the private sector and civil society in efforts to enhance international cybersecurity. Despite the fact that there is growing recognition among scholars and policy makers alike for the need of more public-private partnerships (PPPs), this issue remains outside of the scope of this thesis. The same is valid for questions regarding Internet Governance (IG).

1.4 Definitions

The multi-faceted nature of this research topic requires a broad array of key terms to be defined from the outset. Confidence building measures (CBMs) as defined above aim to reduce the risk of conflict and conflict escalation through communication and the exchange of information. They are often seen as primarily politically binding, laying the groundwork for future legally binding instruments. They can also develop to become legally binding agreements themselves (Baseley-Walker, 2011, p. 32).

Diplomacy can be defined as the "the management of international relations by negotiation" (Nicolson, 1939, reproduced in Zartman, 2009, p. 26). It is situated between international law and war as a way to secure peaceful relations between states, and it has traditionally been seen as the arena of and for countries' official representatives such as ambassadors and diplomats. In the 21st century, the rise of trans-national relations and increased contact between non-

state-actors or non-governmental organizations (NGOs) complicate this picture. “Public diplomacy” emphasizes this trend as is often viewed as the “communication of an international actor’s policies to citizens of foreign countries” (Pamment, 2013, p. 1).

The term ”cyber” is derived from the Greek work “kybernetes*”* meaning “steersman” (Kuehl, 2009, p. 26). The multitude of different words used in combination with cyber can sometimes be confusing; all though “cyberspace”, the “cyber domain” and the “digital domain” in some contexts have nuanced differences, these terms are often used interchangeably and for the sake of simplicity this will also be the case in this thesis.

“Cyberspace” was first coined in Gibson’s science fiction novel in the early 1980s (Gibson, 1986). While a variety of definitions exist, one perspective views cyberspace as a 3-layer-construction: it consists of a physical layer with PCs, routers and other hardware, a syntactic layer of software, and of a semantic layer referring to the information displayed to users (Libicki, 2007). Another view regards cyberspace as a sort of information environment characterized by the use of ICT networks to create, store and diffuse information (Kuehl, 2009, p. 28).

“Cybersecurity” has in recent years developed into becoming a central issue and a complex challenge both to the nation state and to the international community. In broad terms, cybersecurity can be said to deal with the “safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure” (EU, 2013, p. 3). As with the term cyberspace, there are different theoretical approaches to the concept of cybersecurity. These will be further elaborated in the theory chapter.

The “network society” is defined by Castells as «a society whose social structure is made of networks powered by microelectronics-based information and communication technologies» (Castells, 2004, p. 3). Social structure in this context refers to the way human relations are organized, inter alia, with regards to production, consumption, and more generally, power. (Castells, 2009, p. 24). Other definitions additionally put particular emphasis on the media and media networks as fundamental characteristics of the network society (Dijk, 2006, p. 50; Hassan, 2004).

The definition of “power” suggested by Robert Dahl represents one of the most well-known perspectives of power both within and outside of academia: it refers to a behavioral

understanding of power as A's ability to have B do something B otherwise wouldn't do (Dahl, 1957, pp. 202-203).Yet, this definition doesn't capture the whole range of possible power sources, structures or mechanisms. I will present a more thorough discussion of power and power structures below, with a particular focus on power in the cyber domain and what this means for diplomacy.

"Soft power" represents a particularly interesting type of power, as it challenges a more traditional, materialist view of power within international relations (IR) which tends to focus exclusively on states' military or economic power. It is in short, and in the words of the man who coined the term, "the ability to get what you want through attraction rather than coercion or payments" (Nye, 2004, p. x). This ability to "shape the preferences of others" or make others want what you want, is based on resources that produce attraction. In an international setting one of the most important such soft power resources is a country's public diplomacy (Nye, 2008, p. 95).

1.5 Organization of the thesis

In chapter 2, I will outline the theoretical backdrop for this. First, I will discuss cybersecurity as a concept "in the making", followed by an examination of diplomacy and CBMs within diplomacy. Then, I will provide a discussion on the concept of power, with a particular focus on power in the network society. Finally, I will conclude this chapter with a discussion of soft power and its relation to "cyberdiplomacy".

Chapter 3 describes the methodological approach used in this thesis. It draws primarily on in-depth interviewing within the qualitative research tradition, with some inspiration from grounded theory. This chapter also illustrates the procedures used for sampling and analysis, and it discusses the issues of validity and reliability.

In chapter 4 I set out to identify and describe some of the main findings in the empirical data gathered in light of the presented theory. Chapter 5 attempts to bridge the gap between the theoretical perspectives and these findings, viewing the empirical data in a broader perspective and suggesting recommendations for further research.

Finally, chapter 6 offers a summary of the main perspectives and findings presented in this thesis.

2.0 Theory

In this chapter I will present the theoretical framework used to address my research questions. International cybersecurity is a complex, multi-dimensional issue; it relates both to international cooperation or diplomacy, and to cybersecurity which in itself is a multi-faceted issue. While the emphasis on CBMs helps narrow the focus of the thesis, the inter-disciplinary nature of this research topic nonetheless requires a somewhat broad approach drawing on various theoretical contributions.

Firstly I will present cybersecurity as a concept "in the making" both in academic literature and in more practical terms, and I will attempt to situate it as a topic of concern to international cooperation. Then, since the focus of this thesis is international cybersecurity and CBMs, I will continue with a discussion of diplomacy and the role of CBMs within diplomacy in general and within cybersecurity in particular. Part of the argument in this chapter is that diplomacy cannot be comprehended without a certain understanding of power. Therefore, a discussion of power is included in this chapter, followed by a brief debate on soft power, which will then be related to CBMs in this context. Put together, these theoretical contributions provide a useful conceptual framework for approaching the question of how the use of CBMs in diplomacy can strengthen international cybersecurity.

In closing, I will introduce the term "cyberdiplomacy" and begin to examine possible links between this term and CBMs within international cybersecurity. This topic will be further investigated in the analysis chapter.

2.1 Cybersecurity

As suggested above, there is a sense of ambiguity both among practitioners and in academia in relation to some of the key terms used in this thesis – not to mention in the everyday usage of these terms. "Cybersecurity" in the common-sense meaning of the word is often associated with technical issues related to data protection, the use of firewalls and protection against hacking and malicious software, to mention a few. Some might think of cybersecurity as pertaining to social issues such as the use of social media among children, or related to broader political questions, for instance the right to privacy versus freedom of expression.

Cybersecurity in the introduction to this thesis was described as relating to the "safeguards and actions" used to protect the cyber domain from threats to its "interdependent networks and information infrastructure" (EU, 2013, p. 3). Following a somewhat similar definition by the International Telecommunications Union (ITU), cybersecurity can be understood in this way:

- *"The collection of policies and actions that are used to protect connected networks (including, computers, devices, hardware, stored information and information in transit) from unauthorized access, modification, theft, disruption, interruption or other threats."* (ITU, 2008, p. 7).

In short, these definitions refer to the protection of computer- or information networks from various kinds of threats. Typically, a distinction is made between three types of "cyberthreat" actors: criminals – including terrorists – , so called "hacktivists" acting for political purposes and nation-states with malicious intentions (Neuneck, 2013a, pp. 115-116). However, as mentioned in the introduction chapter this thesis focuses on cybersecurity regarding relations between states and the prevention of cyberwarfare[1] among state actors, and not on security in the context of cybercrime as perpetrated by non-state actors (Baseley-Walker, 2011, p. 31).

In other words, I will focus on cybersecurity specifically as a challenge for international cooperation, on what can be called "international cybersecurity". I will specifically examine in what ways CBMs can be used in diplomacy to enhance international cooperation within cybersecurity. This is a difficult area of cooperation for several reasons; to begin with, there is currently no internationally agreed upon definition of the term "cybersecurity". This lack of common understanding makes it difficult to work together across national and cultural borders, despite the fact that most countries acknowledge the need for international cooperation in this context (ENISA, 2012, p. 9). States are of course not one-dimensional, rational actors (Allison, 1969, p. 707). Yet, for the analytic purposes of this thesis I will refer to states in this singular and simplified form in this thesis.

Differences in opinion on key terms and their fundamental meanings vary even between typically like-minded countries; while the United States and the United Kingdom first and foremost relate cybersecurity to national security, the European Union and many Western

[1] For a discussion on the purpose and limits of cyberwar, as well as on the difference between strategic and operational cyberwar, see Martin C. Libicki's *Cyberdeterrence and cyberwar* (2009, pp. 117-158).

European states consider cybersecurity primarily as a national infrastructure problem (Joyner, 2012, p. 163).

Cybersecurity in this sense is a relatively new and still not clearly defined field of research. Yet in the academic literature, approaches to cybersecurity can broadly be divided into three distinct schools: The revolutionists, the traditionalists and the ecologists (Langø, 2013, pp. 230-238).

The revolutionists produced in the mid-90s some of the earliest scholarly work on the consequences of the ICT revolution for warfare. They contributed to a larger debate on American military strategy in the aftermath of the Cold War; here, they emphasized the so called "Revolution in Military Affairs" (RMA) caused by new ICTs and how this would lead to radically new types of war and mechanisms of warfare in the future (Arquilla & Ronfeldt, 1997, p. 23). On the other hand, traditionalists are much more skeptical towards the revolutionizing effects that these ICTs might have on armed conflict or to the whole idea of "cyberwar" (Libicki, 1995, p. 75; Rid, 2011, p. 10). They point out the fact that there has so far been few if any actions or conflicts in cyberspace fitting under the label "war", and they call for more empirical evidence to support the use of this term.

The third school, the ecologists, emphasize cyberspace as a distinct domain or space where the actions by civil and military users are intertwined, requiring this domain to be approached as an "ecosystem of competing and collaborating actors" (Rattray & Healey, 2011, pp. 67-68). Scholars within this tradition understand power and "cyberpower" in a broader sense, and they stress the role that non-state actors play both in terms of power and in relation to security in the cyberspace environment.

In this context, it is worth noting that Joseph Nye arguably fits into this last school of thought. He points out how the cost reduction within ICTs has led to a degree of power diffusion, potentially effecting the power balance between states (Nye, 2010a, p. 19). Later in this chapter, I will investigate to what extent his theory on "soft power" might prove helpful in understanding the role that CBMs can play in enhancing international cybersecurity.

As will be argued in this thesis, cybersecurity can be seen as both a technical, political and a social challenge:

"The real problems of "cybersecurity" are not simply—or even mainly—a technical issue of computer networks, hardware and software any more than war is just a matter of weapon systems; rather, both are about politics, about society, and about understanding the human motivations behind the uses of the technology for better or worse" (Betz, 2012).

This broad understanding of cybersecurity requires a broad approach to the question of how CBMs can be used in diplomacy to strengthen international cybersecurity. For this reason I will discuss the concepts of diplomacy, CBMs and power before rounding up this chapter with a discussion on the role of soft power.

2.2 Diplomacy

Cybersecurity as described above represents a significant element of security politics in our time and requires cooperation across state borders. In this thesis I will focus on diplomacy as one dimension of such cooperation. Diplomacy is arguably an intuitively understandable concept as used in public discourse, yet interestingly complex when put under analytic scrutiny. In defense of the recent first step towards a nuclear deal with Iran after decades of hostility, US President Barack Obama emphasized the role of diplomacy for security efforts:

"We're testing diplomacy; we're not resorting immediately to military conflict (…) Tough talk and bluster may be the easy thing to do politically, but it's not the right thing for our security" (Landler, 2013).

Yet it is not immediately clear what this shift to a more diplomatic approach means in concrete terms. This invokes the question: what are the fundamentals of diplomacy?

Diplomacy as a theoretical concept has more than one definition, as many other key terms in the social sciences. In the introduction chapter of this thesis, diplomacy according to Nicholson was closely linked to negotiations. It can be defined in broad terms as the activity in which "international relations are managed by negotiations" in order to maintain peace and stability between states (Nicolson, 1939, reproduced in Zartman, 2009, p. 26). Furthermore, following his line of thought, what is truly the essence of diplomacy is common sense. This has the somewhat direct implication that "the worst kind of diplomatists are missionaries, fanatics and lawyers; the best kind are reasonable and human skeptics" (Nicolson, 1939, p. 50).

Another and quite different way of looking at diplomacy is suggested by James Der Derian and his emphasis on "alienation" and on diplomacy as the "mediation of estrangement" (Der Derian, 1987a, p. 93). Following this view, diplomacy can be viewed as the conciliation or "mediation between estranged individuals, groups or entities", or in a more modern version, "the mediation of estranged peoples organized in states which interact in a system". Der Derian disputes the view that diplomacy is essentially common sense, arguing instead that common sense is always specific to any given culture and/or time. Furthermore, he claims that the origins of diplomacy cannot be understood as chronologically or geographically fixed; rather, diplomacy should be viewed more as a set of practices and power struggles which have developed over time. These practices developed in tandem with changing circumstances for culture and power (Der Derian, 1987b, p. 42).

A third view of diplomacy presented by Putnam describes the interplay between domestic and international politics as a "two-level game" (Putnam, 1988, p. 427). According to this perspective, at the level of national politics, domestic groups and coalitions among these promote their own interests by lobbying the government to adopt specific policies. At the international level, governments attempt to meet the demands from these domestic groups as far as possible, while simultaneously trying to minimize unfortunate consequences of foreign developments. Putnam argues that central decision makers have to take into account both of these levels or games and the interaction between them when considering various policy options (Putnam, 1988, p. 434).

Today, a distinction is often made between this "traditional" diplomacy as between state representatives and what is known as "public diplomacy". Public diplomacy can be defined as "the communication of an international actor's policies to citizens of foreign countries" (Pamment, 2013, p. 1). Increasingly theories on public diplomacy emphasize this strand as diplomacy *by* rather than *of* publics, meaning that individuals and groups themselves participate in shaping international policies (Melissen, 2005, p. 32).

Despite the differences between them, all of these definitions relate diplomacy to relations between states and to efforts at improving these. This is obviously about power and power relationships, but it is also about communication; be it in the form of negotiations, the mediation of estrangement or public diplomacy efforts, diplomacy is fundamentally about communication between states (Bjola & Kornprobst, 2013, p. 77). After all, the word "communication" derives from the Latin expression "communicare", meaning to share, or

make common.[2] Thus, while communication in a basic way concerns the sharing of information or the production of shared meaning, diplomacy cannot take place without well-functioning communication.

In this thesis diplomacy will be understood in a broad sense as *function*, covering a variety of roles which act or speak on behalf of national interests in an international context. As argued above, diplomats and other government representatives performing diplomatic functions need not only be highly knowledgeable about the culture, history and policies of both their own country as well as about those of "the other", the host country; they need to be well-trained communicators.

2.2.1 The use of CBMs in diplomacy

The central focus of this thesis is as mentioned above confidence building measures (CBMs) within the specific field of international cybersecurity. As will be shown, these types of measures have received a growing level of attention internationally in recent years with a number of parallel processes going on in different international fora. In order to fully understand the nature of CBMs, I will briefly outline the historical context and general purpose of this concept before moving on to a discussion on the specific use of CBMs within the cyber domain. In particular, I will look at CBMs in the context of work done by the Organization for Security and Co-operation in Europe (OSCE).

CBMs are often regarded as one of the most efficient and wide-spread methods for initiating and enhancing international cooperation in various areas. As mentioned in the introduction chapter, CBMs have repeatedly been used in the past in different contexts as means to create trust and reduce the risk of misunderstanding and conflict escalation. In short, the ultimate goal of CBMs is the securing of peace and predictability among states (Neuneck, 2013c, pp. 121-122).

Originating in the Cold War-logic, the term CBMs was first used in the 1950s in relation to initial efforts to increase transparency between the East and the West, such as the American initiative for an "Open Skies"-treaty (OSCE, 2012, pp. 11-12). After the Cuban missile crisis in 1962, the need became apparent for effective, direct communication channels in order to

[2] The nominative form is "communicatio". From the Online Etymology Dictionary (Communication, 2013).

prevent nuclear war due to misunderstandings and lack of communication.

In Europe the OSCE and its predecessor, the Conference on Security and Co-operation in Europe (CSCE) played a pivotal role in confidence building initiatives through the measures agreed upon in the Helsinki Final Act.[3] In this context, a distinction should be made between confidence building measures (CBMs) and confidence- and security building measures (CSBMs); in the early phase of these confidence building processes, CSBMs were primarily directed at so-called "hard security" and military issues such as the exchange of data or pre-notifications of military movements. CBMs, on the other hand, are directed more towards changing perceptions and "(re)building relations between adversaries" (Neukirch, 2012, p. 3). Additionally a third group of measures known as transparency- and confidence building measures (TCBMs) is referred to in some contexts, underlining the role of these measures in reducing threats and increasing transparency. The lines between these terms, however, are not always waterproof and they are often used interchangeably (Neuneck, 2013c, p. 122).

CBMs can be unilateral, bilateral or multilateral, and they can assume many different shapes depending on the context. For instance, the OSCE operates with five categories of non-military CBMs; political, economic, environmental, societal, and cultural CBMs (OSCE, 2012, pp. 9-10). This is not an exclusive list of possible CBMs, but it illuminates some of the variation in the nature and purpose which exists in these measures. CBMs will most likely not resolve conflicts by themselves, but they may lay the foundation for a cooperative environment and thus help to improve relations between states.

While the original intention was to prevent accidental nuclear attacks, CBMs have expanded to other areas as well both within and outside of the military domain (UNODA, 2013a). In short, communication and trust building as a type of safeguards against conflicts lie at the heart of all CBMs.

2.2.2 CBMs within international cybersecurity

[3] This subsequently led to the Stockholm Document in 1986 and the Vienna Document in 1990. See the *OSCE Guide on Non-military Confidence-Building Measures (2012),* available at http://www.osce.org/home/94616

Considerations on CBMs within the cyber domain to a large extent reflect much of the thoughts concerning more traditional CBMs. Through discussion on and implementation of CBMs, states will be better suited at interpreting and understanding each other's intentions and messages, thus decreasing the probability of misled decisions and the possible outbreak of war (Neuneck, 2013c, pp. 121-122). Yet, the unique character of the cyber domain requires to a certain extent new thinking, for instance relating to the attribution problem, the large number of actors involved in cyberspace as well as the rapidly changing nature of the environment. These factors will be further discussed below.

There is an increasing number of processes taking place both on a global and on a regional level related to norms development and CBMs regarding cybersecurity (Weekes & Tikk-Ringas, 2013). These processes may be seen in light of the fact that there are currently no global treaties specifically regulating state behavior in cyberspace. In the United Nations (UN), there have been three Groups of Governmental Experts (GGEs) which have investigated threats from the cyberspace environment and ways to cooperate in order to mitigate these threats (UNODA, 2013b). The third and most recent GGE on this topic within the framework of the UN General Assembly's First Committee on Disarmament finalized its report[4] in June 2013, agreed upon by consensus. This report builds on work done by the previous GGEs and includes recommendations on norms rules of responsible state behavior, CBMs and capacity building measures. Importantly, consensus was reached regarding the applicability of international law to the cyber domain (Stauffacher & Kavanagh, 2013b, p. 5). Yet, further work is needed to describe *how* these laws can be applied to the cyberspace environment.

The growing focus on CBMs in the cyber domain can be understood on the basis of different factors. One such element is precisely the increased recognition of the challenges pertaining to applying international law to activities in cyberspace; another is the presumed digital arm's race or "rush to weaponize" the cyber domain, posing threats to stability and increasing the likelihood of miscalculations that could potentially develop into armed conflicts (UNIDIR, 2012, pp. 13-14).

Within the context of international cybersecurity, such measures are typically divided into four different categories representing main challenges to trust building: transparency

[4] The report, entitled *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/68/98) is available under http://www.un.org/disarmament/topics/informationsecurity/

measures, cooperative measures, communication mechanisms and stability/restraint measures (Stauffacher & Kavanagh, 2013a). I will briefly outline each of these main categories before discussing the applicability or relevance of CBMs in today's cybersecurity reality.

1) Transparency measures

This first set of confidence building measures within the cybersecurity field in broad terms aim at improving stability and predictability. This is what lies at the heart of all CBMs: building trust in and between states through transparent and honest communication, in order to avoid escalation of conflicts. While observation and verification of data are key aspects of reaching predictability, transparency measures in general need three things to work; mutual trust, a deliberation on whether or not to include legal dimensions; and using regional organizations as a form of "repository of nation-state views" (Stauffacher & Kavanagh, 2013a, p. 6). Transparency is particularly important due to the so called "attribution problem", meaning the "difficulty of identifying actual or potential hackers" (Kugler, 2009, p. 309). This constitutes a challenge for deterrence of attacks in cyberspace, and it can be rather costly to verify the true perpetrators behind certain actions.

CBMs are typically initiated as fundamentally politically binding, creating expectations to be followed but without legal obligations. In some cases CBMs develop themselves over time to become legally binding in the form of international treaties (Baseley-Walker, 2011, p. 32). One such example is the so called "Open Skies treaty" which allows for unarmed aerial surveillance flights over the territories of all participating states (OSCE, 2012, p. 12). CBMs serve as important first steps for states to get involved. In the cybersecurity context, specific confidence building measures on transparency could include open-ended consultations on national policies, budgets and strategies, having a national cybersecurity strategy made publicly available, joint simulation exercises and exchange of best practices in responding to threats to ICT security (Stauffacher & Kavanagh, 2013a, pp. 6-8).

2) Cooperative measures

When considering cooperative measures, it can be helpful to distinguish between three different relationship models describing various degrees of cooperation between states. Cooperation can thus take place between;

a) like-minded states, with an already established level of trust, for instance among the Nordic

countries

b) states with existing dialogue channels but lack of trust, such as between the US and Russia

c) states with limited or no dialog and absence of trust, for instance between the US and Iran

These models each have their own specific challenges related to negotiating CBMs. CBMs typically should be used in an incremental approach where trust is built step-by-step over time (Lewis, 2011, p. 59). In this sense these relationship models represent various stages of the trust building process, each with its distinct needs for specific CBMs.

In general, some of the cooperative confidence building measures could include developing and exchanging common terminology for cybersecurity issues, exchanging information on cybersecurity-related organizations and their structures and contact persons, and capacity building on ICT use (Stauffacher & Kavanagh, 2013a, pp. 8-10).

3) Communication and collaborative mechanisms

Al though similar and closely related to the previous category, this third group of CBMs can be identified as a separate category as it includes mechanisms for states to regularly communicate with each other on cybersecurity issues. These measures predominantly focus on ways to share threat and indicator information, also for countries that are not at leading cybersecurity states (Stauffacher & Kavanagh, 2013a, pp. 10-11). Specific communication and collaborative mechanisms can include regular exchanges of information on both bilateral and multilateral levels, joint threat assessments and establishment of common crisis management frameworks, to mention just a few.

4) Stability and restraint measures

Being the most difficult category of CBMs, often times only possible to work with after successful cooperation in the first three categories, stability and restraint measures are usually agreed upon towards the end of a negotiation process. They are important to establish a confidential dialogue among sophisticated cyberpowers, all though it is clear that not all states will have the same need for putting in place such measures yet. While it may be used in various contexts, the term “the digital dive” commonly refers to the gap between those who have access to computers and to the Internet and those who don’t (Dijk, 2006, p. 178). The extent of this divide varies both between and within countries, but it illustrates how different states might have various needs in terms of cybersecurity.

Some examples of stability and restraint measures could be agreement on international technical standards - thus raising the barriers for developing cyber capabilities-, measures to ensure continuity and stability of the Internet during crisis, and pledges to remove incentives for first strike offensive capabilities (Stauffacher & Kavanagh, 2013a, pp. 11-12).

But why the need for international cooperation in relation to cybersecurity issues in general, or for CBMs in particular? What purpose does it serve for states to build confidence among themselves and to create an atmosphere of trust internationally, when so many of the most pressing threats are confined within the state's own borders, among its own citizens? Furthermore in many cases these challenges require timely and coordinated responses, not exactly tenets often attributed to CBM processes.

Part of the answer lies in the very nature of cybersecurity itself; since the "cyberthreat" is an international threat, it needs an international approach with coordinated cooperation among states (ENISA, 2012, p. 9). For instance, a state can have a carefully designed cybersecurity strategy and even implement a number of appropriate measures to follow up this strategy within the state's jurisdiction. Yet this will unlikely mitigate the threat posed by actors operating from abroad, which can violate national security regulations in this state and not necessarily have to worry about being prosecuted back home.

In other words, states are interdependent in this context. They depend on cross-border cooperation in order to meet current security challenges. These challenges relate not only to cybercrime as perpetrated by non-state actors but to relations between states and the prevention of cyberconflict (Baseley-Walker, 2011, p. 31). It is upon this backdrop of interdependence that one can more fully comprehend the theoretical basis for Nye's development of the term "soft power" (Nye, 1990) in general, and in particular its applicability within a cybersecurity context. These issues will be further discussed below.

2.3 Power

2.3.1 Power in the social sciences

Intuitively it can perhaps seem peculiar to debate the concept of power in a study focusing on CBMs and international cooperation within cybersecurity. Yet in this thesis it is argued that it

is very difficult to have a fruitful discussion about diplomacy in any given context without taking into consideration the underlying power dimension. Diplomacy can be defined in many ways, but it is difficult to imagine government representatives from two different states interacting with each other in complete ignorance of the power relationships existing between their respective home countries.

As pointed out earlier, power is one of the most highly debated concepts within the social sciences. Different academic disciplines can have diverging views of, and approaches to the notion of power. Furthermore, there are often contradictory views even within one and the same discipline. In international relations (IR) theory, for instance, one of the main tenets distinguishing the realist tradition from the constructivist school is their understanding of the nature of power (Jackson & Sørensen, 2010, p. 160). Power is in short an "essentially contested term" (Lukes, 1974, p. 9).

Following Weber, in broad terms, power can be understood as possession. Power enables one actor to impose his or her will on someone else, and it is only realized against resistance (Weber, 1991, p. 180). Power in this sense is something which can be possessed, for instance a gun, and which allows the actor in possession of it to force others without a gun to comply. In one way this comes close to the rather common sense view of power as formulated by Dahl and presented in the introduction chapter as "A's ability to have B do something B otherwise wouldn't do" (Dahl, 1957, pp. 202-203).

A somewhat deeper understanding of power takes into account that power may be viewed as relation. Lukes promotes what he calls a radical or three-dimensional view of power (Lukes, 1974). Following this perspective, the one-dimensional view or "first face of power" understands power in a narrow sense as coercion and as manifested in observable conflict, similar to the definition above. A broader and improved understanding is represented by the two-dimensional or "second face" of power, which includes latent conflict and the power of agenda-setting.

A complete understanding of power, however, is according to Lukes only possible through a three-dimensional view in which power may also be understood relationally, existing as power-relations between agents (Lukes, 1974, pp. 37-38). Following the above example with the gun, this view of power would investigate under what circumstances a gun is produced and seek to understand the conditions which enable the possessor to impose his or her will. The "third face of power" in this way relates more closely to the works of other scholars of

sociology with more advanced theories of power[5]. Through the glasses of these sociologists, one does not only look at the immediate sources and consequences of power in its many different shapes and dimensions; rather, the focus is directed to the deep-rooted, structural causes behind power and the complex ways in which power is created, transformed and dispersed through a number of mechanisms operating in the visible and/or invisible social structures.

So why is this relevant for an understanding of cybersecurity and cyberpower? Because as with many things in the cyber domain, what works in the physical, offline world often times works just as well in the virtual, online reality, sometimes even with increased effects. In other words, sources of power in the pre-Internet age are in most cases equal or even stronger sources of power in the cyberspace environment and it is crucial to understand these dynamics in order to succeed with any strategy dealing with the multiple challenges to cybersecurity.

2.3.2 Power in the network society

Social scientists often advocate labels or sets of perceptions and ideas in order to describe the world in which we live in. The "network society" represents one such label. It refers to a kind of society which has emerged during the last few decades where the "social structure is made of networks powered by microelectronics-based information and communication technologies" (Castells, 2004, p. 3). While different processes have led to the emergence of the network society, new ICTs developed in recent years and particularly the Internet have contributed to this societal change. As formulated by Castells:

"As information and communication are the most fundamental dimensions of human activity and organization, a revolutionary change in the material conditions of their performance affects the entire realm of human activity" (Castells, 2004, p. 9).

As demonstrated earlier, an important dimension of any discussion about the relationships between security, society, diplomacy and communication is the question of power and power relationships. But who has power in the interconnected reality of the network society, and what significant changes does this form of power represent?

[5] See for instance Foucault's view of power as domination (Foucault, 1983, p. 212) or Bourdieu's concept "symbolic power" (Bourdieu, 1991, p. 166).

Castells points out how the network society functions through a form of binary logic, based on inclusion an exclusion (Castells, 2004, p. 23). Nodes which contribute to the network are included, be it individuals, places or activities, while nodes of little or no value to the network are excluded. In this environment it is about giving and taking, and influence will only be acquired through membership in a network. In this context diplomacy can be understood as a form of network with various sub-networks related, for instance, to different CBMs processes. In order to benefit from the trust building in these processes states must be ready to contribute by sharing information and create mutual trust (Stauffacher & Kavanagh, 2013a, p. 6). States unwilling to commit to transparency might thus be excluded from these networks.

Networks are not new to human interaction, but the global reach of today's ubiquitous networks in social, business and political life are (Castells, 2009, p. 28). The mosaic metaphor has been used to illustrate how societies traditionally were organized, where places were understood as having unique, separate identities and being relatively isolated from each other (Castree, 2003, p. 174). Such a view appears outdated in today's interconnected world, in which hardly any society can function isolated from its environment (Murray, 2006, pp. 49-51). In the globalized world of today, ICT networks provide the backbone of society and are critical for enabling and upholding social interaction. What is meant by "critical infrastructure" depends on the context and changes over time, but ICTs or cybersystems are increasingly included under this label as vital assets for the functioning of society (McCarthy, Burrow, Dion, & Pacheco, 2009, p. 544).

Following Castells, what counts as valuable in the network society has no final, given answer, but it is defined by whoever has the power at any given point in time, and in each specific network (Castells, 2004, pp. 24-26). For instance, in a worldwide economic network of states dominated by capitalism financial resources most likely will be valued as the supreme value against which all other goods are measured.

A similar line of thought may be found in Castells' concepts of "programmers" and "switchers" (Castells, 2004, p. 32). Programmers define and redefine the network's goals or programs, they are thus the ones with the power to decide what values are important and not. Switchers are those with the ability to connect different networks with each other, and they are important in order to secure cooperation and mutual profits between strategically important networks.

2.3.3 Cyberpower

Another way of analyzing power in the network society is through the lens of so called "cyberpower". Cyberpower can broadly be defined as "the variety of power that circulate in cyberspace and which shape the experiences of those who act in and through cyberspace" (Betz and Stevens, 2011: 44). In this sense, it can be understood as the manifestation of power in cyberspace, rather than an altogether new or different form of power. In broad terms, one can distinguish between four different types of cyberpower; Compulsory, institutional, structural and productive cyberpower (Betz and Stevens, 2011: 45-54). Elements of these categories might overlap with one another and with other power concepts as well.

Compulsory cyberpower is about direct coercion. It is characterized by an attempt to control the behavior of other actors, be it humans, machines or networks, or trying to compel others to do one's will. Thus it is closely related to the power definition presented in the introduction chapter, regarding A's ability to make B do something B otherwise wouldn't do (Dahl, 1957, pp. 202-203). *Institutional cyberpower* is a more indirect form of power, functioning through the mediation of formal or informal institutions. This type of cyberpower can be exercised for instance through setting norms and standards in international organizations which then shape the behavior of actors. *Structural cyberpower* can be understood as the ability to maintain or reshape the structural power positions of different actors (Betz & Stevens, 2012, pp. 45-49).

Last, but not least, *productive cyberpower* may be viewed as the constitution of social subjects through discourse, mediated by and enacted in cyberspace. Subsequently, one could imagine authorities demonstrating productive cyberpower through defining who/what are considered threats to national security, for instance making hackers legitimate targets of national security policies (Betz & Stevens, 2012, pp. 45-54). This understanding of cyberpower therefore has much in common with other concepts of power in the social sciences, and for our purposes here it is particularly interesting to link this power view with the concept of soft power. Both perspectives emphasize the importance of discursive power, or the power to create representations of the social reality through shaping of preferences (Nye, 2004, p. x). Power through influence and attraction represents an important dimension of power in the cyberspace environment, as will be argued below.

2.4 Soft power

As a theoretical concept, soft power was first coined by Nye in his book *Bound to lead: the changing nature of American power* (Nye, 1990). It originated as part of an argument in the early 1990s against the then dominant view that the hegemonic position of the United States in the international system was in decline. Soft power was introduced as a sort of third dimension of power that had to be taken into account to fully comprehend US dominance, in addition to the hard power dimensions of military and economic might (Nye, 2004, p. xi). This draws on previous work he had done with Robert Keohane, particularly concerning the theory of what they called 'complex interdependence' between states (Keohane & Nye, 1977, pp. 24-29). Here, they set out to explain how the processes of modernization and globalization has led to an increase in the importance of transnational ties and 'low politics' while reducing the relative significance of military power and 'high politics'. In this sense, other sources of power become more momentous and these trends will according to Nye continue to grow following the ICT revolution (Nye, 2011, p. xvi).

In the introduction, soft power was defined in Nye's own words as "the ability to get what you want through attraction rather than coercion or payments" (Nye, 2004, p. x). According to his behavioral view, a country's soft power derives from its attractiveness among other countries. While hard power resources can also produce soft power, it is generally based on three intangible sources of such attractive power; a country's culture, political ideals or values, and policies when seen as legitimate in the eyes of others (Nye, 2004, p. 11; 2008, p. 97; 2010b, p. 218). Within an international context, soft power is typically associated with behavior such as co-optation and agenda-setting as opposed to hard power based behavior such as coercion, threats and inducement. Soft power in this sense mainly rests on a country's public diplomacy efforts and multilateral policy approaches rather than military alliances and economic sanctions (Nye, 2004, p. 31).

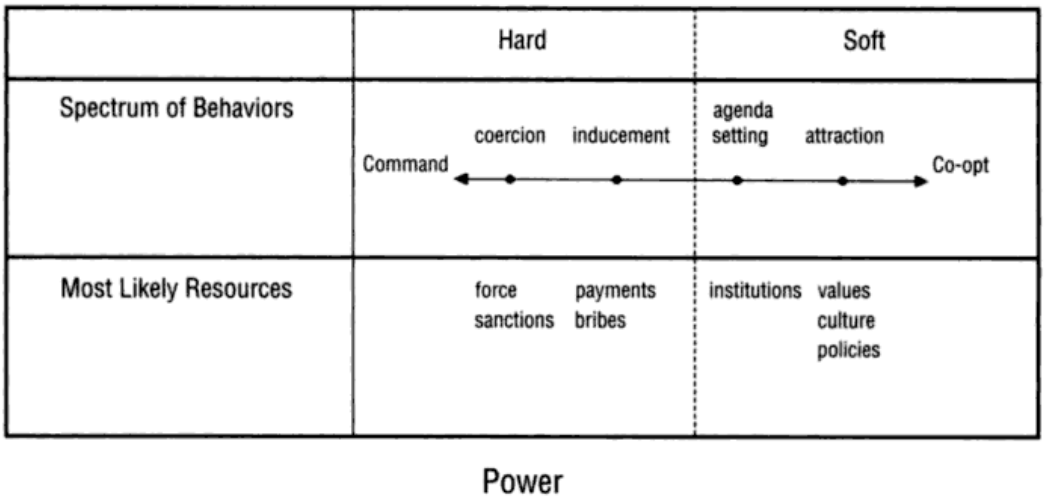

Table 1: Power resources and behaviors (Nye, 2004, p. 8).

As illustrated in the above table, power behavior can be understood as different levels on a spectrum, ranging from the extreme hard power-style of commanding to the purest soft power-behavior of co-opting. Nye emphasizes how cooperation between countries exists in varying degrees; accordingly, a central premise is the assumption that the more attractiveness and legitimacy a country enjoys vis-à-vis other countries, that is to say the more soft power resources it has in its disposition, the easier it will be for this country to reach its foreign policy goals without the use of costly hard power resources (Nye, 2004, p. 83). Importantly, other actors can have source power besides the state, and a state is not in full control over all its actual and potential soft power resources (Nye, 2011)

Despite of, or perhaps because of its increased usage in recent years, a growing number of critiques have been directed at soft power as an analytic concept. Some question the originality of the concept and refers to affinities with Gramsci's work on "hegemony" (Zahran & Ramos, 2010, pp. 12-31), whereas others emphasize the inconsistency between Nye's various definitions of the concept (Gelb, 2009, p. 69). Another critique claims that soft power conflates a relational and a structural view of power, equating the power of agency with the power of social structures, or what was presented earlier as Luke's "second and third faces of power" (Lock, 2010, pp. 34-35; Lukes, 1974, pp. 37-38).

Nye acknowledges that soft power indeed includes both agenda setting and preference setting as described in these two "faces of power", and he emphasizes that soft power can be created both by tangible and intangible resources (Nye, 2010b, p. 217). He later refined the concept

and adapted it to a model with three faces of power behavior (Nye, 2011, p. 91). Notwithstanding these criticisms, soft power constitutes a useful approach to understand power within international relations in a broader sense. Lately, soft power has been given increased attention both by statesmen and by scholars and analysts within international studies, political science and public diplomacy (Chong, 2007; Hayden, 2011; Nye, 2011; Parmar & Cox, 2010; Wang, 2011; Yi & Melissen, 2011).

Yet, it is not intuitively clear how soft power relates to international cooperation within cybersecurity. I will attempt to identify and discuss some of these links in the next section as well as in the analysis chapter dealing more thoroughly with CBMs in the context of international cybersecurity.

2.5 Soft power and cyberdiplomacy

Nye predicts as mentioned above that the role of soft power in international relations will increase following the ICT revolution or in the so called "information age" (Nye, 2004, pp. 97-98; 2011, p. 84). He further stresses how this will benefit not only states but also other actors focusing on soft power strategies. He argues that it is not so much the speed of communication which has changed in the ICT revolution, but more the low cost and the increase in capacity for communication (Nye & Welch, 2013, p. 287).

In this context Nye identifies power transition and power diffusion as some of the key characteristics or trends influencing foreign policies in our time (Nye, 2011, p. 113). He emphasizes how power in the cyber domain is more dispersed among different actors than before, producing, among other things, a narrower gap between state and non-state actors (Nye, 2010a, p. 9). Anyone with a computer, Internet access and the right know-how can according to this perspective cause significant damage in cyberspace, relatively regardless of age, social status, financial resources or geographical location. This is not to say that new ICTs remove differences between social actors in cyberspace, but according to this view, they contribute to a shifting balance of influence in favor of the less resourced:

"The low price of entry, anonymity, and asymmetries in vulnerability means that smaller actors have more capacity to exercise hard and soft power in cyberspace than in many more traditional domains of world politics" (Nye, 2010a, p. 1).

But what is the relation between soft power and CBMs regarding international cooperation within cybersecurity?

This is a broad question, and it is not my intention here to provide definite answers. However, part of an approach to one answer may lie in what is sometimes associated with the concept of "cyberdiplomacy". There is still a limited amount of academic literature specifically targeting this topic, as is the case with cybersecurity. In one of the earliest scholarly books on what was in fact labeled "cyberdiplomacy", the increased influence of non-state actors suggested above was indeed recognized as one of the central consequences of the new ICTs for diplomacy (Potter, 2002, p. 22). Yet, this understanding of cyberdiplomacy primarily relates to the evolution of public diplomacy to encompass new instruments of communication such as the Internet and web-based media.

A somewhat broader view regards cyberdiplomacy as "the general formal state engagement of a nation's diplomatic processes in the overall theme of global security", referring in particular to "multilateral or bilateral activity aimed at managing state-to-state relationships in cyberspace" (Luiijf & Healey, 2011, pp. 127-128). The former view of cyberdiplomacy in this sense rather relates to what is known as "e-diplomacy", referring to the actual use of ICTs in diplomacy, whereas this latter view regards cyberdiplomacy as more pertaining to diplomatic processes concerning cyberspace and cybersecurity.

Following this second perspective, CBMs processes regarding international cybersecurity can be viewed as one area of cyberdiplomacy. In this context, it is not difficult to imagine potential benefits of soft power when negotiating CBMs; the higher the degree of soft power enjoyed by a particular state, enabling it to exercise influence over other states, the greater the chances are for this state to succeed in securing consensus on specific CBMs of particular importance to its national interests. Power always depends upon context, and it is not a given that a certain level of soft power produces desired outcomes in concrete negotiations; rather, soft power often works in a more long term, indirect manner through creating influence over time (Nye, 2004, pp. 16-17). In this way, soft power relates to CBMs in the sense that both can often be linked to strategies aiming at the long term shaping of favorable environments or by shaping the preferences of other actors rather than directly seeking to achieve immediate results (OSCE, 2012, p. 11).

Additionally, soft power can grant access to relevant networks and secure a seat at important negotiating tables (Nye, 2004, p. 10). In one sense this relates to Castells' notion of

"switchers" as presented above, referring to actors with the power to connect different networks with each other (Castells, 2004, p. 32). In the context of cybersecurity, active participation in certain CBMs processes with specific networks of states might increase influence and provide access to other processes with different networks.

In other words, a strategic approach focusing consciously on soft power can help create an environment based on mutual trust and respect between states, thus preparing the ground for fruitful discussions and ultimately the agreement on cyber CBMs. But can CBMs act as sources of soft power in and through themselves? This is an interesting question, but one which remains outside the scope of this thesis.

2.6 Summary

In this chapter it has been argued that cybersecurity constitutes a central dimension of current security politics. While there are many aspects to cybersecurity, this thesis concerns the transnational nature of this issue and views cybersecurity not merely as a technical but as a broader political and social challenge. This multifaceted challenge requires concerted action across state borders to prevent potential conflicts. Furthermore, the focus in this context is directed at the specific form of cooperation represented by diplomacy. My interest here is diplomacy as a function, allowing for a variety of government representatives to be considered part of diplomatic processes. CBMs represent an important dimension of these processes. In the context of international cybersecurity, CBMs have received increased attention in recent years as a promising instrument for cooperation. Finally, it has been argued that power is an important element of issues related to security and diplomacy. For this reason a broader understanding of power is needed in order to more fully comprehend the power dynamics characterizing foreign- and security politics in today's globalized network society. Soft power represents one important approach to these issues.

3.0 Method

3.1 Research design

A research method can be understood as a way to approach a research question. The choice of method involves choices concerning types of sources and ultimately about what kind of knowledge is possible to produce (Ryen, 2002, p. 29).

Qualitative research generally seeks to investigate issues which are difficult to measure or quantify in exact numbers. This thesis is based on an explorative research design using in-depth interviewing within the qualitative research tradition. This approach is also inspired by principles from grounded theory, as described under the sub-chapter "procedure". The reason for choosing this research design is because the kinds of questions I am interested in are broad, open-ended questions. They seek to increase our conceptual understanding of specific topics, such as "international cybersecurity". Furthermore, only a limited amount of research has been done on this topic previously. In this sense, a qualitative approach provides an appropriate entrance to my research question:

- *How can the use of CBMs in diplomacy enhance international cooperation within cybersecurity?*

In order to find data illuminating this research question, I will examine the following set of two operationalized sub-questions:

1) What are the main consequences of the emergence of the network society for diplomacy?

This question serves the important function of drawing out a map of the current status quo for the effects of the network society on international cooperation. Drawing inter alia on Castell's hypothesis as introduced in the theory chapter that radically changing conditions for communication have profound impacts on the "entire realm of human activity" (Castells, 2004, p. 9), I want to explore further the particular consequences of the network society for diplomatic processes. After all, diplomacy is fundamentally about communication and the exchange of information, views and values (Bjola & Kornprobst, 2013, p. 77).

Secondly, upon this backdrop, I will try to answer the following question more directly related to my research question:

2) What are the possibilities and limits of CBMs in terms of enhancing international cybersecurity, and how does soft power relate to CBMs in this context?

This question investigates the problem of how to apply CBMs on international cybersecurity, but it also suggests that there is a link between CBMs in this context and soft power. This connection will be further elaborated in the analysis chapter.

Moreover, this thesis is based on an ideographic and inductive method. In broad terms, ideographic approaches often study single phenomena which are historically or culturally unique. An inductive method typically infers general laws or principles from particular instances (Ryen, 2002, pp. 29-30). However, an inductive inference doesn't necessarily follow as a logical consequence of the premises given, unlike a deductive inference. Thus inductive inferences can't produce unambiguous, verified claims accepted as universal. In this context I will not be able to derive general laws applicable for CBMs and how they may be utilized in all security contexts. Nonetheless I will attempt at exploring the realm of possibilities for CBMs to improve cybersecurity on an international level. In turn this can contribute to a broader understanding of the general utility of CBMs.

3.2 Procedure

In order to find answers to my research question I decided to conduct a number of in-depth interviews with experts within the field. Given the complex and inter-disciplinary nature of the research topic, talking to people with broad experience and detailed knowledge about the issues at hand appeared to be not only advisable but rather necessary to even begin finding answers. Intensive interviewing is particularly well-suited for the kind of in-depth exploration of social processes which I am interested in, seeking to understand reality from the interviewees' or informants' point of view (Kvale & Brinkmann, 2009a, p. 45). While there are many different labels for interview subjects in different contexts, in this thesis I will refer to these interviewees as informants.

Furthermore, this approach is partly inspired by principles from grounded theory, originally developed in the 1960s (Glaser & Strauss, 1967). Grounded theory as a research method

includes, inter alia, constantly jumping between data collection and analysis, the construction of codes and categories based on gathered data as well as theoretical sampling aimed at the construction of theory (Strauss, 1987, pp. 5-6). It is a complex process consisting of various stages which follow a cycled rather than a linear order.[6]

Acknowledging the complexity of this method and the time and scope restraints inherent in this thesis, therefore, my approach draws more on Charmaz and her flexible view of grounded theory as a set of principles and guidelines for the craft of research (Charmaz, 2006, pp. 9-10). In short, my focus has been less on memo writing and more on constructing codes and categories. I have continuously worked with the gathering and analyzing of data as I proceeded with the interviews, and I have constructed and refined the codes throughout the research process. For instance, while the category "threat" emerged in an early phase of the research process and building on codes such as risk, attribution problem and speed, I decided eventually to incorporate this as an element under the broader category of "vulnerabilities".

3.2.1 Sampling

As mentioned earlier I conducted a total of 16 in-depth interviews with experts from 8 countries within the field of international cybersecurity. This is what is called "purposive" or "criteria-based sampling", choosing informants on the basis of their role or fulfillment of a set of criteria rather than seeking a representative sample (Dalen, 2011, p. 47). What constitutes an "expert" is of course always a question of definition, but in this context I consider two particular professions as the main groups of qualified experts on this topic; on the one hand, experienced diplomats who have worked on issues related to cybersecurity and international cooperation, and on the other hand, scholars who have conducted research within this or related fields. After all, the research question for this thesis concerns how CBMs may be used in *diplomacy* to strengthen international cybersecurity. About half of my informants are diplomats from a total of five different countries, whereas the other half primarily consists of researchers. [7]

Deciding on the type of informants proved relatively easy, but determining which specific informants to interview was a different task. A first, sincere challenge with the process of

[6] See Attachment 1: *The grounded theory process*.
[7] An introduction of the informants with short summaries of their professional backgrounds is included in Attachment 2: *List of informants.*

sampling was the problem of entrée, or access to relevant informants. In large, hierarchical organizations, one of the keys to getting entrée is identifying and approaching the right gatekeepers, meaning people with the ability to grant access to relevant contacts (Morrill, Buller, Buller, & Larkey, 1999). In this context, due to my internship with the Norwegian Embassy in Vienna I was able to get in touch with a few interesting informants directly through my own professional network and knowledge of pertinent gatekeepers in various organizations. Accordingly, some of the first informants I interviewed include representatives from the United Nations Organization on Drugs and Crime (UNODC), diplomatic missions to the Organization for Security and Cooperation in Europe (OSCE) and from the Norwegian Ministry of Foreign Affairs. Additionally, my thesis supervisors were instrumental in identifying relevant informants.

Then, proceeding with what is known as "snowball-sampling", I followed up recommendations from my informants to find new potential interview candidates (Small, 2009, p. 14). Some might object to this method because there is a strong chance that several informants might know each other personally. Thus they potentially constitute a social network, which could lead to a biased sample. Indeed, some of these informants are colleagues or have at least done business together. However my aim was not to ensure a representative sample, but rather to secure a strategic sample of informants selected on the basis of their role as experts in this context. Accordingly I don't consider this to be a significant problem.

3.2.2 The interview process

In this thesis I have followed a semi-structured interview model. This means that I had a fixed set of questions used for each interview, but with the possibility for changing the order of questions and adding new follow-up questions, or simply leaving some questions untouched. This model allows for constructive comparison of data provided by different informants, while simultaneously leaving space for individual adjustments appropriate to the particular context (Dalen, 2011, p. 26). For instance, in the interviews with the diplomats I would typically follow up on questions regarding their unique experiences and ask for instance about the relationship between CBMs in the OSCE and other international cybersecurity processes.

I decided to structure the interview guide according to the main topics covered in the theory

chapter. [8] These topics include cybersecurity, diplomacy, power and soft power. In addition, I would start each interview by asking questions related to terminology, inter alia how the informants in their own words would define cybersecurity. Moreover, as the research process progressed I continuously refined both the emerging codes as well as the interview questions according to the accumulated data. For instance, while questions concerning cybercrime were included in the initial phase of the research process, these questions were exchanged with others more related to surveillance and the relationship between trust building and surveillance.

Most of the interviews were done in person at the workplace of my informants. Seven of the informants for this study are based in the same city as this author, in Oslo, making face-to-face interviews easy. I decided to go to Vienna for the OSCE Informal Working Group (IWG) meeting at the negotiations on cyber CBMs October 23-24. I was granted observer status and could thus follow the international process here. During these two days I was able to conduct interviews with four of the diplomats present. Adding the interview conducted previously with the UNODC representative, this means that 12 of 16 interviews were done in person. The remaining four were conducted through phone or Skype due to practical considerations.

Each interview lasted approximately 40 - 45 minutes, with some variation; the shortest one lasted about 30 minutes, while the longest one came close to one hour. I asked each informant for their consent to record the interview, explaining that the recorded audio clips would only be used for transcribing purposes and later be deleted. Most informants accepted, but a few preferred to have the interview done off the record. I never objected to these decisions, being cautious about staging the interview in such a way that the informants felt as comfortable as possible, thus ensuring a more relaxed, free flow of information (Kvale & Brinkmann, 2009a, p. 141). Some of them even let me decide, explaining how I would get one type of answers with the recorder and another kind without. In these cases, following my investigative research instinct, I decided to drop the recorder in order to get as interesting and as unpolished answers as possible.

3.2.3 Mode of analysis

Different methodological traditions have various schools of thought or paradigms. These

[8] See Attachment 3: *Interview guide*

paradigms reflect different ways of approaching or analyzing gathered data (Ryen, 2002, p. 61). In thesis my approach comes close to what is known as the naturalistic paradigm. Following this perspective I analyze the information provided by my informants as representing the truth or the reality from their perspectives. I do not question whether this reality is socially constructed or not, which is typically done in the ethnomethodological or in the post-modern paradigms (Ryen, 2002, p. 144). Additionally my interest is more in *what* is being said rather than *how* my informants convey this information.

The process of analyzing the empirical data gathered for this thesis developed through several stages. After conducting all 16 in-depth interviews I ended up with a total of close to 100 pages of interview transcripts and notes. Not all interviews were recorded, following the requests of each informant, but extensive note-taking both during and after each interview nonetheless provided relatively rich data. These transcripts and notes comprised over 10 hours of recordings and can be considered as the raw data gathered for this thesis.

When the interview transcriptions were complete I began reading and collecting quotes and key sentences. These quotes were organized according to the codes and categories which emerged; some quotes related to more than one code or category, in which case these quotes were duplicated while the categories were further refined. After reaching a level of "theoretical saturation", meaning that these categories had been developed and refined to a point where no new properties seemed to emerge (Charmaz, 2006, p. 91), the selected quotes were then sent for approval by the informants.

These interviews took place within a time period of 3 months. I did not know until the last interview whether or not all informants would agree to be presented by name and title in this thesis. For this reason I decided to anonymize all quotes temporarily while working on the analysis. Ultimately, only one informant requested to remain anonymous. Since this decision was made relatively late in the research process, I decided to keep the anonymous mode of quoting in the analysis chapter. To be transparent about the gathered data, however, I have presented the remaining 15 informants in Attachment 2.

3.3 Reliability and validity

Issues of reliability and validity are or great concern to scholars within both qualitative and quantitative research, but there is often a need to distinguish between the terms used in the respective traditions. Instead of the positivistic terms "reliability" and "validity", some scholars would rather use "credibility" and "transferability" (Lincoln & Guba, 1985, p. 189). Reliability in quantitative research requires that the approach used when collecting and analyzing data is possible to redo and check accurately by other scholars. This is obviously difficult to achieve in qualitative research using interviews, where the role of the researcher and the particularities of the concrete interview contexts are hard to recheck (Dalen, 2011, p. 93). In this sense, the reliability of the data gathered for this thesis is relatively low.

However, a stronger degree of reliability in qualitative interviewing can be reached using other means; for instance through recording and transcribing all interviews, and being transparent about the research procedure (Ryen, 2002, p. 180). For this thesis, most of the 16 interviews where recorded and then later transcribed, but some informants preferred to do the interview without recording. In order to increase the reliability of my data, I have aimed at describing as accurately as possible the different stages of the research process, showing what was done, in what order, and in what ways. I have also been transparent about my informants with the list of informant "mini-biographies" included in Attachment 2.

Validity in quantitative research normally refers to the question of whether or not what is measured is in fact what was intended to be measured. Within qualitative research, rather, the preferred question is whether a method really investigates what it is supposed to investigate (Kvale & Brinkmann, 2009b, p. 246). On the one hand, this has to do with what in quantitative terms is known as "internal validity", meaning to what extent proposals concerning causal connections are supported in a study in a given context (Seale, 1999, p. 38). In this thesis, my focus is not so much on causality as it is on the credibility of the data gathered. I have attempted to increase the credibility of my data by using a version of "member validation", meaning that I have had all quotes used for this thesis approved by my informants before publishing (Ryen, 2002, p. 184). This is also in accordance with the terms agreed upon before each interview.

On the other hand, this has to with "external validity", referring to the degree to which proposals on causal links are likely to be true in other contexts; in other words, it is about generalizability (Seale, 1999, p. 40). For this thesis, I have not chosen a representative selection of informants generalizable to a larger population, but rather what was called a

"purposive" sample above (Dalen, 2011, p. 47). In this sense, I am less concerned about the generalizability and more interested in the transferability of my findings, meaning the to what extent the knowledge produced here is transferable to other issues (Johannessen, Tufte, & Christoffersen, 2010). While I'm examining the specific conditions of CBMs within international cybersecurity, the findings of this thesis can contribute to an understanding of the general role of CBMs within international security and disarmament, as well as suggest ways to move processes of international cooperation in new domains forward.

3.4 Ethical considerations

A research interview should not be considered as a completely open and free dialogue between equals. It is always characterized by a certain power asymmetry between the researcher and the informant (Kvale & Brinkmann, 2009a, p. 52). Typically, the researcher is in a privileged position since he or she has scientific competence, determines the topic of the interview, formulates the questions and decides on which answers to follow up. The research interview in this sense can be viewed as a one-way, instrumental dialogue in which questions are only directed from the researcher to the informant. Furthermore, the researcher has a so-called "monopoly" of interpretation with the privilege to interpret and report what was conveyed in the interview (Kvale & Brinkmann, 2009a, p. 53).

The power asymmetry in this context was partly cancelled out as I conducted interviews with experts or elite informants. Elites are in powerful positions and are used to share their opinions on specific topics (Kvale & Brinkmann, 2009b, p. 147). In order to achieve a certain level of symmetry I made an effort to become knowledgeable about the topic and learn about the informant's professional background before each interview. Furthermore, while still having the privilege of the monopoly of interpretation, I attempted to mitigate the power asymmetry in the other direction by letting the informants approve all quotes used in this thesis. Some quotes were corrected, others removed, and some were made anonymous and only referred to in an indirect way following requests from the informants.

4.0 Analysis

International cybersecurity is as demonstrated in the theory chapter in its very nature a complex, multifaceted issue. Additionally, it is a relatively new topic of research as well as within diplomacy. It was argued earlier that cybersecurity pertains not only to issues of a technical, narrow understanding of the term, but rather pertains to political and social challenges as well (Betz, 2012). Furthermore, international cybersecurity arguably relates to issues of power, communication and trust. It might not be surprising therefore, that cooperation across national and cultural borders is difficult to accomplish at such an early stage in the process of establishing what cybersecurity is all about; in order to work together and find common ground, states first need to clarify what their interests and fears are in relation to the cyberspace environment. This thesis argues that CBMs can be a great resource in this context. It examines in what ways CBMs may be used in diplomacy to strengthen international cybersecurity. As demonstrated in the methodology chapter, it approaches this question through 16 in-depth interviews with diplomats and researchers within the field.

In this chapter I will present the main findings of these interviews. They have been divided into two main parts; following the operationalization presented in the methodology chapter, the first part examines some of the consequences of the emergence of the network society for diplomatic activities. I will attempt to link these findings with some of the issues raised in the theory chapter, inter alia challenges related to interdependence and vulnerability. This provides an overview of the essential backdrop needed to better understand current processes regarding CBMs in the cyber domain.

In the second part of the analysis, I analyze the data provided by my informants further and examine in what way CBMs may be used in diplomacy to enhance international cybersecurity. With inspiration from grounded theory I have worked in tandem with theory and the emerging empirical data throughout the research process, as described earlier. As a result, these findings demonstrate that some of the main possibilities and limits of CBMs within international cybersecurity relate to issues of transparency, terminology and image.

Additionally, in this chapter I will look at the relationship between CBMs and soft power, and I will investigate some of the ways in which the soft power concept might provide insights in

this context. In closing, I will discuss to what extent these findings contribute to our understanding of the concept cyber diplomacy.

4.1 Consequences of the network society for diplomacy

In this thesis it has been argued that the emergence of the network society and new ICTs affect the way we think about issues of power, trust and diplomacy. As demonstrated in the theory chapter, diplomacy is fundamentally about communication (Bjola & Kornprobst, 2013, p. 77). Accordingly, when the conditions for communication radically change, one could expect that diplomacy will change as well. This comes close to Castells' claim that "a revolutionary change in the material conditions of their performance [information and communication] affects the entire realm of human activity" (Castells, 2004, p. 9). Yet, it is not a given that new ICTs requires a completely new understanding of diplomacy. Whether or not one agrees to this claim, however, it is possible to accept that changes in communication patterns have other social consequences as well - revolutionizing or not.

The primary aim of this thesis is not to investigate the general consequences of the emergence of the network society for diplomacy; this could in itself be an interesting topic for a different thesis. However, by looking at how new the network society and new ICTs impact the environment in which diplomacy takes place and by asking diplomats about their own views on these issues, we might begin to get a better grasp of the context surrounding current efforts at strengthening international cybersecurity through the use of CBMs.

While some of the characteristics discussed below might be valid for diplomacy in general, it is important to note that main focus here is diplomacy in relation to cybersecurity.

4.1.1 Interdependence

One of the perhaps most obvious consequences of the network society for diplomatic activities is the increased connectivity across state borders.

When asked about specific consequences for diplomacy, there was both agreement and disagreement among the informants in terms of the nature and significance of these

consequences. Nonetheless, they all agreed that states to a larger extent than before are more interconnected and interdependent in the network society.

As stated by one informant:

- **Informant 6:** ICT is everywhere, and states are more interdependent now than before. Cybersecurity is in its very nature cross-border; for instance, citizens from vastly different countries may use services offered by the same provider regardless of geographic location.

These thoughts resonate well with the theory of "complex interdependence" presented earlier (Keohane & Nye, 1977, pp. 24-29). Never before have more people been connected to each other through local, regional and global networks, and the relations between states have never been more influenced through trans-national or non-governmental ties than at present.

A number of informants emphasized how this interdependence calls for a stronger focus on international cooperation. This is particularly the case for cross-cutting issues such as cybersecurity, which all informants indeed viewed as a global challenge, requiring global, coordinated action. One informant described it in this way:

- **Informant 4:** Cybersecurity is a global phenomenon by its very nature. All questions related to cyber and to the digital domain are. You can sit anywhere and do nearly anything in the digital domain, right? This is why we need international cooperation within cybersecurity; because of the unique threats associated with it.

As mentioned earlier, there are diverging views on what specifically these threats are. Typically, as shown in the theory chapter, one can distinguish between three main types of actors representing cyberthreats; criminals, "hacktivists" and other states (Neuneck, 2013a, pp. 115-116). In this context it is important to note the acknowledgement of the interdependence and the need for concerted, international cooperation to mitigate some of these threats.

Since communication and the exchange of information is less dependent on physical restraints than before, according to some informants, this leads to a new understanding of what is considered to be belonging under the label "critical infrastructure". In a general sense, critical infrastructure is often understood as the assets or resources vital for the functioning of society.

Since more and more assets rely on ICT systems to function, ICTs are increasingly incorporated by governments under this label (McCarthy et al., 2009, p. 544). In some cases, countries even work jointly to secure their respective critical infrastructures. When explaining some of the benefits of cooperation between the Nordic countries in relation to cybersecurity, one informant pointed out the fact that parts of this infrastructure already are crossing the intra-Nordic borders:

> **Informant 8:** Well, the [Norwegian] banks' central management of payment transactions[9]are located in Sweden, right? The computers of these banks are stored centrally. And a lot of Swedish cell-phone conversations are regulated from Fornebu[10], from Telenor, right? So an attack on Fornebu would hurt large parts of Sweden as well.

This illustrates some of the ways in which countries are more interdependent in the network society than before. International cooperation is needed to strengthen international cybersecurity, and government representatives would arguably benefit from always taking into account this level of interdependence when negotiating agreements surrounding cybersecurity issues.

4.1.2 Vulnerability

Several informants explicitly identified an increased state of vulnerability as an important consequence of the network society for diplomacy. This vulnerability obviously relates to the previously discussed level of interdependence, for instance as shown with the example of the Nordic cross-border critical infrastructure above. Higher interdependency can encourage stronger cooperation, but it might also imply increased risk of being hurt by collateral damage to sensitive, integrated systems.

The high level of vulnerability according to some informants also relate to the rapid development of technology and the difficulties for lawmakers to keep pace. As explained by one informant:

[9] In Norwegian: Bankenes Betalings Sentral (BBS), now Point Transaction Systems.
[10] Headquarters of Telenor, the Norwegian multi-national telecommunications company, located outside of Oslo.

- **Informant 1:** In the wake of recent breaches in cybersecurity, it is important to consider both how and why countries have allowed themselves to become so vulnerable. First, our laws have not kept pace with rapid technology improvements and adoption. Second, many countries have underinvested in law enforcement capacity and most law enforcement establishments are unable to manage the volume of incidents as a result. Third, it appears that prosecutorial decisions for regular crime and cybercrime have different thresholds, thus compounding the situation.

This vulnerability is arguably even stronger on an international level due to the difficulties with applying international law on cyberactivities, as demonstrated in the theory chapter (UNIDIR, 2012, pp. 13-14).

The high speed of communication is something one could intuitively imagine would have rather large consequences for diplomatic activities. Yet, as several informants pointed out; the aspect of speed is not really something new to cyberspace. Since the introduction of the telegraph, government representatives abroad have been able to communicate with their ministries at home in a more or less instant manner. But the number of communication channels, and the reach and reliability of these channels does make it harder for these representatives to hide behind tactical excuses concerning the need to wait for responses from their capitals.

As one informant put it:

- **Informant 11:** Usually, the speed or lack of speed could be part of a real world hindrance. But now, this is less and less the case. So for sure, if you see a nation doing that you know for sure they have big issues with it.

According to this view one could argue that the network society indeed impacts the rate at which decisions in diplomatic processes need to be made. In one sense this suggests that the "2-level-game" of diplomacy (Putnam, 1988, p. 427) generally is even more challenging than before the development and diffusion of new ICTs.

Another informant explained the level of vulnerability as having to do with a reduction in the cost of resources which could constitute threats:

- **Informant 4:** The cyber threat is different than conventional threats to security. One reason being that it is cheaper to invest in cyber-resources and still

produce real threats. This is why it is in the interest of most countries to cooperate on these issues.

Several informants further argued that this in a way turns traditional roles of warfare upside-down; in the cyber domain unlike in other domains, according to this perspective, attacking in broad terms is relatively cheap whereas a functioning defense proves very expensive. Nye identifies the reduction of cost related to the use of ICTs as one of the contributing factors to a degree of power diffusion in the cyberspace environment, as shown earlier (Nye, 2010a, p. 1). While states remain the most powerful actors in cyberspace, he argues that the characteristics of this domain contribute to a shifting power balance in favor of less resourceful actors. This enhanced role of non-state actors will be further discussed below.

All though there was consensus among my informants regarding the state of vulnerability in the network society, there were more diverging views on the precise extent of this vulnerability:

- **Informant 7:** There is an exaggerated picture in the media about the vulnerabilities in cyberspace and how easy it is to attack, analyze, create weapons etc. There will always be vulnerabilities, but there is a long way to go from there to saying that anyone can target anything in the cyber domain. I don't believe that smaller actors suddenly have got a new playing card in terms of attacking the bigger players. Because exercising power in the cyber domain is both difficult and intelligence-led.

Following this view the apparent reduced power of the state in the cyber domain is generally overstated. This is due inter alia to the state's superiority in organizational capacity and its ability to produce and gather intelligence. Accordingly, the uncertainty associated with a shifting balance of power in favor of the less resourceful may arguably be exaggerated. Yet, as Nye argues smaller actors will be more capable of exercising both hard and soft power in cyberspace than in other domains due the "low price of entry, anonymity and asymmetries in vulnerability" (Nye, 2010a, p. 19).

Thus, while new ICTs may produce new instruments for government representatives to communicate and cooperate more effectively these same technologies can also lead to an increased level of vulnerability. The scope and sincerity of this vulnerability can be a matter of debate, but according to the views expressed by the informants for this study this issue

needs to be taken into account when approaching diplomacy in today's network society.

4.1.3 Uncertainty

A third key element emphasized by a majority of my informants was a stronger sense of uncertainty as a consequence of the emergence of the network society. As discussed in the theory chapter, cybersecurity is still considered by both scientists and practitioners to be a relatively new field (Langø, 2013, p. 229). Furthermore, as demonstrated earlier there are currently no globally accepted treaties governing state behavior in the cyber domain. In this sense, it is perhaps to be expected that there is a certain degree of uncertainty related to this new domain for diplomacy.

As one informant put it when discussing state activities in cyberspace:

- **Informant 12:** There is a need for establishing rules of the road in this context; everyone should follow these, because it would in the interest of all.

Uncertainty regarding new domains for state cooperation on security issues is not unusual, as several informants pointed out. This was also the case for instance when the air force and new space technologies were first introduced.

However, there are also specific elements characteristic of cyberspace which creates uncertainty among both diplomats and policy makers. One such element is the problem of attribution of cyber-attacks; knowing who's behind various actions in the cyberspace environment (Kugler, 2009, p. 309). One informant stressed this point when referring to the need for diplomacy to prevent conflicts from escalating after a cyber-attack.

- **Informant 7:** But the issue of attribution makes things difficult. It indicates that what you need to do is implement an apparatus, and initiate contact with the presumed actors to say: Are you really the ones behind this? What's your intention? Still, I think very few attacks in the cyber domain will take place in a security-political vacuum.

This increased degree of invisibility or anonymity represented by the problem of attribution in cyberspace makes it difficult to verify which actors have done what actions and for what purposes. Diplomatic negotiations, as stressed by several informants, obviously can be more

challenging when there is uncertainty regarding the true identities behind various actions.

Another complicating factor is the fact that government representatives and the states they represent are no longer the sole actors on the stage of international diplomacy. Indeed, several informants recognized the fact that in today's networked, global society, diplomacy in practical terms is not limited to government-to-government activities. This is particularly the case for cybersecurity, as stated by one informant:

- **Informant 13:** Security in cyberspace is not just the responsibility or even capability of governments. They rely on support from other stakeholders. If you want to secure a safe, open cyberspace, you need the involvement of all stakeholders; those controlling the roots, the hubs and so forth. It's a shared responsibility. That's why you need a multilateral, multi-stakeholder approach. It might be useful to include users who also have a responsibility.

This important role of other actors, such as the private sector, civil society and academia for cybersecurity is increasingly the focus of attention of both researchers and policymakers. For instance, the role of non-state actors in the cyber "ecosystem" is particularly emphasized among scholars in what was introduced earlier as the ecologist school (Rattray & Healey, 2011, pp. 67-68).

4.1.4 Summary

Combined, these findings suggest that there is a considerable need for and lack of trust within the context of international cybersecurity. The described levels of interdependence, vulnerability and uncertainty are symptomatic of a cybersecurity-atmosphere in which trust in and among the state actors is highly desirable, but not sufficiently granted in the present status quo. Cooperation in is context is needed, in the eyes of my informants, but cooperation can be difficult to accomplish in an environment characterized by rapid changes, multiple actors and an increased degree of perceived vulnerability, uncertainty and risk.

This lack of trust might have been further fuelled, according to some informants, by recent revelations of the extended surveillance by American authorities on adversaries as well as on allies. Upon this backdrop, one could argue that the need for trust is strongly felt for a variety of reasons. But how can one build trust in the cyberspace environment? Some suggest by

looking to history, and to how trust has been built in the past. In this sense, CBMs appears to be a promising way to move forward and in the following I will examine how CBMs may be used in diplomacy to strengthen international cybersecurity.

4.2 Possibilities and limits of CBMs within international cybersecurity

Government representatives face a number of challenges in their approaches to cybersecurity. These challenges vary in nature and some of them relate to the interdependence, vulnerability and the uncertainty characteristic of the cyberspace environment as argued above. Similarly, efforts to strengthen international cybersecurity can assume many different shapes.

Confidence building measures (CBMs) represent according to both practitioners and scholars of diplomacy one of the most promising ways to succeed with these efforts. As summed up by one informant to this study:

- **Informant 16:** We have a potential in this new domain for military confrontation and conflict. One of the key challenges in front of states and diplomats at present is the possibility of moderating or precluding cyber conflict via CBMs as agreed among states. This is about 'preventive diplomacy', seeking to head-off a problem before it emerges.

This function to prevent conflicts and conflict escalation is at the core of CBMs, as demonstrated earlier concerning the history of CBMs (OSCE, 2012, p. 11). While these measures primarily aim at trust building they may be beneficial in other ways as well, as will be shown below.

In what follows I will present and discuss some of the most significant possibilities and limits for "cyber CBMs" according to the data gathered in the 16 in-depth interviews conducted for this thesis. In brief these findings relate to issues of transparency, terminology and image. Subsequently, I will discuss to what extent the concept of soft power can contribute to understanding CBMs processes in this context. Finally, a discussion on "cyberdiplomacy" follows.

4.2.1 Transparency

The essence of CBMs is captured in its very name as these measures are aimed at building *confidence.* All though there may exist semantic differences between the two terms, confidence and trust are used interchangeably in this thesis.

In order to understand the role and nature of CBMs within the cyber domain, I asked my informants what they associate with trust in this regard. The basis assumption behind this question was that trust can be built in more than one way, and that it may have various meanings to different people depending on the specific contexts.

In the context of international cybersecurity, according to the views expressed by my informants, trust is both difficult and necessary in order to move the process of strengthening cooperation in this regard forward. In general, CBMs are considered to be the most viable next steps to be taken to create trust. However, there were more divergent views in terms of what trust in this context really means; trust in whom, or in what, and by whom?

Some of the informants stressed the need for trust in the technical systems:

- **Informant 6:** Trust in the systems and in the service providers is fundamental in order to succeed in the long run. Trust in the systems means being confident that they have a satisfactory security level; trust in the service providers means being reassured that they take care of your personal data and make certain that these are not subjected to misuse.

Others acknowledged this need, but put stronger emphasis on the need to differentiate between trust in the systems and trust in the actors using these systems:

- **Informant 8:** Trust is about making sure not to leak information. But there's a difference between trust within technical systems and trust related to CBMs.

Similarly, another informant stressed the need for a systemic trust in combination with trust in other states:

- **Informant 10:** If you want an open, reliable Internet, you need an amount of trust in the system. Trust though confidence in the fact that states don't misuse and

undermine the system.

While these views were shared by several informants, the distinction between trust in the system providers and in the system users seemed less clear in certain cases. This is particularly true in cases where these systems are misused by states: one example often referred to was the recent revelations concerning the extensive surveillance conducted by the American intelligence agency NSA.

Several informants emphasized that trust within cybersecurity pertains to transparency and transparent behavior. In this context transparency as trust building relates to doing what one has promised to do as well as to the obligation to share information. One such example was proposed as public access to information.

As stated by one informant:

- **Informant 14:** Confidence building can be done in many different ways; one way is through so-called "crowd-sourcing", in which media uses readers or consumers to plow through information publicly available, and point out issues of interest. That makes for a more transparent society, forcing governments to be more responsible, and ultimately it can create trust.

In the theory chapter, the first group or main category of CBMs within the cyber domain presented was 'transparency measures' (Stauffacher & Kavanagh, 2013a, p. 6). The fact that transparency is being used as a label for a distinct set of CBMs in this context testifies to the importance of this characteristic. Indeed, as shown earlier in some cases the preferred term is precisely TCBMs or Transparency and Confidence Building Measures (Baseley-Walker, 2011, p. 32). Certain types of information need to remain confidential, obviously, but withholding more information than what is considered strictly necessary creates a difficult starting point for building an atmosphere of trust.

In other words, transparency is widely recognized both in the literature and among my informants as a vital part of CBMs in relation to cybersecurity. But how much transparency is enough? What type of information should be exchanged in order to build confidence among states and among the government representatives in question?

There is no simple answer to this problem, and most likely no "one-size-fits-all" solution to be found. However one plausible answer suggested by some informants was sharing

information about the things that really matter, or about aspects which illuminate significant vulnerabilities.

As put by one informant:

- **Informant 11:** You can only build confidence by showing others that you mean well; that you have no wrong intentions. No one can know that, unless you open up. Unless everyone can see important corners of your vital interests, vital to the country. If you open up yourself, you show your weak spot, then it gives great confidence; because you know that others can use those weak spots in order to hurt you, but you do it anyway. That is called confidence.

Not surprisingly agreeing on CBMs which share information on vital interests might be easier said than done. Importantly, trust needs to be *mutual*, and while one actor can put in extensive effort to open up and build trust this will only be of use if it is reciprocated. Yet according to the views expressed in these interviews it is ultimately in the common interest of all states that there exists a certain level of transparency in terms of cyber capabilities and strategies. This is because transparency is so fundamental to trust (Stauffacher & Kavanagh, 2013a, p. 6). Similarly, cooperation is difficult to carry out without trust. Nonetheless, while transparency regarding vital national interests might be a desirable long term goal, some informants stated it might be overly ambitious at this point given the early stage of current international cybersecurity processes.

One informant stressed the point that trust relates to legitimacy:

- **Informant 3:** The operative term for trust in this context is legitimacy. Not necessarily legal legitimacy, but moral or democratic legitimacy.

Trust in this view can be built not only through transparent behavior but by making sure that one's actions are seen as legitimate – legitimate either by moral or by democratic standard. In this sense CBMs and trust building can be related to soft power, as one of the most important sources of soft power is a state's foreign policies to the extent that these are "seen as legitimate in the eyes of others" (Nye, 2004, p. 12). What counts as legitimate will obviously depend upon context, but transparency in words as well as actions can arguably contribute to a certain degree of legitimacy.

Different opinions on trust don't necessarily mean conflicting perspectives, as they can

supplement each other and be mutually reinforcing. However they illustrate the point that various actors can emphasize different aspects of one and the same concept in their definitions. These definitions are rarely completely neutral, and as we will see agreeing on key concepts related to cybersecurity constitutes one of the great challenges government representatives are working on in current processes.

4.2.2 Terminology

CBMs may be used in different ways to build trust and transparency, as we have seen, in efforts to strengthen international cooperation within cybersecurity. While trust is deemed vital by all informants in this study, some expressed views that trust in and of itself is not enough. To further enhance international cybersecurity, CBMs may be used in diplomacy not just as means to trust one another more but also as ways to understand each other better and to more fully comprehend the mindsets and the intentions of others (Neuneck, 2013c, p. 126). Such understanding may prepare the ground for taking the cybersecurity processes to the next level, agreeing on international treaties; that is, going from politically binding to legally binding agreements, as is often the long term goal with CBMs (Baseley-Walker, 2011, p. 32). But how can government representatives contribute to accomplish this?

Prescribing a universal panacea seems like a dangerous move, as different processes often require unique approaches depending on the specific context and the actors within it. However, a plausible first-step suggested by several informants was trying to agree on relevant terminology.

One informant explained how neither his own country nor many other countries have a repository on cyber terms. In his view, this could be an important first step in order to move current CBMs processes regarding cybersecurity forward. Open or latent disagreement in terminology is a well-known obstacle to diplomatic negotiations according to several informants. It becomes particularly significant in new areas of cooperation where key terms are under the process of being agreed upon.

When discussing concrete measures relating to international cooperation within cybersecurity, therefore, government representatives need to speak the same language - both practically and figuratively. This relates in one sense to the view of diplomacy as the “mediation of

estrangement", as formulated by Der Derian (1987a, p. 93). Drawing on this perspective and assuming that common sense is always culturally and historically specific, agreeing on basic terminology might provide a promising way to mitigate at least some of the "estrangement" or "alienation" separating diplomats with opposing views on specific issues.

Yet, even agreeing on definitions of key terms in this context proves difficult:

- **Informant 11:** One of the biggest issues in cybersecurity is the lack of agreement on terminology. You have to talk until you agree on terminology, carefully drafted in a diplomatic way. It might take a long time to find common denominators, but it is necessary to try and find this.

To an outside observer, nuances in alternative versions of concrete definitions might seem trivial; but to the skilled diplomat, in the eyes of several informants, these different alternatives can represent vastly different perspectives on the subject matter. This is where the politics of language enters the stage, according to these views. Failure to grasp the potential social or political consequences of given definition might prove damaging for the unfortunate government representatives and their strategic goals.

In this context one such key term can be found in the concept of "information security". Interestingly, this concept challenges the term used itself to label the topic for this thesis, namely international *cyber*-security and not international *information* security. This demonstrates the importance of not taking any terms for granted in the context of research.

According to several informants the diverging preferences regarding cybersecurity and information security has to do with different views on what aspects of ICT systems should be regulated by states. One informant summed up the conflict of views in this way:

> **Informant 16:** In this context, Russia and China are talking about information security, and by that seeming to suggest that the content should be controlled. In the West, states are rather discussing cybersecurity, referring to the question of how to make the systems safe or secure. Not the content. Following this view, states should not intervene in content regulation more than necessary.

In the UN the preferred term has been "information security" ever since the Russian Federation presented a resolution on the subject in the First Committee of the General Assembly in 1998. However, regardless of the preferred label, few will contest the fact that a

noticeable level of disagreement has characterized discussions between those wanting to direct the focus at information content and those in favor of addressing only information infrastructures (UNODA, 2013b).

According to several informants this has to with a fundamental conflict of values between countries emphasizing individual freedoms and countries more concerned about state sovereignty and security. While many Western countries regard access to cyberspace as a basic human right, other states are more concerned about limiting such access when it is considered a threat to the stability or even the survival of the regime (Neuneck, 2013b, p. 113). This is arguably about culture, history, and values based on political, social or cultural systems. Some of these differences between countries simply cannot be overcome or ignored, but that doesn't necessarily mean that cooperation is impossible.

Several informants suggested that a feasible next step could be to simply agree to disagree on certain definitions, as long as it is clear to everyone where this disagreement lies.

As one informant put it:

- **Informant 9:** There is definitely a need to agree on glossary. However, the time might not be ripe for setting up a global glossary. If we can't agree on terminology in relation to cybersecurity, then an alternative would be that every country has its own glossary and make this publicly available. In this way, at least we will know precisely what is meant by various key terms.

Confidence building measures seek not only to increase transparency, but also to foster a deeper understanding of the cultural and political values behind key terminology. In this way according to several informants, they offer a promising way forward in this context. Agreed terminology can itself be a source of trust, making clear to all parties that they are in fact talking about the same things and thus removing fear of misperception. However, and more importantly, openness regarding key terminology - whether agreed to by everyone or not – provides a necessary starting point for building a constructive atmosphere where government representatives can more effectively learn about each other's stands in questions relating to cybersecurity.

Terminology in this sense is about representations of reality. The way in which countries and their government representatives view certain aspects of reality also says something about their presentation of self – that is, their image.

4.2.3 Image

When government representatives meet with their colleagues from other countries they never meet in a political or contextual vacuum. As pointed out by several informants they are always faced with whole sets of agendas or policies determined by their respective capitals. In this sense, even though they might be restricted to relatively new and unworked issues, CBMs are always political.

As one informant explained:

- **Informant 11:** We cannot see cyber CBMs isolated from other issues; they're always connected, all issues are always at stake.

This quote illustrates some of the challenges or rather limitations related to CBMs within cybersecurity: Despite the fact that there are indeed significant common interests regarding cybersecurity, there are significant limits to what can be accomplished. While it might be tempting it is simply impossible to agree on CBMs completely isolated without any further political considerations (OSCE, 2012, p. 23). Some informants even warned against what they considered to be "institutionalized naivety":

- **Informant 13:** Trust building is about talking to each other and being involved. It can be done by looking at CBMs and discussing norms, both in bilateral and multi-lateral processes. But we shouldn't be naïve; states have interests, rather than friends, (of course it is impossible for states to meet their interests alone so they do need to form alliances and coalitions) and their primary obligation is to protect their countries. With whatever means, for instance espionage.

While trust and trust building through CBMs is important to most states, this constitutes only one interest out of many. Sometimes, according to several informants, the interest in trust building and cooperation might be subordinated to other interests such as information in the form of intelligence. As stated by one informant regarding recent surveillance activities:

- **Informant 14:** There is a difference between the logic of intelligence services and a more political or diplomatic logic; in the Snowden/NSA-issue, it could seem as

though the intelligence logic has gotten the upper-hand at the expense of a diplomatic logic.

The extensive media coverage regarding the NSA-surveillance recently and subsequent negative reactions among several state leaders suggest that this intelligence-logic indeed might be pursued too excessively. Part of the reason why a narrow focus on intelligence might be contrary to a country's national interest is according to some informants that this might severely damage this country's reputation or image in the international community.

As stated by one informant:

- **Informant 12:** Image in the international system is important. Because it is the easiest way to distribute information about yourself.

In one sense this relates to the type of power called "productive cyberpower", or the constitution of social subjects through discourse, as introduced in the theory chapter (Betz & Stevens, 2012, pp. 50-53). An image is a powerful way to convey information about oneself, as described in the above quote, and CBMs can be seen as one way to help construct or reaffirm one's image. Moreover, this relates to the concept of soft power, as a country's image is an important soft power resource; such an image can produce influence among other states to the extent that the country's culture is seen as attractive and its policies are seen as legitimate in the eyes of others (Nye, 2011, p. 84). Some of the informants view CBMs and soft power as strongly interlinked, and I will deal more with the relationship between CBMs and soft power below.

As shown; despite new possibilities for finding common ground and for cooperation within this new domain, government representatives are still bound by the political and historical practices and values of their countries. Image is thus vital to trust and cooperation, both within and outside of the cyberspace environment, and CBMs can be an important part of constructing one's image.

4.2.4 Summary

Confidence building measures may be viewed as some the most promising means to increase shared understanding concerning cybersecurity-related issues and to strengthen international cooperation in this regard. Fundamentally, as has been argued, CBMs are a form of

communication. It has been argued how CBMs specifically can target transparency, promote the exchange of information on vital interests, reduce uncertainty as well as seek to clear some of the fog surrounding key terms used in the cybersecurity context. These functions of CBMs all contribute to building bridges between actors, or to increase confidence among them and thus reduce the risk of misperception and the possible escalation of conflicts. Additionally, as demonstrated, image is an important aspect of any diplomatic consultation and should therefore always be taken into consideration.

However, while these factors illustrate some of the possible ways in which CBMs may be used in diplomacy to strengthen international cybersecurity, they also demonstrate some of limits in terms of what can be achieved by such measures. As shown, transparency and agreement regarding definitions of key terms are highly desirable but not necessarily easily accomplished by using CBMs. Some countries have fundamentally different political or cultural values, and while CBMs might build bridges between these values they most likely won't change them. Additionally, several informants pointed out that sometimes agreed CBMs can be so "watered out" in efforts to reach consensus that they're almost meaningless. There has to be a genuine political will behind CBMs in order for them to bring about desired results (OSCE, 2012, p. 23).

Furthermore, as stressed by almost all informants, CBMs are primarily state-specific. Yet states can only do so much:

- **Informant 9:** CBMs in the cyber domain are between states only. In the realm of cybersecurity, the focus of only state actors might be problematic. The inclusion of other, in particular non-state actors, is strongly recommendable.

This need to involve the private sector and non-governmental actors in cybersecurity processes was emphasized repeatedly in the interviews. More research is needed to investigate in what ways the private sector and non-state actors might contribute to strengthen international cybersecurity, but this issue remains outside the scope of this thesis.

While CBMs can be a helpful instrument for government representatives to build trust, promote dialogue and increase understanding, it comes down to the actors using this instrument to decide what can be achieved and not. Yet, the findings in this thesis suggest that the mere attempt at agreeing on CBMs is in itself worthwhile. As stated by one informant:

- **Informant 5:** You can certainly achieve a lot with CBMs. Sometimes it is the process itself which is important, not just the outcome. Such processes build trust through creating frameworks for cooperation, and thereby produce common goals.

In other words, and as expressed by several informants: the process of trying to agree on cyber CBMs can itself be viewed as an outcome.

4.3 Cyber CBMs in light of soft power

According to the views expressed by the informants to this thesis there are a number of great strengths as well as important limits to CBMs within international cybersecurity, as demonstrated above. In this regard several informants were optimistic about the possibility of drawing on previous experiences with other kinds of CBMs.

As stated by one informant:

- **Informant 16:** CBMs within cyberspace should be able to benefit from past experiences with CBMs in other domains, and from conventional disarmament work. States and diplomats have been able to reach agreement before despite fundamentally different world views and differences regarding political and cultural values: for instance during the Cold War.

While the cyber domain represents significant new developments and new challenges for cooperation, as shown in this analysis, some of the core obstacles to agreement relate to fundamentally different values. CBMs will most likely not be able to affect such values (Neukirch, 2012, p. 4). Yet precisely because some challenges relate to old and well-known conflicts of values, lessons arguably could be learned from history.

Strategies emphasizing soft power represent one way to approach differences in values in relation to foreign policies and diplomacy. As noted earlier soft power concerns the ability to shape others' preferences and there are typically three main sources of soft power a state has at its disposal: culture, political ideals, and policies (Nye, 2004, p. 11).

Several informants view soft power and CBMs as strongly interlinked:

- **Informant 5:** I see CBMs and soft power as connected; CBMs in a way can be understood as influence. The broader the processes are, the more indirect communication becomes important.

This view reflects an understanding of CBMs and soft power as sharing a fundamental common feature; the ability to produce or function in itself as influence. Following this perspective, one can imagine CBMs regarding cybersecurity serving as a kind of soft power resource to states to the extent that they produce influence among other states involved. A state's foreign policies constitute an important soft power resource when these are seen as legitimate by others (Nye, 2011, p. 84). In this regard CBMs, or at the very least efforts to agreeing upon and signing CBMs in the cyber domain might very well be interpreted as attractive and legitimate policies. Through these efforts, according to some informants, one can show signs of good-will vis-à-vis other states and demonstrate a strong will to ensure peace and predictability.

Another informant emphasized the role of soft power more specifically within cybersecurity:

- **Informant 6:** Soft power will likely be important in the cybersecurity field. Because it is related to trust, and to diplomacy. It is less provocative than other means. And it's about finding common ground.

Soft power in this view can prove particularly useful to enhance cybersecurity in the sense that it is associated with cooperative behavior and multilateral diplomacy rather than coercion and unilateralism (Nye, 2004, p. 8). Cybersecurity is in its nature cross-border, as demonstrated earlier, and there is general agreement about the need for international cooperation and multilateral approaches in this regard (ENISA, 2012, p. 9). Furthermore, soft power may help in the process of identifying common ground through influencing preferences. Similarly this is often emphasized as one of the most significant benefits of CBMs; through trust building and improved understanding of the perspectives of others CBMs can contribute to finding common ground even on highly contentious issues (Baseley-Walker, 2011, p. 34).

One informant provided a somewhat concrete example of one way soft power can be produced and in turn contribute to enhanced cybersecurity:

- **Informant 13:** Soft power in this context could be created for instance if we had a movement of major think tanks from all regions, or if we had some regional confer-

> ences, and they would establish certain norms and principles. Then states could gradually adopt these principles, and that's a classic example of soft power-development and how it can create hard power in the form of legally binding agreements.

This quote highlights on the one hand how soft power resources can sometimes create hard power (Nye, 2004, p. 25); similarly, as demonstrated earlier, CBMs are often politically binding at first and then develop over time to become legally binding (Neuneck, 2013c, p. 121). On the other hand, this example illustrates the way that soft power typically can be wielded in a long term perspective through shaping preferences over time (Nye, 2011, p. 83). In a similar vein, it was argued in the theory chapter that CBMs typically function incrementally, building confidence step-by-step and in the context of cybersecurity acting as a "foundational element in creating stability and security in cyberspace" (Lewis, 2011, p. 59).

In this sense as pointed out by several informants, both CBMs and soft power can act as part of long term strategies aimed at shaping environments for cooperation. Furthermore they can be mutually reinforcing.

Yet CBMs do not necessarily always act as a source of soft power. In some cases, paradoxically, particular CBMs can even contribute to a reduction of both soft power and trust. As described in the theory chapter, states can agree to CBMs both on a bilateral and on a multilateral level (OSCE, 2012, p. 11). Given the wide-spread recognition of the utility of CBMs among practitioners as well as researchers, it could be easy to assume that the more CBMs, the better.

One of the informants suggests, however, that CBMs on the bilateral level can prove damaging for efforts to agree on multilateral level CBMs.

- **Informant 3:** The enemy of multilateral CBMs and discussions are bilateral CBMs: because they delegitimize one another.

According to this perspective, bilateral CBMs might be perceived as threats to multilateral CBMs because the agreement of one reduces the need for or delegitimizes the other. For instance, if a state chooses to sign a number of bilateral CBMs this could signal to other states that these CBMs are more valued than other measures. Multilateral CBMs in this case would be interpreted to be taken less seriously than their bilateral counterparts. In this view while bilateral CBMs might be beneficial to the states involved and their soft power vis-à-vis each

other, the very same measures could potentially reduce their influence among others. Yet, given the general difficulties associated with agreement on cyber CBMs as described earlier, according to some informants one can understand some of the rationale behind such bilateral CBMs; after all, a few bilateral agreements are arguably better than nothing.

4.4 Cyberdiplomacy

One of the aims with this thesis as formulated in the introduction chapter is to contribute to an understanding of what diplomacy means in today's global, interconnected network society. It does not purport to find a definite, indisputable definition of "cyberdiplomacy" but rather seeks to investigate part of the conceptual terrain surrounding this term and contribute to a broader understanding of it. CBMs and international cyber security was chosen as way of entry into this subject matter.

There is generally little consensus on many "cyber"-terms among scholars and practitioners, as demonstrated earlier (ENISA, 2012, p. 9; Joyner, 2012, p. 163; Kuehl, 2009, p. 26). This is no less true in the case of cyberdiplomacy. In the opinions stated by the informants to this thesis, accordingly, views ranged from somewhat direct dismissals of the term to rather precise, carefully considered definitions.

One informant recognized a general increase in the use of the term among researchers as well as government representatives, but called for more empirical data to support the concept:

- **Informant 14:** In my opinion there has so far been a lot of talk, both academic and to a certain extent also diplomatic enthusiasm about cyberdiplomacy, that this is all very new and exciting. And then people talk a lot about how to theorize about it and think about it.. And then there have been a few studies published now, suggesting that there is currently a lot of talk and little action.. I mean, you don't have cyberdiplomacy just because your embassy puts up a Facebook-page, right?

Admittedly, as argued earlier and following the views of several informants, there has been some debate but thus far limited research done on what cyberdiplomacy theoretically or practically entails. What is referred to in the above quote reflects some of the earliest theorizing which was done on this term, understanding cyberdiplomacy primarily as

diplomacy making use of new ICTs (Potter, 2002, p. 22). However, according to a more recent perspective this is not so much cyberdiplomacy but rather something which in the theory chapter was distinguished from this as "e-diplomacy": meaning the conduct of diplomacy through cyber means or "new media" (Luiijf & Healey, 2011, p. 128). In this sense, public diplomacy strategies which include the use of social media such as Facebook or Twitter to reach out to foreign publics might be considered e-diplomacy; cyberdiplomacy, on the other hand, refers to diplomacy in a broader sense pertaining to "multilateral or bilateral activity aimed at managing state-to-state relationships in cyberspace" (Luiijf & Healey, 2011, p. 127).

Another informant was rather skeptical to the general idea of cyberdiplomacy as a distinct and substantial concept:

- **Informant 11:** In my opinion, there is no such thing as cyberdiplomacy. There is diplomacy used in many different areas. The cyber realm or space is merely another dimension where diplomacy is used, albeit making use of some more specific cyber-terminology. So, cyber and diplomacy are certainly distinct, but there is no specific "cyberdiplomacy".

Indeed, several informants were relatively unfamiliar with the term. The lack of research specifically targeting cyberdiplomacy suggests that this term has yet to be established as a viable academic concept. This impression is reinforced by the partly confusion and sometimes strong skepticism expressed by practitioners surrounding its form and substance.

However, as demonstrated in the theory chapter there is an admittedly limited, but growing literature concerning other "cyber"-issues such as cybersecurity and cyberpower (Betz & Stevens, 2012, pp. 42-44; Langø, 2013, pp. 230-238). This could conceivably lead to an increased interest in related issues and thus strengthen the focus also on the cyberdiplomacy-dimension. The growing number of international cyber security processes worldwide (Weekes & Tikk-Ringas, 2013) additionally indicate that this topic might receive increased future attention.

Moreover a number of informants to this study welcomed cyberdiplomacy as signifying an important area of international cooperation in our time. They provided several different perspectives on the nature and definition of this term.

One informant described the difference between diplomacy generally and cyberdiplomacy in this way:

- **Informant 10:** Diplomacy can be seen as the constructive interaction among states. It is a way to articulate national interest. Diplomacy is fundamentally about communication. Cyberdiplomacy can be defined as diplomacy on cyber issues.

This view largely reflects the broad perspective on cyberdiplomacy presented above as activities aimed at "managing state-to-state relationships in cyberspace" (Luiijf & Healey, 2011, p. 127). Both of these views are relatively broad as "cyber issues" and "state-to-state relationships in cyberspace" obviously can refer to a variety of different challenges.

Another informant provided a somewhat more pointed definition:

- **Informant 3:** Cyberdiplomacy is more or less the same as international cyber security. It is a very specific field.

Unlike the previous definition this perspective emphasizes the security aspect of cyberdiplomacy. In this sense CBMs processes regarding international cybersecurity can be viewed as one area of cyberdiplomacy.

Finally, one informant distinguished cyberdiplomacy and international cybersecurity as two different levels of diplomacy:

- **Informant 16:** Diplomacy fundamentally concerns relations between states, and the conduct of those or the influencing of policies of other states. I would see cyberdiplomacy as relating to the relations between states, having to do with the use of cyberspace. International cybersecurity I would say is a subset of cyberdiplomacy, dealing specifically with security. But of course, there is a certain degree of ambiguity in these terms.

All of these definitions combined as well as additional views expressed in the gathered data suggest that cyberdiplomacy is still a concept "in the making". While a few insisted on a general rejection of the term, the majority of informants agreed to the claim that cyberdiplomacy can be seen as relating to international cybersecurity. Some informants further stressed that even if a preliminary level of agreement on the term is reached, this understanding might be obsolete or at least significantly modified in the near future due to the rapid development of new ICTs and their impacts on international security issues.

5.0 Discussion

The central topic in this thesis was identified in the introduction chapter as CBMs and international cybersecurity. The main research question it investigates is:

How can the use of CBMs in diplomacy enhance international cooperation within cybersecurity?

Additionally, in order to operationalize this question and help to understand the conditions surrounding these international cybersecurity processes, the thesis examines the following two sub-questions:

1) What are the main consequences of the emergence of the network society for diplomacy?

2) What are the possibilities and limits of CBMs in terms of enhancing international cybersecurity, and how does soft power relate to CBMs in this context?

Moreover, as an added value it is argued that these findings can contribute to the larger project of understanding what cyberdiplomacy means in today's global network society.

In the course of the in-depth interviews with the selected informants a number of views were expressed on a variety of issues, reflecting the complexity of the topic chosen for this thesis. Not surprisingly these views were partly overlapping in important areas whereas they were more diverging in others. One view all informants shared was the assumption that cybersecurity indeed plays a vital role in modern approaches to national as well as international security. As summed up by one informant:

> **Informant 8:** Cybersecurity is fundamentally what security politics is about or should be about today.

Definitions of cybersecurity vary significantly, as demonstrated in the theory chapter. This is

also the case for perspectives provided in the interviews for this thesis. Yet all informants recognized the need for international cooperation in this regard. In general, all though this is a complex picture, this relates to an increased lack of trust and a growing sense of risk in the globalized network society.

5.1 Consequences of the network society

In order to understand the backdrop for international cooperation and CBMs processes related to cybersecurity I decided to examine some of the main consequences of the emergence of the network society for diplomacy.

Despite differences in opinion regarding the number and nature of these consequences, all informants shared a common view of an increased level of interdependence between states in today's globalized world. This view resonates well both with Castells' notion of the interconnected nature of the network society (2004, p. 3) as well as with Keohane and Nye's concept "complex interdependence" (1977, pp. 24-29). Among other factors, this interdependence is characterized by a growing number of trans-national ties, increased communication and mobility across state borders. Additionally, several informants emphasized how cross-border critical infrastructure dependent on shared ICT systems contribute to this sense of interdependence between states. As demonstrated earlier, ICTs are increasingly incorporated under the label critical infrastructure (McCarthy et al., 2009, p. 544).

Another view shared by the informants to this thesis is a stronger sense of vulnerability as a consequence of the network society. This can be linked to the vital role of ICT systems as part of the critical infrastructure and the danger of collateral damage on cross-border, integrated systems. According to several informants, this pertains to the continuous and rapid development and use of new ICTs and the difficulties associated with keeping relevant laws up-to-date. This is particularly true in the context of international law, as shown in the theory chapter (UNIDIR, 2012, pp. 13-14). There are signs of emerging agreement internationally; the latest UN Group of Governmental Experts (GGE) dealing with these issues reached consensus this year regarding the applicability of existing international law to cyberspace.

However, more future processes will be needed to determine in what ways these laws can be applied (Stauffacher & Kavanagh, 2013b, p. 5).

The increased sense of vulnerability is also interlinked with a stronger degree of uncertainty in the eyes of several informants. The emergence of the network society is still relatively recent in a broader historical perspective (Castells, 2009, p. 28). It has further been demonstrated that cybersecurity is considered even today to be a relatively new field among researchers (Langø, 2013, p. 229). This is true also among practitioners of international cybersecurity, and in this sense it is not surprising that several informants emphasized the general level of uncertainty associated with this new domain for diplomacy.

Additionally, this uncertainty relates to the absence of established and agreed upon rules of behavior for states' activities in cyberspace, as pointed out by some informants. Progress is being made, for instance through the GGE consensus report mentioned above, as well as in a number of different processes both on the local, regional and global level (Weekes & Tikk-Ringas, 2013). Recently, in the OSCE Ministerial Council Summit in Kiev on December 6, consensus was reached among its 57 member states for the first time on a set of CBMs regarding cybersecurity (OSCE, 2013). Despite these trends agreement is difficult to achieve, and there is currently no globally ratified legal instrument specifically regulating state behavior in or through cyberspace.

A number of informants stressed the fact that certain unique characteristics of the cyberspace environment contribute to this sense of uncertainty. One element is the so called "problem of attribution", referring to the "difficulty of identifying actual or potential hackers" (Kugler, 2009, p. 309). In a military sense this makes "cyber deterrence" more difficult, and in a broader social perspective this sense of anonymity makes it challenging to verify who's doing what in cyberspace. Constructive diplomatic dialogue becomes challenging to achieve when it's not clear to all which actors are in fact involved and not, as pointed out by some informants.

Another factor which increases uncertainty is according to the informants the large number of actors involved in modern diplomatic processes. This involvement of non-state actors is reflected in theories on public diplomacy, which increasingly emphasize how individuals and groups participate in shaping international policies (Melissen, 2005, p. 32). Some informants stressed how international cybersecurity is neither the sole responsibility nor capability of states, but instead requires coordinated action and support from all stakeholders or actors

involved.

As stated by one informant:

- **Informant 13:** Trust is a much more fragile construction in the context of international cybersecurity. The whole edifice is depending on so many more people, stakeholders, factors, that you will not be able to have a perfect, watertight system. You could have potential spoilers in the edifice.

Similarly, in an academic context of cybersecurity, scholars of the ecologist school particularly emphasize the role of non-state actors in their understanding of cyberspace as an "ecosystem of competing and collaborating actors" (Rattray & Healey, 2011, p. 68). Furthermore, as demonstrated earlier, Nye argues that the low cost of ICTs and the increased access to information among non-state actors contribute a degree of power diffusion change in power asymmetry. As a consequence, while states are still by far the most powerful players on the world stage they will "find the stage far more crowded and difficult to control" (Nye, 2010a, p. 10).

Finally, it has been argued that these elements of interdependence, vulnerability and uncertainty contribute to an increased sense of risk and fear of misunderstanding in the context of international cybersecurity. Interdependence conceivably can increase trust when collaboration succeeds, and transparency through sharing of values and vulnerabilities is achieved. Yet, according to some informants, interdependence can contribute to reduced trust in areas where cooperation proves difficult.

One the one hand, this perceived risk relates to the relatively new emergence of the cyber domain in general; as pointed out by some informants this was also the case when other domains of potential military confrontation were first introduced such as the air force or outer space. Cybersecurity is still widely considered to be a somewhat new topic of international cooperation and this is underlined by the lack of internationally agreed upon norms and rules of behavior. On the other hand, this increased sense of risk relates to the distinct features of the cyber domain. In particular, according to the views expressed by the informants the degree of anonymity, the speed of communication and the enhanced influence of non-state actors in relation to states in the cyberspace environment contribute to a sense of reduced control. This in turn leads to increased fears and perceived risk of misunderstandings which could result in conflict.

Many informants identified a simultaneous lack of, and need for trust in order to strengthen international cybersecurity. There are obviously many ways to accomplish this; trust building through CBMs represents according to these views one particularly promising alternative. Transparency, cooperation, communication and stability are some of the core elements of such "cyber CBMs" (Stauffacher & Kavanagh, 2013a, pp. 6-12).

5.2 CBMs within international cybersecurity

Confidence building measures are widely recognized among both policymakers and researchers as a useful general way to enhance international security. As demonstrated in the theory chapter CBMs have been successfully used in the past in various contexts to create trust among states and reduce the risk of misperceptions and subsequent escalation of conflicts (OSCE, 2012, pp. 11-14). CBMs have expanded in scope and numbers since then: from the original measures aimed at preventing nuclear war to more current cyber CBMs processes seeking to create trust and predictability in the cyberspace environment. Yet their ultimate goals remain the same, namely to avoid conflict and secure peace and predictability among states (Neukirch, 2012, pp. 121-122).

The views expressed by the informants interviewed for this thesis document that trust is both a scarce resource and necessary element for efforts to strengthen the particular area of international cybersecurity. In this sense, CBMs as an instrument of trust building is acknowledged as one of the most promising ways to build bridges between state actors and move current cybersecurity processes forward.

As shown in the analysis chapter there were more differences in opinion as to what trust in this context entails and how specifically it can be created, however. Some informants emphasized how trust within cybersecurity regards confidence in the functionality and security of the technical systems and in the service providers. In one sense this relates to the overwhelmingly technical definitions of cybersecurity introduced in theory chapter which focused on the protection of "information infrastructure" and "computer networks" (EU, 2013, p. 3; ITU, 2008, p. 7). This view includes the protection of personal and sensitive data and the ability to prevent leakage or misuse of information.

While these elements certainly are vital in any issue concerning cybersecurity, CBMs relate

more to trust in the government users of these systems. In this context, it has been argued that cybersecurity can be seen as not just a technical but also a political and a social challenge (Betz, 2012). In some cases however, the distinction between trust in the system users and system providers can be more blurred when governments to a certain degree are in control of or cooperate with these system providers. One example provided by several informants regarding this issue was the previously mentioned Snowden/NSA affair.

Many informants stressed the role of transparency as one of the most significant building blocks for confidence building in this context. As summed up by one informant:

- **Informant 6:** Transparency is an important part of building trust, and about doing what one says one will do. It's also about the obligation to share; and both parties need to share to build trust.

This quote illustrates an important point made by several informants: that the sharing of information has to go both ways, or in other words that trust needs to be *mutual*. The centrality of transparency is also emphasized through the distinct category of general CBMs known as Transparency and Confidence Building Measures or TCBMs (Baseley-Walker, 2011, p. 32). Additionally, in the theory chapter the first group of "cyber CBMs" presented was labeled "transparency measures" (Stauffacher & Kavanagh, 2013a, pp. 6-8). CBMs can vary significantly both in size and nature and they can have various short and long term goals. Yet they always fundamentally involve a certain focus on transparency.

Transparency however is not an absolute but rather a relative term; as stressed by some informants transparency can exist in varying degrees and relate to various issues. How much transparency is sufficient to strengthen international cooperation within cybersecurity? There is no definite answer to this question, but some informants suggested that sharing information on vital interests or "weak spots" might be one promising approach. Transparency regarding such weak spots obviously means being more vulnerable to attacks, but in this sense it would imply a form of shared vulnerabilities reflecting a degree of interdependence. According to these views this is ultimately what will create mutual confidence as the possibility of doing harm is present but remains untouched by all actors involved.

On the other hand time might not be ripe for transparency at this level yet as there is still diverging views on key terms in this context. Accordingly some informants suggested that states in a sense could agree to disagree on certain terms, but make repositories of key terms

publicly available so that all actors are fully aware of where the main disagreements lie. As demonstrated in the theory chapter, cybersecurity for instance can be defined in many different ways; definitions vary not only between governments (ENISA, 2012, p. 9; Joyner, 2012, p. 163) but also in the academic literature on cybersecurity (Langø, 2013, pp. 229-238). Differences in perspectives on this term were also significant among the informants.

Indeed, agreement on terminology or rather a lack thereof represents one of the most pressing challenges for current international cybersecurity processes according to several informants. Agreeing on key terminology is viewed as significant not just for the practical purposes of ensuring constructive dialogue, all though this is obviously very important; furthermore, discussions on terminology might help the actors involved understand one another better and more fully comprehend the political, social or cultural values attached to specific definitions. Understanding the position and perspectives of adversaries is ultimately one of the most important functions of CBMs (Neuneck, 2013c, p. 126). Such understanding might prevent misunderstanding for instance concerning capabilities and national doctrines, which in turn could lead to misled decisions and armed conflict.

From a slightly different perspective, consultations on terminology can arguably – in the words of Der Derian – help the negotiating actors "mediate estrangement" (1987a, p. 93) or define some of their interdependencies and agree on common goals. Thus even if agreement on key definitions appear difficult at the current stage of diplomatic processes concerning cybersecurity, such consultations might still prove valuable as emphasized by several informants.

Another way CBMs may be used in diplomacy in efforts to strengthen international cybersecurity – albeit in a more indirect manner – is according to some informants to consciously integrate these efforts with coherent strategies concerning the state's general image in the international system. As stressed by several informants, CBMs are always political in the sense that they are always connected to other issues and cannot be considered in isolation.

This conceivably has several implications: firstly, despite the fact that the cyber domain represents a new area for cooperation and creates the potential for states to find common ground, the diplomatic processes are still bound by the practices and values of the respective states. While a shared threat to states posed by transnational actors and a commonly perceived risk of cyberconflict exist, as demonstrated earlier, "translating a shared fear into concrete

action has proven difficult" (Lewis, 2011, p. 52).

Secondly, as stressed by several informants CBMs can be viewed as an instrument to help shape or reaffirm a state's image in the international system. Following this perspective, a state might reaffirm or even improve its image as a trustworthy and predictable collaborative partner by actively immersing itself in CBMs processes which generally are beneficial to all actors involved. Obviously, states have diverging political and cultural values and CBMs will unlikely be able to affect such values or core interests (Neukirch, 2012, p. 4). However states can contribute to build trust and predictability by pursuing policies consistent with their values and by participating constructively in CBMs processes in accordance with these. In this way states can appear as reliable actors with a coherent, stable image and thus contribute to an atmosphere of trust despite the differences between them.

In this context, several informants identified important links between CBMs and soft power. In the theory chapter soft power was defined behaviorally as power through attraction and influence (Nye, 2004, p. x). A country's image can thus be an important soft power resource to the extent that it can attract and influence the preferences of other states. A state's foreign policies is considered particularly useful as means to improve this image and increase influence when these policies are seen as legitimate by others (Nye, 2004, p. 15).

Several informants suggested that CBMs can be understood as a type of influence in themselves. Efforts to promote CBMs can be interpreted as showing signs of good-will and expressing peaceful intentions by the states promoting them. Furthermore, some informants emphasized how both soft power and CBMs primarily function in an indirect, long term manner; indeed, soft power strategies as well as CBMs typically work through shaping the environment or the preferences in question rather than produce directs solutions or immediate outcomes (Lewis, 2011, p. 9; Nye, 2011, p. 83). In the context of international cybersecurity therefore, several informants expressed the view that soft power can prove particularly useful in reaching agreement on "cyber CBMs". Conversely, according to this view CBMs can also produce soft power by contributing to build bridges between actors and promote transparency and cooperation.

However, as emphasized by some informants: CBMs do not necessarily always produce soft power. Sometimes bilateral CBMs might be damaging to multilateral CBMs to the extent that they serve to delegitimize one another. A narrow focus on bilateral CBMs might be beneficial for the two actors involved but at the same time it could hurt their soft power and trust vis-à-

vis other states by potentially reducing the need for multilateral CBMs. Power always depends upon context (Nye, 2011, p. xiv), and efforts at agreeing on CBMs within cybersecurity can arguably benefit from careful considerations of the role of soft power in these processes.

Finally a number of informants provided distinct perspectives on how cyberdiplomacy can be understood in today's globalized network society. Some informants expressed a degree of confusion concerning cyberdiplomacy, reflecting the lack of research on this topic and the variety of definitions of the term. For instance, some informants confused cyberdiplomacy with diplomacy using ICTs, described earlier as e-diplomacy (Luiijf & Healey, 2011, p. 128). Others rejected cyberdiplomacy as a substantial and meaningful concept. Yet the majority of informants shared a broad understanding of cyberdiplomacy as related to international cybersecurity. CBMs processes within international cybersecurity can thus be viewed as one example of modern cyberdiplomacy according to this perspective. More research is needed, however, to determine in more detail the scope and nature of activities which can be included under this label.

6.0 Summary

A central aim with this thesis has been to shed some light on the issue of international cybersecurity. It has attempted to do this by investigating the question: - How can the use of CBMs in diplomacy enhance international cooperation within cybersecurity?

In the quest to find data which could contribute to a conceptual understanding of this topic I interviewed 16 experts from 8 different countries within the fields of diplomacy and/or cybersecurity. Approximately 50 % of these informants are experienced diplomats whereas the other half primarily consists of researchers: some of them are both.

Throughout this study it has been argued that international cybersecurity is a complex, multifaceted field. Firstly, various perspectives emphasize different aspects of the term, as there is currently no universally agreed definition of cybersecurity. Agreement on terminology or rather a lack thereof represents one of the most pressing challenges for current international cybersecurity processes according to several informants. However, as demonstrated cybersecurity or various labels equivalent to it is increasingly recognized internationally as this is one of the central security issues of our time.

Secondly, it is argued that international cybersecurity relates to diplomacy connected to international cooperation in the field of foreign- and security politics. The complex security challenges represented by the cyber domain and its inherent cross-border nature require coordinated action and cooperation among states. No one state can single-handedly thwart off all major threats to its national security in today's global network society.

Thirdly, according to the argument of this thesis one of the central areas of diplomatic activities in relation to cybersecurity is processes of CBMs. In the absence of established norms and rules of behavior regarding cyberspace, states are increasingly worried that potential misunderstandings and misled decision-makings could lead to conflict or conflict escalation. In this context CBMs are acknowledged by numerous government representatives as a fruitful way to approach these issues. Agreeing on cyber CBMs proves to be a difficult, but possible task.

In the analysis chapter of this thesis I have attempted to illustrate some of the main consequences of the network society for diplomatic processes related to cybersecurity. In

short, based on the empirical data gathered for this study as well as related literature we have seen how the general diffusion of ICT systems in today's networked society produce, or at least reinforce a sense of interdependence, vulnerability and uncertainty within diplomacy. This is not an exclusive list of relevant consequences, but it illustrates some of the main characteristics of the environment in which diplomacy takes place today. Furthermore, it was argued that these elements combined contribute to an increased degree of perceived risk among states in the cyberspace environment. The somewhat paradoxical trend of an increasing lack of trust and a simultaneously growing need for trust in this context suggests one of the possible motivations behind the increased attention given to CBMs.

Following the views expressed by the informants to this thesis there are a number of important possibilities as well as limitations of CBMs within international cybersecurity. It has been argued that CBMs specifically can promote transparency, reduce uncertainty, and contribute to shared understandings surrounding key terms used in the cybersecurity context. These functions of CBMs all contribute to building bridges between actors, increasing confidence among them and thus reduce the risk of misperception and the possible escalation of conflicts.

On the other hand agreement can prove difficult between actors with different political and cultural values. Agreeing on terminology represents one of the most significant challenges for current processes within international cybersecurity. There is also a danger that agreed upon CBMs might be watered-down in efforts to reach consensus. Furthermore, CBMs between states will likely not suffice to create a stable and peaceful cyberspace environment without acknowledging the role of non-state actors.

Additionally, as demonstrated earlier "cyber CBMs" in the light of soft power can be viewed as a type of influence. Both CBMs and soft power typically function in an indirect, long term manner through shaping the environment or the preferences of others in a favorable way. They can be mutually reinforcing, as soft power may increase chances of agreeing on CBMs while CBMs processes can enhance the soft power of the actors involved. Similarly, it has been argued, both CBMs and soft power – like diplomacy – is fundamentally about communication.

Thus, as has been argued, the inherent value of CBMs processes can be more important than the instrumental value or sought outcomes; these processes can in themselves help build confidence and serve as CBMs even if final agreement isn't reached. CBMs aim at finding

compromises and common ground despite cultural, political and social differences. This thesis suggests that CBMs within international cybersecurity fundamentally relates to mutual transparency in values and vulnerabilities, interconnectivity and interdependence, as well as communication as trust building.

Further research is needed to investigate specifically under what conditions trust can contribute in both practical and theoretical terms to enhance international cybersecurity. Furthermore, the role of non-state actors in efforts to enhance international cooperation within cybersecurity deserves more scientific attention.

Literature

Allison, G. T. (1969). Conceptual Models and Cuban Missile Crisis. *American Political Science Review, 63*(3), 689-718.

Arquilla, J., & Ronfeldt, D. (1997). *In Athena's camp: preparing for conflict in the information age*. Santa Monica, Calif.: Rand.

Baseley-Walker, B. (2011). Transparancy and confidence-building measures in cyberspace: towards norms of behaviour. In K. Vignar (Ed.), Disarmament Forum: Confronting Cyberconflict (Vol. 4, pp. 31-40.). Geneva: United Nations Institute for Disarmament Research. Retrieved from http://www.unidir.org/publications/disarmament-forum.

Betz, D. J. (2012). Connectivity, War & Beyond Cyber War. Retrieved from http://kingsofwar.org.uk/2012/11/connectivity-war-beyond-cyber-war/

Betz, D. J., & Stevens, T. (2012). *Cyberspace and the state: toward a strategy for cyber-power* (Vol. 424). Abingdon: Routledge.

Bjola, C., & Kornprobst, M. (2013). *Understanding International Diplomacy: Theory, Practice and Ethics*: Taylor & Francis.

Bourdieu, P. (1991). *Language and symbolic power* (J. B. Thompson, Trans.). Cambridge: Polity Press.

Castells, M. (2004). *The Network society: a cross-cultural perspective*. Cheltenham: Edward Elgar.

Castells, M. (2009). *Communication power*. Oxford: Oxford University Press.

Castells, M. (2010). *The rise of the network society: with a new preface* (Vol. 1). Chichester: Wiley-Blackwell.

Castree, N. (2003). Place: Connections and Boundaries in an Interdependent World. In S. P. Rice, G. Valentine & S. L. Holloway (Eds.), *Key concepts in geography* (pp. XVII, 342 s.). London: Sage.

Charmaz, K. (2006). *Constructing grounded theory*. London: Sage.

Chong, A. (2007). *Foreign Policy in Global Information Space: Actualizing Soft Power*: Palgrave Macmillan.

Communication. (2013). Online Etymology Dictionary Retrieved from http://www.etymonline.com/index.php?allowed_in_frame=0&search=communication&searchmode=none

Dahl, R. A. (1957). The concept of power. *Behavioral Science, 2*(3), 201-215.

Dalen, M. (2011). *Intervju som forskningsmetode*. Oslo: Universitetsforl.

Der Derian, J. (1987a). Mediating Estrangement: A Theory for Diplomacy. *Review of International Studies, 13*(2), 91-110.

Der Derian, J. (1987b). *On diplomacy: a genealogy of western estrangement*. Oxford: Blackwell.

Dijk, J. A. G. M. v. (2006). *The network society: social aspects of new media*. London: Sage.

ENISA. (2012). National Cyber Security Strategies. *European Network and Information Security Agency*. Retrieved from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper

EU. (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Retrieved from http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

Foucault, M. (1983). The Subject and Power. In H. L. Dreyfus & P. Rabinow (Eds.), *Michel Foucault: beyond structuralism and hermeneutics* (pp. 208-226). Chicago, [Ill.]: University of Chicago Press.

Gelb, L. H. (2009). *Power Rules: How Common Sense Can Rescue American Foreign Policy*: HarperCollins.

Gibson, W. (1986). *Neuromancer*. New York: Ace Books.

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: strategies for qualitative research*. Chicago: Aldine.

Hassan, R. (2004). *Media, politics and the network society*. Maidenhead: Open University Press.
Hayden, C. (2011). *The Rhetoric of Soft Power: Public Diplomacy in Global Contexts*: Lexington Books.
ITU. (2008). Overview of cybersecurity – Recommendation ITU-T X.1205: Series X: Data Networks, Open System Communications and Security" – Telecommunication security. *International Telecommunication Union*. Retrieved from http://www.itu.int/rec/T-REC-X.1205-200804-I
Jackson, R. H., & Sørensen, G. (2010). *Introduction to international relations: theories and approaches*. Oxford: Oxford University Press.
Johannessen, A., Tufte, P. A., & Christoffersen, L. (2010). *Introduksjon til samfunnsvitenskapelig metode*. Oslo: Abstrakt.
Joyner, J. (2012). Competing Transatlantic Visions of Cybersecurity. In D. S. Reveron (Ed.), *Cyberspace and national security: threats, opportunities, and power in a virtual world* (pp. IX, 246 s.). Washington: Georgetown University Press.
Keohane, R. O., & Nye, J. S. (1977). *Power and interdependence*. Boston, Toronto: Little, Brown and Company.
Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. In F. D. Kramer, S. H. Starr & L. Wentz (Eds.), *Cyberpower and national security*: Potomac Books.
Kugler, R. L. (2009). Deterrence of Cyber Attacks. In F. D. Kramer, S. H. Starr & L. Wentz (Eds.), *Cyberpower and National Security*: Potomac Books.
Kvale, S., & Brinkmann, S. (2009a). *Det kvalitative forskningsintervju* (T. M. Anderssen & J. f. Rygge, Trans.). Oslo: Gyldendal akademisk.
Kvale, S., & Brinkmann, S. (2009b). *Interviews: learning the craft of qualitative research interviewing*. Los Angeles, Calif.: Sage.
Landler, M. (2013). Obama Signals a Shift From Military Might to Diplomacy, *New York Times*. Retrieved from http://www.nytimes.com/2013/11/26/world/middleeast/longer-term-deal-with-iran.html
Langø, H.-I. (2013). Den akademiske debatten om cybersikkerhet. *Internasjonal Politikk*(2).
Lewis, J. A. (2011). Confidence-building and international agreement in cybersecurity. In K. Vignar (Ed.), Disarmament Forum: Confronting Cyberconflict (Vol. 4, pp. 51-62). Geneva: UNIDIR: United Nations Institute for Disarmament Research. Retrieved from http://www.unidir.org/publications/disarmament-forum.
Libicki, M. C. (1995). *What is information warfare?* Washington, D.C.: National Defense University.
Libicki, M. C. (2007). *Conquest in cyberspace: national security and information warfare*. Cambridge: Cambridge University Press.
Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Santa Monica, Calif.: RAND.
Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Beverly Hills, Calif.: Sage.
Lock, E. (2010). Soft power and strategy: Developing a 'strategic' concept of power. In I. Parmar & M. Cox (Eds.), *Soft power and US foreign policy* (pp. 32-50). London: Routledge.
Luce, E. (2013). Edward Snowden has done us all a favour – even Barack Obama, *Financial Times*. Retrieved from http://www.ft.com/cms/s/0/2b36c94e-42e1-11e3-8350-00144feabdc0.html#axzz2l6nZYMgE
Luiijf, E., & Healey, J. (2011). Organisational Structures & Considerations. In A. Klimburg (Ed.), National Cyber Security Framework Manual (pp. 108-145). Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. Retrieved from http://www.ccdcoe.org/369.html.
Lukes, S. (1974). *Power : a radical view*. Basingstoke: Macmillan.
McCarthy, J. A., Burrow, C., Dion, M., & Pacheco, O. (2009). Cyberpower and Critical Infrastructure Protection: A Critical Assesment of Federal Efforts. In F. D. Kramer, S. H. Starr & L. Wentz (Eds.), *Cyberpower and National Security*: Potomac Books.
Melissen, J. (2005). *The New public diplomacy: soft power in international relations*. Basingstoke: Palgrave Macmillan.
Morrill, C., Buller, D., Buller, M., & Larkey, L. (1999). Toward an Organizational Perspective on Identifying and Managing Formal Gatekeepers. *Qualitative Sociology, 22*(1), 51-72.
Murray, W. E. (2006). *Geographies of globalization*. London: Routledge.

Neukirch, C. (2012). Confidence building in the OSCE. *OSCE Magazine, 3*. Retrieved from http://www.osce.org/node/93959
Neuneck, G. (2013a). Civilian and military cyberthreats: shifting identities and attribution. In G. Neuneck & J. A. Lewis (Eds.), *The Cyber Index: International Security Trends and Realities* (Vol. 3). Geneva: UNIDIR: United Nations Institute for Disarmament Research
Neuneck, G. (2013b). Transparency and confidence-building measures: applicability to the cybersphere? In G. Neuneck & J. A. Lewis (Eds.), *The Cyber Index: International Security Trends and Realities* (Vol. 3). Geneva: UNIDIR: United Nations Institute for Disarmament Research
Neuneck, G. (2013c). Types of confidence building measures. In G. Neuneck & J. A. Lewis (Eds.), *The Cyber Index: International Security Trends and Realities* (Vol. 3). Geneva: UNIDIR: United Nations Institute for Disarmament Research
Nicolson, H. G. (1939). *Diplomacy*: Harcourt Brace.
Nye, J. S. (1990). *Bound to lead*. New York: Basic Books.
Nye, J. S. (2004). *Soft power: the means to success in world politics*. New York: Public Affairs.
Nye, J. S. (2008). Public Diplomacy and Soft Power. *The ANNALS of the American Academy of Political and Social Science, 616*(1), 94-109.
Nye, J. S. (2010a). Cyber power. *Paper*. Retrieved from http://belfercenter.ksg.harvard.edu/publication/20162/cyber_power.html
Nye, J. S. (2010b). Responding to my critics and concluding thoughts. In I. Parmar & M. Cox (Eds.), *Soft power and US foreign policy : theoretical, historical and contemporary perspectives*. London: Routledge.
Nye, J. S. (2011). *The future of power*. New York: Public Affairs.
Nye, J. S., & Welch, D. A. (2013). *Understanding global conflict and cooperation: an introduction to theory and history*. Boston: Pearson.
OSCE. (2012). OSCE Guide on Non-military Confidence-Building Measures (CBMs) Retrieved from http://www.osce.org/home/94616
OSCE. (2013). Protracted conflicts, human dimension issues, transnational threats and OSCE future perspectives amongst decisions at Kyiv Ministerial Meeting. *Organization for Security and Co-operation in Europe*. Retrieved from http://www.osce.org/cio/109313
Pamment, J. (2013). *New public diplomacy in the 21st century: a comparative study of policy and practice*. London: Routledge.
Parmar, I., & Cox, M. (2010). *Soft power and US foreign policy : theoretical, historical and contemporary perspectives*. London: Routledge.
Potter, E. H. (2002). *Cyber-diplomacy: Managing Foreign Policy in the Twenty-first Century*: McGill-Queen's University Press.
Putnam, R. D. (1988). Diplomacy and domestic politics: the logic of two-level games. *International Organization, 42*(03), 427-460.
Rattray, G. J., & Healey, J. (2011). Non-State Actors and Cyber Conflict. In K. M. Lord & T. Sharp (Eds.), America's Cyber Future: Security and Prosperity in the Information Age: Volume II (Vol. 2, pp. 65-86). Washington, D.C.: Center for a New American Security. Retrieved from http://www.cnas.org/publications/reports/america-s-cyber-future-security-and-prosperity-in-the-information-age#.UpN_3MSkrWQ.
Rid, T. (2011). Cyber War Will Not Take Place. *Journal of Strategic Studies, 35*(1), 5-32. doi: 10.1080/01402390.2011.608939
Ryen, A. (2002). *Det kvalitative intervjuet: fra vitenskapsteori til feltarbeid*. Bergen: Fagbokforl.
Seale, C. (1999). *The quality of qualitative research*. London: Sage.
Small, M. L. (2009). `How many cases do I need?': On science and the logic of case selection in field-based research. *Ethnography, 10*(1), 5-38.
Stauffacher, D., & Kavanagh, C. (2013a). Confidence building measures and international cyber security. Geneva: ICT4Peace.

Stauffacher, D., & Kavanagh, C. (2013b). The reach of soft power in responding to international cybersecurity challenges. Geneva: ICT4Peace Foundation.
Strauss, A. L. (1987). *Qualitative Analysis for Social Scientists*: Cambridge University Press.
UNIDIR. (2012). The Role of CBMs in Assuring Cyber Stability: UNIDIR Cyber Security Conference 2012 (CS12). *United Nations Institute for Disarmament Research*. Retrieved from http://www.unidir.org/programmes/emerging-security-threats/cyber-security-conference-2012-the-role-of-confidence-building-measures-in-assuring-cyber-stability
UNODA. (2013a). Confidence Building. *2013*. Retrieved from http://www.un.org/disarmament/convarms/infoCBM/
UNODA. (2013b). Fact sheet: Devlopments in the Field of Information and Telecommunications in the Context of International Security. Retrieved from http://www.un.org/disarmament/factsheets/
Wang, J. (2011). *Soft power in China*. New York: Palgrave Macmillan.
Weber, M. (1991). Class, Status, Party. In H. H. Gerth, C. W. Mills & B. S. Turner (Eds.), *From Max Weber: essays in sociology* (pp. 180-195). London: Routledge.
Weekes, B., & Tikk-Ringas, E. (2013). Cyber security affairs: Global and regional processes, agendas and instruments. In B. Weekes & E. Tikk-Ringas (Eds.). Geneva 2013: ICT4Peace Foundation.
Yi, S.-c., & Melissen, J. (2011). *Public diplomacy and soft power in East Asia*. New York: Palgrave Macmillan.
Zahran, G., & Ramos, L. (2010). From hegemony to soft power: Implications of a conceptual change. In I. Parmar & M. Cox (Eds.), *Soft power and US foreign policy* (pp. 12-31). London: Routledge.
Zartman, W. (2009). Diplomacy. In K. Aggestam & M. Jerneck (Eds.), *Diplomacy in theory and practice: essays in honor of Christer Jönsson* (pp. 507 s. : ill.). Malmö: Liber.

Attachments

Attachment 1: The grounded theory process

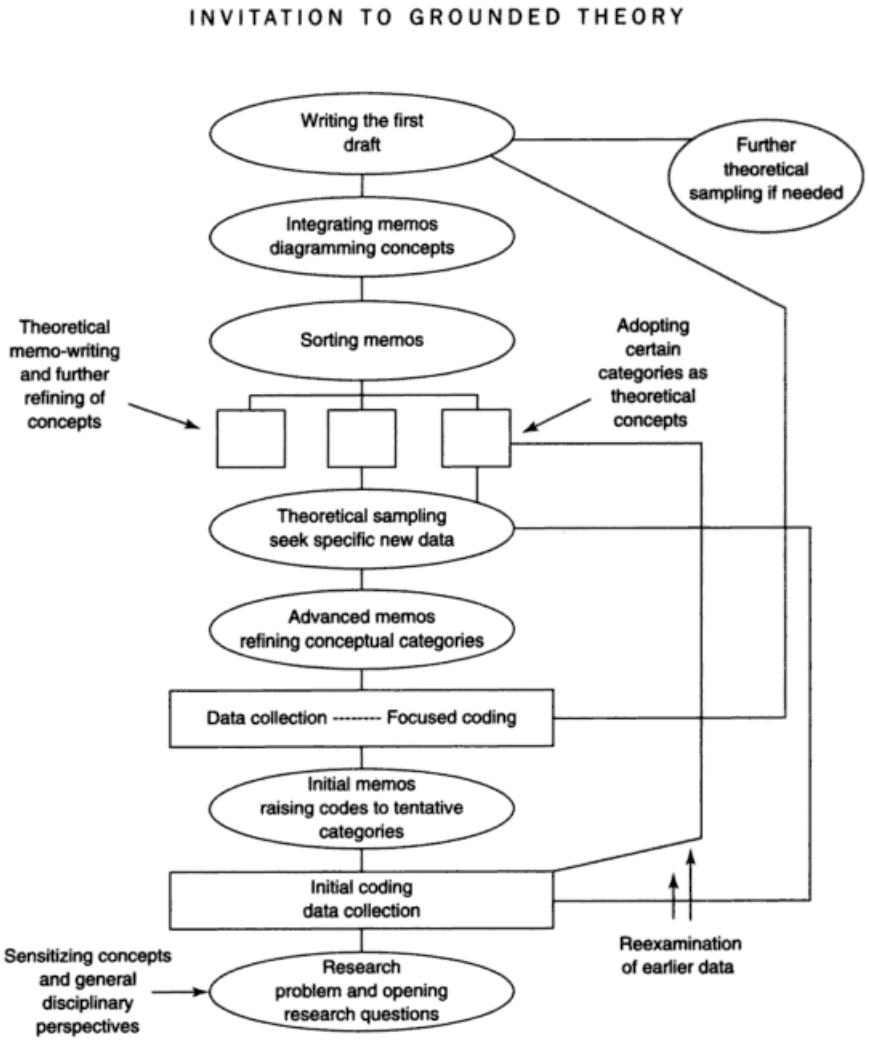

FIGURE 1.1 The grounded theory process

(Charmaz, 2006, p. 11)

Attachment 2: List of informants

1. Melissa Hathaway

Ms. Hathaway is President of Hathaway Global Strategies LLC and a Senior Advisor at Harvard Kennedy School's Belfer Center. She is also a Distinguished Fellow at the Centre for International Governance Innovation in Canada and is the Chairman of the Council of Experts for the Global Cyber Security Center in Italy. She served in two U.S. presidential administrations, where she spearheaded the Cyberspace Policy Review for President Barack Obama and led the Comprehensive National Cybersecurity Initiative for President George W. Bush. Ms. Hathaway is a frequent keynote speaker on cybersecurity matters, and regularly publishes papers and commentary in this field.

2. Steven Malby

Mr. Malby is Prevention and Criminal Justice Officer in Division for Treaty Affairs of the United Nations Office on Drugs and Crime (UNODC), in Vienna.

Mr. Malby's comments are made in his personal capacity and do not reflect in any way the views of the United Nations or UNODC.

3. Alexander Klimburg

Mr. Klimburg is a Fellow at the Austrian Institute for International Affairs. Since joining the Institute in October 2006, Mr. Klimburg has undertaken government national security projects for, among others, the Austrian Federal Chancellery, the Ministry of Defense, and the National Security Council. Mr. Klimburg has partaken in international and intergovernmental discussions, and acts as an advisor to the Austrian delegation to the OSCE as well as other different bodies.

4. **Bjørn Svenungsen**

Mr. Svenungsen is Cyber Coordinator at the Norwegian Ministry of Foreign Affairs (MFA). Mr. Svenungsen graduated with a cand.philol from the Norwegian University of Science and Technology (NTNU) in 1997, and then joined the MFA in 1999. He served at the Permanent Delegation to the OSCE in Vienna and at the Embassy in Ljubljana. Mr. Svenungsen has previously worked as Communication Advisor and Press Officer with the MFA and as Director of Communication with the Norwegian Water Resources and Energy Directorate (NVE).

5. **Eilif Ofigsbø**

Mr. Ofigsbø is Director of the Technology and Operational Support Department at the Norwegian Criminal Investigation Service (KRIPOS). He is former Director of the Operational Department and Director of NorCERT at the Norwegian National Security Authority (NSM). Furthermore, he was Branch Chief at the Information Assurance Branch 2007- 2010, Branch Chief of the Operations, Plans and Requirements Branch 2010-2011, as well as Consultation, Command and Control Staff (NC3HQ Staff) at the NATO Headquarters in Brussels. Mr. Ofigsbø holds a Master's Degree in Computer science from the University of Oslo. In addition he has military education from the Norwegian Military Academy and the Norwegian Defence Command and Staff College.

6. **Robin Bakke**

Mr. Bakke is Specialist Director Cybersecurity at the Norwegian Ministry of Justice and Public Security (JD). He is currently particularly involved in work related to national cybersecurity. Mr. Bakke has a Master of Business Administration (MBA) and a Bachelor of Applied Science – Information Technology – from Swinburne University in Melbourne, Australia.

7. **Ronny Windvik**

Mr. Windvik is Principal Scientist and Project Manager at the Norwegian Defense Research Establishment (FFI). He is currently involved in a number of projects related to cybersecurity and cyberpower, and he has done research within this field since 1999. Mr. Windvik holds a Master's Degree in Communications Systems and Computer Science from the University of Oslo.

8. Sverre Jervell

Mr. Jervell is a Norwegian Diplomat. He graduated from the Norwegian school of business (NHH) 1967, and he studied law as well as languages at the University of Oslo 1967-69. He graduated from College d'Europe Belgium in 1970 and studied at the Center for international affairs (CFIA), Harvard University in 1986. Mr. Jervell is also co-author of the Stoltenberg-Report on Nordic foreign and security policy co-operation.

9. Laura Crespo

Ms. Crespo works at the Division for Security Policy, International Security, within the Swiss Federal Department of Foreign Affairs (FDFA). As a political affairs officer she is involved in the implementation of the strategy on protecting Switzerland against cyber risks in the FDFA. Further, she is engaged in different international processes regarding cybersecurity such as the OSCE process on cyber confidence building measures. Prior to that she worked at the Project Cyber Defense within the Federal Department of Defense, Civil Protection and Sport, which was in charge of developing the cyber strategy. Ms. Crespo has a master's degree in International Relations from the London School of Economics and Political Sciences.

10. Michele Coduri

Mr. Coduri is since 2012 Head of the International Security Section and Deputy Head of the Division for Security Policy within the Federal Department of Foreign Affairs (FDFA). He is leading the Swiss Delegation in the negotiation within the OSCE on confidence building measures in the field of cyber. As career diplomat he has been posted previously in Brussels, Geneva, Sarajevo and Bern. Mr. Coduri has a PhD in international relations from the University of St. Gallen.

11. Robin Mossinkoff

Colonel Mossinkoff is the Senior Military Advisor to the Permanent Mission of the Kingdom of the Netherlands for the Organization for Security and Co-Operation in Europe. He is also accredited as Defense Attaché to Austria. Colonel Mossinkoff's military education includes Airforce Staff College, General Staff College and the Advanced Defense College at the Clingendael Institute. He holds a Master of Arts degree in Public Administration (University of Leiden).

12. Anonymous

Informant number 12 has respectfully decided to remain anonymous in this context.

13. Daniel Stauffacher

Mr. Stauffacher, a former Ambassador of Switzerland, is the Founder and President of ICT4Peace. He is a founding Trustee of Sir Tim Berners Lee's World Wide Web Foundation, and a Member of the Board of the Gulf Research Centre Foundation (GRC), Geneva. He serves as an advisor to the Swiss and other Governments on Cyber-security policy and to the UN Secretariat General and a number of UN organisations, including the Office of the High Commissioner for Human Rights on improving Crisis Information Management Systems (CiMS). Mr. Stauffacher has a Master's degree from Columbia University, New York and a Ph.D. in media and copyright law from the University of Zürich.

14. Halvard Leira

Mr. Leira is a Senior Research Fellow at the Norwegian Institute of International Affairs (NUPI) and Associate Professor (II) at the Norwegian University of Life Sciences. He holds a PhD in Political Science from the University of Oslo, and Master's degrees from the University of Oslo (Political Science) and the LSE (International Relations). Mr. Leira has

published extensively in English and Norwegian on topics such as foreign policy, international relations theory, international history, the history of international thought and diplomacy. He is currently programme chair of the Historical International Relations Section (HIST) of the International Studies Association.

15. Dagfinn Buset

Mr. Buset is a specialist director of the Norwegian National Security Authority (NSM). He is responsible for the agency's national and international relations, and gives strategic advice on national security policy and cybersecurity policy. Prior to his position as specialist director Mr. Buset was responsible for NSM's strategic security assessments and the work on the protection of critical national assets. Before joining the Norwegian NSM, he was head of the secretariat for the government appointed commission for the protection of critical infrastructure (CIP) in Norway. Mr. Buset has also worked as an advisor in the Rescue and Emergency Planning Department within the Norwegian Ministry of Justice and Public Security, primarily with strategic work on CIP and protective security. He has a Bachelor's degree in Political Science, Law and Economics from the University of Oslo.

16. Paul Meyer

Mr. Meyer is a former Canadian diplomat who retired from the Foreign Service in September 2010 after a 35 year career. He joined the then Department of External Affairs in 1975 and served abroad in Oslo (1976-1978), Moscow (1982-1984) and Brussels (1988-1992) where he was Political Counsellor in Canada's delegation to NATO. From 2003 to 2007, he served as Ambassador and Permanent Representative to the United Nations and the Conference on Disarmament in Geneva. In February 2011 he was appointed Fellow in International Security at the Centre for Dialogue and concurrently Adjunct Professor, School for International Studies at Simon Fraser University, Vancouver. His research interests include nuclear non-proliferation and disarmament, outer space security, conflict prevention and cybersecurity.

Attachment 3: Interview guide

Intro

Tell me a little bit about your professional and academic background. How did you first become interested in diplomacy / cybersecurity issues ?

1. How would you define your own words, respectively, cybersecurity and cyberpower?

2. What do you associate with "cyberdiplomacy "? What makes this different from more " traditional diplomacy "?

3. In brief, in your opinion, what are the main consequences of the new ICT and the rise of the network society for diplomatic processes ?

4. What communication challenges do government representatives face in their efforts to strengthen international cybersecurity in the global network society?

5. Have states gotten more or less power as a result of the ICT revolution ? Why / how? What other actors have cyberpower, and what determines their relative strengths and weaknesses?

6. In what ways can CBMs help government representatives strengthen international cooperation in relation to cybersecurity? Why is international cooperation necessary?

7. Which CBMs are most important, in the short and long term, for international cyber-security? What is possible to achieve with these measures, and what are their key constraints?

8. Can CBMs create soft power ? Or conversely, may soft power increase chances to agree on CBMs?

9. What role can/should soft power play in the context of cyberdiplomacy ?

10. What other actors have soft power in the cyber domain? What roles should i.e. NGOs RSOs, the private sector and civil society play in this context?

11. What causes can help explain the extensive monitoring (NSA / Snowden) we've seen between certain countries in recent time?

12. The fact is that there are currently no established "rules of the road ", or even any fi-nally agreed upon confidence-building measures (CBMs) in relation to international cybersecurity. What impacts may this have in terms of trust and surveillance?