Anti-War and the Cyber Triangle

Strategic Implications of Cyber Operations and Cyber Security for the State

Sven Herpig

ACKNOWLEDGEMENT

I would like to thank my loving wife – source of inspiration, firmest believer and harshest critic. For without her, this research would have never progressed beyond the first few paragraphs.

I am deeply grateful for having an amazing family. Their tireless encouragement and support allowed me to pursue my dreams. During the years of research, I was not able to spend as much time with them as I would have wanted, and only a tiny fraction of what they would have deserved.

I would also like to acknowledge Doctor David Lonsdale, brilliant academic and amazing supervisor, without whom this work would have remained a body without soul.

Last but not least, I want to give a shout-out to all the infosec people, cyber libertarians, strategists, hackers, academics and practitioners who helped me with their immense knowledge and vast networks over the last couple of years.

Sven Herpig, January 2016

PhD Thesis, University of Hull

Research: May 2011–March 2015
Approval: August 2015
Editing: January 2016

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

Abbreviation	Full Name
AI	Artificial Intelligence
APT	Advanced Persistent Threat
ARPANET	Advanced Research Projects Agency Network
BMI	Bundesministerium des Innern
C4I	Command, Control, Communications, Computers & Intelligence
CCTV	Closed-Circuit Television
CERN	Organisation Européene pour la Recherche Nucléaire
CERT	Community Emergency Response Team
CIA	Confidentiality, Integrity, Availability
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNII	Critical National Information Infrastructure
CNO	Computer Network Operations
DHS	Department of Homeland Security
DOD	Department of Defence
DPI	Deep Packet Inspection
EMP	Electromagnetic Pulse
EU	European Union
EW	Electronic Warfare
GFW	Great Firewall (of China)
GUI	Graphical User Interface
HERF	High Energy Radio Frequency
HUMINT	Human Intelligence
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum

II	Information Infrastructure
Internet	Interconnected Network
IO	Information Operations
IP	Internet Protocol
ISOC	Internet Society
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
MAD	Mutually Assured Destruction
MILNET	Military Network
MPS	Ministry of Public Security
MSS	Ministry of State Security
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCS	National Cyber Security
NCW	Network Centric Warfare
NII	National Information Infrastructure
NIRPNet	Nonsecure Internet Protocol Router Network
NPL	National Physical Laboratories
NSA	National Security Agency
NSS	National Security Strategy
NW	Network Warfare
PC	Personal Computer
PLA	People's Liberation Army
PRC	People's Republic of China
R&D	Research & Development
RAND	Research and Development (Corporation)
RMA	Revolution in Military Affairs

SCADA	Supervisory Control and Data Acquisition
SIW	Strategic Information Warfare
SMT	Subversive Multi-Vector Threat
TCP	Transmission Control Protocol
UN	United Nations
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network
WAPI	Wireless Local Area Network Authentication and Privacy Infrastructure
WLAN	Wireless Local Area Network

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

1. Introduction

1.1 Introduction of the Subject

The main driver for this choice of research was the growing influence of Internet-related issues in contemporary politics in various fields. 2009 saw an intensification of this link between information and communication technologies and international relations, particularly in the field of intelligence and military, with the revelation of notorious cyber operations such as *AURORA, Ghostnet* and *Night Dragon* (see chapter II). While those events started to attract the broader attention of academics, it was not until the discovery of the *Stuxnet* malware in 2010 (see chapter IV) that the issue gained momentum in other fields as well. A computer malware targeting a nuclear enrichment facility in a foreign country amidst a latent conflict certainly raised a lot of questions that demanded answers. Its sophisticated design and potential implications for international relations as well as strategic studies was one of the main inspirations for this research.

While the emergence of literature on espionage and sabotage in conjunction with the Internet can be traced back to the 1990's, Kello recognises that even in 2013 it remains a weakly developed area, stating that '[t]he range of conceivable cyber conflict is poorly understood by scholars and decision-makers, and it is unclear how conventional security mechanisms, such as deterrence and collective defence apply to this phenomenon' (Kello, 2013: 7). Thus, the aim of this research is to contribute to the literature in this way '[…] in addition to elucidating empirical cyber events, scholars can guide the design of policies to affect them' (Kello, 2013: 38-39). Undertaking research in a field which is state-of-the-art and therefore, highly volatile, presents a particular academic challenge. It does also however enable a researcher to make a potentially crucial contribution, a dent, in the current debate. In areas of research in a vacuum exists, it is imperative for scholars to contribute to filling up that academic lacuna. The main outcome therefore is supposed to be a contribution to the academic debate on the

strategic relevance and conduct of cyber operations[1] and the state's[2] response to it. The intellectual tools developed as part of this research may be of future use for policy-makers. The underlying question for the research is: What are the strategic implications of cyber operations for the state?

The Economist recently saw 'intensifying cyber threats' as one of the top challenges for 2014 (The Economist, 2014). The revelations of the past years, starting with *Stuxnet*, Operation *AURORA, APT-1, Red October* and activities derived from the *NSA Documents* revealed by whistleblower Edward Snowden[3] indicate that this threat will not abate soon. More and more states are readying themselves for future conflicts by developing defensive as well offensive cyber operations capabilities (Lewis, 2013b: 9-55). The latest domain for conflict resolution is currently being explored and exploited too by a growing number of different stakeholders. Based on the increased number of stakeholders and the intensity and number of occurrences of said events (see section 3.5 and appendix), its contemporary relevance is high and has been increasing for several years and looks set to continue. Guiding principles in the field of strategy is an important part of this development. Though the debate on strategic implications of cyber operations started in the early 1990's, and promoted under the auspices of the RAND Corporation, '[i]ntellectually, we are in a position not unlike that faced 65 years ago as we began to develop our thinking about nuclear weapons' (Kramer, 2012: I). Nye agrees, stating that 'in comparison to the nuclear revolution in military affairs, strategic studies of the cyber domain are chronologically equivalent to 1960 but conceptually more

[1] Defined in section 3.1 as 'the targeted use and hack of digital code by any individual, group, organization or state using digital networks, systems and connected devices, which is directed against Critical National Information Infrastructure in order to steal, alter, destroy information or disrupt and deny functionality with the ultimate aim to weaken and/ or harm a targeted political unit'.

[2] As defined in sub-chapter 2.1 to consist of people, territory and legitimate monopoly of power.

[3] Find a comprehensive list of similar events in *Timeline of Events*, chapter II and the Appendix.

equivalent to 1950. Analysts are still not clear about the lessons of offense, defense, deterrence, escalation, norms, arms control, or how they fit together into a national strategy' (Nye, 2011: 19). Thus, an intensive academic analysis of this field is pivotal, especially within the framework of strategic studies, in order to enable strategic adaptation and decision-making (Kello, 2013: 14). The timeliness of events, paired with the lack of a properly developed strategic framework, signify the increased contemporary relevance for research of the strategic implications of cyber operations for the state.

Definitions are very important in political science, and only more so for research in the field of cyber operations. In the absence of commonly agreed upon definitions for cyber operations, and a multitude of other terms such as cyber warfare, digital warfare, information warfare, electronic warfare (see sub-sections 3.1 and 3.2 as well as section 4) which are at once related and disparate, mean that clarity in definitions is centrally important. While definitions might normally differ slightly, all elements included in the definition of cyber operations might vary. This includes the stakeholders (and their representation as entity in the cyber domain), the means to conduct cyber operations, the platform where it is conducted (for example all digital devices, Internet only, electromagnetic spectrum) and the operations through which it is conducted (for example, if cyber espionage is included or not).

Therefore, the coherent and comprehensive definition is of vital importance for the understanding of the research and more so for its outcomes. The terminology of this research applies for the state in the cyber domain, cyber operations and cyber strategy. Thus, the three key definitions which are developed in this research can be found below[4].

[4] These definitions were developed as part of this research. They are partially based on existing definitions in the field. For details about the development of each definition, refer to the respective chapter.

The *state* and its representation in the *cyber domain* is defined in chapter I: The state's representation of the cyber domain is the Critical National Information Infrastructure (CNII). The CNII is composed of a particular part of the information infrastructure which is vital to the function of the state according to the state-teachings of Jellinek: territory, people and legitimate use of violence.

The definition of *cyber* operations as developed in chapter II: A cyber operation is the targeted use and hack of digital code by any individual, group, organization or state using digital networks, systems and connected devices, which is directed against CNII in order to steal, alter, destroy information or disrupt and deny functionality with the ultimate aim to weaken and/ or harm a targeted political unit.

Subsequently, the definition of a *cyber strategy* in chapter IV: The development and employment of cyber operations, potentially integrated and coordinated with other operational domains and forms of information operations, to achieve or support the achievement of political objectives.

1.2 Review of the Related Literature

1.2.1 Development of the Literature

The review of related literature focuses on the academic literature of cyber operations in strategic studies as the focal point of this research. The rise of the Internet is inextricably linked with the rise in the discussion of cyber operations. It was present in academic literature as well as in novels and movies such as the War Game (1983), the Cuckoo's Egg (1990), or the Cryptonomicon (1999). From the outset, the potentially destructive properties of the Internet were spotted. The first academic discussion about the strategic potential of cyber operations was published in 1993 under the auspices of the RAND Corporation by Arquila and Ronfeldt, entitled *Cyberwar is Coming!*. The following twenty years saw the appearance of different schools of thought with some progress, but without overcoming crucial challenges such as establishing a commonly agreed definition of cyber warfare or cyber operations. The following section outlines

the main contributions and milestones in the academic discussion, describes the existing schools of thoughts and identifies the contributions of this research to the existing discourse.

The research identified three seamlessly interconnected periods in the development of cyber operations literature. The *early literature* between 1993 and 2000 includes works by authors such as Arquila and Ronfeldt (1993), Alvin and Heidi Toffler (1993) and Campen, Schwartau, Denning, Libicki (1996). Arquila and Ronfeldt stated in 1993 that they '[…] anticipate that cyberwar, like war in Clausewitz's view, may be a 'chameleon'. [...] Cyberwar may be fought offensively and defensively, at the strategic or tactical levels' (Arquila and Ronfeldt, 1993: 45). Recurring to their concept of netwars, the authors assumed that 'most netwars will probably be non-violent, but in the worst of cases one could combine the possibilities into some mean low-intensity conflict scenarios' (ibid: 30). Research during this time focused on the increasing importance of knowledge in warfare, the avoidance of physical conflicts by the use of non-lethal (knowledge) weapons, as well as their potential ability to decapitate the target and standalone means. After describing cyber warfare (Toffler, 1993: 148-152), Toffler mentions the impact of it by stating that 'knowledge weapons alone, even including the use of the media, may never suffice to prevent war or to limit its spread. But the failure to develop systematic strategies for their use is inexcusable. Transparency, surveillance, weapons monitoring, the use of information technology, intelligence, interdiction of communication services, propaganda, the transition from mass lethality to low-lethal or non-lethal weapons, training, and education are all elements of a peace-form for the future' (ibid: 239). It is the same work in which Toffler discusses the concept of Anti-War which has been adapted in this work (see sub-section 7.6). The research uses meta-level data which includes assumptions and theoretical approaches rather than empirical evidence and analytical conclusions. Definitions are very blurred but some core issues, which are still relevant for the contemporary discussions, such as the idea of Anti-War, are identified.

The *strategic literature* between 2001 and 2009 includes works by Gray (1999), Rattray (2001), Lonsdale (2004), Billo and Chang (2004) as well as Libicki (2007, 2009a and 2009b). During this period, the first accounts of strategic cyber operations were published. These publications include deliberations on meta-discussions such as the mutability of geography in the strategic cyber domain, the general strategic direction of cyber operations as well as more detailed accounts on deterrence and *sub rosa* cyber strategies. Gray for example argues in 1999 that 'on the virtual battlefield of cyberspace, electronic warfare is apt to mock geography, and therefore time' (Gray, 1999: 43). Lonsdale in return focuses on the strategic level of the more general information operations, arguing that 'SIW [Strategic Information Warfare] will only substantially change the nature of warfare if it proves to be independently strategically effective' (135). Many of those writings are comparably sceptical of the possible impact of cyber operations when compared to the early writings. Libicki for example states that 'as a threat, it [cyberwar] may not be believed; as a reality, it may not cause enough cumulative damage to make the target cry uncle' (Libicki, 2007: 137). The supplementary, rather than the standalone role of cyber operations, is stressed and with it, its notion of being a means for intelligence operations rather than being part of the military domain. Gray's account support this statement when attributing as the key goal to cyber war achieving 'information dominance' (Gray, 1999: 268). While the analyses of these writings are much more in-depth as compared to the early writings, empirical evidence or the use of methodologies such as game theory are rare.

The third period since 2010, the post-*Stuxnet* literature, includes *inter alia* writings by Clarke and Knake (2010), Andrees and Winterfield (2011), Rid (2012 and 2013), Betz and Stevens (2011) as well as Lewis (2013b). These writings identify the state's strategic need for developing more than only defensive cyber capabilities (Clarke and Knake, 2010: 99-101 and Betz and Stevens, 2011: 131), a continuing perception of cyber operations as tool for intelligence operations rather than military ones (Betz and Stevens, 2011: 81-82) as well as a first, cautious mentioning of strategic issues which might be similar to the Cold War period (Dipert, 2010: 403). However, the absence of

a continued debate on strategies, hence strategic cyber operations, is apparent. A stronger focus on strategic issues as well as empirical analysis can be expected to be added during this period in the coming years. More and more cyber operations are being discovered and analysed, enabling researchers to conduct in-depth empirical studies and present their conclusions and impact on strategic studies.

1.2.2 Schools of Thought

The earliest school of thought acknowledges cyber operations as a threat to the security of a state, but declares its potential impact as overrated and cyber war an impossibility. Stressing the importance of traditional means of warfare and the low impact of cyber operations, this school can be referred to as the *conventional school*. It is represented by information technology and security experts such as Bruce Schneier and academic as well as military experts such as Libicki, Arquila, Ronfeldt and Rid. Even though authors like Libicki, Arquila and Ronfeldt were the first to tackle this and related issues (which makes them revolutionary)[5], their perspective on the potential impact of cyber operations is rather cautious from a contemporary point of view.

Combining their technical and military background, this school has a solid basis for what they claim as the potential of cyber operations. From a military perspective, cyber operations and cyber attacks are regarded as tools supplementing traditional, conventional warfare, in that war cannot be won by cyber operations alone (Lonsdale, 2004). Cyber operations as a standalone means of attack can be used for intelligence-related activities and in supplement to other forms of warfare in order to create a significant outcome. The authors take into consideration that national cyber security has to be strengthened because of the prevalent and constant threat and attacks from states as well as a variety of non-state actors (Libicki, 2007). From a strategic point of view,

[5] Libicki, M. C. (1994) The Small and the Many. In Arquilla, J. and Ronfeldt, D. (1997) *In Athena's Camp*. Santa Monica: RAND Corporation, pp. 191-216.

the focus is on securing the information infrastructure[6] and pro-active defences. As no serious cyber attack occurred so far, cyber warfare or a *Cyber Pearl-Harbour* is regarded as overrated and deemed unlikely (Schneier, 2009). Due to the high degree of technological reliance of the military as well as the state on information and communication technologies, predominantly in developed countries, severe cyber attacks are only seen as a prelude to conventional warfare. Due to their everyday nature, not too much effort should be spent on retaliating to cyber attacks *per se*. A zero-tolerance (deterrence) policy can only lead to the loss of credibility, as long as it is not enforced. This would, in return, mean that every attack would have to be retaliated against, something which is not deemed to be feasible (Libicki, 2009). The *conventional school* thus acknowledges the need to incorporate cyber means in the defensive, while maintaining that it's offensive potential is less powerful. The latter is referred to as the broad means of information operations (for example Arquilla and Ronfeldt, 1997) rather than to cyber operations in particular[7].

Opposed to the *conventional school*, scholars of the *unconventional school* regard threats arising from cyber operations as dangerous, and therefore as a severe threat to national security. The *conventional school* acknowledges that at some point, cyber operations threats will become more severe in terms of the impact on national security. Thus, the term *unconventional* refers to the authors' belief that this development has already taken place and cyber operations can cause widespread, serious damage and allows for coercion of the enemy without conventional warfare means. Authors belonging to this school are, among others, Denning, Colarik, Kilroy, Janczewski, Carr, Campen, Dearth as well as Clarke and Knake. Cyber operations here have a fast and increasingly destructive potential which can be directed against the CNII of a state. It is mentioned that less networked states are less likely to be vulnerable to cyber operations.

---

[6] Defined in sub-section 2.2.3 as being 'composed of the particular part of the information infrastructure of a given state which is vital to the function of the state according to the state-teachings of Jellinek'.

[7] For the distinction of these two forms of warfare, see chapter II.

Nevertheless, a majority of states have potential targets connected to the Internet, which makes them even more vulnerable (Clarke and Knake, 2010 or Janczewski and Colarik, 2008). Focusing on the more networked and advanced states, authors argue that states such as China, Russia or the United States are already equipped with highly-trained staff and have capable cyber operations means at their disposal. Regarding Russia and China, hackers which are loosely associated with states – and can therefore be counted as state actors - are the focal points of the more contemporary literature (Carr, 2010)[8]. Referring to *Stuxnet,* which is believed to be developed by Israel in cooperation with the United States, warfare has reached another level. *Stuxnet* is described as *cruise virus* which aimed at a specific target (see chapter IV). This school of thought therefore argues that cyber operations are already an important issue for national security and the *Cyber Pearl Harbor* is just an event waiting to happen (Andrees and Winterfield, 2011). Thus, the *unconventional school* urges for immediate defensive measures, acknowledging the powerful impact cyber operations can have. Offensive operations are regarded as viable and threatening for the integrity of the state.

In addition to both afore-mentioned schools, scholars of the *supplementary school* of thought see cyber operations as a supplement to traditional, conventional forms of warfare. Well-known authors supporting this school are Dearth, Williamson, Billo, Chang, Libicki, Lewis and Arquila as well as Ronfeldt. Lonsdale (2004) goes so far that he portrays cyber operations as a weak (standalone) strategy. According to him, cyber operations do not enable a military force to win over another, precisely because it cannot conquer territory. Thus, its impact is better compared with strategic bombing. While these statements do not exclude cyber operations from being conducted as standalone activity, to achieve goals other than conquering territory or overthrowing the enemy, authors of this school argue that cyber operations will only be conducted alongside traditional forms of warfare. In this framework Lewis states that 'a cyberattack will not be decisive. Large industrial countries are not easily defeated by a single strike unless

[8] This might constitute the latest form of mercenaries. Further research in this area might be prudent.

it involves nuclear weapons, and cyberattacks do not reach this level of shock and destruction. The destructiveness of cyberattack is overstated. It can cause physical damage to equipment connected to the Internet, but without the shock, confusion, and violence associated with blast damage' (Lewis, 2013a: 11). Billo and Chang for example argue that a cyber attack can create a moment of surprise which will then be used for a decisive traditional attack while the opponent is disorientated (Billo and Chang, 2004), something which Libicki presents in a more detailed account saying that 'cyberwar can play three key roles: It might cripple adversary capabilities quickly, if the adversary is caught by surprise. It can be used as a rapier in limited situations, thereby affording a temporary but potentially decisive military advantage. It can also inhibit the adversary from using its system confidently' (Libicki, 2007: 142). The supplementary school therefore argues that cyber operations conducted as standalone activity are not decisive and that it should be conducted alongside with conventional warfare. Thus, cyber operations in the *supplementary school* are regarded as an enabling element for offensive operations, whereas the main contribution will come from conventional forms of warfare, such as air, sea or land warfare.

The most recent school of thought is the *standalone school.* Two of the few works which discuss a potentially destructive impact of standalone cyber operations were conducted by Andrees and Winterfield (2011) and Clarke and Knake (2010). The *standalone school* opposes the *supplementary school* on the decisiveness of cyber operations. The perspective is that cyber operations can be decisive and potentially defeat an enemy without relying on other means. Cyber operations do not have the potential to conquer a country, but it might settle a dispute where both parties are hesitant to include/conduct more severe actions such as traditional warfare or nuclear warfare. Cyber operations can lead to the achievement of a political goal through coercion (Clarke and Knake, 2010). This school focuses particularly on the potential impact of cyber operations on the critical information infrastructure which connects public assets such as the power grid, dams or the economy (Andrees and Winterfield, 2011). The latest development of this school of thought is the review of the concept of cyber power and a renewed

discourse about it. Discussions by Nye, Kramer, Betz and Stevens show that an equivalent to sea power and air power can be created in the cyber domain through a variety of different activities in this domain (Nye, 2011; Kramer et al., 2009 and Betz and Stevens, 2011). The *standalone school* does acknowledge that cyber operations can achieve political goals on their own, e. g. by coercion through targeting critical infrastructure.

Structuring those four schools of thought and applying them to a matrix (see table 1) reveals their interconnection with each other. It is rare that works can only be categorized in one school of thought as these schools of thought are only partially mutually exclusive. The *conventional* and *unconventional schools* cancel each other out, similar to the *supplementary* and the *standalone school*. This can be derived from the perspective that the first two schools deal with the potential impact of cyber operations while the other two schools are based on the utilization of it. Thus, in most cases a scholar will find himself affiliated with a combination of two schools of thought.

		Schools (Impact)	
		Conventional	*Unconventional*
Schools (Use)	*Supplementary*	Supplementary Conventional	Supplementary Unconventional
	Standalone	Standalone Conventional	Standalone Unconventional

Table 1

1.2.3 Contribution

There are five significant contributions to the field of strategic cyber operations made by this research:

- First, a collection, extension and addition to existing cyber strategies, their structure, usability and implications.

- Second, a coherent and comprehensive discourse and analysis of the various links of strategic cyber operations, to the tactical, operational and political level.
- Third, a thorough and extensive adaptation of traditional concepts of strategic studies (such as Gray's dimensions of strategy or the Clausewitzian friction) to cyber operations.
- Fourth, a description of the impact of cyber operations on the state of international relations, an Anti-War period following into the footsteps of the Cold War and War on Terror.
- Fifth, the development of a framework to analyse strategic implications of cyber operations in a two-actor arena, based on an adaptation of game theory.

Particular areas of contribution to the current post-*Stuxnet* debate on strategic cyber operations, are extensions of works and contributions presented in the earlier periods. However, their extension and interconnection with issues raised by the contemporary debate is one of the key features which makes this research unique. The research puts emphasis on the strategic literature by providing a comprehensive strategic analysis of relevance, impact and opportunities for cyber operations as a state's tool. This is detached from current struggles to categorize cyber operations as belonging either to the field of intelligence or the field of defence. Additionally, borrowing the issue from the early literature, the research takes up the discourse on the meta-level, more specifically the relevance cyber operations has for the state of international relations and interstate politics.

In conclusion, the overall contribution of this research is to deepen the strategic understanding of cyber operations as a viable tool for conflicts in international relations, regardless of its approach or its affiliation, in order to enable and facilitate state decision-making. In broader terms, the contribution made through this research, continues the development of the contemporary post-*Stuxnet* literature. This research aligns itself to a combination of the *unconventional/standalone schools* of thought.

1.3 Methodological Approach

The methodological approach of this research is designed to follow three steps, 1. conceptual, 2. analytical/ empirical and 3. explorative. Chapters I and II apply the conceptual approach to the basic research. This approach covers the needed definitions as well as the framework on which the later analytical sections are based. The method is applied by pulling together various theories, concepts and ideas and welding them into a solid basis onto which to apply the analytical and explorative discussions. For chapter III and chapter IV, the research applied an analytical approach. The core of those chapters was the adaptations of national security and strategic studies to the cyber domain, based on the framework concluded in the prior chapters. Concepts from authors such as Colin Gray or Sun Tzu were applied to analyse the impact and the relevance of cyber operations for strategic studies and define how these fields interact. In order to showcase those adaptations, two case studies have been analysed to provide empirical evidence, the national cyber security strategy of the People's Republic of China as well as the Olympic Games operation as sample for cyber strategies. Both cases have been chosen owing to the availability of solid sources, something which is comparatively rare in the field of cyber operations. In chapter V, an explorative approach was used to verify the findings of the prior chapters as well as to discover further strategic implications for stakeholders within the conflict arena. More generally speaking, this methodological approach aims to initially cover, gather and form a solid basic research, and then analyse and conclude them in a second step, verifying the findings and creating a tool for decision-makers in the last step.

The initial research framework aimed to cover more case studies and use qualitative expert interviews of different stakeholders and decision-makers in order to provide a broader empirical approach. Both approaches had to be substituted. In the first instance due to the lack of non-classified data and in the second because of the unwillingness of experts to be interviewed or the impotency of including the interview without proper attribution. The latter obstacle was identified and overcome after the first qualitative interview had been conducted with a very high ranking member of the North Atlantic

Treaty Organization (NATO). Therefore, the number of case studies had been reduced to two, making sure proper sources were available. To make up for the lack in numbers, those case studies had been extended far beyond what was originally conceived. To even out the lack of qualitative expert interviews, the author participated in a number of non-classified conferences and workshops, where stakeholders from various backgrounds were present. Through presentations and informal discussions, the experts provided valuable input on the topic. Over the three-year duration of the research, the author attended and participated (through nine presentations) in eight events, gathering expert perspectives from governments, academia, civil society and private sector (see table 2).

Date	**Conference/ Workshop**	**Stakeholders**
September 2011	Rootcon 5 Hacker Conference, Philippines	Academia, Private Sector, Government
July 2012	Revolution in Military Affairs, Royal Military Academy of Sandhurst, England	Academia, Government
September 2012	Rootcon 6 Hacker Conference, Philippines	Academia, Private Sector, Government
October 2012	Hackover 2012, Chaos Computer Club, Germany	Civil Society
April 2013	Cyber Security and Privacy EU Forum 2013, Trust in Digital Life (TDL) and European Association for e-identity and security (EEMA), Brussels	Academia, Private Sector, Government, Civil Society
March 2014	Conference on Contemporary Conflict, University of Birmingham, England	Academia
September 2014	China in Cyberspace: Platform, Content, Governance, University of Hull, England	Academia
October 2014	Hackover 2014, Chaos Computer Club, Germany	Civil Society

Table 2

In chapter V, game theory is to verify the conclusions made in the prior research and analysis, as well as to providing an intellectual tool which may be used by states, for the calculations of conflict scenarios in the cyber domain. The choice of game theory as a method is discussed in detail in the beginning of that chapter. Choosing game theory as a method stems from the theory's analysis of the strategic impact and scenarios of nuclear warfare to calculate outcomes and implications. While this method was not included in the original research layout, it proved to be viable and crucial for the outcome, contributing to the identification of strategic implications of cyber operations for the state.

1.4 Structure of the Chapters

Chapter I briefly presents the underlying definition of state. This serves as the point of reference in understanding the strategic implications of cyber operations. While most cyber attacks are facilitated through the Internet as an underlying technology, it can also be conducted involving systems and networks which are capable of being connected through other means, thus forming the cyber domain. The last section of this chapter merges the notion of the state with the cyber domain, in order to define the state's representation in it. The Critical National Information Infrastructure (CNII) is important for the strategic analysis which follows, understanding offensive and defensive implications of strategic cyber operations towards the state.

Chapter II focuses on the definition and discussion of cyber operations. The terminology in this field is inconsistent, hence the aim of this section is to provide a definition that enables an understanding of the respective implications. The objective was to create a clear and categorical concept as a contribution to the existing literature. The discourse includes *inter alia* discussions on cyber weapons and armours, milestone cyber attacks, and an overview of existing definitions from various fields, such as academia or military. In addition to the clear and categorical definition of cyber operations, this chapter also extends the understanding of the underlying technology of cyber operations

through a comprehensive list of events within which this type of conflict resolution evolved.

How to secure the CNII is the focus of chapter III which focuses on National Cyber Security (NCS). This section establishes a coherent notion of what security in the cyber domain means, starting with the micro level and progressing towards the macro. Possible approaches are integrated into different cyber security behaviours which can be adapted by the state. To visualize NCS, the second part of this chapter presents an empirical case study on the cyber security approach of the People's Republic of China within this framework.

The fourth chapter forms the first half of the core of this research, connecting the previously discussed points and analysing the strategic relevance of cyber operations. The first section in this chapter discusses the different levels of strategic studies, politics, strategy, operations and tactics in order to create a general picture of strategy in the cyber domain. It is followed by an analysis and adaptation of strategic concepts such as the levels of strategy or friction and challenges within the cyber domain. Ultimately, this chapter functions as the glue between the underlying technology and the strategic level, presenting a coherent and comprehensive account of possible cyber strategies. It shows how they are defined and what possible implications the choice of a particular strategy entails. The subsequent parts of this chapter present the idea of a current state of international relations, for the cyber domain, insofar as it is similar to the Cold War: the Anti-War era. It sketches the underlying strategic considerations for states. Analogous to chapter III, this chapter is concluded by an empirical case study on an actual implementation of cyber operations. This case study illustrates the conclusions by focusing on the *Olympic Games* operation against Iran.

The final chapter consists of two parts. First, it adopts game theory as a method to the strategies in cyber operations as an intellectual tool. This toolkit functions as a means through which numeric values can provide the estimated result of a certain cyber conflict. It tool is used in a second step to further explore strategic implications based

on the conclusions of the past chapters, applying it to several scenarios. Thus, this chapter connects the so-far disparate elements of this research and offers additional conclusions for the strategic implications of cyber operations for the state.

CHAPTER I

2. Cyber Domain

2.1 The State

As defined in the main research question, the primary stakeholder of interest for this project is the state. Thus, it is paramount that the concept *state* is defined and adapted to the domain of cyber operations. This research applies Jellinek's definition of the state, the *Drei-Elemente-Lehre*[9] (Jellinek, 1959: 394-414). His teaching is a part of the state-theory school based on Pollock, Sunning *et al.* (see for example Janet and Picot, 1987; Pollock, 1890; Dunning 1902 and Warschauer, 1911). Jellinek's work is internationally accepted and fundamental for *inter alia* European law[10]. Subsequently, a state is formed by three constitutional elements:

1. the territory of the state,
2. the people living within these borders and obeying the laws of that territory,
3. the legitimate use of violence of the monopoly of power.

These three elements can include further indicators such as language or behaviour. However, for the analytical framework of this paper and its questions, these three elements are regarded as the pillars of the state. Those pillars are crucial for the discussion of national cyber security in chapter III as they constitute the key indicators of what needs to be protected in the cyber domain.

2.2 The Internet

The demand for a technology which offers a decentralized communications infrastructure has been developed in the aftermath of the Second World War (Chadwick, 2006: 40-47). One of the outcomes of the Second World War was the invention of the nuclear bomb. During the arms race between the United States and the former Soviet

[9] From German: *teaching of the three elements.*
[10] See for example Stolleis, 1992; Boldt, 2004 and Kersten, 2004.

Union, the nuclear weapon technology was the main tool for threatening the adversaries of the state as a deterrent (Keith and Walton, 2002). The starting point is the communication system because it connects the command and control structure of the military forces of the United States. Subsequently, the communication system became of utmost importance. Certain nodes within the communication infrastructure were vital. If they were to be destroyed, the communication network in the whole country would have broken down. This essentially included military communications and command and control. A communication system which could survive a nuclear strike would enable the military to react. The reaction – called second strike capability – increases the potential deterrence and therefore raises a strategic advantage (Payne and Walton, 2002).

As a result, the United States government focussed its military research and development on finding a technology that would provide a decentralized information and communication infrastructure (Leiner et al., 2000). Two institutes have worked on projects to design said infrastructure during the late 1960's and early 1970's. The British National Physical Laboratories (NPL) and the American Research and Development Corporation (RAND), both stakeholders in the 1970's, working on a packet switching technology to achieve a communication system that could withstand a nuclear strike (Leiner et al., 2000). RAND had been contracted by the US government in 1958 to design a network in which no single element was solely responsible for to the functioning of the information and communication infrastructure (Adams and Scolland, 2006: 30). This infrastructure was called the Advanced Research Projects Agency Network (ARPANET). The ARPANET was up and running in 1969 and composed of four computers. The first host – meaning a node where these computers were connected to each other - was situated in the University of California, Los Angeles (UCLA) (Leiner, 2000 and Adams and Scolland, 2006: 33). While the computers, cables and connections are hardware, the most crucial part for the ARPANET was the software: the protocols. While the initial National Control Protocol (NCP) had been developed in 1970, it was followed by the Transmission Control Protocol in 1975 (TCP). It was only

in 1983 that the Transmission Control Protocol/ Internet Protocol (TCP/IP) - which is currently in use - had been developed and implemented in the ARPANET (Adams and Scolland, 2006: 33-35).

1983 was a crucial year for the development of the Internet. ARPANET at this point has mainly been used and tested in an academic environment. Consequently, the academic community saw an immense value in the ARPANET as a tool to exchange ideas and discuss theories. Here then, RAND decided to split the ARPANET project. One part continued the development of the ARPANET project under civil supervision in order to serve the demands of academia and later also the demands of civil society. This part is known today as the interconnected network, or short: Internet. The second path followed the initial demand for a military network for information and communication based on a decentralized infrastructure. This project has been continued under the name Military Network (MILNET) (Adams and Scolland, 2006: 38). The MILNET later on evolved to the Non-secure Internet Protocol Router Network (NIRPNET) tasked to exchange military, unclassified information.

In the following years, different – mostly American-based – institutions were created to govern the Internet. Their approaches and members varied (Chadwick, 2006: 230-236). Some - such as the Internet Engineering Task Force (IETF) - focused on the technical development of the Internet and its standards. Others, like the Internet Society (ISOC), focused more on the social components while even others dealt with the aspect of political governance of the Internet ever since. One of them is the Internet Governance Forum (IGF) (Chadwick, 2006 and Herpig, 2009: 19-25). In the late 1990's, Tim Berners-Lee from the European Organization for Nuclear Research (CERN) in Switzerland developed the World Wide Web (www) and an easy-to-use graphical user interface (GUI) for the browser (Berners-Lee, 2000: 38-81). However, it was O'Reilly in 1993 that finally made the Internet popular by creating an easy-to-use bundle to go online (Berners-Lee, 2000: 87). During this period the Internet, in its adapted form,

developed in the People's Republic of China[11]. However, the technology, and therefore the basis for cyber operations, is the same all around the world. The next section deals with these technical details.

2.2.1 The Interconnected Network

In order to understand cyber operations and the challenge to national security they pose, it is vital to gain a basic understanding of the technical details of the Internet[12]. It is a network of networks which ultimately consist of connected computers and systems. In order to elucidate further, the explanation will be framed on a common household.

In this house there several computers, smart devices and mobile phones, each connected to each other with cables or via wireless connections. This is called a local area network (LAN). This LAN, like all the other neighbour households, is connected – via cable or wireless - to an Internet Service Provider (ISP). At this point, they are connected to an Internet backbone and are part of the world area network (WAN). These backbones are connected to each other, and this closes the circuit for the Internet. At this point, the devices in the living room is connected to all the other computers, smart devices and other systems in the world that are also connected to the Internet (Lammle, 2006). Laptops, personal computers, tablets and mobile phones are all electronic devices capable of connecting to the Internet. People use them in order to access or share information or communicate with one another. Therefore, the use of these devices defines them as clients. The information they access is saved on servers. With the right software, every personal computer can be a server. Whatever the setup is, servers can be used to host websites, files and databases, function as email servers or as a secure gateway between a company network and the Internet (Cheswick and Bellovin, 1994). All devices connected to the internet have an identification number which is issued to

[11] The development and technical details of the Chinese information infrastructure are discussed in detail in other publications such as Mueller and Tan, 1997; Saich, 2004 and Wacker, 2003.

[12] *Internet* is an abbreviation for *interconnected network*.

them by their ISP. This identification number acts as address, and is called the Internet Protocol address (IP). Server normally have static IPs, while personal computers constantly change their IPs according to their ISPs which owns blocks of IPs and distributes them to their clients every time they log on to the Internet[13]. These addresses are necessary for data to reach their destination (Stewart, 2009).

All digital data consists of strings of 1's and 0's. It does not matter if it is a text file, a picture, a video, or software controlling the industrial appliances of a nuclear power plant. Each can be broken down to 1's and 0's. In order to exchange (read or write) information over the Internet, files such as a picture are split in packets which are then numbered. These packets are then sent from the host – the device where the information are - to the requesting client. The routes these packets take from server to client through the Internet are dynamic. Therefore, the two indicators are how a packet reaches its destination (the route) and how long it takes (the delay). With a little bit tweaking, these can packets take two or more rounds across networks all-over the world before they arrive at their destination. The technologies that can be used therefore are proxy servers (proxies) or virtual privacy networks (VPN) (Cheswick and Bellovin, 1994). Thus, someone who tries to trace back the origin of these packets has to do the same rounds as the packets. There is no shortcut. This is one way to delay the realisation that someone has downloaded critical information from his server.

All of this is only possible because the networks are standardised. The hardware and the software which are used to form the Internet are basically the same everywhere in the world. All electronic devices use the same protocols (software) and they all use the same cables or standard for wireless network (hardware) to link up the Internet[14]. This basic

[13] This is true for the Internet Protocol version 4 standard (IPv4). At the time this paper is written, IPv4 is still the prevalent standard. The coming IPv6 standard issues IPs differently and they are easier to trace back to their respective users. However, the same methods for hiding traces apply for IPv4 and IPv6.

[14] Of course, there is more to the way the Internet functions than these short paragraphs, for example how domain names are attributed by the Domain Name

knowledge should be sufficient to understand the nature of cyber attacks and their strategic implications.

2.2.2 Internet, Cyberspace and Cyber Domain

Before this paper continues to explain the convergence point of the systems and networks and the state, one last distinction has to be made in order to avoid confusion. This section explains the difference and use of the terms *Internet, Cyberspace,* and *Cyber Domain*. While the technical background of the Internet has been described, a concise definition of the Internet has not yet been given. For a broad definition, Mueller et al. state that:

> *'[w]hat we call 'the Internet' is really a standardized set of software instructions (known as protocols) for sending data over a network, and a global set of unique addresses so the data can be told where to go'* (Mueller, Mathiason and Klein, 2007: 244).

Kleinwächter narrows this further: that 'the Internet is a decentralized "network of networks", connected by a joint protocol suite, the Transfer Control Protocol/ Internet Protocol (TCP/IP)' (Kleinwächter, 2005: 209). Elixmann and Scanlan offer a shorter and non-technical definition by concluding that 'the Internet has no nationality, and is made up of over 100,000 networks world-wide' (Elixmann and Scanlan, 2002: 7). Concerning the state character of the Internet, Cerf adds that 'the Internet was designed to be largely insensitive to national boundaries. The IP address structure is not oriented around countries, unlike the telephone system' (Cerf, 2008: 55). This chimes with the previous section's definitions. The Internet is a technology which connects different devices via an open standard software protocol to networks, and then those networks to even larger networks to finally connect all these computers to each other, worldwide.

System, see for example Chadwick, 2006: 235-251; Mueller, 2002: 49 and Mathiason, 2009: 51-52.

Consequently, Berners-Lee argues that 'the Web breaks the [geographic] boundaries we have relied on to define us and protect us [...]' (Berners-Lee, 2000: 217).

From a strategic point of view, mountains or oceans are geographical boundaries offering protection insofar as they are more difficult to pass with tanks for example. The introduction of air power rendered many of those geographical boundaries obsolete, but some were persistent (such as caves or long distances). However, physical anchors exist in the cyber domain (Hare and Zimmerman, 2009: 89-90). Network connections are created and linked for example by undersea cables, satellites and the radio frequency spectrum. Those connections exist physically in form of hardware which can be destroyed, thereby introducing its own form of geographical boundaries. In a cave with no cell reception or satellite uplink, there is no change to connect to a network[15].

The term *cyberspace* was first coined by Gibson in his 1984 science-fiction book *Neuromancer* (Gibson, 1984). One of the frequent users of the term cyberspace is Lawrence Lessig, a well-known Harvard Law professor (see for example Lessig, 1999; Lessig, 2002 and Lessig, 2006). He uses cyberspace as a socio-cultural construct. For him '[c]yberspace is not one place. It is many places' (Lessig, 2006: 84). The Internet is a place where the users can come together and interact with each other. Lessig acknowledges that there is a difference between the Internet and cyberspace (Lessig, 2006). The Internet is the technology, while cyberspace refers to social interactions that form while using this technology (Goldsmith and Wu, 2008: 149-155 and Goldsmith, 2003)[16]. As described, the term is used in social, legal or political settings, thereby offering a softer definition as opposed to the hard, technological definition of the Internet.

[15] For more information, see *geography* as one of the strategic dimensions adapted to the cyber domain in chapter IV.
[16] For an overview over definition of *cyberspace*, see: Kuehl, D. T. (2009) From Cyberspace to Cyberpower: Defining the Problem. In Kramer, F. D., Starr, S. H. and Wentz, L. K. (Eds.) *Cyberpower and National Security*. Washington D.C.: National Defense University, pp. 24-42.

The use of either definition for the following analysis would be slightly flawed. Therefore, this research adopts the term *cyber domain*. While most cyber attacks are carried out using the Internet as enabling element, not all are. Chapter IV discusses the *Stuxnet* malware as major part of the Olympic Games cyber operations campaign against Iran. A key attack vector during this operation was the infection of computer systems which were not directly connected to the Internet. It was only possible to infect the target systems through a bridge, a Universal Serial Bus (USB) device, which carried the malware from a system with an Internet connection to the target system. As chapter IV analyses, this was a fairly sophisticated operation with cyber attacks and malicious software being used over the Internet to custom-tailor a programm which, spreading through the use of mobile devices (USB-stick), infected and manipulated computers which controlled physical machines. On the other hand, the notion of cyberspace is rather a general political, legal and social one. Adopting cyberspace to a framework within strategic studies would therefore confuse the discussion unnecessarily debate. In order to stress it is the environment that is the framework for conflicts carried out by states relying to certain degrees, but not always, on the underlying Internet technology. This research sticks with the common terminology of strategic studies. However, the *cyber domain* as a definition borrows from the Internet as well as from cyberspace, and extends them at certain points. From the definition of cyberspace, it borrows it a soft dimension, the political and social dimension, as conflicts are always political and social. The cyber domain however extends, from a technical point of view, the definition of the Internet by computers, systems and devices that are capable of, with or without the use of intermediaries, being connected to the Internet – whether they are connected to the internet or not

2.2.3 Critical National Information Infrastructure

The information infrastructure (II) is defined as 'long-distance and short-distance communications technologies, private networks, local area networks, future facilities, and the means of connecting to and using networks such as desktops and handhelds, including systems software and relevant application software' (Clark, 2011). Pironti

states that information infrastructure encompasses technologies and tools which deal the creation, use and dissemination of information (Pironti, 2006). If, for example, video and pictures are taken with a digital camera, the device is part of the II because it creates information. The information infrastructure grows larger more complex– almost similar to an organic growth (Barletta *et al*., 2011: 55). It becomes more and more important through the connection of different infrastructures, such as the power grid, to the Internet (Cordesmann, 2000: 4-5 and Touré, 2011a: 10).

The public information infrastructure encompasses all hardware and software which is owned by the state or its subsidies. The computers in the Department of Health, servers of the parliament, or the website of the local government providing e-governance functions, are all part of the public information infrastructure. There are four strategically relevant areas of the public information infrastructure of the state: electronic governance, infrastructure, law enforcement as well as military data, and command and control. Electronic governance (e-governance) can be important for a state because citizens use these services to fill out their tax declaration, change their address or register their car (Leggewie, 1998: 19-22 and Donath, 2001: 269-301). These processes generate data and ultimately information which is transmitted from the client (the citizen) to the server (the local or national administration). If one were to illegally obtain access to this information, one would be in possession of considerable power. At the same time, it is the fault of the state administration if the privacy, thus security of an individual is violated in this way. In that case, the state fails to protect the citizens' information and ultimately the citizens themselves. This is illustrative of but one potential reason for a secure e-governance system.

The infrastructure area of the public information infrastructure includes the power grid, the traffic system, as well as dams and gas- and water supply (if publicly managed – otherwise they are part of the private infrastructure), among innumerable others. The Roosevelt Dam case in 1998 demonstrates the deadly potential of losing control of a state’s infrastructure (Nagpal, 2002). It can lead to high casualties, villages being flooded and people killed. A similar outcome can be generated by a malfunctioning

traffic system. If an adversary gains access to the traffic system and disables it (or just sets all traffic lights to green) during rush hour in a capital, casualties are extremely likely. In both cases, the state as owner and maintainer of these infrastructures will have ultimately failed to protect its citizens.

As a recent case has shown, law enforcement can be the target of cyber attacks too (Lischka and Rosenbach, 2011). Law enforcement serves the state in its pursuit of Jellinek's *monopoly of power* in order to protect citizens, and the state's interests. An attack against law enforcement can be vital because it might disrupt the state's efforts to keep the citizen safe. This is precisely the point where vital state interests are thwarted. In Germany, hackers obtained data from the State Police. This data consisted of the 2009 and 2010 records of Global Positioning System (GPS) tracking logs of potential criminals (Lischka and Rosenbach, 2011). As the tables show the agencies handling it, car brands as well as start and expiry dates (some tracking is still ongoing), this action can seriously damage the efforts of the law enforcement to apprehend criminals. Criminals *qua* definition violate state rules and therefore are a threat to citizen and state. Subsequently, the vital interests of the state are at stake.

A highly sensitive issue of the public information infrastructure is the military sector. Being part of the state, the military is subsumed under the public information infrastructure. For the military, there are two potential dangers which consequently affect the state. First, classified or non-classified information and data might be stolen and downloaded during cyber operations. This information might include any manner of strategic plans, for example troop deployments (McCurry, 2009). For adversaries, this information can be very valuable in order to identify weaknesses and ultimately can lead to casualties. A vital interest of the state to secure its borders, following Jellinek's principle of territorial integrity, might be endangered. A cyber attack to overtake command a control of a state's military would be in the same vein. The private information infrastructure, on the other hand, encompasses all hardware and software which is owned by private companies affiliated to a state. The Deutsche Bank could be an example of this, in that it stores information about a state. Therefore, in certain cases

that are discussed below, a cyber attack against a Deutsche Bank branch in the Philippines could be regarded as an attack against the private information infrastructure of Germany. Before these details are discussed, it is important to distinguish the private information infrastructure further from the public information infrastructure. While the state has direct influence on the public information infrastructure, the private information infrastructure can only be influenced by policies and laws. Those have to be in line with economic fairness, amongst other issues. Therefore, the process of protecting its affiliated private information infrastructure is much more difficult for the state than it is to protect its public information infrastructure. Another important difference is that stakeholders in the private information infrastructure are likely to be beholden to their shareholders. Therefore, threats and attacks against them might not be made public, in order to leave the share price unaffected. While incidents in the public information infrastructure are being reported to some state authority – because they happen within the state – incidents happening in the private information infrastructure are not that likely being announced to the state authorities. This behaviour adds up to the difficulty for the state to protect its private information infrastructure.

There are two main areas that belong to the private information infrastructure and at the same time are of vital interest of the state. The first area includes industrial complexes owned by private companies. The Supervisory Control and Data Acquisition (SCADA) controls might get attacked – which are also used in power plants and other infrastructure mentioned above - and therefore lead to malfunctions, and consequently to casualties (Bill and Chang, 2004: 125-139). Private ownership of power plants, dams and other infrastructural facilities raises the same problem as in the public sphere. The only differences in this case might be caused by the inherent different nature of public information infrastructure and private information infrastructure.

A second area of the private information infrastructure which might endanger the information infrastructure of the state in general, and subsequently its vital interests if attacked, is information about the state. One possible private institution belonging to this area is a private research and development (R&D) company which develops

military technologies and is contracted by a state. As it is outsourced to a private company, it does not fall under the military area of the public information infrastructure. If this information is stolen it can be used to counter this technology. In any case, it is clear that this action is directed against the vital interest of the state which contracted the company. Territorial integrity would be undermined if adversaries are be able to understand and use the same military technologies as the respective state. As a part of the whole, the information infrastructure is mostly privately owned (DoD, 2011: 5).

The Critical National Information Infrastructure (CNII) is a term derived from the Information Infrastructure. It relies on the aforementioned information infrastructure. While the information infrastructure is spread world-wide, with clients and servers around the globe, the CNII narrows down to specific devices within the borders of a sovereign state, or data affiliated with a certain state - such as websites or databases. The CNII involves 'political, economic, civilian, and military dimensions' (Knapp and Boulton, 2008: 18 and Arquilla and Ronfeldt, 1993: 31). It refers to the parts of the II which are crucial for the functioning of a state. This includes clients and servers where attacks can cause severe – also physical – damage to the state. Examples for the CNII as mentioned above are power grids, hospitals, or controls of industrial complexes (Westby, 2011a). A server on which the covert operations database of the Central Intelligence Agency (CIA) is hosted would be part of the American CNII. The geographical location of that server is irrelevant to the ownership of a nation's CNII. The distinction is made where the content or device is vital for the state. Vital in this sense means important for a functioning state and/ or where malfunction can lead to casualties and/ or violate state sovereignty based on Jellinek's three indicators for a state.

Ultimately, the CNII is used to define an attack against the sovereignty of a state. The CNII is the state's representation in the cyber domain. Attacks on it can be considered an attack on a nation's sovereignty, and hence the state itself. A defacement of a parliament's website is unlikely to resemble an attack against the CNII, whereas shutting down the power grid would be. The vitality to the state is analysed on the basis of its inherent functions *people*, *monopoly of power* and *territory* according to Jellinek the

definition of the state (see section 2.1). To conclude the definition, *the Critical National Information Infrastructure (CNII) is composed of the particular part of the information infrastructure of a given state which is vital to the function of the state according to the state-teachings of Jellinek.*

This definition offers a valuable insight for the main question of this research. In order to be able to discuss the strategic implications of cyber operations for the state, it is vital to not only define cyber operations and the domain it takes place in, but also the state's representation in this domain. The state as an entity was broken down into three elements based on the framework of Jellinek's state-teachings. These single elements were then transferred into the cyber domain in order to form the state's representation in it. Chapter III builds the notion of cyber security in this definition. Without the state's representation in the cyber domain, it would be impossible to develop a security framework for it. Subsequently, the research on cyber security forms a crucial element of the cyber strategies debate (chapter IV) which ultimately leads to the strategic implications of cyber operations (chapter IV and chapter V) for the state.

CHAPTER II

3. Cyber Operations

3.1 Defining Cyber Operations

Operations and Warfare

Sections 3 and 4 of this work deal with the definition, description and distinction of cyber activities which form the focal point of analysing strategic implications for the state in the cyber domain. There is a vast field of definitions and terminologies applied to offensive activities taking place in the cyber domain such as *information warfare*, *intelligence operations, network warfare, computer network operations* and so on. The more traditional and broader definition is information warfare which has lately been transforming into *information operations* (see sub-section 4.1). Taking into account the discussion of the cyber domain (see sub-section 2.2.2), a more suitable term would be *cyber warfare* – a term that has also been widely used in the past (see for example Andrees and Winterfield, 2011; Ball, 2011; Billo and Chang, 2004; Carr, 2010 and Janczewski and Colarik, 2008). While this wording had actually been applied to an earlier draft of this research, it was not able to sufficiently reflect the complexity of the activity being discussed. The reasons for the abandonment of the notion cyber warfare at expense of *cyber operations* - similar to the linguistic transition in favour of information operations - has been the extensive scalability of intensity of offensive cyber activities, applicability during peace and war times (see sub-section 7.4) as well as their partial congruency with espionage and sabotage activities, hence intelligence operations (see sub-section 3.2). The only remainder of the former notion is the *cyber war* strategy (see sub-section 7.4.6), a high intensity application of cyber operations with an imminent risk of escalation – or even being applied *ex post* conflict escalation anyway.

The reason why the applicability of cyber warfare would fall short when discussing offensive cyber activities (*cyber operations*) is its genuine link to war whereas cyber

operations can be conducted during every stage of international relations, as stated above. Cohen argues whereas war is a situation, warfare refers to an activity (Cohen, 2002). Clausewitz refers to it also as the 'conduct of war' (Clausewitz, 1997). Szafranski simply defines warfare as 'the set of all lethal and nonlethal activities undertaken to subdue the hostile will of an adversary or enemy' without any direct reference to war (Szafranski, 1996: 232). Luttwak however distinguishes warfare from peace activities, stating that 'the entire conduct of warfare and peacetime preparation for war are in turn subordinate expressions of national struggles […]' (Luttwak, 1987 70). Gray attributes to warfare a qualifying attribute based on its conduct, such as 'regular warfare' - a concept where cyber warfare would come in (Gray, 1999: 23). With warfare being the conducted set of activities of one or more kinds, it is prudent to quickly look at the concept of war in general. Weber simply states that war is historically a state in international relations which is formally declared by one or more states against another (Weber, 2004: 15). While the description as a state of international relations seems prudent, a formal declaration of war might not be a state-of-the-art concept anymore as the concepts of *asymmetrical warfare* and *terrorism* show (for example Hoffmann, 1998 and Laquer, 1996). Other authors such as Bull agree on the existence of war without requiring a formal declaration. He states that war is 'organised violence carried on by political units against each other' (Bull, 1977: 184). Clausewitz also sees violence of political units as one of the primary indicators form war (Clausewitz, 1997: 1-24). Whereas the political dimension is a substantial part of cyber operations (discussed in the following paragraphs), violence, as mentioned above, can but does not have to be a part of it - due to the varying levels of intensity cyber operations can be carried out with (see sub-section 7.4). Therefore, only for cyber operations conducted under the umbrella of a *cyber war* strategy (high intensity) would it technically be correct to refer to them as *cyber warfare* (see sub-section 7.4.6). However, this paper tries to avoid that particular application as it might cause confusion and thus refers to the offensive activities conducted in the cyber domain as *cyber operations.*

Cyber Operations

In order to define cyber operations and therefore differentiate them from other forms of operations, the next section analyses cyber operations using the indicators such as battle space, weapons and targets[17]. These indicators are chosen because they belong to the characteristics of operations and help to understand the uniqueness of cyber operations. In academic literature, cyber operations is said to take place in the 'electromagnetic battle space' (Department of Defence, 2002: 8 and Gray, 1999: 228). However, this term is only used for a very theoretic description of battle space. Cyber operations can be conducted across any devices that can be linked up to a network (Gray, 1999: 26). Examples therefore are the Internet or an autarkic classified military or industrial network (see chapter IV, *Stuxnet*). The latter might not be connected to the Internet but an attack – if following the pattern of a cyber attack (as described later) – would still qualify as cyber operations.

Authors sometimes refer to the connections between digital devices as the *virtuality* of the network (Taylor, 1997). Cyber operations are not conducted in a virtual space *per se*. Billo and Chang state that 'cyber refers to the virtual world in which attacks take place, although the wall between the virtual world and the so-called real world is rapidly crumbling. Actions in the virtual world [...] have physical impacts on the real world' (Billo and Chang, 2004: 140). Thus, the people conducting cyber operations, and also the target systems, are in the real world and might face a real impact from cyber operations. However, the electromagnetic spectrum is always the medium which attacks have to pass through. Therefore, this kind of operations is distinct from land-, sea-, air-, nuclear-, and space operations. This battle space has been identified and is referred to as *cyber domain* (see chapter I).

[17] The analysis is done under the premise that a certain knowledge of the different forms of warfare is existent. For further information see for example: Gray, C. S. (1999) *Modern Strategy*. Oxford: Oxford University Press.

Due to the battle space, the weapons used to conduct cyber operations are distinct and different from those used in other operations. Malawer put it broadly when stating that 'cyber warfare uses computer technologies as defensive and offensive weapons in international relations' (Malawer, 2010: 28). Tordilla goes more into detail: 'cyber weapons are usually basic programmes that have the objective to defend or attack a target. Most of them are freely available on the internet but some more sophisticated or newer ones are kept privately or are commercial' (Tordilla, 2011: 2). All cyber weapons are computer programmes which are made of code. Some are off-the-shelf and are freely available on the Internet, some, such as *Stuxnet* are custom made. While a worm or a denial-of-service programme is obviously a tool to conduct cyber operations, there are also other programmes that can be used as weapons. Most of them are network maintenance programmes. When used in a specific way – for example vulnerability probing – they can become the weapon of choice[18]. Cyber weapons are code strings of 1's and 0's, executed by digital devices, such as personal computers. Some follow the dual-use analogy, while others can be clearly identified as weapons. Subsequently, a physical destruction of computer systems by an explosive cannot be attributed to a cyber weapon. A programme however, which leads to the destruction of computer parts – for example via disabling heat sensors which prevent the device overheating – would be a cyber weapon. No other weapons consist of digital codes, and this gives another distinct indicator.

Having identified the weapons and the battle space of cyber operations, the subsequent discussion deals with the targets. The target of cyber operations is the CNII (see sub-section 2.2.3) of a country (Lonsdale, 2004: 135 and Lewis, 2002: 1). Based on the weapons and battle space, it is predominantly those infrastructures, systems and digital devices which can be connected to a network – most likely the Internet – that qualify as targets. The battle space within which cyber operations are carried out, the weapons

[18] For a more technical description, refer to Cheswick, W. R. and Bellovin, S. M. (1994) *Firewalls and Internet Security. Repelling Wily the Hacker*. Boston: Addison-Wesley Professional Computing, Pearson Education.

utilized, and the targets they aims at, collectively distinguish it from any other kind of operations.

Definition

The differences between cyber operations and other forms of information operations need to be discussed and analysed. This chapter focuses precisely on the distinguishing features of cyber operations and a later section describes and discusses other forms of information warfare and operations. Cutting the *Gordian Knot* in the semantics of information operations has not yet been widely undertaken in academic literature. Schneier, catchily, described the issue thus: 'separating cyberwar, cyber terrorism and cyber crime isn't easy; these days you need a scorecard to tell the difference' (Schneier, 2008a). In this case, the scorecard includes the nature of cyber attacks, their layers, the stakeholders and intentions for cyber operations.

While hacker[19] attacks can take many shapes, such as 'acquisition of objective data' (Libicki, 1996: 93-94), cyber operations are limited in their forms. According to Malawer, cyber attacks are 'deliberate actions to alter, disrupt, deceive, degrade or destroy computer systems or networks of the information and/ or programmes resident in or transiting these systems or networks' (Malawer, 2010: 30). Zanini and Edwards state that:

> *'(...) malicious viruses and worms can be used to permanently destroy (erase) or corrupt (spoof) data and cause economic damage. In the worst case, these same software tools can be used to cause destructive failure in a critical*

[19] A common misperception is the negative appreciation of the term *hacker*. Being a hacker means nothing else than a person who likes to tinker with devices, for example hard- and software. Hacker usually try to access systems for fun or reputation with no negative intentions. Owners of insecure systems are subsequently being informed about the vulnerabilities. *Cracker* on the other hand are people who do the exact same thing but with the ultimate goal to harm someone else or to gain from it. In order to apply commonly used terminology, this work only uses the term *hacking*, even though in some instances *cracking* would be the more precise term.

infrastructure like air traffic control, power, or water systems, which can lead to casualties' (Zanini and Edwards, 2001: 44-45).

Casualties however are not a defining characteristic of cyber operations. The strong suit of cyber operations is their coercive power, which it owes to its potential to disrupt and degrade services and infrastructures. Downloading information therefore would not fall under this definition of cyber operations as long as the information is not used to achieve one of the above-mentioned goals (for example destroying data) or weaken/ harm a target political entity with the overarching aim to achieve a political objective. In that case in can be used as means of coercion of the adversary. Coercion can be achieved by the theft, destruction, alteration or degradation of data or the threat thereof, targeting the CNII.

There are also certain layers within the CNII which are targeted by cyber attacks. Janczewski and Colarik list certain targets for exploits and vulnerability probing such as 'Emails, Web Browsers, Chat Clients, Remote Software, Web-Enabled Applications [...]' (Janczewski and Colarik, 2008: xvii-xxi). One target, which has also been involved in the *Stuxnet* attacks, is the Supervisory Control and Data Acquisition (SCADA) software used in industrial complexes to control for example machines. (Lewis, 2002: 11 and Billo and Chang: 2004: 124-125). In contrast to electronic warfare, which is based on the hardware layer for example by chipping, cyber operations' transport layer is the software.

Due to the nature of cyber weapons and the battle space discussed earlier this chapter, the potential exponents of cyber operations range from individuals to states (Winkler et al., 2004: 79; Kilroy, 2008: 445 and de Caro, 1996: 210). The reach of cyber attacks is global and the weapons are cheap. An individual is as capable of conducting cyber operations as a government-funded cyber army, this coupled with the anonymity of these attacks, makes traces such act difficult (Schneier, 2008b). The inability to narrow the circle of stakeholders distinguishes cyber operations from electronic warfare, among others. It is highly improbable that a single individual would be capable of chipping

devices which are used in military vehicles Intention plays a crucial role in differentiating between cyber operations and other forms of information operations and warfare (Janczewski and Colarik, 2008: xiv). Cyber operations can be used in support of a traditional attack on a state, for example, as in conventional terrorist attacks (Clark, 2003). The intention to conduct cyber operations is therefore to harm a hostile political unit. This can be a state, a terrorist organization or even an individual. If a group of hackers target a national agency in order to steal information and sell them it is an act of crime not a cyber operation. If the same group of hackers targets a national agency in order to cause havoc and subsequently weaken the state, it is a cyber operation by intention.

In order to not confuse these indicators, a brief example elucidates the point. The target of a hypothetical attack is a nuclear power plant which is part of the power grid and subsequently a part of the CNII. The attacker is a group of hackers paid by state A. The intention is to demonstrate state A's superiority in order to get state B to agree to something. The attack subsequently aims to disrupt the service of a power plant to shut it down. The weapon is an off-the-shelf Trojan horse which enables the remote control of the software layer for the control systems, for example the SCADA. This would be a classic cyber operation where the coercion can work as result of a successful attack or by the mere threat of such an operation.

Krepinevich discusses cyber as the '10th military revolution' (Krepinevich, 2008: 5), Westby refers to it as 'the brain-child of the Cold War is turned into the weapon of the 21st century' (Westby, 2011a), the link between computers and warfare comes in different forms. One of them is cyber operations. This chapter analysed cyber operations and distinguished them from other forms of operations. Cyber operations are uniquely defined by its battle space, weapons, targets, stakeholders, intentions, layer and nature of attacks. According to this analysis, *cyber operations are the targeted use and hack of digital code by any individual, group, organization or state using digital networks, systems and connected devices, which is directed against Critical National Information*

Infrastructure in order to steal, alter, destroy information or disrupt and deny functionality with the ultimate aim to weaken and/ or harm a targeted political unit.

3.2 Levelling the Cyber Playing Field

Sub-section 3.1 outlined well the definition of cyber operations and its relation to cyber warfare and cyber war. In order to level the playing field, the relation of cyber operations to cyber activities and attacks such as cyber espionage, cyber terrorism, cyber crime and cyber civil disobedience has to be analysed. Therefore, this section matches terrorism, crime, espionage and civil disobedience with the indicators for cyber operations concluded above. If these indicators match with the indicators for cyber operations, it means that in this respective field it is cyber operations which are being conducted. The indicators for cyber operations are:

1. the action has to be a targeted use and hack of digital code,
2. the action has to be carried out by an individual, group, organization or state,
3. the action has to be directed against the Critical National Information Infrastructure,
4. the action steals, alters, destroys information or disrupts and denies functionality,
5. the action aims at weaken and/ or harm a political unit.

There has always been a blurring between cyber operations, cyber warfare, cyber terrorism, cyber crime, cyber civil disobedience and cyber espionage. The discussions revolve *inter alia* around the idea that cyber espionage takes place, but that this espionage is not cyber war (see for example Webster, 2003, Cilhuffo and Nicholas, 2006: 3 or Carr, 2010: 31-32). Indeed, it is not, but as too, cyber operations are not necessarily cyber war, this section discusses if cyber espionage is using cyber operations to achieve its aims. Figure 1 shows the outcome of this analysis[20].

[20] Focal point of the Venn diagram are cyber operations and their intersection with the other actions. It does not include any qualification about the intersection of the other actions with each other.

Cyber Terrorism

Terrorism, according to Laquer, is defined as 'substate application of violence or threatened violence intended to sow panic in a society, to weaken or overthrow the incumbents, and to bring about political change' (Laquer, 1996: 24). Janczewski and Colarik define cyber terrorism as 'means premeditated, politically motivated attacks by sub national groups or clandestine agents, or individuals against information and computer systems, computer programmes, and data that result in violence against non-combatant targets' (Janczewski and Colarik, 2008: xiii)[21]. Connecting this definition to Laquer's, reveals that the direct targets may be non-combatants but should ultimately be the state.

In order to bring about political change, terrorism has to target certain, politically important, institutions or stakeholders of a state. Therefore, in order to *sow panic in a society* or *overthrow incumbents*, a terrorist would need to target the CNII. Furthermore, disrupting or denying services (such as the power grid) might be more beneficial to achieving this goal than altering, destroying or stealing sensitive information.

When using the systems, digital devices and networks to carry out an attack, it is very often a targeted operation, for example an e-mail spearfishing attack with malware attachments[22]. Terrorism is conducted by individuals or groups and therefore matches the second indicator for cyber operations.

[21] For more information about terrorism and the Internet, see Zanini, M. and Edwards, S. J. A. (2001) The Networking of Terror in the Information Age. In Arquilla, J. and Ronfeldt, D. *Networks and Netwars: The Future of Terror, Crime, and Militancy*, pp. 29-60.

[22] This kind of attack specifically targets important stakeholders in an institution, such as chief executive officers, lead researchers or IT-administrators. E-mails with malware attached or linked are sent out to the victims with the aim to trick (social engineer) the target into opening the attachment or link which will ultimately compromise the system.

Said aim of bringing about political change through coercion by either the threat or the conduct of violent actions coincides with the cyber operations definition of *weakening or harming a political unit*.

From this matching of indicators, it can be assumed that terrorist goals can be achieved by conducting cyber operations. It does not necessary mean that all terrorist acts are cyber operations, but it shows that terrorists who use digital networks, systems and devices to attack the CNII of a nations-state would, *qua definition*, conduct cyber operations to do so.

Cyber Crime

According to the Encyclopaedia Britannica, crime is 'the intentional commission of an act usually deemed socially harmful or dangerous and specifically defined, prohibited, and punishable under criminal law' (Clarke, 2012)[23]. Crime can be conducted using digital code. The mere act of getting access to the computer of another without authorisation by the means of hacking, is deemed illegal in most counties and therefore a crime.

Crimes can be carried out by individuals, groups or organizations. Crimes involving systems, devices and digital networks can be aim to generate income. Therefore, targeting the CNII can be an option from which valuable data might be sold. In these cases, the purpose is to steal information for financial rewards, and not to disrupt or deny functionality. Those stolen information are unlikely to be used to harm or weaken a political entity. Weakening the CNII may result from cyber crime, but that is not the aim. Therefore, cyber criminals do not conduct cyber operations, mainly due to the difference in intention and motivation.

[23] For more information on crime and its relation to networks, see William, P. (2001) Transnational Criminal Networks. In Arquilla, J. and Ronfeldt, D. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica: RAND Corporation, pp.: 61-98.

Cyber Espionage

Cyber espionage basically refers to gathering of information via computer networks about a political stakeholder (Denning, 2000: 131-152) to support the security, foreign, defence, economic policy of a political actor. It is a targeted use of code because espionage is concerned with intelligence gathering about a particular person, department, institution or state.

In order to gain access to specific computer systems, the attack has to be targeted. Cyber espionage is also carried out by either states or someone contracted by them. Corporate espionage in this case would be subsumed under cyber crime.

Espionage is directed against the CNII which can also involve private military contractors. It is commonly understood as gaining access to a system, stealing information, exiting a system and is attributed to the need to disguise this act. However, an integral part of espionage requires the logging and tweaking of files in order to gain access. Therefore, at least an alteration, if not degradation, of data is conducted in cases of espionage in order hide traces.

The ultimate aim is to support their own policy goals while potentially weakening the target political unit, as it creates an imbalance *vis-à-vis* the perpetrator in terms of information superiority.

Cyber espionage therefore matches the pattern of cyber operations to a certain degree. This view is also supported by Gervais, although in his work, he refers to cyber espionage as 'cyber exploitation' (Gervais, 2011: 7-9). Thus, espionage conducted using digital networks, systems and devices conducts (in certain cases) cyber operations to achieve its aims.

Cyber Civil Disobedience

Civil disobedience is a public non-violent act which violates existing laws and aims to bring about political change (Rawls, 1971: 364-372). Civil disobedience is referred to,

for example, in the Anonymous case, where groups use denial-of-service attacks (see section 3.3) to deny the access to *inter alia* government websites.

It is a targeted use of digital code by a group. These actions normally do not target the CNII. In order to achieve the highest degree of publicity, government websites are brought down which are only used for information sharing or communication between government and citizens. Other actions, such as the attacks conducted by the Anti-Sec movement, target critical infrastructure,[24] though this is rather an exemption and may in fact border on cyber terrorism or cyber crime already.

As targeting the CNII can be regarded as an unintended side-effect of cyber civil disobedience activities, it should be reiterated that civil disobedience is not conducted using cyber operations to achieve its goals[25]. The lack of intention to harm or weaken the targeted political stakeholder differentiates it from cyber operations.

[24] More information about Anonymous and Anti-Sec: see Kaplan, 2011; The Guardian, 2010 and Fleming, 2010.

[25] For an elaborate account on the distinction between cyber civil disobedience and other forms of information warfare, see Meikle, G. (2009) Electronic civil disobedience and symbolic power. In Karatzogianni, A. (Ed.) *Cyber Conflict and Global Politics*. New York: Routledge, pp. 177-187.

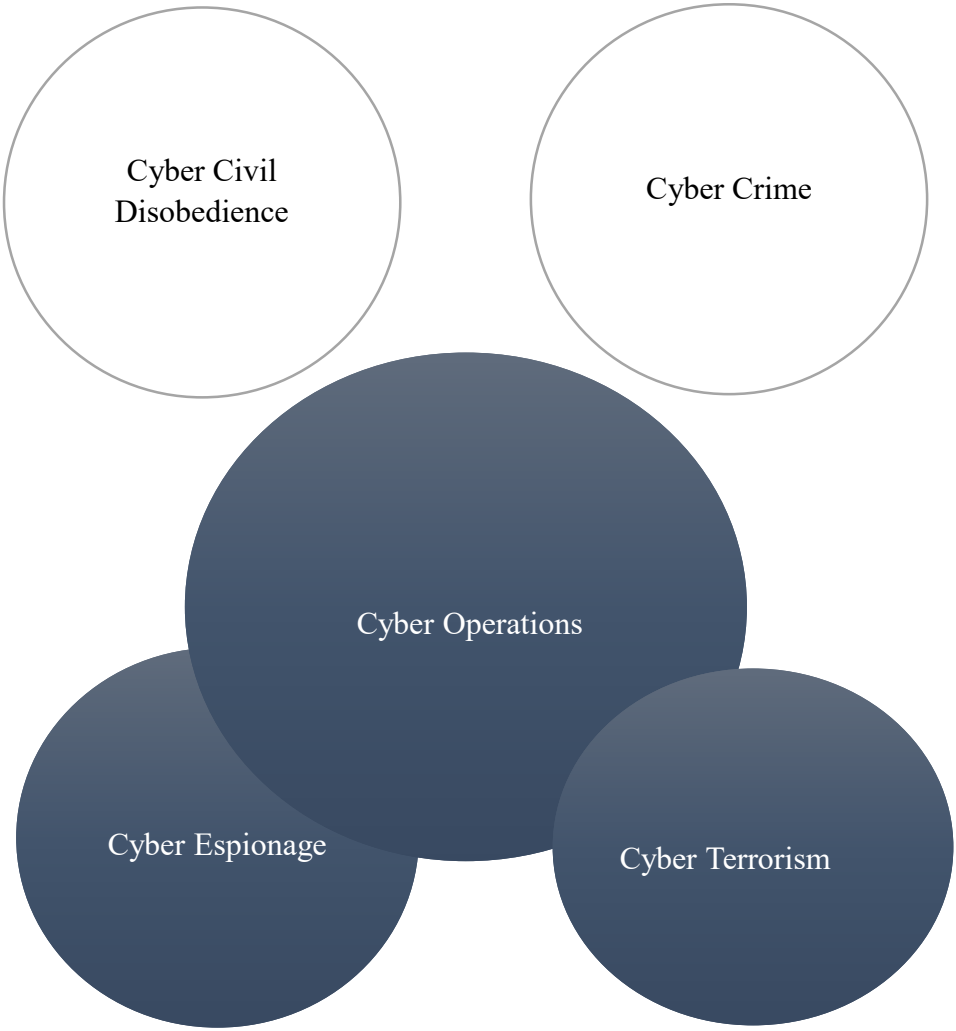

Figure 1[26]

[26] This Venn diagram is limited to the connections of the mentioned activities with cyber operations. It does not entail any proposition about intersections of the other activities with each other, for example if there is a link between cyber terrorism and cyber crime.

3.3 Cyber Armoury

3.3.1 Remarks

The following section provides an overview of the weapons and defence mechanisms/ armours in the framework of cyber operations. The tools which have been chosen do not conclude an exhaustive list, but highlight the most common attack vectors and defence mechanisms in cyber operations. In order to be able to conduct strategic research in any field of operations, it is important to know and understand the weapons and counter measures. The strategic level controls the tactical level, mediated by the operational level, which ultimately needs to have an understanding of the weapons which can be used (Gray, 1999: 22-23; Clausewitz, 1997: 74). An important point which is true for both weapons and armour in cyber operations is that these tools are dual-use (Schneier, 2008a). A tool developed by corporate penetration testers to secure their own company network can also be used to attack the CNII of a state. 'Cyber weapons are usually basic programmes that have the objective to defend or attack a target. Most of them are freely available on the internet but some more sophisticated or newer ones are kept privately or are commercial' (Tordilla, 2011: 2). By definition, if an encryption programme is used by an individual user to secure his files it is for private security. When the same tool is used in government, it is a defence mechanism. In addition to being dual-use, sophisticated cyber weapons may only allow for one-time usage. Cyber weapons necessarily need to exploit vulnerabilities. If there are no vulnerabilities to be exploited, the cyber weapon does not work. If an adversary's system is attacked via exploitation of vulnerability A, vulnerability A will – in theory – be fixed on all adversary's systems after he noticed the attack and gathered forensic evidence. This vulnerability then will not be of any use for the attacker, against this adversary and those who he shares his information with.

3.3.2 Cyber Weapons

Riley and Vance state that '[c]yber weaponry appears to be entering a golden age of rapid development—a new arms race' (Riley and Vance, 2011). This section provides a general overview about the tools being used, referred to as *cyber weapons*. Thereby, it does not give a holistic picture of all cyber weapons, rather than an introduction of the most commonly known cyber weapons and combinations thereof. Described in this section are: brute-force attacks, viruses, worms, Trojan horses, and rootkits, advanced persistent threats, advanced volatile threats as well as subversive multi-vector threats (SMT). All those weapons can be directed against systems and devices, as well as against digital networks. Commonly used to hack passwords in computers, networks and encrypted files, a Brute-Force (BF) attack is an:

> *'[…] attempt to decrypt the message exhaustively, working through all possible keys. Most attempts will fail, but eventually one of the attempts will succeed and either allow the cracker into the system or permit the ciphertext (encrypted data) to be decrypted. Most commonly, brute force is applied to locate cryptographic keys and user passwords'* (Robotis and Tzouramanis, 2008: 136).

An averagely secured computer system will deny any further access from sources which incorrectly entered passwords several times. A well-chosen password policy can help to reduce the risk caused by a Brute-Force attack to close to zero.

Denial of Service (DoS) attacks are used mostly to deny access to certain websites. A DoS attack is '[...] an attack that overwhelms a cyberspace resource with requests so as to prevent authorized persons from using the resource' (Rowe and Custy, 2008: 96). If more than one computer is using a DoS attack against a particular target, it is called

Distributed Denial-of-Service (DDoS). This can be conducted by volunteers or by zombies or botnets[27].

> *'Botnets are networks of compromised, remotely controlled computer systems. So far, their main purposes include the distribution of spam e-mails, coordination of distributed denial-of-service attacks, and automated identity theft, for example credit card information and general banking data for financial fraud. Their presence is supported by the increasing global availability of broadband access to the Internet for network-enabled devices, which at the same time increases the value of the assets they threaten'* (Hogben, 2011: 4).

The owner of the botnet, the herder, can then direct all the zombified computers to attack one target. This attack is then called a DDoS attack which is more effective than a single DoS attack. DoS and DDoS attacks only temporarily harm and deny or disrupt services without altering or destroying anything. These attacks are very visible to the victim, but they need to have a well-equipped infrastructure to be able to withstand such an attack.

A Trojan horse is the digital equivalent to the ancient version used on Troy. It appears as a legitimate file which opens access to the computer system it was installed on. This access can be used then by the author of the Trojan horse. A 'special and universal Trojan horse is a specialised piece of code that is purpose built to attack a particular computer system in such a way that it allows the attacker unauthorised and universal access to the victim computer system' (Kiltz, Lang and Dittman, 2008: 156). A Trojan horse is tasked to stay on the computer undetected and to execute the commands of its controller.

[27] Zombies are computers that are controlled by someone else without the knowledge of the owner. Several zombies combined are called botnet, see Disterer, G., Alles, A. and Hervatin A. (2008) Denial-of-Service (DoS) Attacks: Prevention, Intrusion Detection, and Mitigation. In Janczewski, L. J. and Colarik, A. M. (Eds.) *Cyber Warfare and Cyber Terrorism*. Hershey and New York: IGI Global, pp. 254-272.

Viruses and worms are less targeted than rootkits or Trojan horses. They 'can be used to permanently destroy (erase) or corrupt (spoof) data and cause economic damage. In the worst case, these same software tools can be used to cause destructive failure in a critical infrastructure like air traffic control, power, or water systems, which can lead to casualties' (Zanini and Edwards, 2001: 45). While viruses have limited reach and are more likely to be used for vandalism and file corruption, worms spread quickly over networks by exploiting security vulnerabilities (TrendLabs Security Intelligence Blog, 2011). These tools normally try to cause damage immediately and are not tasked to stay *in the dark* [28].

A rootkit is a complex programme, and due to its deep rooting within computer systems, also referred to as advanced persistent threat (APT)(see figure 2). It is 'a set of programmes and code that allows a permanent or consistent, undetectable presence on a computer' (Enconado, 2011). Hogben defines a rootkit as 'a collection of tools that help developers prevent certain routines and processes from being detected or disabled' (Hogben, 2011: 13). Rootkits are difficult to detect and even more difficult to remove. Once a rootkit is installed on a system, the only way to clean the system is to re-install or install from a backup. APTs, however encompass much more than just rootkits. They include very sophisticated attacks, be it rootkits or other forms which are carried out by 'sophisticated, highly professional groups, perhaps organised by intelligence agencies or well-funded criminal gangs' (Graumann, 2012: 41).

Advanced Volatile Threats (AVT) have similar functions to APTs. However, they do not take 'root' in the target system. This non-rooting in the system leads to a higher immunity from detection but also to less persistent access to the victim's system. If an AVT is not hooked, therefore becoming an APT, every trace of it will be gone after the

[28] For an elaborate list of cyber attack/ hacking/ cracking tools, see Denning, D. E. (2000) *Information Warfare and Security*. Oxford: Association for Computer Machinery (ACM) Press.

next reboot of the system[29].While there are different standard weapons, attack vectors and even sophisticated combinations thereof, there is also a very sophisticated weapon including different attack vectors- the subversive multi-vector threat (SMT) (see figure 3) SMTs may contain any number of malicious software, APTs, AVTs, attack vectors and combinations thereof. They study the target's behaviour and are able to identify vulnerabilities for exploitation (Gragido and Pirc, 2011: 150). Gragido and Pirc, who did an exceptional analysis on SMTs described them as 'sinister in their elegance and again, as mentioned previously, their elegance is often achieved via their simplicity. They are efficient in utilizing and exploiting people, process, and technology [...]' (Gragido and Pirc, 2011: 149). The Olympic Games' tools, as discussed in chapter IV, can be regarded as SMTs.

3.3.3 Cyber Attack Vectors

In order for cyber weapons to reach their target system and be able to compromise it, there are three main ways – attack vectors[30] – how this can be achieved: social engineering, chipping, and exploitation of software‘s vulnerabilities.

Social engineering is not necessarily conducted via the use of code. It is a '[...] process and techniques involved in getting people to comply with one’s wishes and requests such that one is able to access unauthorized (usually sensitive) information' (Bhagyavati, 2008: 190) or simply put 'human elicitation a.k.a spying' (Winkler, 2007: 9). This can be achieved by a person calling someone else and asking for a password

[29] For more information on Advanced Volatile Threats, see Wilson, T. (2013) *Move Over, APTs -- The RAM-Based Advanced Volatile Threat Is Spinning Up Fast* [online], San Francisco: Dark Reading. Available: http://www.darkreading.com/advanced-threats/167901091/security/vulnerabilities/240149192/move-over-apts-the-ram-based-advanced-volatile-threat-is-spinning-up-fast.html/ [Accessed 17 March 2013].

[30] For a comprehensive technical description of attack vectors, see Elisan, C. C. (2013) *Malware, Rootkits & Botnets: A Beginner's Guide*. Columbus: McGraw-Hill, pp. 157-184.

while under the guise of the system administrator. However, social engineering can also include a legitimate seeming download link for an antivirus programme which is a rootkit in disguise, as in the Ghostnet incident (see sub-section 3.3.1).

Chipping is a process where the hardware itself is tinkered with. Hardware which is required to run a network or system (for example a network card or router) is inserted with a backdoor code included in its manufacture. This backdoor is almost impossible to find and trace. It can then be exploited by the one who inserted it while the device is in use.

Flaws in a software that the target a running system is another attack vector. This flaw in the software (also called bug or exploit), can then be exploited through directly accessing the system. Flaws in software can also be used when the user opens a certain website which is infected. In contrast to social engineering, the user does not have to do anything apart from opening the website. If the software in use is vulnerable to the exploit, the system is automatically infected.

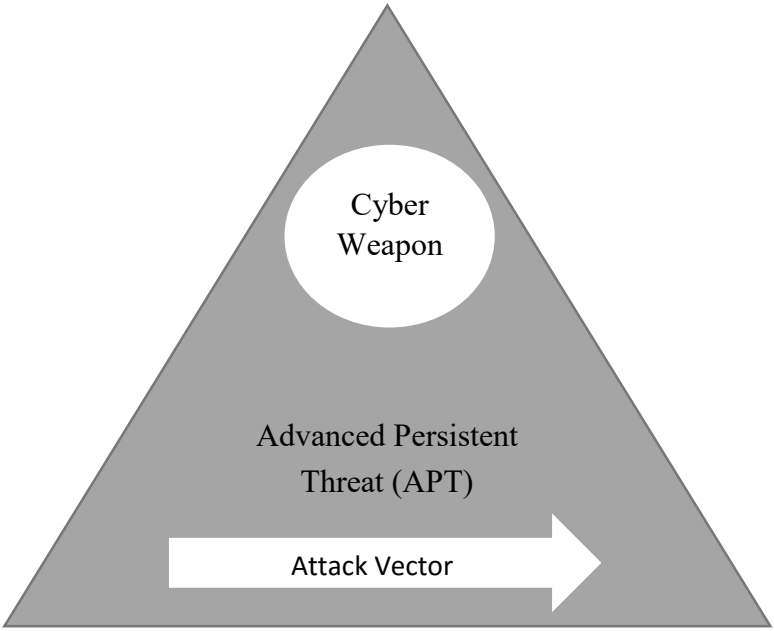

Figure 2

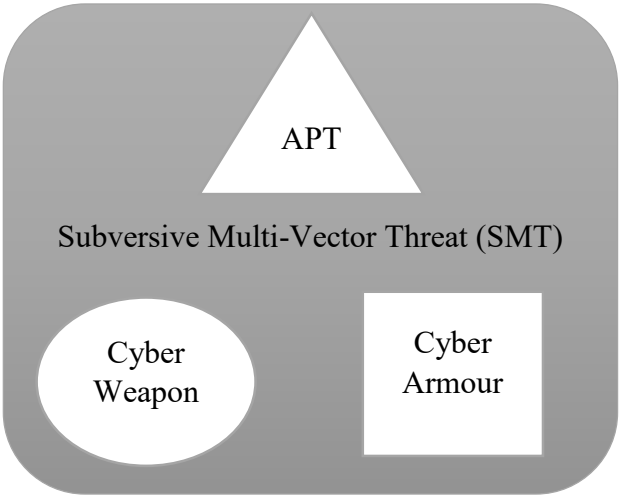

Figure 3

3.3.4 Cyber Armours

Cyber armour not only refers to certain pieces of hardware and/ or software but also to changes in behaviour in order to obstruct cyber weapons and defeat cyber attack vectors. Following the principle of defence-in-the-depth, cyber armour can either neutralize an attack vector (for example social engineering), or destroy the cyber weapon (as with anti-virus software) or even defend the target against the impact of a cyber weapon (for example, encryption). The following cyber armours do not establish an exclusive list of software, hardware and behaviours to defend against cyber attacks, but represent the most common types.

Sometimes referred to as *going dark*, disconnecting a network completely from other networks including the Internet might be a last resort in the heat of an attack or a viable solution for a classified network. A dark network operates like other networks, but does not offer any connection to networks, any wireless hotspots, and most importantly no options for employees etc. to plugin devices that enable connections to other networks to infect the system.

Anti-social engineering is not a software or a hardware, it is a particular form of situational awareness achieved through training. Social engineering relies on the *wetware* (the human) factor to succeed. Because it tricks users into installing malicious software or opening an email. At its root, the most straight forward means of dealing with the risk of social engineers is rigorous training to lessen and ultimately erase this risk. Social engineering can serve as a single point of entry which means that it can be used to deliver other attack vectors such as rootkits, Trojan horses or worms.

A honeypot is a tool which is not entirely defensive. It '[...] is a computer system whose only purpose is to collect data on trespassers' (Rowe, 2008: 103). It enables attackers to hit a system which has no other use than to collect data on how the attacker conducts his cyber operations. Therefore, it gathers valuable information on attack vectors and tactics of the enemy. The logs created by this tool can be used for further research. A firewall is a piece of software which can be installed on personal computers or on

servers. It is '[...] a collection of components placed between two networks that collectively have the following properties: All traffic from inside to outside, and vice-versa, must pass through the firewall. Only authorized traffic, as defined by the local security policy, will be allowed to pass. The firewall itself is immune to penetration' (Cheswick and Bellovin, 2004: 9). A firewall is vital. Additionally, it can be monitored by security personnel. This might already give a clue about the attack vectors and the origin of an attack. An Intrusion Detection System (IDS) or Deep Packet Inspection (DPI) scans and analyses the incoming traffic over the networks and searches them for potentially harmful content/ code (Clarke and Knake, 2010: 161-163, 191-193). It can be run on networks, but also centrally on the Tier 1 Internet Service Provider in order to cover all systems that are connected to this ISP. More advanced, the Intrusion Prevention System (IPS) is a software which scans the network for hostile behaviour and penetration attempts – like the IDS - and, if found, launches appropriate counter measures to this attack. It can be trained and configured in various ways (Skoudis, 2009b: 199). The latest attempts aim to developing tools that automatically detect and fix vulnerabilities (Cooney, 2013).

In order to deal with malware such as viruses, Trojan horses, worms and sometimes also rootkits, special software can be used. In general, this is called anti-virus software. 'Antivirus software is a computer programme that detects, prevents, and takes action to disarm or remove malicious software programmes, such as viruses and worms' (Microsoft Corporation, 2009). Anti-virus software only reacts. In order to find malware, malware has to be identified and put in the anti-virus database first by companies such as Microsoft. Until that point, it will rarely be found and disarmed. In case of a piece of malware is coded for a certain network or computer system, this software will not provide any meaningful defensive cover. As average security against existing threats, anti-virus software definitely belongs to the standard repertoire of security tools. Encryption uses algorithms to obfuscate data in a way that it can neither be reconstructed nor read. Only with the knowledge of the encryption algorithm and the password, can one reconstruct encrypted data. Encryption can be broken by BF attacks

and by the use of a Trojan horse. If the Trojan horse is tasked to log and transmit keystrokes, the password for the decryption is stolen[31]. Steganography[32] is similar to encryption. It does not obfuscate information or data, but is able to store data in a picture without being noticeable to the user. So even if the picture is obtained by an enemy, he would not know what he really obtained. It is rather deception, security through obscurity, than direct security[33].

Interestingly, cyber armour can also be used to shield malware from discovery or neutralisation. Modern, professional malware can utilize several tools and mechanisms (for example encryption) to hide itself, disguise itself as something else or bypass malware detection algorithms[34]. This kind of modification is especially useful for deception, for example in *sub rosa* operations or to infiltrate networks and stay dormant until a particular date or event triggers it. This serves as an example of how Luttwak's paradoxical logic (see chapter IV, *paradoxical logic*) might apply to the strategic dimension of cyber operations.

[31] For more information on encryption, see Curran, K., Smyth, N. and Mc Grory, B. (2008) Cryptography. In Janczewski, L. J. and Colarik, A. M. (Eds.) *Cyber Warfare and Cyber Terrorism*. Hershey and New York: IGI Global, pp. 57-64.

[32] For more information about steganography, see Markentin, M., Schmidt, M. B. and Bekkering, E. (2008) Steganography. In Janczewski, L. J. and Colarik, A. M. (Eds.) *Cyber Warfare and Cyber Terrorism*. Hershey and New York: IGI Global, pp. 50-56.

[33] For an elaborate list of cyber attack/ hacking/ cracking tools, see Denning, D. E. (2000) *Information Warfare and Security*. Oxford: Association for Computer Machinery (ACM) Press, pp. 345-396.

[34] For a comprehensive technical description and examples of armoured malware, see Elisan, C. C. (2013) *Malware, Rootkits & Botnets: A Beginner's Guide*. Columbus: McGraw-Hill, pp. 140-145.

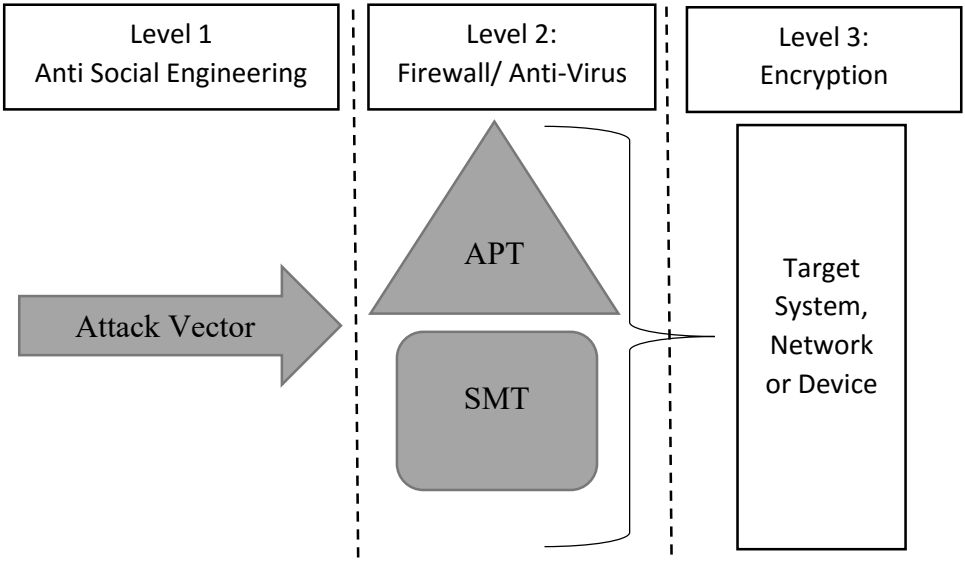

Figure 4[35]

3.4 Facets of Operations

3.4.1 Framework

Cyber operations, potentially combined with other operations, are channelled towards the successful implementation of a cyber strategy, leading to the achievement of political goals. Thus, one or more kinds of operations can be part of a cyber strategy. An example would be a deterrence strategy which includes denial and disruption operations. The intermediary aims of both kinds of operations are to demonstrate to the adversary what would happen should he attack. Those aims coerce the adversary away from taking action, hence achieving the strategic goal of deterrence. The operations themselves vary by the demands of the strategies chosen, and the political objectives which limit and define the scope of the strategy itself. Within this framework, cyber operations may apply one or more combinations of subversive multi-vector threats,

[35] The countermeasures mentioned in the levels 1-3 are just samples for each stage, therefore do not establish a conclusive list.

cyber weapons and attack vectors to achieve their aim. Cyber operations can be regarded as the operational level of a cyber strategy, and thus as the offensive equivalent of cyber security pillars (see chapter III). Taking into account the specifics of cyber weapons (see section 3.3), and the general strategic discussion of cyber operations (see section 7.2), it can be assumed that cyber operations need to prioritise adaptation to the adversary's environment, rather than a focus on their own capabilities. As Libicki puts it: 'the attacker's strategy is hostage to the target's behavior' (Libicki, 2009b: 9). As the subsequent discussion shows, cyber operations can be identified by the means they are applying and by their inherent objectives. Therefore, this section discusses the different cyber operations according to their objectives, categorized by the intensity level of the respective operation, starting with the lowest level.

Different cyber operations are discussed in the literature, most of the time mistaken for strategies. In general, cyber operations aim at lines of communication, intelligence gathering and critical infrastructure (Stiennon, 2010: 75). Libicki states that operational objectives can be: deception, disruption, corruption, eruption (Libicki, 2009: 143-149) as well as denial (Libicki, 2007: 80-81) and the creation of errors. Andrees and Winterfield state in regard to computer network attacks that, 'actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves' (Andrees and Winterfield, 2011: 167). Gardner adds the theft of information to this list (Gardner, 2009: 27-29). With respect to achieving cyber dominance, Hughes refers to the objectives detection, deterrence, deception, disruption, defence, denial and defeat (Hughes, 2007: 22). Thus, aims of cyber operations commonly stated are: *detection, defence, deterrence, deception, theft, denial, disruption and corruption, degradation, destruction.* While detection and defence operations are discussed in the chapter on national cyber security (chapter III), deterrence is treated as a full-fledged strategy consisting of operational level coordination of several tactical actions (see sub-section 7.2.5). Subsequently, the operations discussed in this section are deception of the

adversary, denial of services, extraction of information, and disruption of services and degradation of information.

3.4.2 Deception Operations

Deception is described by Shimeall *et al*. as '[...] to increase the "fog of war" for the enemy and to reduce it for one's own forces' (Shimeall, *et al.*2002: 17). The term *fog of war* at this point is very bold. Deception is about increasing one's own knowledge about the adversarial systems, networks and actions while decreasing the opponent's knowledge about one's infrastructure and intentions. Deception of the enemy does not necessarily improve knowledge about the adversarial systems and other details *per se*. It can be applied in the sense that an adversary is goaded into action in order to test its response. Based on their response weakness can be deduced. With this knowledge, more sophisticated attacks can then be developed. However, the main focus for deception operations is to decrease the adversary's knowledge and to distracting him. These operations can be implemented by the use of various cyber weapons. Deception aims to attract an adversary's response and resources while another, stealthier, operation can be carried out against the target system without detection.

One operational pattern for deception is to conduct (distributed) denial-of-service attacks. Those attacks are to be targeted against a CNII which relies on the online delivery of services or information. An example for this would be a server which is used for electronic voting during an election. The server can be attacked with denial-of-service attacks, and in the case of success, the whole election would be thrown into chaos. In order to prevent this from happening, resources are diverted to protecting the system. While the resources are diverted other attacks can be launched against another target which cannot access the resources bound in the deceiving operation. A deception operation usually implements other operations such as denial, not to achieve the intermediate goal of denial, but the intermediate goal of distraction and deception. Another, more widely known deception operation is to avoid proper attribution by the adversary through co-opting third party systems. The operation takes over systems in

another country and deletes the evidence that those systems have been compromised. Those systems can then be used to launch other operations against an adversary. When tracking back the origin of the attack, the adversary will be led to the third party's system – which had been compromised during the deceiving operation. One case which illustrates this kind of operations was the 1994 Rome Lab's Incident (see section 3.5).

3.4.3 Denial Operations

Denial-of-service operations refer to an attack pattern which floods the target system or network with bogus requests. The immense amount of bogus requests prevents legitimate requests from reaching the target system or network and therefore effectively takes it off the grid. This operation usually applies cyber weaponry with the same name, called distributed- or denial-of-service tools. As shown above, denial-of-service operations can be well-connected to deception operations. Usually, denial-of-service attacks are launched from numerous attacking systems against the adversary's system. The attacker compromises target systems (called *bots* or *zombies* or *bro's*) from which those attacks are launched but are controlled by the original attacker. The inherent deception is a side-effect, but the main reason behind this pattern is that denial-of-service needs bandwidth and different systems; otherwise it is too easily rendered useless by the target. Denial operations can be directed against a range of targets including websites, email servers and databases. The timeline in section 3.5 and the appendix shows, in reference to the *First Cyber War*, the attacks against Estonia in 2007, the impact a denial operation can have when directed against several targets in the same state, if the latter relies heavily on the accessibility of its information infrastructure.

3.4.4 Extraction Operations

The *extraction* operation refers to both the interception of communications within networks, and the theft of information from systems. For the attack pattern to be successful, it can use several subversive multi-vector threats and advanced persistent threats. The aim is not only to extract information but to generate the capacity to

perpetually do so at any time. Therefore, the weapons used in extraction operations have to stay hidden and extract information over a period of time. This is especially important for the interception of communications. Extraction operations can be linked to deception operations. In order to obfuscate tracks and decrease the risk of proper attribution of the attack, the attacker might co-opt a third party system. After the target system has been compromised, the information would be extracted and uploaded to a third party system which had been compromised. The information is then downloaded from the third party system and the evidence erased. When tracking the incident, the adversary would be able to trace the attack back to the third party system only. Extraction operations might aim at different kinds of information such as pictures, videos, maps, passwords and account names, as well as captures of audio-video equipment attached to the compromised systems and networks. The latter could include switching on web cameras attached to a compromised system and recording (as well as later on extracting) the video feed. The 1998 Moonlight Maze as well as the 2009 Ghostnet incident represents an extraction operation (see section 3.5).

3.4.5 Disruption Operations

Disruption operations aim to change or slow processes, hence impacting services for some time. Thereby, disruption operations might cause a physical impact. Disruption has been identified as the one of the most significant operations Clarke and Knake, 'it refers to actions by a state to penetrate another nation's computers or networks for the purposes of causing damage or disruption' (Clarke and Knake, 2010: 6). Brows supports this view when, in reference to the term information warfare, it 'will aim at reducing an adversary to the equivalent of an Industrial Age power – to eliminate his ability to collect, process, store and disseminate information' (Brown, 1996: 43). It is also sometimes referred to as weapons of mass disruption (see Andrees and Winterfield, 2011: 8).

Disruption operations can rely completely on the output of an extraction operation. In this case, the extraction operation would provide vital information for the disruption

operation on the way and nature of cyber weapons it uses. Disruption operations can be easily mistaken for denial operations. Denial, to return to our knife analogy, is blunt; disruption on the other hand is closer to a scalpel. It can be targeted at services deep down in adversary's systems and networks, taking out specific services or changing the way they operate. If the target system or network can be accessed remotely, the weapons used usually try to reach and compromise the target system and then wait for commands of the attacker to be carried out. However, in systems which cannot be accessed remotely (because they are air-gaped for example), more sophisticated weapons are needed (such as subversive multi-vector threats) which, once the target system is compromised, automatically disrupt services following a programmed pattern. A good example for a disruption operation, utilizing a subversive multi-vector threat and relying on a prior extraction operation is the Stuxnet operation in the Olympic Games case study (see section 8).

3.4.6 Degradation Operations

The term degradation, as opposed to destruction, has been chosen to avoid misconceptions about the direct physical impact of operations. As for the operations described in this research, the disruption operation is the only one that can have direct physical impact, for example in destroying hardware. The name of the operation always refers to the virtual aim and impact of it. Therefore, degradation operations aim to degrade and destroy information and data. It does not refer to the destruction of physical items – this would more likely fall in the category of electromagnetic warfare.

Degradation operations can be linked to deception operations. In order to erase tracks, degradation operations might aim to destroy a third party system. This would be the role of a degradation operation. In this framework, degradation operations can also be linked to extraction and operations (after they are completed) in order to cover tracks through the wiping of all data for the respective systems. Degradation operations can use different kinds of cyber weapons. Similar to extraction and disruption operations, the most important aspect is the attack vector – to get the cyber weapons to the place where

they can be used. An example for a degradation operation is the 2012 Shamoon case (see Jeffers, 2012).

3.5 History of Cyber Operations

3.5.1 Timeline of Events

To fully grasp the extent of cyber operations, it is useful to look at the historical progress of the field. This part of the research delivers the historical context to understand cyber operations. This section compiles some of the most intense cyber incidents and cyber attacks. All events mentioned here are commonly regarded as major incidents of cyber attacks in academic discourse. A more comprehensive list can be found in the appendix. The second part of this section gives short accounts on some of those incidents and attacks to illustrate them further. The incidents were selected for the sample insofar as they can be distinguished from one another in their nature. These differences are explained in the penultimate part of this section. The last section traces and analyses the evolution of cyber attacks based on those events.

Important cyber incidents and attacks include: the 1994 *Rome Labs Incident* (IEEE Computer Society's Technical Committee on Security and Privacy, 2011), the 1998 operation *Moonlight Maze* (Public Broadcasting Service, 2003), the 1998 operation *Solar Sunrise* (Cordesmann 2000), 2001 *Code Red* (Public Broadcasting Service, 2003), 2003 *Titan Rain* (Clarke and Knake, 2010), the 2007 *First Cyberwar in Estonia* (Bronk, 2008), 2009 *Aurora* (Andrees and Winterfield, 2011), the 2010 operation *Olympic Games* (Sanger, 2012), the 2012 operation *Red October* (Global Research & Analysis Team, 2013c), the 2013 activities of the *Comment Crew* (MANDIANT, 2013) as well the activities of the American *National Security Agency* (The Guardian, 2013) and the 2014 operations *Careto* (Global Research & Analysis Team, 2014b), *Uroburos* (G DATA SecurityLabs, 2014), *Ke3chang* (Villeneuve *et al.*, 2014) and *Equation* (Global Research & Analysis Team, 2015a),.

3.5.2 Early Developments of Cyber Operations

The following describes briefly some of the well-known cyber attacks since the 1990's: the Rome Labs Incident, Moonlight Maze and the Cyber War in Estonia. Chapter IV includes a dedicated case study of the latest development stage of cyber operations, namely the Olympic Games campaign. The described events give perspective of the different ways through which cyber operations has been conducted over time.

In spring of 1994, two hackers, calling themselves *Datastream Cowboy* and *Kuji* breached security measures at the Rome Air Development Center, New York. While Datastream Cowboy, a 16-year old teenager from the United Kingdom was apprehended, the real person behind Kuji – and with him the stolen data - has never been discovered. Not counting the expenses for the apprehension of Datastream Cowboy, the damage has been estimated around $500,000 (Billo and Chang, 2004: 128-129). The Rome Lab network has been compromised and wire-tapped by these hackers. Subsequently, the hackers used the Rome Labs computer system as a platform from which to launch attacks against other infrastructures such as the headquarters of the NATO and a Southern Korean Atomic Research Institute (Cordesmann, 2000: 62-64). A distinct feature of this act of cyber operations is that it took only two hackers to compromise the Air Force's whole computer system with only an exploit and a wire-tapping programme. Another distinct feature is that during the times when tensions between the United States and North Korea where high due to the research on nuclear weapons, it appeared as if a United States Air Force computer system would attack a Korean atomic research institute. In the beginning it was unclear if the research institute was from North or South Korea. Subsequently, this attack could have had severe consequences to the diplomatic relations between North Korea and the United States.

While a lot of information about this incident has still not disclosed to the public, it is clear that hackers broke into the systems of the Department of Defense of the United States, the Energy Department's nuclear weapons research laboratory and NASA among other facilities. Only unclassified information was stolen (Cordesmann, 2000: 59-60).

Stolen information included maps of military installations and troop configurations among others (Public Broadcasting Service, 2003). The attacks could be traced back to a Russian Internet Service Provider near Moscow which is closely connected to the Russian Academy of Science. Analysing the attacks, law enforcement found out that the attacks mainly took place between 8 am and 5 pm Russian time – during Russian working hours (Cordesmann, 200: 61). These hacks had been going on for almost two years (Public Broadcasting Service, 2003). In contrast to the Rome Labs Incident, vital information for national security - such as the whereabouts of military installations - was targeted. Tracing the attacks back to an institution which has close ties to a foreign country added to the precarious situation. Russia denied any involvement in the attacks

In 2007, an event took place which is often described as the *First Cyberwar*. Estonian government officials wanted to relocate a Soviet World War II memorial. As the diplomatic tensions rose, cyber operations were conducted targeting the CNII, including websites of banks, the government ministries and newspapers (Schneier, 2009 and Malawer, 2010). Here, it is important to acknowledge that Estonia is the most-wired country in Europe – if not worldwide (Richardson, 2009). If a cyber attack can cripple the CNII of a country, then Estonia would be among the most vulnerable. While the attacks could be traced back to stakeholders, mainly inside Estonia, no direct involvement of Russia could be proved. The Estonian sites were attacked for almost three weeks using Denial-of-Service attacks and subsequently 'effectively shutting [it] off […] from the rest of the world' (Richardson, 2009). The extensive use and reliance on information- and communication infrastructure made Estonia particularly vulnerable to cyber attacks. Estonia was, and is spearheading different IT projects, including e-governance. Unable to access governmental websites, citizens of Estonia were also unable to access e-government services. Additionally, the incident not only impacted Estonia, but also NATO. Colarik and Janczweski state that:

> *'Estonia is a NATO and EU member and member states have offered help. Computer security experts converged on Tallinn to offer assistance and to learn what they can about cyber war in the digital age. For NATO, the attack*

> *may lead to a discussion of whether it needs to modify its policies related to collective defense of the North Atlantic Treaty Organization member states'* (Janczweski and Colarik, 2008: 478).

In an event of an attack, NATO members support each other. While the NATO did not reach any decisions until the attacks against Estonia were over, it was naturally part of its agenda in the aftermath. In 2009, a network of compromised computers was discovered. The so-called *Ghostnet* included over 1300 computers in several countries targeting organizations which dealt with Tibet (Clarke and Knake, 2010: 58-62). The team that investigated this incident concluded that there is 'documented evidence of a cyber espionage network that *compromise*d government, business, and academic computer systems in India, the Office of the Dalai Lama, and the United Nations' (Information Warfare Monitor and Shadowserver Foundation, 2010: IV)[36]. Ghostnet, and the theft of classified information about the Grand Strategy of Tibet and its allies, has been attributed to the People's Republic of China. The investigating team states that:

> *'[c]learly this investigation and our analysis tracks back directly to the PRC, and to known entities within the criminal underground of the PRC. There is also an obvious correlation to be drawn between the victims, the nature of the documents stolen, and the strategic interests of the Chinese state [...] but we have no evidence to prove that assertion'* (Information Warfare Monitor and Shadowserver Foundation, 2010: 40).

As data has been altered in order to obtain those information and classified information which could have caused political impact has been stolen, this incident clearly marks a new development in cyber operations and aligns the focus on espionage and theft of

[36] For the technical details of the Ghostnet as well as of the counter-operation, see Information Warfare Monitor and Shadowserver Foundation (2010) *Shadows in the Cloud: Investigating Cyber Espionage 2.0, Joint Report of the Information Warfare Monitor and the Shadowserver Foundation (JR03-2010)*. Ottawa: The SecDev Group, pp. 12 -21.

information within the framework of political power and harming other political entities - though Tibet does not currently constitute a sovereign state.

The Olympic Games along with Red October, Careto and the other published operations of the National Security Agency (NSA) and its allies, form another milestone in the development of cyber operations. Chapter IV presents a case study on Olympic Games as cyber operations campaign to illustrate the most recent step in cyber operations evolution.

3.5.3 Evolution of Cyber Operations

A distinction can be made between different stages of cyber operations. The first stage of events is solely focused on the theft of information. Cyber operations have been conducted against the CNII and thus following the pattern of cyber attacks which qualifies them cyber operations. However, damage has been avoided in the main. The primary aim was data theft of vital information of the respective state caused *inter alia* by alteration of data, and occurred roughly between 1994 and 1998. The second category mainly focuses on attacks against the website of the adversary in order to leave a message there or to deface the website. An exemption should be made here for the Internet Black Tigers, which used email bombs against the information infrastructure of NATO. This category can be dated to 1998-2001. The last category includes the aforementioned strategies but adds the attempted shutdown of CNII systems. The best-known example are the cyber operations against Estonia in 2007. It should also be noted that the attack methods became more sophisticated and stealthier over time (Rhodes, 2001). The latter is particularly obvious when regarding cyber attacks after 2007 – particularly with the Ghostnet in 2009. The events in Estonia can be regarded as direct act of aggression – sending data to block vital services. It is not necessarily stealthy even though the problem of attribution remains. The Ghostnet and similar attacks demonstrate sophistication and stealth compared with earlier attacks. The aim was not to block services but to gain access to as much information as possible without arousing suspicion – which is the opposite of what the attacks on Estonia aimed at. The growing

use and sophistication of information- and communication technologies might be the main reason for these developments. The development surpassed acts of cyber civil disobedience and small scale information gathering, and eventually reached a complete DoS attacks against an entire CNII and highly sophisticated espionage attacks. It is the time of advanced persistent threats or as Graumann puts it: 'cloak-and-dagger' warfare (Graumann, 2012: 41).

4. Information Operations

4.1 Framework

After establishing the definition of cyber operations, its elements and its indicators, there is one final de-construction of the term needed in order to arrive at the strategic implications of cyber operations, and that is to further narrow it to identify and isolate cyber operations in the field of *information warfare*. Information warfare is an umbrella term for different kinds of operations using or relying on information, including cyber operations. The United States' army has stopped using the term information warfare. It has been renamed *information operations* though it is not clear as to why the terminology has been adapted (Kuehl and Armistead, 2007: 11). This paper will adapt this terminology as it seems more fitting (compare to the discussion in 3.1), even though most sources still refer to it as information warfare (IW). The following section first defines information operations in general and then examines all the areas that are subsumed under their umbrella. The last paragraph deals with the blurred areas of information operations which can be mistaken as cyber operations and are not clearly distinguished in many works. This paragraph constitutes the core of this section: the identification of cyber operations and their distinction from other kinds of similar activities subsumed under the information operations umbrella. In order to be able to distinguish one kind of operations from the other, this section identified similar kinds of operations and matched them with the indicators for the definition of cyber operations, which has been developed in the previous section. This method of matching will highlight the demarcation within information operations.

4.2 Nature of Information Operations

Several authors already contributed to the vast definition of information operations. For instance, Campen states that 'Information Warfare, in much larger construct, merges the miracles of modern information technology to an ancient strategy of victory without violence. Here information is a weapon and target onto itself: not just magnifier for physical forces engaged in traditional, legal wars' (Campen, 1996: 253). On the other

hand, Knecht sees it as 'the preparation for and use of physical or logic-based weapons to disrupt or destroy information and information systems in order to degrade or disrupt a function(s) that depend upon the information or information systems' (Knecht, 1996: 165) while Curran *et al.* highlight the method of transport, stating that 'IW [Information Warfare] can be seen as societal-level conflict waged, in part, through the worldwide interconnected means of information and communication' (Curran et al., 2008: 6). Denning stresses the platforms for information operations, while stating that 'it [information warfare] encompasses information in any form and transmitted over every media, from people and their physical environments to print to the telephone to radio and TV to computer networks' (Denning, 2000: 12). All of the authors acknowledge that information operations use (Webster, 2003: 101-106) and target information (Brown, 1996: 43 and Hutchinson, 2006: 213).

The destructive potential of information operations targets the information, and the information systems of the adversary in order to affect the decision-making processes and eventually generate strategic advantage (Yoshihara, 2001: 4 and Libicki, 2007: 20-24). Influencing the decision-making processes can be done in different ways, all which constitute individual streams within information warfare. Some of the streams include: eavesdropping, chipping, psychological operations or high frequency weapons (HERF) (Schwartau, 1996: 245). From a strategic perspective, information warfare is thought of as a continuous, simultaneous, accelerated and non-linear form of warfare (Dearth and Williamson, 1996: 23-24), carried out by ‘knowledge warriors’ in order to fight a 'clean war' in a 'post-heroic setting' (Webster, 2003: 103) whereby 'knowledge becomes the core of military power and the central resource of destructivity, rather than brute force' (Campen et al., 1996: 1).

It can be derived from the above mentioned definitions, that every form of information operations needs a platform (such as networks, television, radio etc.), that can be either physical or virtual, targets people, societies or governments, and either disrupts and alters, or propagates the flow of information. In order to distinguish one kind of

information operations from the other, the following indicators will serve as a useful scorecard:

1. the platform the operations are carried out on,
2. the means they are carried out with,
3. the target(s), and
4. the aim of the operation.

4.3 Under the Umbrella of Information Operations

Before referring to various authors to highlight the different forms of operations, there is a need to clarify one aspect. The term cyber operations has been used interchangeably with different names. Terms used sometimes synonymously are: computer network operations (CNO), computer network attacks (CNA), computer network defense (CND), computer network exploitation (CNE), hacker warfare, digital warfare and cyber warfare (Siegel, 2007: 27; Kuehl and Armistead, 2007: 10 and Zimet and Barry, 2009). They ought to refer to the same concept, but for reasons of clarity and consistency, this this paper will use the term cyber operations throughout (see section 3).

On the other hand, depending on the author, there are different terms categorised under information operations. Libicki lists command and control warfare, intelligence-based warfare, electronic warfare, psychological warfare, hacker warfare (CNO) and economic information warfare (Libicki, 2007: 16-17). Yoshihara defines American information warfare as kinetic attacks, electronic warfare, computer network attack, military deception, psychological operations and operations security (Yoshihara, 2001: 4-18). Kuehl lists psychological operations, military deception, operational security, electronic warfare and computer network operations (Kuehl, 2007: 1) while Wilson simply names information warfare, cyber warfare and net warfare (Wilson, 2004: I). Zimet and Barry distinguish between information operations (IO), which is the umbrella of electromagnetic warfare (EW), and computer network operations (CNO) amongst others where the latter is the umbrella of computer network attack (CNA), computer

network defense (CND) and computer network exploitation (CNE) (Zimet and Barry, 2009: 291-293). Additionally, one of the key works which is vital for cyber operations was Arquilla and Ronfeldt's 1996 *Networks and Netwars*. The network warfare – or network centric warfare (NCW) - mentioned in this work has – to a large degree – nothing directly to do with cyber warfare or cyber operations, though the opposite is often claimed (Arquilla and Ronfeldt, 1996 and Zimet and Barry, 2009: 291-293). The *network* in network centric warfare refers to an organizational form rather than to computer networks as parts of the cyber domain in which cyber operations are carried out, something which is explained in more detail in section 4.4.

Of all the activities mentioned, most of the confusion with cyber operations arises with the terms electronic warfare and network. Therefore, in this section, these two forms of information operations will be matched to the indicators mentioned. The results then will be compared to the results of cyber operations when the same indicators are applied. This will sketch a clearer picture of cyber operations and its distinction from other forms of information operations in order to be able to work with a concise definition later on. It is important to note that distinction from other forms of information operations was not deemed necessary.

4.4 Cyber, Electronic and Network Warfare

As defined in sub-section 3.1, cyber operations are *the targeted use and hack of digital code by any individual, group, organization or state using digital networks, systems and connected devices, which is directed against Critical National Information Infrastructure in order to steal, alter, destroy information or disrupt and deny functionality with the ultimate aim to weaken and/ or harm a targeted political unit.* This definition will be used in comparison to electronic warfare and network warfare, and therefore represents cyber operations, cyber warfare, computer network operations (including computer network attack, computer network defence and computer network exploitation), hacker warfare and digital warfare.

Andrees and Winterfield state that electronic warfare relies on and influences the physical world and is therefore similar to cyber operations (Andrees and Winterfield: 168). Without clearly distinguishing between cyber operations and electronic warfare, the authors attribute chipping to this area (Andrees and Winterfield: 169). Kuehl and Armistead state that cyber operations rely on the electromagnetic spectrum as battle space (Kuehl and Armistead, 2007: 10). Denning and Libicki clearly state that electromagnetic pulse attacks (EMP) are physical and count as electronic warfare (Denning, 2000: 152-153 and Libicki, 2007: 29). EMP refers to 'creating directed energy electromagnetic pulses to disrupt or destroy targeted military computer hardware or networks' (Wilson, 2004: 2-3). Wilson states that 'Electronic Warfare defined as any military action involving the direction or control of electromagnetic spectrum energy to deceive or attack the enemy' (Wilson, 2004: 5). The main difference between electronic warfare and cyber operations is the direct reliance on and use of the physical world and computer hardware, rather than the virtual world and computer software. To highlight the difference, take the task of destroying information which is stored on a hard disc device. Destroying the information on the device via electronic warfare would mean to target it with an EMP. Destroying the hard disc via cyber operations would require access to the computer, via a computer network or device and the insertion of malicious code.

A broad definition of what network warfare is – in particular in connection to cyber operations – is given by Hubbard. The author says that '[n]etwork warfare (NW) operations are the integrated planning and employment of military capabilities to achieve desired effects across the digital battle space in support of operational objectives. Network attack and network defences are operational elements of NW operations' (Hubbard, 2007: 47). This definition focuses on the network character, but does not distinctively differ from the definition of cyber operations. Arquilla and Ronfeldt deliver a concise and inclusive definition. They state that

> *'[...] the term netwar refers to an emerging mode of conflict (and crime) at societal levels, short of traditional military warfare, in which the protagonists*

> *use network forms of organization and related doctrines, strategies, and technologies attuned to the information age. These protagonists are likely to consist of dispersed organizations, small groups, and individuals who communicate, coordinate, and conduct their campaigns in an internetted manner, often without a precise central command'* (Arquilla and Ronfeldt, 2001: 6).

Arquilla and Ronfeldt, as well as Ahrari, highlight that the *term network* refers to the organizational structure of this form of warfare, and not to the battle space it is carried out in (Ahrari, 1997: 1170 and Arquilla and Ronfeldt, 2001: 8-10). Fritz puts this observation simply, network warfare 'seeks to translate an information advantage [⋯] into a military advantage through networking of well informed, geographically-dispersed forces' (Fritz, 2008: 40). Weber even concludes that network warfare is not limited to military use only (Weber, 2004: 11). Some empirical examples of network warfare (military and non-military) are mentioned by Armond and Fritz. Armond (2001) describes the tactics used by networked protesters. Fritz gives a brief overview of how network warfare was used during the last wars which were fought by the United States military (Fritz, 2008: 28). Thus, network warfare is clearly distinct from cyber operations. While network warfare refers to the use of information technologies for structural and organizational advantages, cyber operations use those technologies as platform for attacks. While clearly distinct, it is possible that a group of stakeholders planning to conduct cyber operations is organized and communicates through a pattern that relies on network warfare. Though both forms of warfare are distinct from each other, they are not mutually exclusive.

4.5 Demarcation Lines

The platforms used in cyber operations are digital networks, systems and connected devices. These can be copper or optic fibre cables as well radio frequencies (wireless, bluetooth, and mobile phone standards) and satellite connections. In sum, it uses the electromagnetic spectrum as a platform. The means which are used to carry out cyber

operations are virtual or software. This can be complex programmes, or just commands typed into a computer console. The target of cyber operations is information. Everything which can be accessed by the means mentioned above through the electromagnetic spectrum consists of 1's and 0's – computer code – and is therefore information. Even when a computer system is manipulated so that a dam goes haywire, opens and floods an entire city, the target remains information. The aim of cyber operations is theft, degradation, and alteration of information as well as disruption or denial of information flow. The ultimate aim is to achieve policy objectives is similar in all kinds of warfare and therefore does not help to differentiate them from one another.

The platform for electronic warfare is either computer hardware (through chipping), or radio frequency for HERF and EMP attacks. Though physical components are involved, it eventually uses the electromagnetic spectrum as a platform. The means to carry out electronic warfare are electronic gadgets and hardware in general. This can reach from a small bug which is connected to a router and inserts bogus code at will, to a nuclear bomb detonated 20 – 40 km's above the surface (Federation of American Scientists, 1998). The targets of electronic warfare are all electronic devices including computers, cell phones, and factory systems controlled by computer, military Command, Control, Communications, Computers & Intelligence (C4I). The aim of electronic warfare is to disrupt or deny functioning of electronic devices or to destroy them.

The platform for network warfare can be virtually anything which connects different stakeholders. It can be the Internet, which includes the entire electromagnetic spectrum, and can also be meetings in coffee shops or similar. The means of network warfare is to share information to ultimately increase the efficiency of whatever other form of operations is also applied. Within the network of army troops for example, the units share information which each other. The target of network warfare is the organizational structure and information distribution systems. The aim of network warfare is to empower other forms of operations.

After applying the indicators to the terms cyber operations, electronic warfare and network warfare, all within the field information operations, it is now clearer that

network warfare is distinctively different from cyber operations and electronic warfare. Network warfare refers to an organizational structure which facilitates information distribution and communication, and not to offensive actions. Electronic warfare and cyber operations, on the other hand have more common denominators than network warfare. However similar they are though, these forms of warfare are different. While both forms of warfare rely on the electromagnetic spectrum to carry out attacks, cyber operations rely on software. Meanwhile, electronic warfare relies on hardware to conduct warfare. Electronic warfare targets hardware and can destroy, alter, disrupt or deny functionality and through it, affect information. Cyber operations, on the other hand, target information directly and can steal, degrade, alter, disrupt or deny hardware functionality through changing information. While network warfare is an organizational form and electronic warfare uses hardware to affect hardware, cyber operations apply software in order to affect software, which in turn can ultimately affect hardware.

CHAPTER III

5. Cyber Security

5.1 National Security

Chapter I defined the state and its representation in the cyber domain through its CNII. The discussion on national security will serve as a basis for the overall cyber security framework, which aims at securing the CNII, and thus the state itself. Chapter IV will further examine the integration of cyber security into cyber strategies. The following section discusses and defines the term *National Security Strategy* (NSS). NSS is a fairly new term in the literature- only coined in the past two decades, and perhaps obviously drawing on the idea of *national security* (Bush, 2002 and Cabinet Office, 2008). To understand the scope of a NSS, a basic understanding of national security is needed. National security as a concept has been mentioned early in history, Confucius was among the first (Sosmeňa, 2009: 84-86). At least in the western hemisphere, *national security* has been discussed more thoroughly since the Peace Treaty of Westphalia in 1648 (Del Rosso, 1995). The term has been coined by then Secretary of the United States Navy, James Forrestal during the 1940's (Del Rosso, 1995: 184). The basic principle of national security is described as the duty of the state to protect its borders and citizens (Bush, 2002 and Ripsman and Paul, 2005). However, the duty to keep one's own state safe might be interpreted in a broader sense - 'national security may be both, an end and a means' (Sosmeňa, 2009: 85). Bush argues that ending tyranny in the world, promoting democratic states, fighting terrorism and advancing freedom, are part of national security (Bush, 2006: 1-7). The protection of borders therefore, could conceivably take place outside of these borders. The former German minister of defence raised this principle when he stated that 'die Sicherheit Deutschlands wird auch am Hindukusch verteidigt'[37] (Struck, 2002). Linking to the chapter on the state, national security relies on the three essential pillars of a state: territory, people and monopoly of

[37] From the German: *Germany's security is also being upheld at the Hindukush.*

power. According to the aforementioned, national security means to protect the integrity of the territory. Secondly, national security means to protect its citizens. All of this is done via the state and its monopoly of power.

The scope and definition of national security evolved over the past 400 years. However, it was in the 20th century that national security discussions have been turned into a turf war between two schools of thought. Some influential authors (Waltz, 1979 and Morgenthau, 1985) argued that though there are more recent threats to national security and actors in the security sphere, the state is still the single most important entity through which to maintain peace and establish national security. This schools' focus on physical/ military security of the state, it is regarded as the vital point for national security. Other threats to the state in this school of thought can include: 'non-military phenomena as environmental degradation, migration, narcotics trafficking, AIDS, and global population growth' (Del Rosso, 1995: 176). On the other hand, several authors (Mathews, 1997; Mandel, 1994 and Klare, 2001) argues that these threats cannot be tackled by single states or organisations any more. The interconnectedness of states and other entities, as well as the nature of these *new threats* demands collective action. States can only provide national security when partnering with other states and organisations. A study by Ripsman and Paul (Ripsman and Paul, 2005) has shown that neither one school nor the other has the upper hand. It depends on the specific circumstances – involving threat and stability of region and state – which approach would suit the demands of the unique state.

The term *National Security Strategy* is currently only used in Anglo-American countries. While, for example, the leading German party suggested a National Security Strategy in 2008 (Röttgen and Koschyk, 2008), it has not been implemented as such. In these countries, NSS has formerly been known as defence policy; though there are distinct differences (compare for example Bush, 2006 and Cabinet Office, 2008). Defence policy in this way has been subsumed within the NSS. However, the NSS offers a broader perspective (see figure 5). The term *Defence Policy Paper* or similar is still prevalent in other countries in the world like China (China, 2002 and Bolt and Gray,

2007). Subsequently, discussing the definition of NSS refers mainly to the NSS of the United States (Bush, 2002 and 2006 and Obama, 2010) and the United Kingdom (Cabinet Office, 2008 and HM Government, 2010). A brief definition is given in the UK NSS:

> *'[…] like any strategy, must be a combination of ends (what we are seeking to achieve), ways (the ways by which we seek to achieve those ends) and means (the resources we can devote to achieving the ends)'* (HM Government, 2010: 10).

Though distinctive in scope, these NSS address the same three issues. First, these strategies outline objects of national security that have to be protected, such as borders, citizens, economy, human rights and democracy. Secondly, challenges and threats to these objects are stated in the NSS. Lastly, counter-measures to oppose those threats are suggested. These NSS also follow both schools of thought. With respect to the unique challenge, they either address threats as a single state, or together with partners via collective actions.

There are three distinctive issues which form the pillars on which a NSS is built. The first, the core values of the respective state. For the US, UK and German cases those values are the protection of human rights and dignity, and the promotion of democracy around the world (for example Bush, 2006: 3-7). The second pillar which forms a NSS is composed of national duties. National duties are those duties a state owes to itself and its citizens. These duties include the safety of citizens and protection of national borders (for examples Bush, 2002: 6 and Obama, 2010: 9). The last pillar is composed of duties arising from the international involvement of the state. A member of the North Atlantic Treaty Organization (NATO) might have to participate in certain conflicts due to its involvement with NATO. Therefore, the NSS has to cover all challenges arising from it. While security is coined as a broad term, the membership of the European Union (EU) might result in the adoption of certain economic policies to the NSS (for example Röttgen and Koschyk, 2008: 3 and Cabinet office, 2008: 58-60).

In order to encompass the duties and values which arise from the pillars, the NSS first splits them into different fields. One field within the NSS is *cyber security* (for example Obama, 2010: 18). All the different duties and values concerning cyber security would then be included within that field. After mentioning the threats and challenges within that field, the NSS proposes different strategies to oppose them. If, for example, one issue raised within the field of cybersecurity is the high infection rate of personal computers (PCs) due to the lack of awareness of individuals, a suitable strategy might be *education* (for example Obama, 2010: 27-28). Again, this strategy might be suitable to oppose more than just one threat subsumed under the field *cyber security*. After the strategies have been established, the last level is reached. This level specifies which policies can be used to realise the specific strategy and therefore address the threat. Homeland security policy therefore would be a subset of the general national security (Newmann, 2002: 126). At this point it is vital to mention that though the NSS evolved from defence policy, NSS suggestions are not limited to foreign policy and national security policy. Educational policies and environmental policies among others might suit the specific needs of the problem and therefore are addressed too. This is also one of the most important differences to the former defence policy approach (Cabinet Office, 2008). It is a general strategy for the security of the state in order to boost the effectiveness and not only a military one (Clark, 1982: 63).

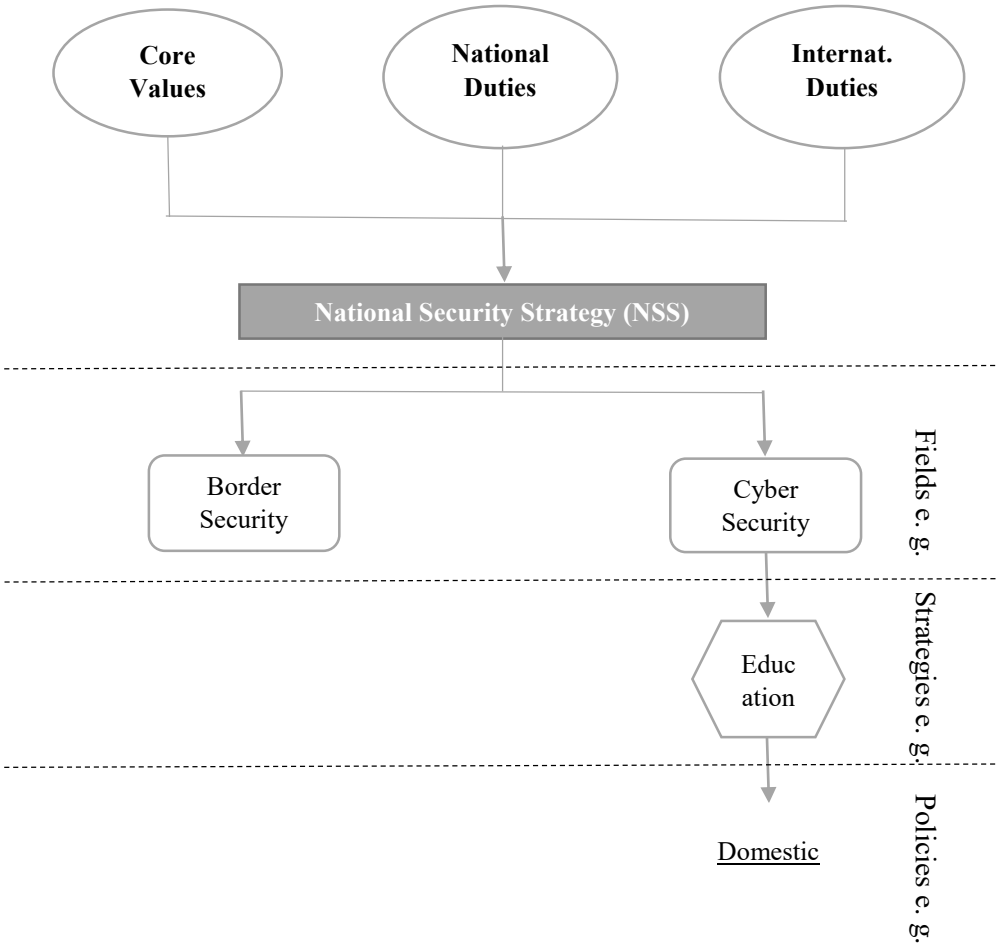
Core Values
National Duties
Internat. Duties
National Security Strategy (NSS)
Border Security
Cyber Security
Educ ation
Domestic
Fields e. g.
Strategies e. g.
Policies e. g.

Figure 5

5.2 National Cyber Security

The last section on NSS outlined the framework for the National Cyber Security (NCS). In the broader context of this paper, NCS is vital because it constitutes a part of how a state can strategize within the field of cyber operations. Discussing the strategic implications of cyber operations for a given state ultimately comes to how a state can secure its borders against cyber operations. This is what NCS is all about learning how to protect the state against cyber threats. While a cyber strategy, discussed in chapter IV, is made of several actions, including offensive ones, NCS is included here. The setup and implementation of a national cyber security has certainly become *en vogue* recently. The 2013 UN study shows that '[...] more than half of all United Nations Member States have some kind of national effort to secure critical networks and to respond to cyber threats' (United Nations, 2013: 1)[38]. To summarize, the first section shows which areas are covered by NCS and which are not. The three pillars of NCS: securing the state, protection of infrastructure and security of information, are all analysed in the second section. After illustrating the scope and the foundations of NCS, the third section discusses the approaches which, individually or combined with other approaches, can affect the three pillars which build the NCS. This last section covers the more abstract ideas connected with a strategic perspective on cyber security. It deals with the strategic options a state can pursue in order to implement cyber security.

In 1996, Steele defined the need for NCS. He stated that in order 'to survive at the dawn of the 21st Century, we must have a National Information Strategy' (Steele, 1996: 87). This need was addressed and highlighted in the 21st century by Malawer, among others. He reiterated that 'cyber security is the newest and most unique national security issue of the twenty-first century' (Malawer, 2010: 28). While these calls came from academia,

[38] Details accounts on the particular cyber security approaches of UN member states can be found in Lewis, J. A. (2013b) Cybersecurity and cyberwarfare: assessment of national doctrine and organization. In United Nations *The Cyber Index. International Security Trends and Realities.* New York and Geneva: United Nations Institute for Disarmament Research, pp. pp. 55-90.

they resounded effectively across different sectors, as President Barack Obama announced to 'make cyber security the top priority that it should be in the 21st century […]' (Obama, 2008), continuing a debate the past administration has started (for example Rollins and Henning, 2009). While the discussions on the NSS and cyber operations already gives a framework for what cyber security is, and understand of what cyber security *is not* can also be useful. Cyber security does not deal with issues such as protecting children online or more general cyber crimes[39]; this can be subsumed under cyber safety and not cyber security (Australian Government, 2009: 5-6). NCS does not pertain to active filtering or censorship[40] of the state towards its citizens and others living within its borders (Carr, 2010: 38-39). However, recent developments in Turkey complicate this discussion. In Turkey, the president implemented a censorship of the popular social media outlets Twitter and Youtube after confidential telephone conversations between him and high ranking members of his administration were leaked, claiming that the leakage would endanger national security (Tuysuz and Watson, 2014). Censoring information on the Internet contributes little to the overall national security as the leaked information could still have been made available directly to the concerned parties. Thus, some aspects of it fall under cyber safety, others can be subsumed under public relations. The *national* in NCS limits the discussion on the approach of securing the own infrastructure. Therefore, it does not include *extended cyber defence* (Wegener, 2011: 81), securing the CNII of other states.

[39] A list of cyber crimes which can be regarded as targeted by cyber safety can be found in Carr, J. (2010) Inside Cyber Warfare. *Mapping the Cyber Underworld*. Sebastopol: O Reilly and Wall, David S. (2003) Mapping out Cybercrimes in a Cyberspatial Surveillant Assemblage. In Ball, K. and Webster, F. (Eds.) *The Intensification of Surveillance. Crime, Terrorism and Warfare in the Information Age*. London: Pluto Press, pp. 112-136.

[40] For more information on filters and censorship, see EPIC (2001) *Filters and Freedom 2.0: Free Speech Perspectives on Internet Content Controls*. Washington D.C.: Electronic Privacy Information Center (EPIC).

5.3 The Pillars of National Cyber Security

Securing the complete state or *inclusiveness* means 'the maintenance of a secure, resilient and trusted electronic operating environment that supports [...] national security and maximises the benefits of the digital economy' (Australian Government, 2009: v). The Australian cyber security strategy indicates that NCS is 'not just an issue of national security but also one of economic security' (Australian Government, 2009: 4). The statements show that there is an overlapping responsibility between the public and private sector to guarantee NCS. One of the reasons for this is that 'in Cybersecurity there is no difference between military and civilian infrastructure as many targets are non-military but indirectly are involved in military infrastructure' (Tordilla, 2011: 3), for example power grids (Clarke and Knake, 2011: 143-144). Denning states that in 2000 more than 85% of military communications ran via civillian networks (Denning, 2000: 17) and Rhodes states that 'most of the nation's critical infrastructure is owned by the private sector' (Rhodes, 2001: 8). Therefore, a cooperation between state and private sector for cyber security should be achieved (Touré, 2011c: 92-93 and Raduege, 2010: 4). The relationship between the state and private sector is two-fold. First, the private sector has to spend more resources to secure its own systems because vulnerable systems of private companies can cause havoc and subsequently threaten the state (Habiger, 2010: 6 and Cordesmann, 2000: 9). At the same time, the state has to create an environment (both legally and for policy) in which the private sector can pursue these paths (Libicki, 1996: 100). Secondly, the private sector's research and development is crucial for the state as the public sector is often too slow to keep pace with cutting edge technologies (Shawnna and Rault, 2012 and Wilkinson, 2011). In order to secure the state, it is therefore imperative that civilian, military, public and private information infrastructures are protected. This can only work if NCS is pursued by through a joint approach between the private sector and the state itself. Working together towards NCS leads to mutual re-enforcement towards a more secure information infrastructure.

The CNII is crucial for the state and therefore its protection is of utmost importance for a NCS. The American, the British and the German cyber security strategies, among

others, regard the *protection of the CNII* as vital (DHS, 2003; DHS, 2010; Cabinet Office, 2011: 27 and BMI, 2011: 6-8). In addition to the role described for CNII in various NCS, experts in this field also rate the protection and securing the CNII as vital (Denning, 2000: 400-404, Wilkinson, 2011 and Fritsche, 2011: 4-5). The CNII is very vulnerable (Habiger, 2010: 4). The reasons for the vulnerability of these insecure systems are flaws in the design of the Internet, flaws in hardware and software as well as the decision to connect more and more critical systems (smart systems) to the Internet (Clarke and Knake, 2010: 73-74). The protection of the CNII is not only significant but essential because it does not only prevent casualties but also affect economic considerations. The economy increasingly depends on digital goods and devices. Touré emphatically concluded that the protection of CNII must be integrated as part of the NCS when he stated that '[...] enhancing cybersecurity and protecting critical information infrastructures are now essential elements of each nation's security and economic well-being' (Touré, 2011a: 8).

The third pillar of NCS is promoting *information security* or InfoSec. According to Denning, 'Information Security is concerned mainly with owned resources and with protecting against errors, accidents, and natural disasters as well as intentional acts' (Denning, 2000: 12). Therefore, it does not matter if that information is owned by the government, a company in the private sector or an individual. The German NCS, for example, included the setup of an initiative to help citizens clean their computers from *botnet* infections (BMI, 2011). As discussed in the section on weapons used in cyber operations, the smaller botnets are, the less damage they can do. Therefore, InfoSec targets not only the government or private sector but also the individual citizens. InfoSec does not only refer to the different stakeholders, but also refers to several approaches including: secure computer systems, regular penetration testing of systems, and resiliency of systems or redundancy (Habiger, 2010: 5; Cabinet Office, 2011: 27; Westby, 2011b: 2 and Libicki, 2007: 55-57)[41]. To list all the possible approaches that

[41] For more information on how to technically secure information, see for example Denning, D. E. (2000) *Information Warfare and Security*. Oxford: Association for

can be taken in the discussion of InfoSec would be too technical. However, all these actions follow a certain pattern and this is often described as CIA. CIA stands for confidentiality, integrity and availability. InfoSec can be achieved through making the systems which store information follow this pattern (Cebula and Young, 2010: 1 and Trites, 2008: 1; Denning, 2000: 41 and Janczewski and Colarik, 2008: xxiv).

5.4 Cyber Security Approaches

After NCS has been defined as relying on the three factors - inclusivity, CNII and InfoSec - this section identifies several approaches which can considered to achieve those three indicators of NCS. The approaches themselves consist of actions and tools – such as the weapons and armour used in cyber operations that are shown in the previous chapter (see figure 6 as extension of figure 5).

Computer Machinery (ACM) Press, pp. 285-344 and Clarke, R. A. and Knake, R. K. (2010) *Cyber War. The Next Threat To National Security And What To Do About It.* New York: Harper-Collings Publisher, pp. 139-143.

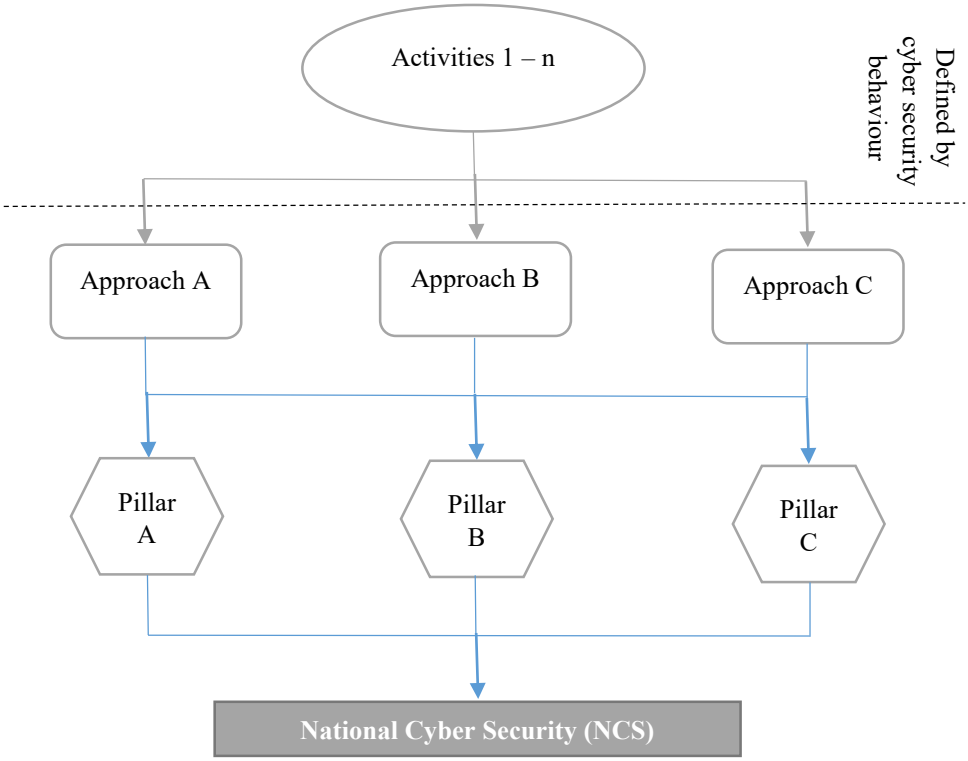

Figure 6

The first approach includes actions which can be considered *training*. Training in cyber security includes, but is not limited to, awareness raising, capacity building, open source intelligence and penetration testing. Awareness raising is a crucial part of the training component of cyber security (IGF Secretariat, 2006: 8 and Touré, 2011c: 90-91). Awareness raising means informing groups about cyber security and how it can be achieved. To raise awareness particularly especially in the private sector makes sense not only because the private sector owns most of the CNII, but also because it is the target of cyber attacks (see for example AURORA in history of cyber operations, chapter II). Botnets exist on the compromised computers of individuals. Thus, the fewer computers are infected, the weaker the effects of the botnets are. Raising awareness of the general public might therefore decrease the number of *zombie* computers within a

given botnet, and subsequently weaken the botnet, a weapon that can be used against the CNII of the state. Raising awareness is therefore a proactive approach towards national cyber security.

The next training component is closely affiliated to awareness raising. It is all about capacity building of the people responsible for safeguarding the national cyber security, be it in law enforcement, the judiciary, military or other sectors. The aim is to have a well-educated and skilled work force in cyber security (Touré, 2011b: 105-109; DoD, 2011: 10-11; Cabinet Office, 2011: 18-19 and Australian Government, 2009: 17). The Department of Homeland Security phrased it in the way that it 'is moving aggressively to build a world-class cyber security team' (DHS, 2010). While equipping people with new and better skills is certainly one side of the coin, limiting the chances of inappropriate staff behaviour and thus reducing security gaps, through social engineering, is another viable path (Janczewski and Colarik, 2008: xxiv).[42] A third aspect of training to achieve national cyber security is penetration testing, war games and red teams. These refer to either hiring external contractors or using staff to either conduct an attack against the own systems (red teams), or allowing two teams virtually fight against each other (war games) (DoD, 2011: 6). These actions are well-known in other fields of security and have been introduced to the arena of national cyber security, for example through the American based Cyber Storm war game. In 2010, it was discussed thus:

> *'Cyber Storm III, a response exercise in which members of the cyber incident response community address the scenario of a coordinated cyber event in which the National Cyber Incident Response Plan is activated, testing the National Cyber security and Communications Integration Center and the*

[42] For a coherent account on IT security training, see Winkler, I. (2007) *Zen and the Art of Information Security*. Rockland: Syngress.

federal government's full suite of cyber security response capabilities' (DHS, 2010).

The last part of education is using open source intelligence. Unlike other sectors of security and warfare related areas, cyber operations, through its dual use capacity, has a well-developed open intelligence[43] accessible area which includes, for example hacker conferences (Clarke and Knacke, 2010: 129-131). This area is already an intersection between education and research.

Research and Development (R&D) is focused on the hard problems of cyber security. It is a process of identifying problems and allocating funding in a coordinated manner (Lewis, 2011: 14). Described below are some of the areas crucial in the framework research and development in cyber security. The first aim of increasing cyber security is to improve the security of the CNII and subsequently the systems it runs on. Habiger describes it as closing the gap for potential attacks and making the systems less complex and more secure (Habiger, 2010: 44-45). Shimeall *et al.* put it more precisely in arguing that 'network design should integrate notions of robustness and survivability [...] Insulated intranets that can operate efficiently and safely without wider connections offer considerable promise in this respect' (Shimeall et al., 2002: 18). The point, however is the same: invest in research and development which focuses on making existing systems more secure, or come up with new systems that are more secure than their predecessors. Even if a system is less vulnerable to attacks, it might encounter the same amount or an even higher amount of attacks. However, as a product of an effective R&D, it is more able to withstand those attacks and therefore increases cyber security.

While the first approach dealt with the systems and how to make them more secure, the next set of actions falls under the umbrella of research and development of defensive programmes and tools. These, which fall under the aforementioned category of armours

[43] For more information, see Gibson, S. (2004) Open Source Intelligence. An Intelligence Lifeline, *RUSI Journal*, February 2014, pp. 16-23.

and tools, include Intrusion Detection Systems (IDS), such as the Einstein series (Habiger, 2010: 46). These tools are helpful against automated attacks but not currently against malware such as Trojan horses or non-automated attacks. Those attacks could be defended against by Deep Packet Inspection for ISPs, or the hardening of the single computer systems with patches etc. Another useful tool is the honeypot or DNS-based blackholing (Ramachandran et al., 2006: 1). While it does not directly lead to an improved cyber security, it enables the user to collect information about attack patterns which later can be studied. Another, more passive, way of increasing cyber security is the development and application of improved encryption technologies (Piper, 2002 and EPIC, 2001). While increasing research and development efforts on their own systems might be one way to look at it, certainly another way is to make the whole infrastructure of the Internet and its protocols more resilient and secure. The US Department of Defense is already promoting this: 'DoD will explore game changing approaches, including new architectures, to strengthen DoD's defense capabilities and make DoD systems more resistant to malicious activity. DoD will pursue revolutionary technologies that rethink the technological foundations of cyberspace' (DoD, 2011: 12). One way to improve the architecture of the Internet is to implement the DNSSEC protocol in order to secure against attacks coming over the Domain Name Service (Avri and Kleinwächter, 2008: 392). Another useful framework for research and development is the development of more offensive tools such as logic bombs or escrow backdoors in programs. Those programs can be used to level the playing field by preparing the cyber domain and using them, for example to deter attacks through the use of offensive capabilities (Denning, 2003 and Forward Consortium, 2010: 44-45). Creating stealthy remote programmes which can remain undetected long-term, deep inside the systems of potential adversaries is a quite complex challenge and therefore requires intense research and development - along with zero-day exploits which are only value insofar as they remain highly secret.

Cyber operations, as shown in chapter II, represent a cross-cutting field which can only be dealt with if the opposing cyber security approach is equally cross-cutting, therefore

fostering *coordination and cooperation*. Legal approaches, for example, are an efficient way to deal with attackers where their motivations, be they criminal, activism or the acts of foreign military (Touré, 2011b: 105-109). One way to foster coordination is to bring together stakeholders from different law enforcement agencies, intelligence services, military and even the private sector to set up a joint operations centres (Cordesmann, 2010: 15). These centres can be led by the military that have liaison officers in the mentioned agencies. Several countries, including the United States, the United Kingdom, Australia and Germany have already set up joint operations centres for cyber security (Cabinet Office, 2011: 25; BMI, 2011: 5; Australian Government, 2009: 23 and DoD, 2011: 2-3). If a joint centre cannot be realised, it is advisable to have at least developed processes of information sharing (Snow, 2011).

Having coordinated and cooperated at the national level, the next logical step for a state would be to achieve the same at international level (Touré, 2011b, 105-109 and Winkler et al., 2004: 81). The authors of a recent study state that '[g]iven the degree and speed of interconnectivity among states in cyberspace, a purely national approach to cybersecurity could never be adequate for national defence or to meet existing obligations under international law' (United Nations, 2013: 4). The need for international cooperation becomes obvious in the aforementioned framework of law enforcement[44]. While it is regarded as a vital tool to clamp down on those involved in cyber attacks, law enforcement loses credibility when applied abroad. This is especially true for states without legislation against cyber attacks (Cilluffo and Nicholas, 2006: 5). Thus, only international cooperation can lead to the avoidance of cyber havens (Pisanti, 2009: 51). A first step towards such an international system would be the exchange of

[44] Further information on the international law perspective on cyber operations and warfare can be found in the 2013 Tallinn Manual, see Schmitt, M. N. (2013) T*allinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press.

best practices on cyber security as spearheaded by the Australian Government (Australian Government, 2009: 22).

Cyber havens not only harbor cyber criminals, but also offer great value to cyber mercenaries- guns for hire- for engaging in cyber operations. While all these actions can be done by states individually, international laws and agreements, such as arms control, have to be introduced and implemented on the international level (Clarke and Knake, 2010: 216-255 and Fritsche, 2011: 5) especially through international organizations such as NATO and the UN. The latter discusses the role of international organizations to strengthen cyber security as follows: '[w]hile most of the concrete work on cyber defence is organized by states, international organizations can discuss, coordinate, and develop proposals to enhance global strategies for the creation of appropriate regional and international structures, institutions, and policies' (Neuneck, 2013: 93)[45]. A first step in this direction has already been taken by the NATO. It '[…] announced today it is forming a cyberattack Rapid Reaction Team whose mission will be to counter attacks as they take place and, where possible, take the fight back to the enemy' (Fogarty, 2012).

A similar cooperative approach which is not confined to inter-governmental discussions and agreements and less limited by politics has been coined the *Whole of System* (WoS) approach. The WoS approach is derived from international development aid and refers to the cooperation among non-state, like-minded actors in order to fight cyber insecurity (Klimburg and Healey, 2012: 95-100 and Luiijif and Healey, 2012: 138-139). An increasingly implemented outcome of the WoS approach is the setup of so-called Computer Emergency Response Teams (CERTs), which are interconnected non-government organizations aiming to secure information infrastructures. Not confined to

[45] Detailed accounts on the current progress of international entities can be found in Neuneck, G: (2013) Assessment of international and regional organizations and activities. In United Nations *The Cyber Index. International Security Trends and Realities*. New York and Geneva: United Nations Institute for Disarmament Research, pp. 91-109 and in Goldsmith, J. L. (2011) *Cybersecurity Treaties. A Skeptical View*. Stanford: Hoover Institution.

international politics allows those entities to work with each other across borders, quickly and efficiently, for example by sharing information on malware developments or coordinate botnet take-downs. This research is focused on the state. All those mentioned cooperation efforts however can either be supported or not be supported by the state. It can choose to sign certain agreements (and adhere to them), fund CERTs or join multilateral treaties.

5.5 Cyber Security Behaviour

According to Tordilla, strategies in cyber security are defined by the behavior of the acting party. He catalogues four types of behaviour: Reactive, Planned, Proactive and Chaotic (Tordilla, 2011: 3-5). Reactive behaviour is characterised by a strategy implemented in response to external events. Planned behaviour tries to include as much as possible in its planning and prevention measures, but leaves space for things it simply cannot plan for (for example chaotic behaviour of an opponent). Proactive behaviour includes actions such as testing its own security. Chaotic behaviour simply means behaviour which fails to adhere to a rational logic, and will be disregarded here as it represents the lack of strategy. To give an example: though the economy is dependent on access to the Internet, a state might decide to go dark, cutting all Internet connections to other countries. It might be a very effective cyber security strategy but at the same time can be devastating to the economy. The paper does not discount this behaviour as strategic studies have shown that paradox logic might even provide the edge for a decisive victory (Luttwak, 1987: 7-17, 120). Although these behaviours are defined distinctly, the transition between these different behaviors is seamless and their differences are recognised by a blunt index of majority. The adoption of strategies and the circumstances that give rise to such actions, produces the interplay of these behaviours that defines the strategy of cyber security. As behaviour here is attributed to a state, it translates well into a concept of strategy. If a state acts in a particular way towards cyber attacks, it can be regarded as the cyber security strategy of such state in the cyber domain. As it only defines the defensive approach – though it can include offensive actions – it does not constitute the holistic cyber strategy of the state.

Therefore, this section – which includes cyber operations tools and cyber security approaches - will form part of the discussion and analysis of the cyber strategy.

On one hand, *reactive cyber security* means that there is only a reaction to cyber attacks, an *ex post facto* set of actions. On the other hand, it also means that the approach focuses on a defensive position, or an *ex ante* action. This strategy considers a point of reference which is an existing or perceived behaviour of another state. This includes fostering isolation and fast reconstitution of systems (Cordesmann, 2010: 5) and a re-design of defence network systems to make them slimmer and smaller and hence easier to defend (Troiani, 2012). The technical vocabulary for this is *air-gapping networks* (Touré, 2011c: 86). In short: disable the opponent from getting your information by making the systems more secure and enabling your own forces to defend the systems. Shimeall *et al.* strike a connection to Clausewitz, saying that, 'the aim, in Clausewitzian terms, is to increase the "fog of war" for the enemy and to reduce it for one's own forces' (Shimeall *et al.,* 2002: 17). A R&D approach matching reactive cyber security is to focus on soft- and hardware that increases systems security and hardens them. This includes development of anti-virus software, firewalls, Intrusion Detection Systems (IDS) and the implementation of Deep Packet Inspection (DPI) amongst other actions. Regarding appropriate training in the framework of reactive cyber security, it can be regarded as an almost inclusive approach. In order to successfully pursue a reactive cyber security, training has to include information security behaviour, awareness raising for both staff and citizens, as well as general education for everyone and special education for a future work force. Coordination and cooperation to foster reactive cyber security should focus on involving the private sector and academia in R&D as well as in training. Incidents that happened have to be thoroughly studied in order to deal with similar attacks in the future. Academia and the private sector can make valuable contributions towards achieving this aim. It is evident then that the coordination and cooperation approach is applied only to strengthen the other two approaches. It can be said that a reactive cyber security relies only on R&D and training. Reactive cyber security put a premium on defensive measures and actions and does not include any offensive attempts. Attacks

follow a pattern so cyber defences should be constructed to detect and harden as response (Reitiniger, 2011: 6).

Planned cyber security can be regarded as 'active defenses' (Carr, 2010: 72 and Cordesmann, 2010: 15) or the intermediate level while shifting from reactivity to proactivity (Touré, 2011c: 88). It means 'looking into the future threat landscape' (Pisanti, 2009: 47)[46]. In comparison to reactive cyber security, planned cyber security tries to anticipate possibilities, for example attack vectors, and set up the defences based on the results. R&D is very important for planned security as it is needed to develop tools such as honeypots which attract attackers. In that way, the activities of attackers can be studied. This information can then be used to harden the defences and fix vulnerabilities. The latter actions also rely on R&D. Training in the framework of planned cyber security focuses mainly on capacity training so that the staff can setup honeypots and similar programmes and analyse the information that has been gathered. Training can be useful to help spot the latest trends in cyber attacks for example tools or techniques even before they can be analysed through honeypots. In the field of coordination and cooperation, planned cyber security will rely on information sharing with other agencies and departments. This information can contain attack patterns, latest incident reports and also defence techniques that have been discovered and implemented by those departments or agencies. The planned cyber security is still focused on defence while more resources are spent for the above mentioned activities in order to increase the security level. Compared to reactive cyber security, it might be more effective as attacks can be prevented by anticipating the way they are carried out and securing against it. While a reactive cyber security might take one or several hits before it can adopt protective measures, planned cyber security might already sustain

[46] Pisanti was originally referring to proactive as opposite to reactive without having something in between. His account however reflects well to what is referred to as *planned* in this paper.

the first hit – if the threat has been identified correctly and subsequent preparations were conducted properly.

As early as 1996, Schwartau discussed *proactive defensive information* warfare which included inserting malicious code in products (Schwartau, 1996: 246). Clarke, Knake and Denning mentioned the preparation of the battlefield for proactive cyber operations or *proactive cyber security*. This preparation takes place before the hostilities break-out and includes logic bombs planted in adversaries' infrastructure that can be triggered at any time (Denning, 2000: 154) – such as the alleged Chinese planting of logic bombs in the American power grids in 2009 (Clarke and Knake, 2010: 197-199). In the field of R&D, proactive cyber security includes software tools and malicious code or backdoors and escrow components which are integrated into regular programmes. It also includes the development of logic bomb programmes that can be used to prepare the battlefield. In training, staff have to be trained on how to penetrate systems, trace adversaries, setup honeypots which trick the attacker into opening files that will infect his own system (and therefore deviate from the honeypot referred to under planned cyber security). Training can also provide other skills to stealthily infect systems in order to cut them off in case of an attack. In the area of coordination and cooperation, proactive security includes fostering international cooperation under the UN umbrella, for example. It might also be an international agreement on banning botnets or similar tools that can be used for crimes and warfare alike but are easier to attack as a means of fighting organized crime. Proactive cyber security does not ignore the security of a state's own systems. In fact, it builds on a high level of security for the own systems and extends it by the option to respond to hostilities in an offensive manner. Clarke and Knake state that a good offense in the cyber domain cannot make up for the lack of defence (Clarke and Knake, 2010: 148). Not neglecting one's own defence, proactive cyber security can be regarded as top of the line cyber security behavior. It is the only approach which can both inflict casualties on the adversary while protecting the own systems, fostering deterrence by punishment. Hare and Zimmerman support this view, arguing that '[w]e must be prepared to counter an attack in cyberspace, just as we do it

in the other domains' (Hare and Zimmerman, 2009: 92). Striking a comparison to air warfare, planned and reactive cyber security would resemble as building a bunker and hoping that damage would be mitigated by the bunker. Proactive cyber security however would resemble building a bunker and installing an anti-aircraft missile launcher on top of it. This way, people and components in the bunker would be secured while the missiles could inflict casualties by shooting down attacking bombers.

5.6 Conclusion

NCS consists of a secured CNII, a strengthened information security in all relevant government and private agencies, as well as inclusivity of the state. The various approaches to achieving national cyber security are: research and development, training and cooperation and coordination. These approaches can be realised through different actions and tools, which have been mentioned in the chapter on cyber operations. Securing one's own borders is vital for a coherent cyber strategy. Identifying the national cyber security therefore forms one of the components of it. The behaviours of states towards achieving national cyber security have been analysed in this section. They will be taken into account when discussing cyber strategies. These behaviours should be regarded as stages rather than different options to choose from. While reactive cyber security is the lowest stage, planned cyber security is an intermediary stage and proactive cyber security is the final stage of achieving national cyber security. The higher the level, the more secure a strategy, but also the more expensive the behaviour becomes, even without considering the potential risk of escalation. Between planned cyber security and reactive cyber security, and proactive cyber security there is an important distinction which can be regarded as a choice as well as a higher stage. Proactive cyber security includes offensive elements.

In conclusion, a state can find itself in one of the four stages: without any cyber security, reactive cyber security, planned cyber security or proactive cyber security[47]. Currently, states can be found in all of these stages. The stage where a country is gives a clue about how much resources are spent and consequently how effective its cyber security is. However, a country with no cyber security at all, coupled with a complete absence of CNII, might be less vulnerable than other states. However, a country with a reactive cyber security but a high dependence on the CNII might be more vulnerable than the aforementioned country with no cyber security to speak of. Putting it in terms of this paper's broader aims, NCS will serve as an important part towards identifying and analysing cyber strategies. In order to be able to come up with strategies, one needs to know basic elements such as weapons and stakeholders (covered in chapter II) as well as vulnerabilities, points to attack and how those can be secured (covered in this chapter). Additionally, one needs to know about the environment, here the cyber domain (covered in chapter I). Having discussed these, the next step is to put it together in different strategies. Before this paper proceeds to this point, it will highlight NCS by an empirical example. The next section showcases the NCS approach of the People's Republic of China.

[47] It has to be noted, that planned cyber security and reactive cyber security are regarded as one stage in some academic discussions. However, as the distinction above has shown, it makes sense to divide them into two separate stages.

6. Case Study: China's National Cyber Security

6.1 Introduction

Having discussed National Cyber Security in general as well as its different behaviours, this section illustrates National Cyber Security (NCS) in the case of China. Examining the Chinese case means conducting a study of the cyber security measures and approaches conducted by the Chinese government in order to secure the Critical National Information Infrastructure (CNII) of China.

The analysis of the Chinese case is based on the theoretical framework of what NCS is (see section 5). The data which has been used for an empirical evaluation of the Chinese cyber security approach comes from a variety of sources. It includes news articles (for example Lee, 2012), technical reports and analyses (for example Information Warfare Monitor and Shadowserver Foundation, 2010), government reports (for example Wolf, 2012), as well as Western and Eastern authors (for example Libicki, 2007 and Qiu, 1999). The section is comprised of data retrieved from documents ranging from the earliest precursors of Chinese NCS to the latest developments in 2012. The literature is attributed to various research areas such as Chinese socio-economic development through the Internet, organizational descriptions of institutions and networks, cyber operations and electronic warfare doctrines as well as literature about the application of technologies for surveillance, and detailed technical descriptions. There is little specific literature about Chinese cyber security for several reasons. First, cyber security belongs to the defence sector which is mostly classified. Additionally, cyber security is the youngest subcategory of national security. Second, most relevant literature is either subsumed under cyber operations, cyber warfare, information warfare strategy or under surveillance in the Chinese case. Studying this literature offers hints with which one can deduct China’s approach, even though it is not specifically marked as such. Due to the confidentiality that surrounds the security sector, the author tried to conduct interviews with Chinese government officials from the PLA as well as from the Ministry of Defense through existing networks between October 2011 and September 2012 with no

significant outcome. Though the Ministry of Defense was generally interested in the author's perspective on this topic as well as in sharing of the Chinese perspective (as opposed to the mainly western literature), no agreement could be reached. Relying on research and empirical evidence regardless, a Chinese contribution would have had little to no impact on the outcome of this section. However, a Chinese perspective might have given insights to motivations, strategies and a future agenda.

The first part covers those China's cyber security pillars. It discusses if and to what extent China's National Cyber Security is built on the same three pillars (inclusiveness, protection of CNII and information security) which have been explored in section 5. Chinese activities towards achieving national cyber security are discussed in the second section. Like in the analytical framework of section 5, those activities are grouped into the three cyber security approaches: training, research and development and coordination and cooperation. This part also discusses into which particular cyber security pillars the respective cyber security approach and its activities feed. The last piece of this section concludes China's cyber security behaviour based on the different behaviours identified in the last section and the empirical findings of this section.

6.2 Mapping China's Cyber Security Pillars

That *inclusiveness* is also a cyber security pillar in the Chinese case becomes obvious when examining the Chinese telecommunication companies. One distinct feature of China regarding its telecommunication companies and other private sector entities, which own the public critical information infrastructure, is that most of those companies are *de facto* or *de jure* state-owned. Those state-owned entities, such as Chinacom, are in close contact and utilized by China through the People's Liberation Army or agencies and ministries (Ball, 2011: 83). The close connection and integration into the hierarchical order of the state allows China to directly influence those entities, including their cyber security guidelines. Instead of creating an enabling environment or using incentives to push for research in a certain cyber security relevant area, China can directly steer the entities that own the CNII. On the other hand, there are also private

companies in China which are in control of parts of the CNII. In the case of one of China's largest private telecommunication companies, Wolf argues that 'over the last several years, Huawei's top executives' deep connections to the People's Liberation Army and Chinese intelligence have been well documented' (Wolf, 2012). Krekel, Bakos and Barnett state that Chinese high tech firms can be regarded as collaborators of the state (Krekel; Bakos and Barnett, 2009: 49-50). Foster and Goodman state that 'now that JiTong, Unicom, and China Netcom have been given permission [by the RPC] to run backbones, they too will be expected to safeguard the national interest.' (Foster and Goodman, 2000: 31). This last point shows the close connection between the private sector and the government in China. It can be deduced that the government can heavily influence the private sector in order to implement cyber security activities. The Huawei case shows that there is a joint approach, for example towards research in the area of cyber security (Wolf, 2012). In conclusion, inclusiveness is a pillar of cyber security in the Chinese case. Additional to a joint approach of private sector and government, there is also the joint approach of government and state-owned companies towards cyber security. In terms of efficiency, it allows the government to have more direct influence on the companies. This can be an advantage, assuming that private companies and state-owned companies perform equally. These examples give an overview of the nature of collaboration. Due to confidentiality reasons, there is a lack of detailed information about joint programs, the intensity of the cooperation and the connections between the government and companies, save for global players such as Huawei and ZTE.

Discourses on China and the *protection of CNII* often include a discussion on the Golden Shield Project, also known as Great Firewall of China (GFW). The GFW is regarded as one of China's approaches to adapt the internet to the geographical borders of China via control and regulations (Goldsmith and Wu, 2008: 89-90) through state-owned and private sector telecommunication companies (Qiu, 1999; Sohmen, 2001: 18-19 and Harwit and Clark, 2001: 383-387). The GFW also shows that the CNII is regarded as a vital pillar towards cyber security in China.

To highlight a common misconception, the GFW was initially designed as a network and database project, connecting law enforcement agencies, close circuit television (CCTV) among others (Lyons, 2009: 5-11). It has however evolved into the '[...] world's most sophisticated information barrier, a semi-permeable membrane that lets in what the government wants and blocks what it doesn't' (Goldsmith and Wu, 2008: 92). The GFW is:

> *'[…] in effect a giant distributed firewall connected to all of the edge routers in China. All border routers in China route through the Great Shield. A major function of the Great Shield is to block access to content by preventing IP addresses from being routed through the Shield. This portion of the Great Shield consists of conventional firewalls, DNS Servers and Proxy Servers. The proxy servers map undesired foreign IP address to an internal server in China (transparently). The Great Shield also runs its own DNS Servers which engage in DNS Cache Poisoning. Because of the elaborate edge infrastructure architecture of the Great Shield from the rest of the world it acts like a private routing domain'* (Sing, 2012).

Put simply, information leaves and reaches China only through certain gateways. Each of these gateways has a filter running (Goldsmith and Wu, 2008: 93) which has been built by the American leading network infrastructure company Cisco (Goldsmith and Wu, 2008: 93).

One of GFW's main tasks has been to provide the tools for surveillance and censorship of Chinese Internet traffic. This role however diminishes increasingly as key economic interests clash with the rigid censorship policy (Fritz, 2008: 47-49). China recently opened up for international business, while backing Chinese companies to compete internationally. This kind of business can only be conducted if the companies maintain a free information flow between their offices and their clients abroad. Censorship intervenes at this point and therefore decreases the international competitiveness of the offices in China. As an example, imagine an international data mining company with

headquarters in the United States and a research facility in China. If the researchers and analysts in China cannot properly conduct Internet research because of censorship, they will not be able to provide accurate information to the headquarters. In an increasingly globalized world censorship is an obstacle. An example for this is the Southeast Asian front runner in terms of economic development: Singapore. In Singapore, censorship has been applied differently on the public and the private levels to allow economic growth of the private sector. Whereas stronger censorship was enforced for the public, the private sector has much more freedom in accessing websites to maintain their international competitiveness (Ang and Nadarajan, 2002: 2-4).

Closely affiliated with the GFW but not part of the initial plan, are the intra Chinese networks. Those networks such as ChinaNet, 169 or Next Carrying Network, are designed to provide cheap access to information and to keep its users within the domain of Chinese websites without the opportunity to access the (global) Internet (Goldsmith and Wu, 2008: 102-103 and Foster and Goodman, 2000: 49-50). Users on those networks stay within the GFW and cannot pass the gateways. In case the gateways of the GFW close, there is still a working national network which provides access to Chinese websites. While the GFW's functions as surveillance tool and database are well-known, less attention has been paid to the opportunity to use the GFW to secure the Chinese CNII. Singh put it boldly:

> *'Cyber War organizations see the Great Firewall as a major defensive weapon as well. The Chinese have a much better idea of what is coming into their country via the Internet, and that makes it easier to identify hostile traffic, and deal with it. Some American Cyber War officials are broaching the idea of building something like Golden Shield, just for military purposes. But that would be difficult in most Western countries, because of privacy issues. But with Golden Shield, China could unleash worms and viruses on the Internet, and use their Great Firewall to prevent Chinese systems from becoming infected'* (Singh, 2012).

As mentioned above, having the GFW in place allows for a complete shutdown of the gateways, *going dark*, hence disconnecting the intra-Chinese networks from the Internet. Subsequently, the CNII would be disconnected from the Internet and therefore resilient to most cyber attacks (Clarke and Knake, 2010: 146, Pandey, 2010: 2 and Walton, 2001: 9). Additionally, 'regulations introduced in January 2000 require all computer information systems involving state secrets to be neither directly nor indirectly linked with the international Internet' (Hughes, 2003: 227). As mentioned in the previous chapters, going dark can only be temporary response to an emergency. Due to the opportunities the GFW provides, and the effort that has been spent on developing and maintaining the GFW, it can be concluded that China regards its CNII as one of the pillars of its overall cyber security.

Activities focusing on the increase of *information security* in China have been taking place since the late 1990's already (for example Foster and Goodman, 2000). That information security is regarded as a crucial issue to increase Chinese cyber security is reflected by its approach towards the development of software.

China developed the Green Dam software which automatically censors content that could be accessed on the Internet. It was due to be deployed, installed on every computer that would have been sold in China from 2009 (Clarke and Knake, 2010: 56-57). Hedberg summarizes that '[...] the Chinese government issues a decree that all computer manufacturers in the country must install the censor software Green Dam Youth Escort in newly produced computers. After intense protests, the decree has been changed, now the software does not need to be installed but should be enclosed with each computer' (Hedberg, 2012). This represents a weakening of the Chinese security policy. Giving in to demands not to oblige vendors to sell all computers pre-installed with this software will lead to a lower number of people installing and actually using it. While the software ensures the implementation of censorship policies, it could also be used to block potentially harmful websites - harmful in the sense of opposing to information security. If this software would have been installed on all Chinese computers, it would have given China the option to filter potentially dangerous websites easily. No Chinese computer

would then have been able to access this website (with certain exceptions) and subsequently get infected this way, posing a threat to the overall Chinese information security.

Another software development target has been a Chinese operating system. China, for various reasons, chiefly information security, planned to develop its own operating system, based on the open Linux standard, as early as the late 1990's (Foster and Goodman, 2000: 32). The first project was codenamed *Red Flag*. Red Flag has never been deployed on a larger scale. Years later, China started the second project under the name *Kylin* (Amores, 2011). 'It [the PRC] has mandated the use of Kylin, a highly secure, Unix-based operating system, apparently much more secure than Microsoft server software, which China's University of Science and Technology for National Defence developed ' (Ball, 2011: 100).

Until 2000 China also developed its own encryption software. The software would have enabled China to use encryption technology without the fear that a backdoor has been inserted by the developer which could be abused through key escrow by a foreign state[48]. The Chinese encryption software was designed to have a strong encryption algorithm but a key escrow itself. The government would have been able to decrypt all data encrypted with this software using a master key. This project has officially been abandoned in 2000 due to commercial interests (Foster and Goodman, 2000: 25-26). Private entities would not use this software knowing the government could decrypt the data. This was a particular issue for foreign companies which could take their business elsewhere if regulations are in place that oblige companies and government agencies to use this software. After abandoning the project, China issued a regulation which limits the strength of foreign encryption tools used in China (Hughes, 2003: 227). Software

[48] For a detailed technical description, see Schneier, B., Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Neumann, P. G., Rivest, R. L. and Schiller, J. I. (1997) *The Risks of Key Recovery, Key Escrow , and Trusted Third – Party Encryption. Final Report* [online], Bruce Schneier. Available: http://www.schneier.com/paper-key-escrow.pdf [Accessed 10 October 2010].

developments are only one category of activities undertaken to increase the Chinese information security. It shows that China recognised the importance of data on government computers and its need to be secured (Grauman, 2012: 55). The section also shows that even though effort has been exerted to increase information security through the development of software, it also highlights that they were not overly successful. This is a crucial issue that is being addressed in the discussion of China's cyber security behaviour.

6.3 Identifying China's Cyber Security Approaches

In terms of *training*, China's military, the People Liberation's Army (PLA) 'has long had a doctrine of 'informatization'. It considers cyber operations as a leapfrog technology, one that will allow it to achieve military parity with the West' (Schneier, 2008b). The introduction of information operations into the curriculum of the PLA took place before 2001 (Thomas, 2000: 10-12). The PLA cooperates with hackers to increase its knowledge about cyber operations and attack vectors (MacWilliam, 2006 and Graumann, 2012: 56). The activities do not only aim to understand cyber security but also include detailed knowledge of developing and planting malware as well as cyber attack patterns (Rawnsley, 2005: 1069-1072). Additionally, 'special training corps for cyberwarfare have also been established in some areas, such as the one established by an armored division in the Nanjing Military Region to coach personnel in computer skills, software development and Internet warfare' (Hughes, 2003: 222). Training in cyber security, hacking and malware development is not only offered to the Chinese military but also has found its way into the curriculum of Chinese universities (Fritz, 2008: 43). Civilians are encouraged to learn how to become a 'network warrior' (Thomas, 2000: 2-4). Furthermore, the cyber police guarding the GFW, as well as other security forces, have received cyber security training (Hachigian, 2001: 126). In terms of cyber security, these training activities enable the military, police and civilians to provide information security as well as protect China's CNII. China also conducts regular cyber security exercises and cyber operations manoeuvres to train its forces for the event that a cyber war should take place (Krekel; Bakos and Barnett, 2009: 16-17

and Ball, 2011: 84). The Chinese Ministry of Public Security (MPS) has been conducting cyber security exercises as early as 2000 (Foster and Goodman, 2000: 33). Krekel *et al.* report that 'in 2008, a Guangzhou MR electronic countermeasures regimen formed an internal blue team to act as a simulated information combat detachment to develop training methods for the unit to counter various forms of computer network attack' (Krekel; Adams and Bakos, 2012: 24). While this reflects rather small exercises, Minemura reports that information and cyber operations manoeuvre has been carried out in 2011. 'In October, China conducted its first large-scale information warfare exercise in Bohai Bay, involving the army, the navy, the air force and the Second Artillery Corps, or China's strategic missile forces. The exercise was designed to nullify the functions of an enemy headquarters with cyber attacks and by jamming communications using electromagnetic waves' (Minemura, 2011). China's approach to cyber security through training and education feeds into the two cyber security pillars-CNII and information security. While there are several activities that can be subsumed under the training approach, activities either belong to the area of education and training or to exercises and manoeuvres.

China puts a strong focus on *research and development* of cyber security capabilities. Research is done by the private sector, by the military, by academia as well as by the state-owned companies (Hughes, 2003: 229-230 and Lam, 2010: 3). It is fostered by a mix of incentives and cooperation with academia and private companies as well as direct steering of military and state-owned companies. Krekel *et al*. state that 'the PRC government actively funds grant programs to support CNO related research in both offensive and defensive in orientation at commercial IT companies and civilian and military universities' (Krekel; Adams and Bakos, 2012: 9). These co-operations show that China follows an inclusive research and development approach. Section 6.2 discussed the development of software as the key indicator for the Chinese recognition of information security as crucial for the overall national cyber security of the country. The software encompassed operating systems as well as filters and encryption tools. In addition to the research and development of software which directly leads to an

increased security, China also researches and develops software for offensive use such as rootkits and advanced persistent threats (Krekel; Bakos and Barnett, 2009: 18-19 and The SecDev Group, 2009). Offensive capabilities can be counted towards an increase of cyber security in the framework of the proactive cyber security behaviour. In terms of protecting the CNII of China, research and development has been conducted especially within the GFW project. While important pieces of the hardware, such as the CISCO routers, were not developed by China itself, other parts were (Adams, 2001: 103). Additionally, China has also been developing its own wireless networking standard. The Wireless Local Area Network (WLAN) Authentication and Privacy Infrastructure (WAPI) allows for a better traffic filtering via wireless networks and therefore stands for a compromise between security through filtering and competitiveness of private companies in China (Goldsmith and Wu, 2008: 100-102).

In terms of *coordination and cooperation,* the Ministry of Public Security (MPS), the Ministry of Industry as well as the Ministry of State Security (MSS) and the People's Liberation Army (PLA) are tasked with providing cyber security for China together. There are however obstacles in the coordination caused by lack of proper communication between those entities (Fraumann, 2012: 56). The MPS takes a leading role in inclusiveness, bringing together military and civilian sectors on the topic of information security. Krekel *et al.* state that:

> *'the Ministry of Public Security's active support of information security research, certification of commercial sector products for use in PRC government systems, control of commercial information security companies, and funding of academic grants for research on subjects of interest to MPS provides an important window into how the PRC state encourages and directs information security research and standards in both the Chinese commercial sector and academia. The MPS Third Institute is responsible for the creation of information security standards for all hardware and software used in the PLA and in civilian government'* (Krekel; Adams and Bakos, 2012: 48).

In terms of coordination towards a more secure CNII, there are close ties between the government and the ISPs in regard to the GFW. The ISPs implement government regulations concerned with filtering of Internet traffic (Grauman, 2012: 56). At the same time, the GFW provides 'a computer network linking national and local police agencies nationwide' (Hachigian, 2001: 127). The PLA has been bringing together its own resources, academia and the private sector to work on cyber security and cyber operations related issues since 2002 (Krekel; Bakos and Barnett, 2009: 37).

A rather loose link exists between the government/ military sector and the Chinese hacker scene, for example the loosely connected Chinese hacker group 'Honker Union' (Gragido and Pirc, 2011: 125-126). This relationship is sometimes referred to as preparing for the 'People's War'- deducing the concept from Mao Zedong (Marquand and Arnoldy, 2007). It ranges from joint attacks against websites and servers (Delio, 2001) to the provision of offensive or defensive software to the Chinese government and the PLA, as well as direct consolidated efforts between hackers and the military (Hjortdal, 2011: 11). The relationship with Chinese hackers enables the military to tap professional manpower as well as research and development. It also gives leeway to plausible denial and deception. Having a high number of sophisticated hackers who are given leeway by the government might also endanger the government itself. Not all hackers are pro-government and, in some circumstances, those hackers might use their skills against government agencies and therefore pose a serious threat to the state. Not only do they operate within the borders of the GFW (and therefore are technically able to avoid the restrictions of it) but they can also dig holes inside the GFW and allow outside attackers a way in – therefore weakening the Chinese NCS.

In terms of international cooperation, China has been cooperating with one of the leading IT security companies- Symantec. It was the only partnership of this kind between a foreign cyber security company and China. The joint operations has just been terminated by Symantec owing to concern over intellectual property violations from 2012 (Krekel; Adams and Bakos, 2012: 12-13). China participates in international forums to push for international collaboration towards cyber security agreements and

countering a possible arms race (Graumann, 2012: 55). Recently, China implemented a Computer Emergency Response Team (CERT) in accordance to international standards (Graumann, 2012: 55) which is regarded as a first step towards international commitment to battling cyber crime and similar attacks. Hjortdal argues that the latter participation in international meetings to adopt agreements on cyber security/ cyber operations is only part of the Chinese agenda because it will not lead to any substantial outcome while China can boast itself doing something about ongoing cyber operations (Hjortdal, 2011: 12). While the main outcomes are produced by activities within coordination, Chinese coordination and cooperation efforts feed into all three cyber security pillars inclusiveness, information security and Critical National Information Infrastructure.

6.4 China's Cyber Security Behaviour

The choice of cyber security behaviour can be determined by cyber security approaches, as well as some additional information about the general cyber operations / cyber security strategy. In the Chinese case, it can be deducted from its activities, that China did not implement a 'no cyber security' behaviour. The development of its own operating system, among other activities, shows that China has a strategy to ensure a certain level of cyber security.

In terms of CNII, China does fairly well. As the discussion has shown, the Great Firewall is a potentially vital tool to protect the domestic critical information infrastructure but is also able to contribute substantially towards information security by filtering harmful websites for the Chinese Internet users. In case of emergency, it would stop the network traffic between the intra-Chinese networks and the Internet. Due to the linkages between government, military and private sector, China maintains a strong grip on the telecommunications sector which is vital for protecting the CNII. This behaviour also shows that inclusiveness is another strong suit of the Chinese cyber security. Several companies which contribute to cyber security are state-owned. Additionally, research and development as well as training are offered by Chinese

universities. Furthermore, joint ventures between private companies and government as well as military are in place. China also maintains cooperation with information security experts for reasons stated above. Cooperation between the government agencies lacks communication and is therefore inefficient.

In terms of information security, the track record of China shows several failures. Even if China finally develops its own operating system, earlier attempts towards filtering software, encryption software as well as operating system software have failed. In cooperating with hackers, China treads a delicate line, in allowing hackers access to the military the potential for abuse poses a national risk which is joined by a general lack of security awareness (lan and Xin, 2010: 2). Ball stated in 2003 that 'a two-month survey conducted in mid-2003 by officials of the Ministry of Public Security showed that 85 percent of computers in China were infected with a computer virus' (Ball, 2011: 98). It did not get better, as shown by a 2012 ranking of cyber readiness. Lee states that the Chinese lack of cyber security is derived from a high vulnerability and the lack of a joint strategy due to its focus on offensive capabilities (Lee, 2012). Ball states that 'the gap between the sophistication of the anti-virus and network security programs available to China's cyber warriors as compared to those of their counterparts in the more open, advanced IT societies, is immense' (Ball, 2011: 101).

China's general strategy towards the cyber domain focuses on propaganda, denial and deception (Yoshihara, 2001: 5). As discussed above, research and development in the area of cyber operations/ cyber security includes the development of malware, also for levelling up to the United States in asymmetrical terms (Rawnsley, 2009: 85)[49]. Additionally, exercises and training include penetration of foreign systems rather than a focus on defensive cyber security. The PRC has a rich history of alleged and confirmed (by a third party) successful cyber attacks. These include operation Titan Rain in 2005

[49] For an elaborate overview over the potentially offensive cyber capabilities of China, see Thomas, T. L. (2009) Nation-State Cyber Strategies: Examples from China and Russia. . In Kramer, F. D., Starr, S. H. and Wentz, L. K. (Eds.) *Cyberpower and National Security*. Washington D.C.: National Defense University, pp. 465-476.

(Winkler, 2005a), the penetration and download of information from the unclassified American intelligence network NIRPnet (Tkakic, 2007: 2-3), blackouts in American cities in 2003 and 2007 (Habiger, 2010: 42), as well as the setup of an international espionage network, penetrating government computers all over the world, nicknamed 'Ghostnet' (Information Warfare Monitor and Shadowserver Foundation, 2010). Winkler therefore concludes that 'in the computer world, there are many real dragons out there. The most notorious includes the Chinese military, which is systematically scouring the Internet for any system that might contain anything valuable. They have been documented to be able to fully compromise a computer system and erase all their tracks within 20 minutes. These people are extremely professional' (Winkler, 2007: 68). Tkakic adds that in his opinion the Chinese military will soon be able to even disable the unclassified American military network NIRPnet (Tkakic, 2007: 2-3). While the Chinese cyber operations/ cyber security strategy should focus mainly on defensive and counter-offensive capabilities, indicators point towards a focus on offensive capabilities (Mulvenon, 2009: 259 and Ball, 2011: 81). Fritz states that the Chinese behaviour shows a progressively improved understanding of defensive capabilities along with the development of offensive capabilities (Fritz, 2008: 45-46). While in terms of the CNII, China does well, inclusivity and information security are weak. This, taken together with the development of offensive capabilities and a focus on cyber strategy rather than a cyber security strategy, leads to the conclusion that China is pursuing a proactive rather than a planned or reactive cyber security approach. The behaviour has a strong focus on offensive capabilities and minor efforts – mostly relying on the Great Firewall of China – towards defensive cyber security. The next chapter defines cyber operations in the field of strategy, integrating cyber security as an integral part of every cyber strategy.

CHAPTER IV

7. A Conceptual Framework for Cyber Strategy

7.1 What is Strategy

7.1.1 Framework and Strategy

This chapter deals with the cyber strategy framework. The previous chapters laid out the basis of cyber operations and national cyber security and discussed their status from the perspective of national security. This chapter lays the predicate for the discussion of game theory which follows. It describes in particular the framework of cyber strategy, zooming in the plan of war itself. It explains what strategy is, and focuses on the essential parts of strategy, the differentiation between tactics, the operational level of strategy, the link between strategy and politics as well as the levels of strategy and the complexity of strategy. After those components of strategy have been discussed, section 7.2 deals with their adaptation to the domain of cyber operations. Therefore, the goal of this section is to provide an overview of strategy for adaptation as cyber strategy which will then be used to identify and analyse different cyber strategies, their aims and distinct characteristics. The framework for strategy will serve as a general, non-cyber specific overview of strategy and not an attempt of an in-depth analysis of strategy which has been covered in detail by previous scholars. For a more in-depth understanding of strategy, the work of thinkers such as Sun Tzu, Carl v. Clausewitz, Basil Liddell-Hart, Gerrard Chaliand, Edward Luttwak, Colin Gray, among others are essential readings.

According to Chaliand, strategy '[…] is the art of directing force to the ends in view' (Chaliand, 1994: 831) or even broader, strategy is a process that translates warfare to a policy effect (Griffith, 1963 and Jomini, 1968). The relationship of strategy and warfare has always been the same; the scope of the definition of strategy however has shifted over the centuries (Craig and Gilbert, 1991: 869 and Baylis et al., 2002: 20-25). Gray supports this particular perspective, stating that '[t]he character and conduct of war and

strategy may vary with time and opponents, but their nature and function are permanent' (Gray, 1999: 296). Craig and Gilbert conclude that strategy 'is also, in a broader sense, the modern equivalent of what was, in the seventeenth and eighteenth centuries, called *ragione di stato* or *raison d'état'* [highlighting by the author] (Craig and Gilbert, 1991: 869). Simply put by Gray, '[s]trategy is the bridge that relates military power to political purpose; it is neither military power *per se* nor political purpose' (Gray, 1999: 17).

7.1.2 The Strategic-, Political-, Operational- and Tactical Level

Elaborating further on the bridge between the strategic and the political level that Baylis mentions, Gray states that strategy is 'the use that is made of force and the threat of force for the ends of policy' (Gray, 1999: 17). While strategy is the means to achieve the political goal, it requires guidance from the political level. Without guidance, 'it [strategy] becomes mindless and heedless, and it is then that war assumes that absolute form that Clausewitz dreaded' (Craig and Gilbert, 1991: 865-866). Cohen highlights the prevalence of politics in this relationship, stating that '[p]olitics pervades all of war: the notion that politicians step aside during it is empirically untrue and theoretically undesirable' (Cohen, 2002: 84). Subsequently, there is a mutually enforcing relationship between the political and the strategic level. While it would be tempting to assume that the political level, a superior level, dictates the direction of the strategy, reality presents a different picture. Gray states that 'although the political dimension of strategy necessarily is logically superior to the operational military dimension, the latter field-tests the viability of the goals generated by the former' (Gray, 1999: 30). Though it holds true that 'the defence planner, the strategist, and the military field commander are disarmed by the absence of clear political guidance' (Gray 1999: 57), it is also the case that political guidance without understanding of the strategic reality can do a lot of harm. It is therefore vital that the political level has a certain understanding of the strategic level[50]. This understanding might be even more difficult to attain when the strategic

[50] For an elaborate account on frictions that can arise if this is not the case, see Gray, C. S. (1999) *Modern Strategy.* Oxford: Oxford University Press, pp. 59-68.

level includes new technologies. As it was with nuclear weaponry, cyber weapons are new and have not yet really been established, in contrast to the machinery of traditional warfare. It can therefore be derived that strategy is used to acquire political goals under the prerequisite of political control whereas mutual understanding is vital to the success of the outcome.

The operational level in warfare is probably one of the most underestimated (Luttwak, 1980: 60-63). Luttwak addressed this issue in his works *inter alia* in 'The Operational Level of War'. He states that '[...] the operational level of warfare is precisely the level that is most salient in the modern tradition of military thought in continental Europe' (Luttwak, 1980: 61). Even others such as Chaliand have also given credit to the operational level under the term 'grand tactics' (Chaliand, 1994: 736). Mostly however, it can be boiled down to the credo of the relationship between strategy and tactics. Chaliand, for example, states in the same work that '[…] in the most important operations in war, strategy fixes the direction of movements, and that we depend upon tactics for their execution' (Chaliand, 1994: 742) leaving out the operational level again. Luttwak defines the operational level as follows: '[i]n the operational dimension, by contrast, schemes of warfare such as blitzkrieg and defense in depth evolve or are exploited. Such schemes seek to attain the goals set by theater strategy through suitable combinations of tactics' (Luttwak, 1980: 61). Lonsdale adds that:

> *'[t]he operational level can be thought of in both conceptual and material terms. Conceptually, it links tactical engagements together in the service of military strategy. Materially, we can think in terms of a geographic area of operations, within which the operational-level commander moves his forces from objective to objective. The operational level contains a whole range of factors essential to the success of a military campaign'* (Lonsdale, 2007: 7).

The operational level therefore connects tactics horizontally with each other as well as vertically to the strategic level. Straight-forwardly, it can be regarded as the glue between the strategic and the tactical level. The operational level 'links tactical engagements with the overall strategy' (Lonsdale, 2007: 7) to ultimately support the

fulfillment of political objectives. In academic literature, there are several different terminologies used to describe the component parts of warfare. The terminology ranges from strategy and tactics to grand tactics to the art of the engineer (Chaliand, 1994: 736). The most commonly used terms to describe warfare are tactics and strategy. Tactics and strategy are inherently different and therefore should not be mistaken for one another. Gray defines strategy as the plan of war while the actions that take place in war are tactics (Gray, 1999: 22-23). Referring to another milestone literature in strategy, the definition and terminology of Clausewitz coincides with the ones mentioned above. He simply states that the formation in combat and the conduct of combats are tactics while the combination of both is strategy (Clausewitz, 1997: II, 74). Clausewitz argues that strategy is the '*Gebrauch des Gefechts zum Zweck des Krieges*'[51] (Clausewitz, 2003: 157). It leaves the conclusion that strategy defines what actions are to be taken in order to pursue the political goals. Thus, 'the perfection of strategy would be […] to produce a decision without any serious fighting' (Liddell-Hart, 1929: 925). This conclusion only holds true in cases where the political objective does not require the physical destruction of the enemy. At the same time, the discussion leads to the assertion that tactics refer to taking the actions dictated by the strategy and how they are being conducted. Though this research aims to explain the *strategic* implications of cyber operations for the state, tactics will not be entirely disregarded. In order to determine the implications of certain strategies, it is vital to know the underlying layers, such as tactics, and their reliance on the technology, explained in chapter II. As this research aims to deliver a holistic perspective on cyber operations and their strategic implications, tactics in cyber operations are briefly being analysed in section 7.2 which deals with the translation of strategic aspects into the cyber domain.

7.1.3 Dimensions and Complexity of Strategy

As discussed, warfare can be separated into strategy, the operational level and tactics. Strategy however can further be divided into sub-categories. While there are different

[51] From the German: *the conduct of a battle for the means of war.*

terminologies used to describe these categories, this research will stick to the terminology used by Colin Gray which defines these categories as 'dimensions of strategy' (Gray, 1999). Regardless of the terminology, the definitions of the dimensions of strategy are also different. Howard defines the dimensions of strategy as: 1. operational, 2. logistical, 3. social and 4. technological (Howard, 1979: 975-978). Chaliand, for example, sees eight dimensions: 1. theatre of war, 2. decisive geographical points, 3. base area, 4. tactical behaviour, 5. line of defence and offence, 6. manoeuvre, 7. sieges and 8. *têtes de pont*[52] (Chaliand, 1994: 737-747). While Chaliand's dimensions focus on the micro level, Clausewitz' perspective is broader in terms of macro and micro management. He identifies ten dimensions which also incorporate those of Chaliand: 1. perseverance, 2. superiority of number, 3. surprise, 4. stratagem, 5. space, 6. time, 7. strategic reserve, 8. economy of forces, 9. geometrical elements and 10. suspension (Clausewitz, 1997: III, 163-197). This research applies not only Gray's terminology but also adopts his definition as the framework for the dimensions of strategy. The reason for that is that Gray's work on modern strategy already encompasses the ideas of the former. His work offers a more holistic approach while incorporating all dimensions mentioned by Howard, Clausewitz and Chaliand and extends the literature. Gray's definition is coherent and comprehensive and offers a good starting point for the adaptation of the levels of strategy to the cyber domain in the following section. The dimensions of strategy identified by Gray are: 1. people, 2. society, 3. culture, 4. politics, 5. ethics, 6. economics/ logistics, 7. organization, 8. military administration, 9. information/ intelligence, 10. strategic theory/ doctrine, 11. technology, 12. military operations, 13. command, 14. geography, 15. friction, chance and uncertainty, 16. adversary and 17. time (Gray, 1999: 24). All of these dimensions have to be taken into account when drafting and implementing a strategy.

[52] From the French: *Bridgepoint.*

Levels of strategy according to the authors

Howard	Chaliand	Clausewitz	Gray
operational	theatre of war	perseverance	people
logistical	decisive geographical points	superiority in number	society
social	base area	surprise	culture
technological	tactical behaviour	stratagem	politics
	line of defence and offence	space	ethics
	manoeuvre	time	economics/ logistics
	sieges	strategic reserve	organization
	têtes de pont	economy of forces	military administration
		geometrical elements	information/ intelligence
		suspension	strategic theory/ doctrine
			technology
			military operations
			command
			geography
			friction/ chance/ uncertainty
			adversary
			time

Figure 7

Attention has to be directed to all levels of strategy. This is one of the reasons why strategy is a highly complex issue. Lonsdale surmises that 'the complexity of strategy is such that achieving a satisfactory end state at reasonable cost, and within a reasonable time-frame, is often elusive' (Lonsdale, 2007: 5). Lonsdale and Luttwak present two

comprehensive accounts on the indicators for the complexity of strategy. Luttwak states that relying on paradoxical logic in strategy can provide the edge to win a war (Luttwak, 1987: 234–235) and therefore refers to the French Maginot-Doctrine which he qualifies as 'over successful' (Luttwak, 1987: 120). The French relied on the Maginot-Line to be able to defend themselves against a German attack. The French defence was so successful – not in battle but as a means of deterrence – that the Germans did not attack it. They were looking for a weaker spot to attack, even if that meant attacking two other countries, Belgium and the Netherlands, first. Thus, it was so successful that it actually rendered it unsuccessful. It was because of the deterrence represented by the Maginot-Line that the Germans evaded it, and were able to attack France's weaknesses and therefore conquer large parts of the country.

That a strategy can be too successful is a paradox. Another indicator that shows how complex strategy is was introduced by Clausewitz: friction (Luttwak, 1987: 11–17 and Clausewitz, 2003). Clausewitz defines frictions as the '*Aneinanderreihung kleiner Probleme*'[53] (Clausewitz, 2003: 86). Friction refers *inter alia* to the obstacles that arise from unclear communications, organizational and logistical failures and such alike. They are, in the narrow sense, the resistance within one's own forces (Lonsdale, 2007: 12). Several problems which on their own are not that important but in sequence can cause severe damage.

Further to the issues above, the momentum of surprise and uncertainty, including the intelligence of the opposing leader, plays a major role in the complexity of strategy (Lonsdale, 2007: 7-20 and Luttwak, 1987: 7-10). Even superior plans and their perfect implementations can be flawed if the strategy does not pay attention to flexibility in dealing with unforeseen events. An adversary who tries to outsmart the strategist by using – what seems to be – paradoxical actions or unforeseen events have to be

[53] From the German: *chain of minor problems.*

considered. Nevertheless, reacting to a surprise is a challenge and therefore demands strategic considerations.

Lastly, the 'polymorphous character of war' adds up to the complexity of strategy (Lonsdale, 2007: 15-20). Arreguín-Toft refers to it as 'strategic interaction thesis' where 'strong actors will lose asymmetric conflicts when they use the wrong strategy vis-à-vis their opponents' strategy' (Arreguín-Toft, 2001: 95). Knowledge of the enemy and his strategy and the development of a counter-strategy is important (Griffith, 1963). The constant adaptation of one's own strategy to the demands of the changing environment is crucial. The outcome of this analysis is a distinct feature of strategy. A good strategy is a polymorphous idea, rather than a framework set solidly in stone. If a fixed framework would be sufficient, strategists such as Napoleon would not have been so important, in that their strategies could simply be replicated, but true strategic genius is rare (Clausewitz, 1997, Gray, 2009 and Lonsdale 2009). Thus, adaptability and preparedness for the yet-to-come are valuable for strategy and required to for responsiveness in fast changing environments. It is intrinsic to a decisive strategy that it can respond to elements such as paradox behaviour of enemies or surprise attacks. Strategy is an umbrella and guidance.

7.1.4 Definition of Strategy

Concluding, strategy is a mindful and controlled plan to achieve political goals through military force. It forms the basis of every kind of warfare and is both offensive and defensive in nature. Strategy is a highly complex issue which relies on different dimensions and levels which have to be considered in order to form a coherent and decisive strategy. The best strategy therefore would be the virtual threat of warfare which does not spark a war with real casualties but helps to achieve political goals. This only holds true where the political objectives differ from causing real casualties or sparking a war. A good strategy therefore has to exist before the event of a threat. Strategy should neither be underestimated nor be abandoned during times of peace. Furthermore, the ability and the options to react to certain developments are vital for

strategic considerations; otherwise the risk is that the 'strategy', fixed and immovable, becomes useless. This is the task of the next section: adapting strategy to the cyber domain. Adapting strategy to the cyber domain faces an additional challenge to those mentioned above: it is entirely new. While nuclear warfare revolutionized parts of strategic studies previously, so too will the cyber domain. It does not only add another weapon to the arsenal. The cyber domain does something no revolution in military affairs has done before: it negates time and space almost completely. This, among other elements, make cyber operations a unique strategic challenge.

7.2 Adaptation to Cyber Strategy

7.2.1 The Cyber Political Level

In order to understand the interaction between the political level and cyber strategy, it is necessary to understand the intersection between political, strategic and technical realities from the discussion in sub-section 7.1.2. The political level offers guidance and exerts control over the strategic level in order to ensure certain ends are met. For the political level to achieve this goal, it has to understand the strategic level. For it to understand the strategic level, it has to take into account the technical details of the means used (Cohen, 2002: 49). Sub-section 7.1.2 left unanswered the question as to which extent the technical details of the means 'cyber operations' play a role in understanding the strategic level.

In one of the earliest writings on the strategic implications of cyber operations, Rattray states that '[t]he analysis of strategic information warfare requires a deeper understanding of the linkage between applying digital force and intended political effects' (Rattray, 2001: 480). Geers goes further, arguing that '[a]t the political level, the intangible nature of cyberspace can make the calculation of victory, defeat, and battle damage a highly subjective undertaking' (Geers, 2001: 11). At the political level, offering guidance requires decision-making. In order to make decisions, the political level has to be aware of the environment and all implications of its decision. According to Carr, '[...] technological limitations on attack detection, attack classification, and

attack traces are likely to further complicate state decision-making during cyber attack analysis. Ideally, attacks would be easy to detect, classify, and trace. Unfortunately, this is not the case' (Carr, 2010: 69). Subsequently, the technical details of cyber operations are not only vital for the understanding of the strategic implications of cyber means towards political ends, but are also not likely to be entirely accurate.

To answer the question as to whether it is important for the political level to understand the technical details of the cyber operations means, the answer is yes, to a certain degree. It is not necessary to understand how a certain cyber weapon has been coded but it is of utmost importance to understand the implications that can be derived from the problem of attribution, the damage that a cyber weapon can cause and what the implications of retaliation through the use of another cyber weapon could mean. In order for the political level to fulfil its role as guide towards the targeted ends, it is pertinent to understand what the likelihood of retaliation, and the severity of it. The case study of the Olympic Games illustrates this point well – when the cyber weapon did not contain itself to the Iranian sub-network but accidentally spread to other parts of the world via an Internet connection due to a programming error. Thus, strategy as a bridge between means and goals has to properly present technical details and implications of the means of the cyber operations to the political level. This only functions well, if at the strategic level itself, cyber means are well-understood.

Cyber strategies cannot be understood in isolation from the rest of the state's strategies (Thomas, 2009: 487-488). The political level therefore has to make sure that the cyber strategy is embedded in the overall state's strategic approach. This however does not mean that cyber operations' means cannot be deployed separately to achieve a certain aim without being connected to other means, as the supplementary school of thought argues. In this case, the end could be the denial of service of an adversary's command-and-control network, where the means would be purely cyber operations means (Andrees and Winterfield, 2001: 6). Cyber operations as such are to be regarded as a means rather than an end. Kugler argues that cyber attacks are to be 'conducted with an explicit political or strategic goal: as a means to an end rather than an end in themselves'

(Kugler, 2009: 318). Geers supports this view arguing that '[a] cyber attack is best understood not as an end in itself, but as an extraordinary means to accomplish almost any objective' (Geers, 2011: 105). Subsequently, cyber strategy has to be embedded into the overall strategy but can be used as a means either as standalone or as a supplement to other means (for example diplomatic negotiations).

Kugler argues that even if a political agenda does not include cyber operations as conflict resolution mechanism, it cannot be completely neglected (Kugler, 2009: 320). Offensive and defensive cyber capabilities still have to be developed. Thus, even states which are not planning on conducting cyber operations still have to develop cyber capabilities in order to defend themselves against those who are. The reason for this is the growing importance of information- and communication technologies as cross-sectional area linked to other means, for example the economy or traditional military intervention. For example, if a country focuses solely on the development of naval and land power, it will implement more and more information- and communication technologies into their destroyers and tanks. That information system can be targeted by adversary's cyber operations capabilities and therefore require the sample state to pay attention to cyber operations capabilities though it is not pursuing it itself. Thus, cyber operations will become part of every political agenda which involves conflict resolution.

7.2.2 The Cyber Strategy Level

The strategic level is the umbrella for operations and steers them into certain directions in order to achieving policy objectives which have been set by the political level, the same is true for the cyber domain. The details of strategy in the cyber domain are discussed in the next paragraph. On a larger scale, the cyber domain offers several opportunities for a strategist in order to pursue policies. Firstly, as Owen argues, cyber operations capabilities allow for the targeting of critical and non-critical infrastructures, where the latter is little expected but can already achieve a lot (Owen, 2008: 35-40). In addition to pure military damage, cyber operations capabilities can be a comparatively

cost effective option, at once low cost and highly economically damaging. Owen states that '[a] war-waging state does not need to develop a nuclear warhead or fly an airplane into a building in order to cause billions of dollars in economic damage; a campaign using malicious software could do the job if economic damage rather than political attention is the primary objective' (Owen, 2008: 38).

For a cyber strategist, cyber operations capabilities also have another advantage. As the analysis of the different cyber strategies and operations this chapter will demonstrate is the latter parts, cyber operations have a high level of scalability in terms of covertness as well as in terms of intensity. A cyber strategy can therefore be highly complex mix of covert and overt operations with various levels of intensity. Compared to cyber operations, nuclear warfare's scalability is less precise. Though nuclear warfare offers the option to destruct smaller, strategic targets in addition to entire cities, it does not offer the destruction of very small internal targets. The scalability of cyber operations increases its complexity, hence the difficulty of decisions that a cyber strategist has to deal with.

Since cyber operations can also cause an unintended impact, it bears the potential for retaliation and subsequently entering an escalation cycle. This increases the complexity of decisions on the strategic end and requires from the strategist a complete understanding of technical details and possible implications of the cyber means used.

7.2.3 The Cyber Strategic Dimensions

This section deals with the adaptation of Gray's 17 dimensions of strategy to cyber strategy as– is discussed in sub-section 7.1.3. As this research adapts Gray's dimensions of strategy – which are overlapping with those of the other authors – every dimension will be introduced with a brief statement from Gray, describing the strategic importance of this dimension for the overall strategy. What follows is a brief analysis of this dimension in the framework of cyber operations. The outcome of this discussion is a level of importance of these dimensions for strategy in the cyber operations context. A dimension can be crucial for cyber strategy while another can be less useful. In the

conclusion, the most important dimensions are summarized in order to highlight the strategic implications of cyber operations.

1. People

'Strategy is done by tactics; tactics is 'done' by combat forces, *inter alia;* and the most important element in combat and support forces is people' (Gray, 1999: 26).

People play a major, if not the most important, role in cyber operations. Rios states that people are more important than the cyber weapons they wield (Rios, 2009: 9-10). As mentioned in sub-section 3.3.3, attack vectors such as social engineering are required to make a successful cyber attack possible. If the people who ought to defend against those attacks are prepared, skilled and well-educated as chapter III suggests in regard to cyber security approaches, there is a good chance that no harm will be done, or as Gray put it: 'skill and determination matter more than the latest technology' (Gray, 2009: 38). As discussed in sub-section 3.3.2 there are very sophisticated weapons which are dual-use and easy to obtain. In order to handle and develop them, it needs high-skill people. Unlike in traditional forms of warfare, there is a vast variety of knowledge that needs to be acquired before someone can become an effective 'cyber soldier'. Physical fitness is unimportant for cyber soldiers, unlike their traditional counterparts, knowledge and skills are what count (Clarke and Knake, 2010: 34). In the development of new weapons and armour (*inter alia* automated defences) as well as in carrying out defensive and offensive actions, people are the ultimate core of strategic cyber operations capabilities.

2. Society

'Appreciation of the social dimension of strategy requires recognition that strategy is made and executed by the institutions of particular societies in ways that express cultural preferences. In modern times, societies as a whole have prepared for, and made, war' (Gray, 1999: 28).

For a society, cyber attacks can be a major inconvenience, as the 2007 attack on Estonia proves. So far, however, cyber attacks have not been reported to have caused physical

harm to individuals. It is sometimes even referred to as non-lethal means; this may not be strictly correct, but points to the limited collateral damage which is central to cyber attacks (Schwartau, 1996: 246-248). Cyber operations can cause physical destruction and therefore has the potential to inflict physical harm. In addition to non-lethal impact, cyber operations do not require a lot of resources to be carried out or to be defended against: see section 3.3. Thus, preparations for cyber operations will not put a similar (financial) burden on the society in the way that preparation for air warfare or nuclear warfare would. As in section 3.4, cyber operations are currently regarded mainly as a *sub rosa* tool, involving clandestine espionage and sabotage operations, and therefore not directly interfering with society. The strategy therefore is less dependent on the social structure. Cyber operations seem to be congruent with what Luttwak calls 'post-heroic warfare' (Luttwak, 1995) which does not require for individuals to engage in lethal traditional war. That said, habits matter. As discussed during the cyber security section, awareness and training is important to counter one of the prime attack vectors in cyber operations: social engineering. If people are in the habit of doing something in the most convenient and easy way, they are at wont to sacrifice security to preserve it. This will in return open up vulnerabilities. The prevalence of the password *password* is testament to this. Paying attention to the habits of the people engaged in cyber operations and CNII is necessary to prevent crucial resources falling prey to an adversary's attack. It can however be assumed that as of the moment, society does not play a crucial role in the strategic dimension of cyber operations.

3. Culture

'Strategic culture provides the context for events and behaviour. Context refers not only to something 'beyond', 'out there', but also a framework of beliefs, attitudes, and habits, of which human beings are an integral part' (Gray, 1999: 28).

The cultural dimension of strategic cyber operations is noteworthy due to the influence of hacker culture (Graham, 2004). As mentioned, a cyber soldier cannot necessarily be portrayed as a regular, physically fit soldier. In addition, weapons and amour are

developed not only by governmental contractors, but also by individuals. A hacker could be of immense value to the military, as well as a patriotic group of hackers or mercenary hackers (Kellermann, 2012 and Rattray, 2001: 198-201). This requires the strategist to possess an understanding of the hacker culture that Graham describes. Without understanding this particular culture, with its background and ideologies, it is difficult to match it to the requirements of the military. Carrying out cyber operations for a state against another state does not differ significantly from a hacker penetration testing a large company, following the dual-use logic of cyber weapons (see sub-section 3.3.1). In addition to the culture of the individuals participating in strategic cyber operations, the general culture of strategic cyber operations matters. Luttwak in his work after the end of the Cold War, compares Napoleonic warfare to Cabinet warfare and subsumes that: 'present circumstances call for even more than a new concept of war, but for a new mentality that would inject unheroic realism into military endeavour precisely to overcome excessive timidity in employing military means' (Luttwak, 1995: 122). What he refers to is an extended culture of restraint present during the Cold War due to no side wanting to risk turning the war hot (Luttwak, 1995: 110-111). The post-heroic culture of warfare Luttwak describes aims to minimise one's own causalities through attrition, with operations like trade embargoes. Admiral Owens portrays the cultural impact of information in the framework for RMA. According to Owens, information have direct influence on way of managing troops on the battlefield (Owens, 2000: 97-99), concluding that this is '[...] an era where the computer and new information and communication technologies both liberate us from the past while destroying the sense of space and time that for centuries defines our context of existence' (*ibid*: 236). The fallout of which is targeted by Lonsdale's discussion on artificial intelligence (AI) to support decision-making in Strategic Information Warfare (SIW) (Lonsdale, 2004: 111-117). Examining these strategies in section 7.4, these influences on the culture in the information age are reflected in several of them. Thus, to excel in strategic cyber operations, one has to understand the unique cultural background of the information-age and hacking as well as the concept of post-heroic warfare and its implications.

4. Politics

'The political dimensions of strategy is the one that gives it meaning' (Gray, 1999: 29).

This issue is sufficiently discussed in section 7.2.1. There are but two further comments to make. First, the political level has to understand the technology used in cyber operations as potential impact of false decisions could be devastating. Second, cyber operations encompass various levels including '[...] a range of conflict types covering political, economic, criminal, security, civilian, and military dimensions' (Knapp and Boulton, 2008: 18). The political level therefore has to keep in mind that an abundance of cyber operations capabilities leads to more vulnerability. The more developed and sophisticated states are, technology-wise and governance-wise, coined 'vulnerable sophisticates' by Szafranski, the more vulnerable they are (Szafranski, 1996: 237-239). If this development coincides with a decision to not engage in cyber operations capabilities, it will definitely limit future strategic and policy options. Therefore, a further development of technological capabilities has to pay close attention to their genuine stability and progress towards redundancy and security rather than only convenience and efficiency.

5. Ethics

'Questions of justice can be hugely relevant to strategic performance. At the minimum, those questions can be reduced to the need to recognize the occasional tension between fighting well in an ethical sense and fighting effectively in pursuit of an economical victory' (Gray, 1999: 31).

A distinct difference between ethics in other forms of warfare and ethics in cyber operations is that a decisive strike with a very low number of collateral damage is possible through cyber operations. It is therefore less likely that cyber operations demand decisions such as bombing a house of strategic value where civilians are hiding and might end up as collateral. At the same time, it should be noted that those conducting cyber operations sit far from the theatre of war. It therefore possesses a

similar physical distance to those who are in charge of launching intercontinental ballistic missiles (ICBMs). Research on the impact of being distant from the theatre of war – especially in the area of unmanned drones – is currently being undertaken as it is a very new development. For now, the ethical dimension is still not well-explored and that 'traditional ethical and political theories [...] cast so little light on this new, and difficult domain' (Dipert, 2010: 406). Cyber attacks can easily default on the issues of discrimination and proportionality. Especially the automation of cyber weapons can lead to unintended consequences. While the Morris Worm accidently brought down the Internet for a brief period, some parts of the Olympic Games operations escaped their designated theatre of war, Iran (see section 8). The Ghostnet operation, though intended to steal information about Tibetan politics from around the world, infected governmental computer systems. This potentially causes escalation. Dipert defines the key questions as the main area to tackle for further reach in this area (Dipert, 2010: 392), e. g. if '[…] a cyberattack [is] ever morally justified in cases where the enemy has launched neither a cyber- nor a conventional attack'. The most crucial point however is the lack of proper attribution for the most cases of cyber attacks. Even though, Dipert discusses in an earlier work (Dipert, 2006) the potential of a certain threshold for attribution in order to allow for a reaction, he concludes that '[t]his epistemic uncertainty [attribution problem] is one of the peculiarities of responding to a cyberattack that makes it similar to preemptive and preventive war' (Dipert, 2010: 393). Ethics is a growing field of importance in the field of strategic studies, hence also cyber operations (for example Arquilla, 2013; Dipert, 2010 and Dipert, 2013). In this early stage of strategic analysis of cyber operations, it does not feature the same importance to be dealt with as for example intelligence. At this stage, the ethical dimension of cyber operations can be regarded as underdeveloped and more research would be vital as it is certainly an important field.

6. Economic and Logistics

'Strategy requires the use or development of scarce economic resources. It rests completely upon economic activity, and relies entirely upon logistical performance, i.e. the supply and movement of armed forces' (Gray, 1999: 31-32).

For the strategic dimension of cyber operations, the economic dimension is fairly unimportant. The *resources* that are needed are a couple of systems-networks and computers-which are inexpensive and readily available (Betz and Stevens, 2011: 9-10), as well as skilled and educated people. People are discussed as their own dimension of strategy above, and accounts for the need for them to be knowledgeable the adversary's systems and possible vulnerabilities. These are also subsumed under the dimension of strategy *intelligence/ information*. Neither economic nor logistics have a decisive impact on cyber strategies. For the different levels, especially the organizational level, this means less friction and complexity among other things. Not having to consider supply lines, time schedules for reinforcements, or the strategic distribution of gasoline would certainly simplify every strategist's job. Thus, though this dimension does not have a decisive impact on cyber strategies, the implications for the strategic, operational and tactical level if compared to other kinds of warfare are important.

7. Organization

'Just as strategy is 'done' by tactical activity, it is also, 'done' by a bureaucratic organization that staffs alternatives critically, coordinates rival inputs, and oversees execution and feedback on the effect of execution' (Gray, 1999: 34).

From the organizational and/ or oversight point of view, cyber operations offer some distinct problems. First, it is difficult to control every keystroke a cyber soldier makes during a cyber operations incident (Libicki, 2007: 96-97). While he ought to defend the enemy, he might just be opening a back-door for the adversary to destroy the own system. This is similar with larger-scale problems such as the Olympic Games. Another challenge is the often quoted attribution problem (Wilson, 2009: 428-430). Second,

information operations produce an entirely new environment where the new speed of events creates a need to shift from a traditional command-structured organisation to a leaner, network-structure. From this discussion, Lonsdale derives the *digital imperative*, to keep up with the speed of the adversary's decision-making and acting (Lonsdale, 2004: 111). Therefore, he foresees the implementation of AI to support but not supplement the commander (*ibid*: 111-118). Thus, organization in the framework of cyber operations is important insofar as it has to follow the requirements of Lonsdale's *digital imperative* as it is not only true for SIW but also for cyber operations. A slower, hierarchical and traditional command structure might not be compatible with the organizational needs of cyber operations.

8. Military Administration

'By administration we mean the activities of military preparation that eventually provide suitable armed forces ready to be moved by the logisticians so that the generals can exercise command. Those activities must include all aspects of military recruitment, training, and armament' (Gray, 1999: 34).

It can be derived from the analysis of the people and the economic and logistics section above, that military administration does not face a heavy challenge when it comes to cyber operations. The focal point here is clearly the recruitment and training of the cyber soldiers, other concerns are not a high priority. That the level of military administration only has to focus on one issue however does not mean it is not of importance in the cyber domain. The opposite is true. Military administration is important because only with the right (skilled) people, cyber operations capabilities can be realised at all. In addition, the points discussed under the cultural dimension might create an obstacle. Military administration therefore rates highly on the priority scale of cyber operations dimensions of strategy.

9. Information and Intelligence

'The prospective strategy likely to be harvested from superior information and intelligence, however, has varied radically with the salient technologies, politics, geographies, and logistics of war' (Gray, 1999: 35).

As mentioned in chapter II and III, information is vital to stay ahead of the cyber operations game in terms of weapon and armour development, and attack vectors. Without information about the latest vulnerabilities and exploits and how to fix them, strategic cyber operations is impossible to wage. While one of the dimensions of strategy is technology, it is really information which gives cyber weapons and armour the edge, not new technologies. At the same time, section 8 discusses the importance of good and thorough intelligence for a feasible cyber operation. The Olympic Games case study illustrates how important it is to know about the standards and procedures used, and the systems and equipment used by the adversary. Without proper intelligence, cyber operations can be a blunt sword rather than a sophisticated dagger. If weaknesses are not known, they cannot be exploited. Without exploit, technical or individual, success of cyber operations is almost impossible. In addition to these issues, intelligence can help to solve the problem of attribution. With good intelligence, the origin of a hostile cyber operation might be discovered, whereas just defending would not be sufficient to trace the attack back. With proper attribution, strategic cyber operations include less friction. Information and intelligence are the *condiciones sine quibus non*[54] of strategic warfare in the cyber domain.

10. Strategic Theory and Doctrine

'If strategic theory educates the mind by providing intellectual organization, defining terms, suggesting connections among apparently disparate matters, and offering speculative consequentialist postulates, strategic (and operational, and tactical) doctrine

[54] From the Latin: *essential conditions.*

states beliefs. Doctrine teaches what to think and what to do, rather than how to think and how to be prepared to do it' (Gray, 1999: 36).

For now, there are two reasons, why strategic theory and doctrine need to be addressed and closely monitored in the domain of strategic cyber operations. First, as Rattray puts it 'technological developments create new means of waging wars and theories about how to employ these tools' (Rattray, 2001: 77). The development of the Internet and computers were those technological developments. This development is fairly new, and therefore it is a field to be explored. This is also one of the main reasons for this research: a new field needs thorough attention to properly develop it. Strategic theory and doctrine are in their nascent phase in the domain of cyber operations and therefore have the vital need to be explored. The second reason for the importance of this dimension is that the cyber domain, as compared to the other domains, is highly dynamic (Kramer, 2009: 5). The speed of developments in this domain is very quick; see for example the development of cyber operations in chapter II. Even if strategic theories and doctrines are established, they need to be constantly revised in adaptation to developments in cyber operations.

11. Technology

'Technology, as weaponry or as equipment in support of weaponry, does not determine the outbreak, course, and outcome of conflicts, but it constitutes an important dimension' (Gray, 1999: 37).

Naturally, without the Internet and computers there would be no discussion of strategic cyber operations or cyber at all. That being said, with reference to the dimensions *people* and *information and intelligence*, the weaponry which Gray sees in the technology dimension is being developed as pieces of information and put to good use by people. With reference to section 3.3, a newly developed subversive multi-vector threat is not a new technology; rather it is pieces of information uniquely arranged by people. Something which is regarded as a new technology in a traditional domain does not necessarily translate to a new technology in the cyber domain. Air power for example

regards the development of the stealth technology as technological advancement. Translating it into the cyber domain would mean the programming of a new piece of software which helps the attacker to disguise its origin (point of connection to the Internet) better. This new software rather belongs to the dimensions *people* (who programmed it) and *information and intelligence* (which were used to programme it) than to the dimension of technology.

Depending on the point of view, however, major new steps in hard- and software design, concerning CNII, cyber weapons and armour, could also be attributed to technological advances and therefore giving the technological level much more importance. In reference to Gray's definition of the strategic dimensions, *technology* is a crucial component of cyber operations. The ambivalent relationship between *people*, *information*, and *technology* should, however be kept in mind.

12. Military Operations

'This dimension of strategy [Military Operations] expresses the reality of the relationship between strategy and tactics' (Gray, 1999: 39).

Military operations as a dimension of strategy therefore refers to the operational level of cyber operations discussed thoroughly in sub-section 7.2.2. As shown, the operational level in the cyber domain offers considerable opportunities and can therefore be regarded as important to cyber operations.

13. Command

'Command refers to the quality of military and political leadership' (Gray, 1999: 39).

For the political leadership, the importance in the cyber operations is discussed in section 7.2.1. For the military leadership, which also applies to the political leadership, it is vital that it is of good quality. Weapons used in the cyber domain are – if the adversary is sophisticated – mostly single-use (see sub-section 3.3). If a weapon can only be used once, it takes extreme precaution, preparedness and command to

effectively wield Further, the impact can go beyond planning and imagination, and even leading to an unintended escalation (see section 9 for more details). Additional challenges are the high complexity of cyber operations as well as the general framework of cyber operations with increased speed, adversary's ability to hide its tracks, ultimate range and low-cost for entry (Betz and Stevens, 2011: 9-10). A further distinct point is that a cyber commander does not lead his forces into a situation where physical harm can occur to them. Commanding forces which will be not shot at also has implications on the way a command can be conducted. Command therefore qualifies as a vital dimension of strategy in the cyber domain[55].

14. Geography

'There is always a geographical dimension to conflict' (Gray, 1999: 40).

The common perception of geography in the cyber domain is illustrated by Glabus, '[t]he virus allows one to leapfrog across geography—it is easier to inject a computer virus across oceans than other kinds of viruses' (Glabus, 2000: 83) and Gray, arguing that, '[o]n the virtual battlefield of cyberspace, electronic warfare is apt to mock geography, and therefore time' (Gray, 1999: 43). This assumption is correct but it leaves out a crucial part, that the electromagnetic spectrum which forms the geography for cyber operations is bound to physical restrictions as well. As discussed in chapter I, the Internet, among other networks, is made of computers connected to each other via cable, satellites and various wireless technologies. These devices however exist in the physical world. If the command centre which houses the cyber soldiers of state A is cut off from the Internet, state A is unable to engage in any further cyber operations. The physical component of cyber operations is very often underrated. The Olympic Game case study shows the challenge of the physical component for cyber operations and how it can be overcome as well (see chapter IV). An additional unique feature of the geography for cyber operations is that it is man-made (Rattray, 2009: 268). It is not only man-made

[55] This is issue offers a vast potential for further research in the field of strategic studies and cyber operations, especially in the context of ethics and military culture.

but highly mutable – as Rattray describes it, 'the environment for strategic information warfare is much more mutable than that for land, sea, air, and space warfare' (Rattray, 2001: 65). All systems and networks can be changed by their respective owner, on the physical level (pulling plugs) as well as on the virtual level (using different software). This is the reason for a cyber attack to seek ownership of the target system. It allows the attacker to alter the environment and can even prevent the original owner – the defender – from changing his virtual environment. As compared to land warfare, this would mean that the current owner – the defending party – would be able to move mountains and lakes however they like. In order to summarize the discussion above, it might be prudent to refer to Lonsdale's concept of the *infosphere*, the domain in which cyber operations take place as the fifth domain of war fighting with strategic resources being crucial in a highly amorphous environment (Lonsdale, 2004). The electromagnetic spectrum, bound to the physical world (for example, through computers), does not only allow cyber operations to take place as well as allowing cyber operations to affect other domains (for example through a cyber attack against the communication systems of a jet fighter) but also for other domains to make use of the cyber domain. Using a real-time command-and-control system to direct and coordinate land and naval forces in order to, for example, conquer an adversary's military port would be such a projection. The strategic importance of geography for cyber operations is very high.

15. Friction, Chance, and Uncertainty

'The would-be rational and prudent defence planner lives in a world of uncertainty. Chance does not quite rule but it is always a player, and friction can impede cumulatively the smooth performance of anything and everything' (Gray, 1999: 41).

The heavy impact of friction on cyber operations will become more obvious when adapting Clausewitz' definition of friction to the cyber domain as Arquilla and Ronfeldt did. They state that the Clausewitzian concept of friction is substituted by entropy in the information warfare domain (Arquilla and Ronfeldt, 1996: 156). As everything in the

cyber omain basically runs on information, entropy refers to an overload of information. Overload of information is commonly known as spam on the Internet and as noise in the strategic field of cyber operations (Skoudis, 2009a: 163 and Libicki, 2007: 50). Libicki therefore assumes that, '[b]ecause cyberspace is noisy […] signals […] present in the nuclear realm may be nearly indecipherable in the new medium. Noise destroys communication, hence signalling' (Libicki, 2009: 115). An example why noise serves as a potentially dangerous form of friction can be taken from the thousands of daily attacks against the networks and systems of the American Department of Defense (Panetta, 2012). Dealing with this number of attacks might take lots of resources but it is even more difficult is to establish which of those many attacks – which resemble noise – are potentially decisive ones, possibly backed by a foreign government. Noise also leads to the main uncertainty of cyber operations: the attribution or safe haven problem (Schneier, 2004: 21). Campen surmises: '[t]he enemy will be unseen and even unknown [...]' (Campen, 1996: 71) - if you don't know who attacked you there is no way of retaliating. The only options left are deterrence and focussing on defence capabilities or the attribution through analysis of the contemporary political environment. Asking the question of who would benefit from it might provide more insight than technical logs. These are but the two most important indicators of friction, chances and uncertainty in the cyber domain. Many more can be derived from the other dimensions of strategy discussed, such as the highly mutable geography. More traditional forms of frictions still apply to cyber operations, some with an even higher level of impact. A natural disaster such as a storm which shuts down parts of the power grid can effectively stall any cyber operation. Though the headquarters of the cyber unit might be equipped with emergency generators, the adversary's might not be – therefore disconnecting the target from any connecting networks, rendering it air-gapped. It is therefore of vital importance to address this dimension with special care.

16. Adversary

'Strategy is so difficult to design and do well that consideration of an intelligent and self-willed foe is frequently a complication too far' (Gray, 1999: 42).

As far as the cyber domain of warfare is concerned, there is but one distinct feature that should be mentioned: the nature of adversaries. Dearth and Williamson stated that, '[i]n a future characterized by cyberwar, technology offers the prospect of non-state possession in abundance of the 'non-lethal' means of violence' (Dearth and Williamson, 1996: 28). Due to the easily obtainable and dual-use nature of cyber weapons, non-state actors can play, to a certain degree, a vital role when it comes to cyber operations (see chapter II). It is much easier for non-state actors to obtain off-the-shelf cyber weapons (even for free from the Internet), than it is for them to buy a F-35 Lightning II Joint Strike Fighter. The non-state stakeholders are not covered in great detail in this research due to the focus on the state. In addition to that, the Olympic Games case study shows that major cyber operations still need a state carrying it out rather than a group of hackers. This however should not undermine the credible threat that these and similar groups can pose in the cyber domain for a state however. Their threat is similar to the threat another state poses, but is less sophisticated and therefore does not offer any new insight to the strategic dimension of the adversary in the cyber domain. In more general terms however, the adversarial relationship still exists in the cyber domain, and hence in cyber operations. A strategy is a strategy, regardless of the domain it is applied in. In the same way a strategy is still a strategy in cyberspace, it also has still to take into account the adversary or adversaries it is carried out against. Thus the level of the adversary does not deserve more attention than usual but equally, no less.

17. Time

'But in all forms of combat for which the speed of light cannot govern time and eliminate space, time will rule tactically and operationally (politically and strategically, the significance cannot be diminished by technical advances)' (Gray 1999: 43).

In the case of cyber operations, speed of light governs time and eliminates space (the latter only to a certain degree, see the dimension of geography). However, its importance has to be taken with a grain of salt. First of all, an attacker who manually probes the vulnerabilities of a system and tries to find weaknesses operates in real-time.

Therefore, he can be countered by someone who notices this behaviour. If the attacker then stops his advances in order to write an automated tool, such as a subversive multi-vector threat, the defender has time to harden the systems against whatever the attacker was looking for. Automation is a limited option in defence and attack planning. Knowing that automated cyber weapons exist, the only answer would be to work on automated cyber armour because only a machine working at very high speed, can counter another machine attacking it with the same level of speed. Even though cyber attacks can be carried out quickly, it certainly takes time to prepare them. It also takes additional time to analyse the impact that the cyber attacks caused. With the impact identified, it is only then that the cyber attack can mature to effect a policy. Thus, the time between the conceptualisation of a cyber attack and the implications it has for the political level, can be as long as in other domains and forms of warfare. Bearing these things in mind, it is fairly obvious that time is a relevant consideration in the cyber domain. It works differently to how time works in other domains, but remains an important strategic dimension.

Out of the seventeen dimensions of strategy discussed by Gray, ten dimensions matter to a greater extent than others in regard to cyber operations are: *people, technology, information and intelligence, geography, friction, military administration, strategic theory and doctrine, military operations, command* and *time*. Of these ten dimensions, the most important ones are *people, technology, information and intelligence, friction* and *geography*. These deserve special attention in the design and implementation of cyber operations.

7.2.4 The Cyber Operational Level

The operational level as the glue between the tactical level and the strategic level also exists in the cyber domain. Geers points this out without referring to it as the operational level in the cyber domain. Similar to the operational level in general (compare to sub-section 7.1.2), the operational level in the cyber domain is rarely referred to as such. Geers states that:

> *'[a]s national security thinkers attempt to defend their interests in cyberspace, a key to success will be to bridge the gap between cyber strategy and cyber tactics. Goals such as the security of national critical infrastructures and strategies like military deterrence and arms control demand a greater appreciation for the capabilities and challenges of computer scientists, who fight their battles on the front lines of cryptography, intrusion detection, reverse engineering, and other highly technical disciplines'* (Geers, 2011: 31).

This paragraph from Geers already points to an issue that has been discussed in the analysis of the political level of cyber operations: knowledge of cyber operations itself.

While on the political level, cyber operations call for a thorough understanding of cyber capabilities, potential problems and probably implications, the sophistication of knowledge about cyber operations on the operational level has to be a higher. Rattray argues that '[o]rganizations formed to carry out strategic information warfare activities face the complex and demanding task of developing technological mastery over the tools and knowledge required for waging such warfare successfully' (Rattray 2001: 165). The organizations he mentions might be on the tactical as well as on the operational level. Nonetheless, it shows that a high degree of knowledge and understanding, a level of *mastery*, has to be obtained on the operational level in order to carry out cyber operations. Hence, in order for the operational level to work, matching tactics to achieve strategic objectives in the cyber domain, those institutions which, and people who are implementing actions on this level, have to master the technology, for example through a thorough understanding of weapons and armour (see chapter II).

The operational level in the cyber domain looks very similar to the operational level in any other domain. It is a horizontal connection of different tactics to pursue a strategic objective. Germany was successful in conquering a large part of France during the Second World War due to the latter's reliance on the Maginot-Line. The German troops circumvented this strong line of defence by adopting the *Blitzkrieg* doctrine and moving their troops through formerly neutral countries into France. The Germans invaded

France at its weakest spot: a strip of the border where no heavy defences were in place because it bordered a neutral neighbour. Having had strong defences not only on the borders to Germany but also inside the country, an operational action called defence in the depth, would have prevented, if not the invasion itself, at least the high speed with which the German troops were able to capture France (Luttwak, 1987: 120). A Maginot-Line translated into the cyber domain is called candy security (Mitnick and Simon, 2002: 79). It means that no matter how the network is protected on the outside, as soon as an adversary finds a weak spot, he will make faster progress in weakening such network as there are almost no defences behind that security line. In order to counter that, cyber operations would also have to incorporate the technological equivalent of defence in the depth. It refers to policies, software and hardware measures (several tactical means) in order to stall an adversary who managed to breach the network in order to stop him from getting to the vital parts of the system (strategic objective) (Andrees and Winterfield, 2011: 20-21 and Winkler, 2005b). This example shows that the operational level exists in the cyber domain but also that is can be very similar to the operational levels in other domains – even using a similar terminology.

The cyber domain is volatile due to the underlying technical structure (see chapter I), it can be changed by those owning the systems and networks or can even be disconnected – air gapped - at will. Thus, the theatre of operations is potentially highly amorphous and requires constant attention and adaptation from the operational level. For someone commanding land operations, the geography of the battlefield is unchanging. A cyber unit commander would not know if the system he was supposed to launch an attack against will still be there tomorrow. This is a geographical rather than conceptual approach to operations in the cyber domain and is also referred to as operational art. As shown, a strategist has to be well-versed in operational art when dealing with activities taking place in the respective domain. The theatre of operations which, in other forms of warfare, are mostly unchanging (cloudy and stormy weather or clear skies in air warfare), can be entirely different within a very small amount of time. If for example, the target switches his network from the Internet Protocol version 4 (IPv4) to the version

6 (IPv6) standard during the beginning and the end of an operation, weapons might be rendered useless, attribution be possible and target systems nowhere to be found. Operational art is a rather crucial element of cyber operations – and a very unique one as well.

Another point that has to be mentioned in relation to the operational level is a possible automation of it. Reitinger hints at such, '[i]n this future, cyber devices have innate capabilities that enable them to work together to anticipate and prevent cyber attacks, limit the spread of attacks across participating devices, minimize the consequences of attacks, and recover to a trusted state' (Reitinger, 2011: 5). What Reitinger alludes to at exists today and resembles the intrusion prevention system mentioned in section 3.3 in a more basic form. It can make use of different tactical tools such as traffic encryption or network shut-down in order to achieve the strategic objective of securing a critical network by conducting an air gaping operation. It would therefore function on the operational level completely or partially automated. This research is not going to analyse implications, advantages and disadvantages of automation but also highlighting the possibilities of it and how it might shape the cyber operational level.

7.2.5 The Cyber Tactical Level

As discussed in 3.3, the cyber armoury offers a variety of different tools. The cyber tactical level consists of the usage of these tools and their interconnection to the operational level. The ultimate aim is to achieve strategic requirements. Consequently, it can be derived from this assumption that the weapons create as well as prevent tactical choices. Malicious software and attack vectors are being used as weapons in the cyber domain (Schneier, 2004: 152-175). The combination thereof and the way they are implemented can be regarded as cyber tactical level. A tactical cyber attack pattern, an operation, follows seven subsequent steps (Andrees and Winterfield, 2011: 84-117 and Gragido and Pirc, 2011: 154):

1. reconnaissance of the target and possible exploits to be used,
2. scanning of the adversary's systems for vulnerabilities and weak spots,

3. gaining access to one of the connected systems of the adversary's infrastructure,
4. escalation of the current access level in order to be able to carry out further attacks,
5. extraction of data (for data stealing) and information about the system (for further attacks),
6. assaulting the system or connected units (see case study on the 'Olympic Games'),
7. and sustaining access and hiding tracks allowing for stealthy re-entry into the systems.

In reference to the German *Blitzkrieg* against France in the Second World War, it must be considered that without tanks, as used by the Germans, a *Blitzkrieg* could not have been implemented as it was. Comparatively, a tactical cyber operation was demonstrated in the 2009 Ghostnet (see section 3.5) attack against Tibetan institutions all around the world. The attacker sent emails with an attachment which looked genuine – an invitation or a conference presentation – while in reality it was a Trojan horse. When the person opened the presentation, it still showed a presentation but the malicious software installed itself on his or her computer. The cyber weapon, the Trojan horse, then sent all the information on the computer to the attacker. Without this specific cyber weapon, the attacker would not have been able to carry out his attack. Therefore, his tactical choices would have been limited. The tactics for the Ghostnet operation was to con the victim into opening a valid looking document (social engineering). Sanger in his account of the Olympic Games states that 'cyberattacks, unlike nuclear missiles, are so stealthy that they offer the opportunity to wreak damage that may take an adversary months to detect and years to repair' (Sanger, 2012: 247). Betz and Stevens go as far as to state that cyber operations are more capable of striking directly against an adversary's CNII than air power is (Betz and Stevens, 2011: 84-88).

Geers however points out a tactical disadvantage when stating that 'it is also true that cyber attacks are constrained by the limited terrain of cyberspace. [...] Basically, tactical

victories amount to a successful reshuffling of the bits – the ones and zeroes – inside a computer. Then the attacker must wait to see if anything happens in the real world' (Geers, 2011: 10). There is not even a need for something to happen in the real world. Cyber operations can take place entirely in the virtual world, the cyber domain. An example for this would be the attack against Saudi Aramco using the Shamoon malware. The Shamoon virus was deployed in the network of the company; infecting office computers and wiping their hard drives clean (Jackson Higgins, 2013). Soon after the attack started, the company shut down its network, denying the attackers any access to it. From this point onwards, there was no telling if the attackers achieved their aim or not. The only real world response was the press statement made by the company afterwards.

7.2.6 The Cyber Complexity

It is important to address the complexity of strategy in the framework of cyber operations because, as Schneier states, 'complexity is the worst enemy of security' (Schneier, 2004: xi). The complexity of cyber operations is composed of several main components. Some components that introduce a high level of complexity to the strategic considerations of cyber operations have already been mentioned in the other parts of this chapter. Additional components that increase the level of complexity can be deduced from the need to pay attention to seventeen dimensions of strategy as well as the general assumptions of strategic surprise, friction paradoxical actions (Luttwak, 1987: 7-17). The following paragraphs subsume and discuss all the mentioned and additional complexities under the three categories: attribution, amorphousness, and ubiquity.

Attribution

The problems of attribution are manifold, beyond simply the challenge of tracing an attack accurately. Sulek and Moran conclude 'not only is strategic surprise possible in cyberspace, but it is also possible to veil the source of the attack. To complicate matters, there may be a number of actors (rival states, rogue states, terrorist groups, and others)

with an interest in not only launching a surprise attack, but potentially even attempting to stimulate conflict between the victim and a third party' (Sulek and Moran, 2009: 129). Due the opportunity of non-state actors to participate in cyber operations (see *Adversary*), tracing an attack back to a country does not necessarily mean that the country has, as such, authorized and backed this attack. It is also highly likely that non-state groups operate under the guidance and backing of the state which claims that it has nothing to do with an attack but will find the perpetrators – which they do not do. This is also called the safe haven problem (see *Friction, Chance, Uncertainty*). To complicate matters further, third parties might also attack the same target (Libicki, 2009: 62-63). Determining the existence of another party when identifying the original adversary seems virtually impossible – if carried out in a sophisticated way. For the defending actor in the cyber domain, attribution is a strategic nightmare. The context, current political conflicts, and frictions or expected retaliation, might give away the attacker without necessarily having to have solid technical evidence for attribution. However, relying on the context alone opens up the opportunities for third parties to create chaos and escaping unscathed.

Amorphousness

The potentially high degree of amorphousness in the cyber domain due to the underlying technical structure (see chapter I, sub-section 7.2.4 and the explanation in *Geography*) is an additional challenge which increases the complexity. Arquilla and Ronfeldt state that for cyber operations '[w]e anticipate that cyberwar, like war in Clausewitz's view, may be a 'chameleon' (Arquilla and Ronfeldt, 1993: 45). Additionally, certain strategies which work in other forms of warfare might not be applicable to cyber operations. One assumption can be derived from the attribution problem together with 'chameleon'-like character mentioned by Arquilla and Ronfeldt. Habiger states that, '[...] deterrence and pre-emption are based on certainties that do not exist in the amorphous, anonymous and fluid realm of cyberspace' (Habiger, 2010: 4). Nye concludes that '[a]mbiguity is ubiquitous [in cyber operations] and reinforces the normal fog of war' (Nye, 2011: 125), which can *inter alia* be attributed to the dual-use character of cyber

weapons (see *People*, *Culture*, *Adversary*). The amorphousness tasks the strategist with constant adaptation and maintenance of plans, as crucial elements concerning cyber operations are likely to change.

Ubiquity

For strategists concerned with cyber operations, there is no way of ignoring other domains. According to Andrees and Winterfield, the '[c]yber [Domain] is ubiquitous in all the other modern domains' (Andrees and Winterfield, 2011: 28). Jet fighters which are used to fight in the air power domain contain lots of electronics that are vulnerable to surface controlled cyber attacks. For Cohen '[t]he real and the virtual battlefields had become a complex and inextricable whole' (Cohen, 2002: 250). It is the strategic level that ensures that the cross-domain junctions get the attention they deserve. As an additional point towards the ubiquity of cyber operations, Kilroy states that '[u]nlike other forms of warfare, however, a cyber war could break out at any time; and if these cyber defenders are successful, the public may never even know it happened' (Kilroy, 2008: 444). Cyber *troops* do not need to be brought to the front lines (see *Economic and Logistics* and *Geography*). Whenever they are ready to strike and get the signal to do so, they will be able to carry out their attacks within an astonishing short amount of time, compared to other forms of warfare (exact time depends on the sophistication of the attack, the level of vulnerability and other factors). The take-away from this challenge is that a cyber attack can take place anywhere and at any time.

7.3 Cyber Operations – Strategy in the Fifth Dimension

Cyber operations represent a new area of operation, adding to the domains of land, sea, air and space. Even though a recent study identified that only '[...] six states have published military cyber strategies (with varying degrees of detail and specificity)' (United Nations, 2013: 2), the number of states actually implementing cyber strategies is higher (Lewis, 2013b: 9-55).

In this new field of operations, the traditional levels exist in the same way they exist in the other fields; there is a political level which deals with the strategic level in order to achieve political objectives within certain frameworks. The strategic level guides the operational level to ensure that the tactics that are combined into operations serve as the right means to the overall end. And the tactical level makes sure resources are sued effectively. Thus, in general, there is no ground-breaking difference between those levels and the same levels in other kinds of warfare. There are however certain nuances within the particular levels which differentiate them. The political level for example, has a deeper knowledge of cyber operations their strategies and complexity that can be very beneficial although is not necessarily required. Cyber operations offer various options, they can be used for coercion, for deterrence, as well as for *sub rosa* activities (see the cyber strategies in section 7.4). The strategic level is unique. Analysing it in the framework of Gray's 17 dimensions of strategy shows that several dimensions, which ultimately portray the character of a strategy, are crucial to cyber operations. Of the 17 dimensions, nine deserve special attention and five dimensions are vital to be carefully considered in every cyber strategy. Especially the dimensions *people*, *technology*, *information and intelligence*, *friction* and *geography*, are crucial for the strategic conduct of cyber operations. In addition to this, cyber operations put a strategist in a challenging position. The three indicators: attribution, amorphousness and ubiquity make the conduct of cyber operations extremely complex and volatile. On the strategic level, cyber operations need intensive, constant attention. Adaptations and quick reactions to new developments are vital. While offensive and defensive capabilities exist in the cyber domain, they are unlikely to be the reaction of one another. Cyber capabilities can be implemented for deterrence or offensive operations. It is however questionable if the coercive power of cyber operations suffices to retaliate against a more lethal form of operations or warfare such as air warfare – for example through a precision-bomb air strike. If retaliation via cyber operations can achieve a high-enough level of intensity, it can work. For example, if the retaliation to an air strike which kills dozens of soldiers is a cyber attack that shuts down a power plant for a day, the coercion through retaliation is low. If the response however is the shutdown of the entire national

power grid for two weeks through a cyber attack, the coercive power might more likely be high enough to have severe impact and therefore can be regarded as a retaliation threat. Defensive operations are necessary if deterrence fails – therefore they can be part of the deterrence strategy (see section 7.4).

Similar to general debates about the operational and the tactical levels, cyber operations also struggle to distinguish them. The cyber tactical level is concerned with the combination of cyber weapons and attack vectors in order to exploit vulnerabilities in systems and overpower the defences, as well as with defensive counter-measures. The operational level, however, adds further important elements to the tactical level, such as the degree of stealth and the timing of an operation. The operational level transforms strategic objectives into successes through tactical measures using available resources. In addition to this, the operational level in the cyber domain has to pay special attention to the theatre of operations, which is constantly changing and in flow, making operational art a crucial point. The cyber domain, unlike land, air, sea and space, is not only volatile but also very prone to manipulation and change by those that own the networks and systems. The operational level differs from the same level in other kinds of warfare because of the configuration of the cyber domain, its *geography*.

The cyber tactical level provides new opportunities and challenges. Due to the dual-use feature of cyber weapons, militaries, as well as private companies, are using the same resources and can – in theory – create the same weapons and armour and use the same attack vectors. This means that military-private cooperation can be fruitful, owning to the pre-existing expertise in the private sector. An indicator of this are the detailed reports referred to in section 3.5 and the appendix on various cyber operations campaigns. On the down side, the military is competing with the private sector for the main resource for cyber operations: skilled and well-educated people. In addition to this, the constantly changing environment of cyber operations allows for new threats to the national defence (exploits, vulnerabilities amongst others) to appear at any given time. Offensive capabilities that have been developed to strike enemies might be rendered useless in an instant (through patches, bug fixes, change of software and hardware). The

cyber tactical level is highly complex and asks for constant preparation and adaptation on the defensive level, and for thorough research and quick responses.

The strategic implications that can be derived from this adaptation of strategy to the cyber domain that can be pinpointed so far are that the state has to:

1. have a high degree of knowledge about and understanding of the technical details and implications of cyber operations,
2. constantly monitor the ongoing situation, respond to changes quickly and adapt its strategies on a regular basis, and
3. pay particular attention to the junctions of the cross-domain dimensions of its national strategy.

7.4 Cyber Strategies and Implications

7.4.1 State-of-the-Art and Framework

After discussing strategy in general and its adaptation to the cyber domain, this section identifies and analyses several cyber strategies. Knowing and implementing cyber strategies are important because '[a] grand strategic vision of cyberspace can assist states in navigating the informational turbulence in which contemporary international politics appears to find itself. [...] Cyberspace has its myriad problems, but a true strategic sensibility demands that long-term interests prevail over short-term opportunism' (Betz and Stevens, 2011: 139). Kuehl identifies cyber strategy as, 'the development and employment of strategic capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power in support of national security strategy' (Kuehl, 2009: 40), a perspective that is supported by Starr (Starr, 2009: 5). Though they provide a rich framework, those definitions focus on the meta-level of cyber strategy, which refers to the use of information warfare. Cyber operations are a subcategory of information warfare/ information operations, among others (see section 4). Cyber strategies therefore can be regarded as a subsection of a general cyber strategy of a state, leading to cyber power (see section 7.5). Cyber strategies only include actions

which can be summarized under the definition of cyber operations which have been identified as *the targeted use and hack of digital code by any individual, group, organization or state using digital networks, systems and connected devices, which is directed against CNII in order to steal, alter, destroy information or disrupt or deny functionality with the ultimate aim to weaken and/ or harm the targeted political unit*.

The strategic perspective which has been discussed in the last two sections shows that a cyber strategy consists of one or more operations. A cyber strategy therefore is *the development and employment of cyber operations, potentially integrated and coordinated with other operational domains and forms of information operations, to achieve or support the achievement of political objectives*. Figure 8 shows the composition of a cyber strategy. It is made up of one or more operations which themselves rely on advanced persistent threats (APTs), subversive multi-vector threats (SMTs) or other cyber weapons.

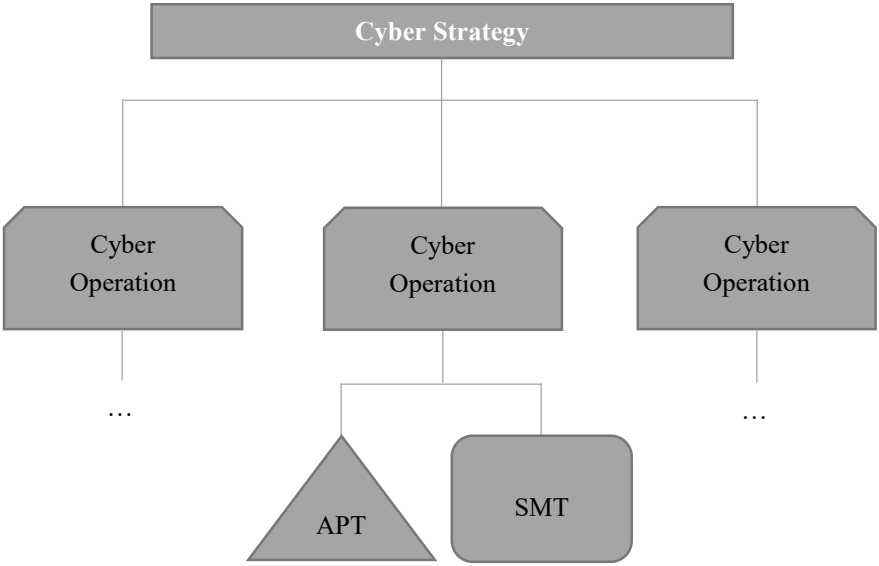

Figure 8

The cyber strategies that are identified and analysed below are deduced from the literature on cyber operations since the 1990's. Some of those strategies have been recurring themes since then (for example cyber deterrence). Others can be derived from traditional strategies such as protracted warfare. Even others are currently being developed and implemented (for example cyber war). This research aims to cover vast parts of the literature on cyber operations in order to derive a complete scale of potential cyber strategies from it. In addition, thinkers from supplementary fields such as Sun Tzu or Bernhard Brodie are integrated to provide a holistic strategic picture. The field of cyber operations is still very young and subject to constant change. Therefore, this section not only serves as a structured collection of cyber strategies, but also as an attempt to further elaborate on those strategies and embed them in a broader strategic framework. From a literature point of view, the strategies of cyber deterrence and *sub rosa* are already substantially researched which in large part is owed to Martin Libicki and the RAND Corporation. This research builds on those contributions but also takes a critical perspective on some of the issues involved. For cyber war, there is no concise definition. Especially the potential for a sole cyber-to-cyber war and attacks using cyber weapons to destroy data and information on computers all over a country (or world) are not yet addressed. For the other two strategies identified in this chapter, *going dark* and *shashou jian*, they are not currently covered in detail in the literature. This is understandable for *going dark* as it is a less complex strategy which is based on reducing vulnerability through disconnecting from the warfare domain. It is not possible in any other domain. This is why the strategy has to be addressed when talking about cyber operations. *Shashou jian* is an ancient Chinese concept which seems to be revitalized in the domain of cyber operations. Therefore, older works have been and are currently being adapted (as this work shows) to the cyber domain in order to analyse this option focussing on a more destructive approach as compared to the *sub rosa* strategy (see discussions below).

The structure of the discussion of the cyber strategies follows Winton's framework on warfare theories which contain the following steps: describe, categorise, explain,

connect and anticipate (Winton, 2006). For this chapter, the description and the explanation are merged. Due to the highly asymmetrical nature of cyber operations (Rowe, 2008: 97), its prowess to deception (Libicki, 2007: 80-87) as well as it being '[...] soaked in intelligence' (Libicki, 2009a: 155), the structure is being extended by the point *stratagems* (mentioned by Chaliand, see sub-section 7.1.3). In the first step, the strategy is explained and named. References are made to works of authors which deal with this kind of strategy and how they describe it. In the second step, the cyber strategy is categorized. According to Geers and Rattray, there are three categories of strategic information warfare/ cyber war (Geers, 2011 and Rattray, 2001). These three categories vary by their level of intensity ranging from low to high. Geers defines these categories as: adjunct, limited and unrestricted (Geers, 2011: 26). In addition, the cyber strategies will be analysed based on their possible implementation during peace/ war times and their correlation with other domains. The third step discusses which cyber operations could be subsumed under this particular cyber strategy. Additionally, a connection will also be made to suitable or beneficial cyber security behaviours which are part of the national cyber security strategy. Based on this evaluation, the fourth step discusses potential implications of the strategy and anticipation of its future usability.

A broader look at the strategic picture suggests that cyber strategies in general carry a moderate to high likelihood of escalation and retaliation, despite their intentions to the contrary. Cyber strategies are stealthier and have an increased element of *sub rosa* activities comparted to other kinds of warfare. Winkler gives his advice towards cyber attacks when recommending, '[l]ook for Snakes, not Dragons. Dragons are mythical beasts. Snakes are real and pervasive' (Winkler, 2007: 72). Cyber operations, then, are pervasive. Thus, except for cyber war, all cyber strategies are first and foremost conducted as intelligence-like activities, whereas most of them are still being useful during times of war. The genuine and inherent *sub rosa* character of cyber strategies, 'cyberwarfare qua warfare is soaked in intelligence' (Libicki, 2009: 155), allowed for the borrowing of stratagems from Chinese thinkers because their main strategic perspective was an asymmetrical and deceptive conduct of warfare. A stratagem is 'a

strategic plan that contains a trap or a ruse for the enemy. Many of these stratagems had their origins in events that occurred during the Warring States Period (475-221BC) and the Three Kingdoms Periods (220-280) in China' (Tung and Tung, 2010: xv) and its distinction from strategy is the inclusion of a ruse (Tung and Tung, 2010: xvii). The stratagems however, have an additional use: they help to understand the nuances of differences between the strategies. The strategies have distinct differences but most of them are somehow affiliated with intelligence operations as mentioned. In order to avoid confusion, the stratagems help to point out the unique character of each of those strategies. They therefore help to understand the signalling better as the cyber strategies do not necessarily aim to escalate conflict. It is therefore imperative to understand if the opponent is conducting intelligence operations to siphon information (*sub rosa*) or exert coercive force (*shashou jian*) in order to achieve a specific political objective. Due to the points mentioned above, and the inclusion of stratagems in contemporary cyber operations doctrines such as the Chinese and Russian (Thomas, 2000: 4-5 and Thomas, 2009), the last step deals with the attribution of proper stratagems to each cyber strategy. The subsequent structure for each cyber strategy looks like this:

1. definition and explanation of the strategy with reference to existing works,
2. categorization of the strategy level of intensity, peace or war time operation and linkage to other domains,
3. connection to cyber operations and a cyber security behaviour,
4. anticipation of strategic implications and
5. attribution of matching stratagems.

Table 3 provides an overview over the different cyber strategies, their potential operations, favourable cyber security behaviour, state of international relations, level of intensity, risk of escalation and main objective.

	Cyber Operations	Cyber Security Behaviour	State	Maximum Intensity	Risk of Escalation	Main Objective
Going Dark	None	Reactive, Planned	Peace, War	Adjunct	Not Possible	Decreasing the adversary's chances of realizing his objectives which he tries to achieve through the reliance on deterrence, *sub rosa*, *shashou jian* and/ or cyber war strategies.
Deterrence	Denial, Disruption, Degradation	Pro-Active	Peace, War	Unrestricted	Possible	Deterring adversaries from conducting offensive operations.
Sub Rosa	Deception, Denial, Extraction, Degradation	Planned, Pro-Active	Peace, War	Limited	Possible	Information dominance over adversaries and potential adversaries.
Shashou Jian	Deception, Denial, Extraction, Disruption, Degradation	Pro-Active	Peace, War	Unrestricted	Likely	Surgically taking out of adversary's centres of gravity to coerce the enemy.
Cyber War	Denial, Extraction, Disruption, Degradation	Reactive, Planned, Pro-Active	War	Unrestricted	Possible	Supplementing other kinds of operations to achieve their strategic and political objectives. Possible adding a new layer of escalation between intelligence operations and open war: a cyber-to-cyber war.

Table 3

7.4.2 Going Dark

Definition

This strategy is an extended and broader implementation of the security mechanism of air-gaping networks. Going Dark means that all systems and networks which are part of the CNII of a country are neither connected neither to wider networks nor to the

Internet. Gervais mentions this strategy, stating that: '[...] when it comes to states, like North Korea, that are less technologically advanced, cyber reprisals have little effect. Reprisals to cyber attacks, therefore, ought to manifest themselves as physical countermeasures when necessary' (Gervais, 2011: 26). It can also mean that there is no CNII to speak of yet, due to the low level of development of this state. Relying on this strategy shows that the adopting state does not believe in its ability to defend its networks properly – or their vitality, therefore making them go dark completely. Implementing this strategy can be done partially – only the classified networks are air-gaped – or for the active networks and systems structure. The case study in the subsequent chapter shows a practical implementation (and failure) of going dark as cyber strategy for a vital part of the CNII.

Categorization

In discussions of intensity, going dark is an adjunct cyber strategy. It does not provide any offensive capabilities *per se*. Furthermore, this strategy can be conducted during both peace and war times. The going dark strategy is however a supplementary as well as a preventive strategy. It is preventive in the sense that it prevents hostile cyber operations from successful completion to a degree. At the same time, it is a supplementary to other warfare domains. Although relying on a going dark strategy might decrease strategic capabilities which can be derived from the information sharing that would be possible with connected systems and networks (for example between air and ground units for coordination), it does reduce the vulnerabilities of warfare in other domains. As an example, without going dark, information sharing between command and control and bombers in an air power combat situation is possible. If the state decided to go dark, the pilot has to visually identify and manually destroy the target without assistance from command and control. If the state did not decide to go dark, but an attacker exploits the vulnerability arising from it – having a computer network up and running which can be attacked by means of cyber operations – the pilot might receive false coordinates. This does not mean that going dark is a strategic net advantage for other domains, it does however shows that it reduces vulnerabilities.

Connection

As there are no offensive capabilities, this strategy is not linked to any cyber operations. In terms of cyber security behaviour, it can include a reactive and a planned approach. As systems and networks exist though they are not connected to broader networks, they are still vulnerable (as the Olympic Games case study shows). It is therefore possible to adapt a reactive cyber security behaviour, which leads to the hardening of systems and networks whenever they are attacked or compromised. A planned, limited cyber security behaviour can also be implemented though it is less likely to succeed if the networks and systems are connected to the Internet or other networks and therefore could gather more information about how to preventively harden the networks and systems – as a planned approach makes use of available information to protect the systems better.

Anticipation

From a strategic perspective, going dark offers the most vital solution for the security of the CNII. In terms of strategic implications for the state, this strategy might be applicable for some core systems but not across the network of CNII – most systems have to be connected to larger networks, for example the Internet, to be efficient. Going dark means cutting communication and therefore having a negative impact on the economic domain, among others. Applying this approach bluntly only work for countries which have no CNII to speak of. For all other countries, going dark makes only sense when applied to particular systems and networks which do not gain a substantial advantage from being connected to broader networks and/ or the Internet (for example, a computer which controls the processes in a nuclear power plant). It is pertinent for states to identify systems of the CNII which have a positive trade-off from going dark and applying this strategy to them. For the majority of the CNII however (for example military communications or electronic governance) a different strategy has to be adopted.

Stratagems

Two closely related stratagems which fit to the going dark strategy are *retreat in order to go forward* (Tung and Tung, 2010: 89-91) and *watch the fire across the river* (Tung and Tung, 2010: 30-34). These stratagems mean that one should wait patiently or even fall back and choose the right moment to shift to the offense. This can be translated to the adoption of going dark as a strategy during the period when the state has not secured its information infrastructure in order to reduce the vulnerability of such area to attacks. Then, connecting them and using their strategic advantage when vulnerabilities have been reduced and a net advantage of using them – connected to a broader network – has been created. Another stratagem that suits here is *remove the ladder after the ascent* (Tung and Tung, 2010: 237-241). In the case of going dark, there has not been a ladder (connection to a broader network) to begin with. The implication is that the enemy has to fight in the adversary's turf without instruction or back up, as there is no direct connection between the battleground (the air-gaped network) and the origin of the attack. A last stratagem appropriate to going dark would be *the plum tree dies for the peach tree* (Tung and Tung, 2010: 303-307), which translates to sacrificing the least valuable resource. In the case of going dark it means sacrificing the advantages arising from the system being connected to a broader network or the Internet for a decreased vulnerability, to achieve a higher security of the system as a result of the disconnection from any network. Also in this case, this only holds true if through those actions a positive trade-off can be achieved.

7.4.3 Deterrence

Definition

Deterrence in the cyber domain is the most developed and analysed cyber strategy today, if not the only one that has been discussed thoroughly so far. This may partly be the case because deterrence as a strategy has been thoroughly researched, including a glut of literature in game theory, during the advent of nuclear warfare. Therefore, to understand cyber deterrence, it might be prudent to take a look at how nuclear deterrence

worked first[56]. Deterrence is subdivided into deterrence by denial and deterrence by punishment[57]. Deterrence by denial is '[...] to deny an adversary the ability to achieve its military and political objectives [...]' (Gerson, 2009: 33) whereas '[t]he goal of deterrence by punishment is to prevent aggression by threatening greater aggression in the form of painful and perhaps fatal retaliation' (Geers, 2011: 117). Nuclear deterrence, by the allied powers, aimed to generate plausible threat of a nuclear strike in case the Soviet Union would attack, and thus overrun Western Europe with its conventional forces. As the Soviet Union acquired nuclear weapons, nuclear deterrence was the threat of the use of nuclear weapons in case the other party would either start a large-scale conventional war or use nuclear weapons. All this led to an arms race, second strike capabilities, and ultimately to escalation containing smaller-scale strike options (Kugler, 2009: 321-323). The role of the nuclear bomb was subsequently not to win wars but to avert them (Brodie, 1946: 1002). According to Lonsdale,

> *'[f]or any deterrence posture to have a chance of success it must fulfil three criteria. These are commonly referred to as the three Cs of deterrence: capability, commitment and communication. To deter, one must have the capability to prosecute the punishment or denial operations effectively. One must also possess the commitment to go through with the act. [...] Finally, the possession of the said capability and commitment, along with the purpose of the deterrent policy, must be communicated to the actor to be deterred'* (Lonsdale, 2007: 15-16).

[56] For more information on the strategic dimension of nuclear deterrence, see for example Kaplan, F. (1983) *The Wizards of Armageddon*. New York: Simon & Schuster and Kahn, H. (2007) *On Thermonuclear War*. London: Transaction Publishers.

[57] For more information on the difference of deterrence by denial and deterrence by punishment see Snyder, G. (1961) *Deterrence and Defense: Toward a Theory of National Security*. Princeton: Princeton University Press.

The three indicators lead to the most important point, deterrence has to be credible (Kugler, 2009: 324). The adversary has to believe that the opponent's threat of retaliation is credible. If the adversary believes it, he will not attack and is therefore deterred, or as Gray put it: '[t]he deterree has to agree to be deterred, no matter how unwillingly' (Gray, 1999: 338). Nuclear deterrence however has so far only been effective against states, not so much against individuals and groups (Kristensen, 2008: 808).

One common misconception about cyber deterrence is to be highlighted first. Deriving cyber deterrence from nuclear deterrence means that cyber operations are used as a means to deter any domain adversarial aggression. Cyber deterrence does not mean the use of any domain means to deter an adversarial cyber aggression. The threat of use of nuclear weapons as retaliation for a cyber attack is not *cyber* deterrence but *nuclear* deterrence. If both stakeholders then implement cyber retaliation, it might lead to a 'mutually assured disruption' (Geers, 2011: 122)[58]. For a cyber deterrence strategy to be effective, Kugler sets the following requirements (Kugler, 2009: 331-336):

1. strong declaratory policy,
2. high global situational awareness,
3. effective command and control,
4. strong cyber defenses,
5. multifaceted counter-cyber offensive capabilities,
6. interagency cooperation and collaboration with allies and partners,
7. metrics and experiments.

This list shows that deterrence in the cyber domain needs offensive and defensive capabilities to be in place at the same time to create a credible deterrence unlike the concept of Mutually Assured Destruction (MAD) in the nuclear realm. However, airtight defensive security could make up for the lack of offensive capabilities. The

[58] More information about possible escalation deduced from cyber strategies can be found in chapter V.

ultimate aim subsequently is to increase the own security. Kugler states that '[...] the potential payoff of a well-conceived cyber deterrence strategy is considerably greater security than exists today' (Kugler, 2009: 340). Deterrence using cyber operations can be implemented in various ways. Payne and Walton define three types of deterrence 1. deterrence as direct attack, 2. deterrence as preventing from doing a provocative act and 3. aggression becomes unprofitable (Payne and Walton, 2002: 166). Kugler's suggestions are similar. He states that the three types of how deterrence in the framework of cyber operations could work are 1. deterrence by denying benefits, 2. deterrence by incentives as well as 3. deterrence by imposing costs (Kugler, 2009: 327).

Deterrence is not an either-or decision. Strategies can all work at once, or equally fail together. Therefore, Starr suggested a concept where cyber deterrence is custom-tailored to the adversary (Starr, 2009: 22). In the case of states, Starr suggests to carry out cyber espionage activities against them to be able to tailor the deterrence strategy. This conclusion can be derived from the nature of cyber armoury (see chapter II). If state A were able to penetrate the networks of state B, it can be assumed that malicious software has been planted, the perception is a persuasive here as actuality. Therefore, state B might be deterred from attacking A because it assumes that A can detonate those *timebombs* any time. In addition, A might have gained knowledge about the weapons that B has and can harden and shield its networks from likely retaliation which effectively render B's potential attacks useless. A might have even found more vulnerabilities to exploit B's networks for future endeavours. Therefore, a credible cyber deterrence needs to be custom-tailored and relies on information acquired through intelligence operations.

Despite the opportunities mentioned, cyber deterrence faces several challenges and some authors therefore regard it as void (Clarke and Knake, 2010: 46 and Lan and Xin, 2010: 1). Lewis for example states that, '[t]he fundamental assumption is that a correct interpretation by opponents will lead them to reject certain courses of action as too risky or too expensive. The problem is that potential opponents may misinterpret deterrent threats while others may be not feel threatened, and are therefore harder to deter' (Lewis,

2010: 1). In case of cyber deterrence against cyber attacks, the primary challenge is proper attribution, mentioned earlier this chapter, which undermines the credibility of cyber deterrence to a large degree. If an attacker cannot be properly identified, it cannot produce deterrence. Thus, cyber deterrence fails. If an attacker can be identified, it can still be an act of deception. There can be no proof whether the clues leading to the possible attacker are genuine or as distraction as part of a deceiving cyber operation. Therefore, cyber deterrence would also fail as long as no perpetrator officially takes responsibility for the attack. Even then, terrorists for example might claim ownership of a cyber attack to spread terror, whereas the actual attacker does not want to make his involvement public. Hence, the lack of proper attribution is a large problem for credibility, and hence successful deterrence.

Another challenge is that some cyber attacks might be too small to retaliate against (Kugler, 2009: 329) and subsequently undermine a zero tolerance policy (Habiger, 2010: 28). If a state communicates that it will retaliate against every cyber attack (zero tolerance) it is doomed to fail because of the sheer number of attacks and the lack of resources to respond to them. Having declared retaliation against every cyber attack but failing to do so, undermines a state's credibility. The political level therefore has to set and communicate a threshold: how much damage a cyber attack has to do for a cyber retaliation to trigger and therefore deterrence to take place. All cyber attacks below this threshold do not produce the effect of deterrence. The other option would be the implementation of a zero tolerance policy which would inadvertently fail and therefore diminish the credibility of cyber deterrence.

Cyber deterrence against cyber attacks (as well as other attacks) struggles to deal effectively with non-state stakeholders (Libicki, 2009b: 2-3). While not covered by this research, this potential challenge warrants mention. The threat of wiping an individual's computer is not credible enough to prevent him from trying to shut down the power grid of a country. This leads to the next challenge, the lack of impact in case of cyber retaliation against a state. Compared to nuclear weapons, cyber operations lack the ability for mutual assured destruction (Adams, 2001: 106-107) or 'unexpected higher-

order effects' (Starr, 2009: 22). If country A plans to invade country B and has a high chance of success, A would unlikely be deterred by B's potential to shut down the power grid and wipe important databases. A is more likely to be deterred, however if B could wipe-out A's capital city as a response to the invasion. Due to the nature of cyber weapons, cyber deterrence as a strategy also faces the problem that most cyber weapons are one use only (Habiger, 2010: 32). They exploit vulnerabilities and once the adversary notices, he can fix the vulnerability and therefore render the weapon useless (against him). The knowledge of this increases the threshold of retaliation for the deterrer owing to a hesitancy to use up his cyber arsenal. This increases the threshold to a level that retaliation as a result from cyber deterrence always borders between escalation and impunity, (Kugler, 2009: 330-331) or as Hjortdal puts it '[t]he strategy of deterrence is thus two-sided and, as such, contradictory—a balancing act is needed between hiding the maximum level of capability on the one hand, and communicating and proving that the capability exists on a sufficiently high level to deter other states on the other' (Hjortdal, 2011: 4), a thin line. For further research on this issue, when taking into account a multi-stakeholder setting, cyber deterrence faces the challenge of extended cyber defence and collective cyber retaliation only to work if applied *sub rosa* but not publicly (Libicki, 2009a: 105).

Sharma sees cyber deterrence as the only vital defence against cyber attacks (Sharma, 2009: 12). This is partly accurate. It is the only viable cyber defence strategy which can be applied across the CNII - as opposed to going dark which can only be partly applied. However, cyber deterrence is heavily restricted in what it can do. As discussed in chapter two on cyber armoury, deterrence by denial of access to the technology is not possible. As shown in the discussion above, deterrence by punishment is however viable under certain conditions. It only works against cyber operations or other low intensity applications of warfare. A full scale traditional invasion or the use of nuclear weapons can hardly be deterred by the punishment with cyber operations. Deterrence by punishment through cyber operations against low level applications of warfare can be implemented through imposing costs (for example through a direct attack), through

denying benefits (for example due to a strong defence) as well as through incentives (for example a mutual agreement to stop *sub rosa* activities). A cyber deterrence strategy, while it exists, has limited usability.

Categorization

For deterrence to be credible, a possible retaliation should the carried out with a similar or higher level of intensity than the original attack, without necessarily entering into a circle of escalation. Deterrence can be applied during any stage of international relations, also intra-war as escalation dominance. Therefore, for cyber deterrence to be credible, the intensity level of the offensive actions can either be adjunct, limited or unrestricted, putting the highest level of intensity to unrestricted.

Deterrence is, in general, perceived as a peacetime activity – to deter the enemy from certain actions which might lead to a war. As mentioned, deterrence also works as an intra-war strategy. In this case, one or more stakeholder is deterred from increasing the intensity of their actions. Referring to the Cold War, the NATO and the Soviet Union were supporting armies in what is known as 'proxy wars', without any use of nuclear weapons. In case that either of those stakeholders would have tried to seize West/ East Germany however, they threatened each other with the use of nuclear weapons. This deterrence worked effectively due to the possible negative pay-off for the attacker. Cyber operations have proven to be able to affect CNII such as nuclear enrichment and research facilities (see case study on Olympic Games). In addition, cyber operations benefit from the element of surprise. Neither literature nor incidents allow for a coherent analysis of what cyber operations are capable of disrupting or destroying yet. It casts a fog of war over its potential. For those two reasons, cyber deterrence can be used as a peace and as a war time strategy.

Though cyber deterrence aims to prevent war or preventing increased violence (intensity), it has the potential to escalate both. If the deterring threat is not credible – or not being perceived to be so - an attack might be answered with a retaliation of higher intensity. This can lead to a vicious circle of escalation.

Connection

Cyber deterrence relies on a close connection of offensive and defensive cyber capabilities. Libicki summarized it coherently, saying '[i]f cyber deterrence works, less money has to be spent on cyber defense – if cyber defense is perfect, there is no need for cyber deterrence – for cyber deterrence to work there have to be cyber defense (catching the culprit) and cyber offense (finding him, dealing damage to him' (Libicki, 2009a: 35-36). Cyber deterrence puts increased weight on the offensive side (Graumann, 2012: 16-17) unless it focuses on deterrence by denial which can be achieved through robust defences. Comparing it to nuclear deterrence, Sulek and Moran state that '[t]oday in cyberspace, developing offensive capabilities is inexpensive, especially compared to the enormous costs of developing cyber defense-in-depth strategies. The obvious differences between SDI and cyber warfare center on their application. SDI was inherently defensive in nature, whereas cyber warfare is perceived as primarily a stealthy, offensive weapon' (Sulek and Moran, 2009: 124).

In terms of cyber security behaviour, it is the pro-active cyber security which can form a vital part of the cyber deterrence strategy. It puts premium on network security and encourages planning, for example through honey pots, and creates opportunities for offensive actions through the implementation of back doors amongst others. This behaviour therefore might be closely connected to extraction cyber operations. In terms of offensive cyber capabilities, a cyber deterrence strategy is based on denying, disrupting and degrading operations. Which operations or combinations thereof are implemented depends on the level of intensity. To retaliate against a low intensity attack, a denial operation might be sufficient, while the complete degradation and disruption of an adversary's system and networks can be an attempt to stall the intensity of a war based on escalation dominance.

Anticipation

Kugler assumes that a good cyber deterrence strategy reduces the probability of medium intensity cyber attacks as well as the probability of full-scale cyber attacks (they will then only be of medium intensity at most) (Kugler, 2009: 326). Most of the remaining

cyber attacks would then be taken care of by the increased defensive capabilities of the cyber deterrence strategy. Full-scale cyber attacks would be reduced because going 'all-in' would likely result into *escalation dominance* (Clarke and Knake, 2010: 206-209). This escalation might then be fought with more than only cyber weapons. The more military and crucial private sectors (for example power) become interconnected and 'smart', the vaster the CNII becomes. This does not only allow for new vulnerabilities but also for a more damaging impact of a cyber attack. Therefore, cyber deterrence is going to play a crucial role not only deterring cyber attacks, but also deterring against conventional attacks. Though Olympic Games demonstrated the current abilities of a potent cyber attack, not much is yet known about possible impact and the states which have the ability to cause this kind of damage. The more we will see attacks of this kind, the more cyber deterrence will establish as a deterring activity also against conventional warfare.

Stratagems

There are several stratagems which fit to the cyber deterrence strategy. The first one called *take counsel in one's temple* (Tung and Tung, 2010: 41-46). It refers to introspection. As discussed, a vital part of deterrence by denial is a strong protection/ security of CNII. If an adversary cannot find a way to overcome the protection and subsequently realise his strategic or political objectives, deterrence can work. A second stratagem which has reference to deterrence is to *offend in order to defend* (Tung and Tung, 2010: 216-218). While the other stratagem referred to deterrence by denial, this stratagem has a closer connection to deterrence by punishment. As a reaction to the adversary's actions, the defending party can react with offensive measures in order to deter the enemy from further attacks or increasing the intensity of the conflict. That is, if proper attribution is possible. Another stratagem which can be connected to deterrence is *decorate the tree with bogus blossoms* (Tung and Tung, 2010: 157-160). As mentioned above, deterrence is in general based on the four Cs: capability, commitment and communication as well as, ultimately, credibility. For the deterred, the threat has to be credible. This does not mean, that the threat has to exist in actuality, it

just means that the adversary has to perceive it as a credible threat. If the deterring party is not able to create a deterring threat (for example strong defences or strong offenses), it can still try to create the image of a credible threat: *bogus blossoms* – a deception or ruse. As much as deterrence can fail, though there is a credible threat, deterrence can also succeed without it. It depends on the perception of the party that is to be deterred.

7.4.4 *Sub Rosa*

Definition

Extraction and disruption operations using networks and computer system have been coined *sub rosa* activities by Libicki. Subsequently, *sub rosa* cyber strategy 'has some aspects of intelligence operations, and some aspects of special operations – although it is neither. Of note, sub rosa warfare is almost impossible to conduct with tanks, much less nuclear weapons' (Libicki, 2009b: 1-2). *Sub rosa* cyber strategy are covered in some works in a blurred pool of cyber operations, information warfare and intelligence operations, but not often distinctly discussed as a single and genuine strategy or approach. It bears close resemblance with traditional *sub rosa* activities such as espionage or sabotage but is conducted through cyber operations. Thus, a *sub rosa* cyber strategy can be part of a major intelligence operation which also involves other elements such as human intelligence (HUMINT).

States are aware of this strategy, as Gervais suggests when stating that '[a]necdotal evidence suggests that cyber espionage is a familiar practice of state governments' (Gervais, 2011: 8). Betz and Stevens even suggest that *sub rosa* cyber strategy are aspiring to be the most prevalent cyber strategy, as compared with strategies with a higher level of intensity (Betz and Stevens, 2011: 81-82). The distinction between *sub rosa* operations and other strategies is coherently summarized by Libicki,

> *'[a]n attack can be sub rosa only if the effects are limited to entities (such as state entities whose outputs are opaque and who believe in keeping secrets) or if the attacks could conceivably be ascribed to something other than hacking. The target has a good deal to say about whether an attack is sub rosa; yet, if attackers want to leave open the possibility of a sub rosa attack*

> *they have to avoid having such attacks affect the broad public but in ways that cannot be credibly ascribed to accident. They cannot take credit for an attack, which means that it cannot be used for certain forms of coercion'* (Libicki, 2009b: 6).

A *sub rosa* cyber strategy is only *sub rosa* as long as both parties agree it to be, or as Libicki phrases it: '[p]aradoxically, maintaining sub rosa warfare requires the tacit assent of the other side, and is therefore quite fragile' (Libicki, 2009b: 13). The reason to keep it secret is that the less the public knows, the easier it is to de-escalate the conflict (Libicki, 2009b: 8). If one of the stakeholders decides to end its secretive conduct, the *sub rosa* operations, if continued, turn into for example *shashou jian* strategy (explained below). This strategy has a higher level of intensity and therefore does not only mean to turn a covert operation overt, but also to increase the risk of escalation and subsequent retaliation. Keeping operations *sub rosa* through this strategy means decreasing the likelihood of entering the retaliation cycle (Libicki, 2009b: 2). The more intense and physical *sub rosa* operations are, the more likely they are to escalate. If state A shuts down state B's power grid, B is politically pressured to react – even more so if the perpetrator becomes public knowledge. The *sub rosa* cyber strategy is therefore a limited intensity strategy with a likelihood of the involved stakeholders being aware of the operations but deliberately keeping them covert in order to avoid decreasing political leeway.

There is a thin line between a *sub rosa* cyber strategy and the *shashou jian* cyber strategy which is explained later. It is prudent however to differentiate those two strategies from one another for several reasons. Apart from the difference in indicators which are discussed in the respective categorization paragraphs, the core distinction is that the *sub rosa* strategy mainly refers to intelligence, not sabotage. This crucial element coincides with the covertness of a *sub rosa* cyber strategy as compared to a potentially overt character of *shashou jian* operations as acts of sabotage are more difficult to keep covert. *Sub rosa*, is not, however, anything new. It is covert intelligence operations carried out through the use of cyber operations. Therefore it is necessary to distinguish it from other cyber strategies, it is less necessary to do so from other intelligence operations.

Categorization

The intensity of a *sub rosa* cyber strategy is limited. It can range from simple reconnaissance (probing the adversary's systems) to extraction (siphoning information) or even disruption (denial-of-services). As explained above, the latter is unlikely to remain covert or accepted by the adversary and ignored. Sharma describes cyber sabotage (disruption) as pre-war activity (Sharma, 2009: 8-9) because it possibly leads to more intense hostilities, possibly ending in the outbreak of a war. Therefore, it would more likely to fall under the framework of the *shashou jian* strategy. The intensity of a *sub rosa* cyber strategy therefore ranges from adjunct to limited. A *sub rosa* cyber strategy can be carried out during peace and war times similar to other intelligence operations. A *sub rosa* cyber strategy can be a supplement to other intelligence operations, as well as the conduct of various kinds of warfare. The strategy bears a potential for escalation if discovered and properly attributed. However, owing to the difficulties of attribution, the potential for escalation is reasonably low.

Connection

The four kinds of cyber operations which can be associated with the *sub rosa* cyber strategy: deception, denial, extraction and disruption. Deception aims to keep the strategy and its operations covert as long as possible. In the event of discovery, deception operations can support a victim's desire to maintain *sub rosa* conditions and retaliate instead of making it public. Denial operations can be used in supplement to other operations during war time. During peace periods, denial operations can prod the enemy into action or support deceptive or extraction operations by diverting the attention. Extraction operations within the framework of a *sub rosa* cyber strategy are used to steal information either as an ends or as means to further exploit the enemies networks and systems. A *sub rosa* cyber strategy therefore can be a prelude to more intense strategies of cyber operations (finding possible vulnerabilities) or less intense strategies of cyber operations (knowing the adversary's weapons and how to defend against it). Disruption operations are used as means of sabotage. They are situated on the higher level of escalation risk within this strategy and might be the prelude to a more

intense cyber strategy (such as *shashou jian*) or even war. These operations might also be carried out in the framework of a *sub rosa* cyber strategy during war times to support other intelligence operations. Implementing a *sub rosa* cyber strategy comes with a risk of attracting offensive counter operations. Therefore, a planned or pro-active cyber security is deemed necessary to go along with the adoption of the *sub rosa* cyber strategy. As a *sub rosa* cyber strategy might also be aim to discover the adversary's cyber armoury, it might be a mutual benefit to adopt a planned or pro-active cyber security behaviour as it can be improved based on the information which are derived from the *sub rosa* cyber strategy itself.

Anticipation

If a state runs intelligence operations, it is likely to adopt a *sub rosa* cyber strategy as well. As discussed earlier, the resources needed to conduct cyber operations are comparatively low, as is the risk of discovery. The s*ub rosa* cyber strategy is also very versatile as it can be conducted any time with a range of intensity and different operations. Due to such characteristics, the strategy is likely to be the most adopted one. A state adopting a *sub rosa* cyber strategy should however be aware that it bears a risk of retaliation and escalation.

Stratagems

As a *sub rosa* cyber strategy is conducted covertly, it is a reasonable approach to test an adversary's response. Therefore, the two stratagems: *find the way in the dark by throwing a stone* (Tung and Tung, 2010: 36-40) and *beat the grass to startle the snake* (Tung and Tung, 2010: 185-188) go well with this cyber strategy. They refer to a testing of boundaries and provoking reactions from the enemy. If a *sub rosa* cyber strategy is used as a preparation for war, this stratagem can also be interpreted in the way that vulnerabilities are being discovered by poking the adversary's defences to see what happens – or even prodding the adversary.

Carrying out a *sub rosa* cyber strategy in order to gain information dominance over the enemy is referred to by Tung and Tung as *to win hands down* (Tung and Tung, 2010: 46-49). This stratagem is more prominently known as: '[k]now the enemy and know

yourself; in a hundred battles you will never be in peril' (Griffith, 1963: 84). The *sub rosa* cyber strategy might lead to the possession of vital information about the adversary which ultimately gives an advantage in a conflict. In case of cyber operations, this stratagem becomes even more important as information about cyber armoury and vulnerabilities can render weapons completely useless and open doors to the enemy's CNII without much effort.

Due to the possible deception operations which are genuine to a *sub rosa* cyber strategy, another stratagem might fit the strategy: *pretend to advance along one path while secretly going along another* (Tung and Tung, 2010: 79-82). This refers to the use of deception operations in order to throw the adversary off the trail and so efficiently carry out extraction or disruption operations. Keeping the complexity of cyber operations and their frictions in mind, instead of just throwing the victim off the trail, a *sub rosa* cyber strategy could aim at making someone else take the fall through setting him up. Cyber weapons often include lines of code which are not part of the coding, for example a link to a flag or a citation from a religious work, as indicator who created the weapon. This can be used to set a state up the same way as the re-direction of an attack through the server of a foreign state could. In this case, the stratagem to *kill with a borrowed knife* (Tung and Tung, 2010: 128-132) would be suitable.

7.4.5 *Shashou Jian*

Definition

Shashou jian is the Chinese translation for *assassin's mace*, a strategy which refers to the ability of striking the enemy decisively and stealthily - making the fight fit the weapons (Clarke and Knacke, 2010: 51 and Navrozov, 2005). Incorporating this strategy into the cyber operations framework is based on the evident Chinese use of *shashou jian* as a means to achieve its geo-strategic goals (Navrozov, 2005). The use of the term in this work might exceed the depth of *shashou jian* in the Chinese original meaning. It seems however useful to keep the term and extend the description as it reflects not only the use by Chinese strategists in general but also the connection of Sun

Tzu's[59] teachings to this concept. Sun Tzu describes this kind of strategy in his writings as relying on speed, stating that '[s]peed is the essence of war. Take advantage of the enemy's unpreparedness, travel by unexpected routes and strike him where he has taken no precautions' (Griffith, 1963: 134). In conventional terms, an assassin's mace strategy can be pictured as an attacker coming out from cover to deal a swift blow to the victim – and at once disappearing. One of the earliest incidents which can be attributed to a *shashou jian* cyber strategy was the 1982 Siberian pipeline explosion, caused by rigged software (Rid, 2012: 6). It fits the profile of *shashou jian* but evidence that this event happened the way Rid describes it is scarce. Riley and Vance refer to the current environment as chaotic, stating that '[t]his Code War era is no superpower stare-down; it's more like Europe in 1938, when the Continent was in chaos and global conflict seemed inevitable' (Riley and Vance, 2011). In the aftermath of the attack, there is increased noise (for example of signals) offering an enabling environment for an assassin's mace strategy. The assassin will be able to easily find cover in this noise. Various stakeholders, such as cyber criminals and states engage in numerous cyber attacks. Paired with the problem of proper attribution, attacks can go unnoticed or unattributed. There is so much activity going on that one attack is difficult to pinpoint and trace.

Libicki discusses three key roles which a cyber attack might play: '[i]t might cripple adversary capabilities quickly, if the adversary is caught by surprise. It can be used as a rapier in limited situations, thereby affording a temporary but potentially decisive military advantage. It can also inhibit the adversary from using its system confidently' (Libicki, 2009a: 142). All the three roles are goals that can be achieved with a *shashou jian* cyber strategy. It aims at the decisive points (Jomini, 1868: 85-87) or centres of gravity (Rattray, 2001: 130) of the enemy to carry out a precise blow, ignoring the rules

[59] The author acknowledges at this point that it might be prudent to write a stand-alone comparative work of Sun Tzu's teachings and contemporary strategic use of cyber operations.

of conduct (Fritz, 2008: 64) to achieve a *coup de grâce*[60] (Tse-Tung, 1867: 162-163). One targeted blow against parts of the CNII that bring about a huge impact (for example bringing down the state's entire power grid). Fritz, for example, discusses that a possible attack carried out within the *shashou jian* strategy could aim to shut down American relay stations, hence ceasing the US satellite's reliability (Fritz, 2008: 64). This would be an intra-war use of a *shashou jian* cyber strategy. As the case study in section 8 shows, the immediate impact was the loss of confidence in the systems, as the engineers could not find why their systems went haywire and what caused it.

Shashou jian is very versatile can be carried out in the framework of warfare or under the umbrella of intelligence operations. When linked to the latter, it is most likely affiliated with *sabotage* rather than espionage activities. Based on the terminology of this work, it relies more on disruption than extraction operations. *Shashou jian* does not necessarily work in supplement to other forms of warfare or intelligence operations, but can be a standalone strategy. Hence, *sub rosa* and *shashou jian* are not only cyber strategies, but can also be conducted under the umbrella of intelligence operations. Even if to distinguish between espionage and sabotage activities seems arbitrary, it is not. The genuine difference between *sub rosa* and *shashou jian* strategies is that *shashou jian* still works as an overt operation after it has successfully been carried out stealthily. The Olympic Games case study in is an example for operations carried out in the framework of a *shashou jian* cyber strategy (see section 8).

Categorization

The *shashou jian* strategy is implemented with a limited to unrestricted level of intensity. As discussed, it can be used during time of peace as a very strong instrument for coercion or to demonstrate force. It can also have a vital role as a strategy during war, in order to supplement conventional warfare or as standalone tool. Due to the nature of cyber operations, the weaker stakeholder might put a premium on *shashou jian* in order to make up for its lack of conventional forces – aiming to negate the

[60] From the French: *death blow.*

advantage of the adversary as much as possible. As mentioned above, the shutdown of relay stations and therefore the denial of the use of satellite imagery would ultimately decrease the power of the superior forces. Due to its intensity, with a premium on disruption and degradation operations, this strategy bears a strong potential for escalation – though it does contain elements of stealth and deception, if carried out covertly.

Anticipation

In order to deliver a political message or coerce an enemy, *shashou jian* has to sacrifice some of its secrecy and stealth for signalling the adversary who sends the message. All of this increases the likelihood of proper attribution and therefore the probability of escalation. Hence, it can be distinguished from the *sub rosa* operations strategy, which does rely on sending a message and is risk-averse (in terms of escalation).

Contrary to what Libicki assumes, when he argues that '[a]s a threat, it [cyberwar] may not be believed; as a reality, it may not cause enough cumulative damage to make the target cry uncle' (Libicki, 2009a: 137), the *shashou jian* strategy has the ability to coerce an enemy. The case study of the Olympic Games shows the impact of the implementation of a *shashou jian* strategy. It can also be used to breaking the will of an adversary so that the attacker actually never has to fight him (Kilroy, 2008: 443) in a conventional way. This statement reflects the standalone functionality of cyber operations in general which is supported by Billo and Chang. They argue that cyber operations might be a 'substitute for being outgunned in traditional military' (Billo and Chang, 2004: 34). Subsequently, cyber operations in general can be implemented not only in supplement to traditional warfare, but also as a surrogate for conventional warfare. This is especially the case with the *shashou jian* strategy as it has the potential to coerce an adversary by hitting the centres of gravity – the CNII – even without being a supplement to, or supplemented by, conventional forms of warfare.

In conclusion, *shashou jian* is the most universal of the cyber strategies presented in this paper as it includes offensive capabilities in varying degrees during peace and war

times with a range of different operations. It can be carried out overtly or covertly and includes decisive strikes with the potential for escalation and coercion.

Connection

Shashou jian encompasses the whole spectrum of cyber operations. Deception and denial operations, in combination with extraction operations, can be used in order to disguise the attacks and allow for plausible deniability. Those operations, metaphorically speaking, create the assassin's mentality of hiding in the shadows. Disruption and degradation operations on the other hand – also in possible combination with extraction operations – can be implemented to strike against the adversary's centres of gravity. They constitute, metaphorically speaking, the mace. As *shashou jian* is an entirely offensive strategy, the most suitable cyber security behaviour is a pro-active cyber security. It adds to the offensive capabilities of this strategy.

Stratagems

There are a number of stratagems which highlight the features and characteristics of *shashou jian*. The resemblance is high due to the fact that Chinese strategies, especially in the field of cyber operations, are based on the writing of Chinese strategists such as Sun Tzu or Mao Tse-Tung, as well as of those who brought together the initial 36 stratagems. The following stratagems describe well the deceiving and stealthy character of the *shashou jian* strategy. From a perspective about deception, suitable stratagems include *make a feint to the east and attack the west* (Tung and Tung, 2010: 76-78). A deception supporting the opportunity of finding the weak spot of the enemy to strike at. This kind of operation can also be read from the stratagem to *play double-faced and attack somebody from behind* (Tung and Tung, 2010: 110-112) or to 'march by an indirect route and divert the enemy by enticing him with bait. In doing so, you may set out after him and arrive before him. One who is able to do this understands the strategy of the direct and the indirect' (Griffith, 1963: 102). A concise and popular stratagem simply says *hide a dagger in a smile* (Tung and Tung, 2010: 110-112) as reference to moving in secret and then striking decisively.

How decisive a strike through the *shashou jian* strategy can be is also represented in several stratagems. The most popular one is to *offend in order to defend* (Tung and Tung, 2010: 169-173). This offense however should *aim at swift victory and avoid prolonged campaign* (Tung and Tung, 2010: 265-267). Taking into account the nature of cyber weapons and the ability to defend against them once they have been used, supports this perspective of achieving the aim as soon as possible. In the framework of stratagems, the goal of a swift attack should be to either *remove the firewood under the cooking pot* (Tung and Tung, 2010: 169-173) or simply to *defeat the enemy by capturing their chief* (Tung and Tung, 2010: 233-237). Those stratagems reflect the shock and awe impact, aiming at a figurative decapitation.

Intrinsic to the *shashou jian* is, as mentioned by Fritz, a high level of flexibility and adaptability, ignoring rules of conduct, translated: *not to be bound by fixed rules, but vary the plan according to the situation of the enemy* (Tung and Tung, 2010: 249-251). In order to bear respect to the high level of complexity of this strategy, with its multiple options for means and aims, *shashou jian* uses *the stratagem with a set of interlocking stratagems* (Tung and Tung, 2010: 292-298). Those stratagems are to be carried out simultaneously, after one another or linked through what-if connections. Being a peace and war time strategy as supplement and even as surrogate warfare, *shashou jian* can be highly complex, universal and valuable.

7.4.6 Cyber War

Definition

Schneier analyses the strategy of cyber war appropriately, '[a]nd for there to be a cyberwar, there first needs to be a war' (Schneier, 2009). Libicki phrased it similarly arguing that, '[o]perational cyberwar consists of wartime cyber attacks against military targets and military-related civilian targets' (Libicki, 2009a: 139). One of the options for cyber operations is to supplement conventional warfare (Clarke and Knake, 2010: 9-11) the research refers to this strategy as cyber war. The often hyped 'First Cyberwar' against Estonia was merely a precursor to fully-fledged cyber war; conducted with low

technology means and without any formal declaration of war (Cavelty, 2007: 15). At the same time, there were no conventional forms of warfare which those attacks supplemented. If a state of war had been acknowledged by either one or both of the participating states (Estonia and, arguably, Russia), the operations could have been described as being embedded in a cyber war strategy. Assuming that a state was behind the attacks against Estonia, the 'first cyber war' looks more like cyber civil disobedience or, at most, operations within the *shashou jian* framework rather than part of a cyber war strategy.

The intensity and objectives with which cyber war can supplement conventional warfarevaries. Lonsdale mentioned the ability of cyber warfare to substitute tactical bombing (Lonsdale, 2004: 137). In general, the intensity of cyber operations during a cyber war is not limited. As Libicki puts it: 'once something is called war, a victim's responsibility for the consequences of its acts dissipates' (Libicki, 1996: 104-105). Compared to the other kinds of cyber operations, escalation plays a minor role, given that war is already underway. The war can still turn from conventional and cyber weapons to using nuclear weapons (an escalation) but the probability that cyber operations contribute to this escalation rather than conventional warfare is comparatively low. A state would probably more be worried and prone to escalate as response to armies invading its territory and killing its citizens and armies than about the loss of electricity in the capital for example.

The difference between *shashou jian* and cyber war is not only the setting (cyber war can only take place during war). In addition, cyber war does not necessarily strike stealthily or at decisive points. A cyber war operation could, for example, aim to use distributed denial-of-service attacks to deny the whole country Internet access. It could also utilize destructive viruses to destroy as much data and information within the adversary's state (including private computers, companies etc.) as possible. These broad, destructive and overt operations could be part of a coercing cyber war strategy. They would not fall within a *shashou jian* framework.

Categorization

The intensity level of cyber operations implemented through a cyber war strategy can vary in intensity, reaching towards unrestricted. Operations during a cyber war are supplementary to the conventional war efforts, if there are any. This does not mean that cyber operations during cyber war cannot be conducted as standalone operations. It rather means that cyber operations follow the same objectives as the war *per se* and are implemented as yet another means to achieve them – or to help achieve them. An example would be the shutdown of the Syrian air defences during an air raid as it arguably happened in the Israel-Syria conflict (Page, 2007). A war solely conducted with cyber operations, a pure cyber war, did not take place, yet. It would mean that two or more states are attacking each other overtly solely with cyber means (viruses, denial-of-service attacks etc.). This then would constitute the first cyber war.

Connection

Cyber operations used in a cyber war strategy can be either denial, disruption, degradation or extraction. Extraction operations can be vital to gather intelligence on the enemy and on the deployment of its troops. As shown in the Israel-Syria case, disruption and denial operations can aim to temporarily provide forces with an edge over the adversary through disabling defences and alike. Degradation operations can be implemented to counter adversary's cyber capabilities or delete their intelligence gathering as well as shutting down systems and networks for a longer period of time than disruption or denial operations.

A cyber war strategy focuses primarily on supplementing conventional warfare efforts to be more efficient in achieving their aims. Therefore, cyber security behaviour can either be reactive, planned or pro-active. It depends to a large degree on the enemy how well maintained the own cyber security has to be. During war time, other – conventional – security might be more important than cyber security, depending on one's own cyber vulnerabilities. In the case of a sole cyber-to-cyber war, cyber security has necessarily to be pro-active. In those circumstances, cyber security will be of utmost importance.

Anticipation

The cyber war strategy adds a new kind of warfare or domain to the existing domains of land, sea, air and space. Subsequently, states which are keen on their military forces will start to prepare for a cyber war strategy along with the other four. Compared to the other domains, the cyber domain has the advantage of being easier and cheaper to implement and catch up with. It offers at the same time a benefit in the asymmetrical framework of war. Therefore, it can be anticipated that states would rather push for the implementation of warfare capabilities within the cyber domain than in other domains. Other powers, which have a higher budget and better levels of sophistication are currently focusing on warfare capabilities in this area – such as the United States, the United Kingdom, Russia, China and Australia. In the years to come, cyber war will likely become a standard strategy accompanying conventional war, wherever it goes. It remains yet to be seen if sole cyber-to-cyber wars might become a surrogate for traditional wars or an escalation level between intelligence operations and traditional war. It is also very likely that, as Dipert puts it, 'a Cyber Cold War would be multilateral rather than bilateral' (Dipert, 2010: 403), attracting a number of third parties. This kind of setup is unlikely to be desired by the involved powers. The probability of a cyber-to-cyber war can therefore be regarded as low for now.

Stratagems

The stratagem to *outwit by novelty* (Tung and Tung, 2010: 226-230) fits cyber war very well. More and more states are working on their capabilities, but most of them are still vulnerable to operations within the cyber war framework. In addition, cyber war has not yet been implemented on a large scale as supplement to conventional war, therefore not shown its entire capabilities. This allows for a moment of surprise when this happens.

During a state of war, cyber war might only fulfil a support function. This allows operations in cyber war to wait and take advantage of opportunities that might open up. As to the stratagems, there are two which describe this behaviour, one is to *avoid the important and dwell on the trivial* (Tung and Tung, 2010: 260-264) and the other is to *take away a goat in passing* (Tung and Tung, 2010: 57-60). Operations will be

implemented during an opportune moment but do not always need to be implemented to be efficient.

Looking at it from a different perspective, the cyber war strategy might also allow the enemy to use the stratagem of *fish*[ing] *in murky waters* (Tung and Tung, 2010: 154-157). Through disruption and denial operations, alongside occasional degradation operations, the adversary will be dragged into chaos and defeated by the conventional war efforts. This would be the case if the power grids are shut down and the use of military communications is disrupted with cyber operations before the conventional forces can strike easily.

7.5 Cyber Strategy, Political Objectives and National Power

Every cyber strategy is composed not only of cyber operations but also on suitable cyber security behaviour. Therefore, a cyber strategy, together with a cyber security strategy, allow for the implementation of a political objective. As shown in the discussions of the cyber strategies, it makes sense to integrate a mentioning of valuable cyber security behaviours into the strategies themselves. Therefore, matching the national cyber security strategy with a cyber strategy in order to achieve a political objective is a requirement. Due to the overlapping domains on both sides, for example pro-active cyber security or the deterrence strategy, an interconnection between those two fields is necessary and vital in order to achieve political objectives.

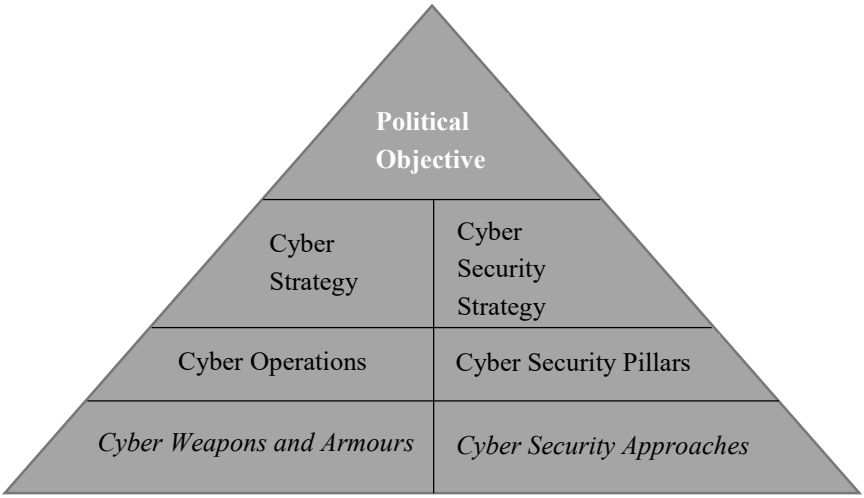

Figure 9

Looking at the five strategies identified it is clear that cyber operations did not 're-invent' the proverbial wheel of strategy. Cyber strategies come in different forms but are not genuinely different from traditional strategies. The strategies also show that the stakeholders implementing cyber strategies are not different to those implementing conventional strategies, '[t]he primary threat comes from other states and intelligence services' (Aljazeera, 2010). In order to put a cyber strategy in general into perspective, it does seem appropriate to adopt the framework of cyber power of Joseph Nye. According to Nye, one part of the national power of a state is cyber power (Nye, 2003). Cyber power however relies on information warfare/ information operations in general rather than only cyber operations and is built on P/DIME: Political/Diplomatic, Information, Military and Economic powers[61]. The cyber strategy aims to achieving political objectives based on military (M) or information (I) power and therefore

[61] For a concise discussion on P/DIME and cyber power see: Starr, S: H. (2009) Towards an Evolving Theory of Cyberpower. In Czosseck, C. and Geers, K. (Eds.) *The Virtual Battlefield: Perspectives on Cyber-Warfare*. Amsterdam: IOS Press, pp. 18-52 and Nye, J. S. (2003) The Information Revolution and the Paradox of American Power, *Proceedings of the Annual Meeting (American Society of International Law)*, 97, pp. 67-75.

represents a part of the national cyber power, hence a fraction of the national power of a given state (see figure 10). Translated into the Nye's framework, the definition would translate to information instruments for the implementation of hard power intra- and extra-cyberspace[62].

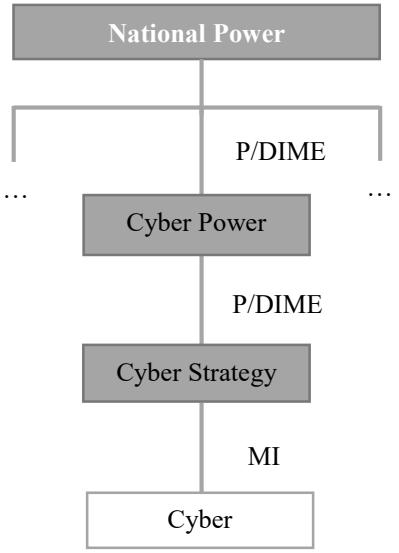

Figure 10

Rattray identified an enabling framework for strategic operations, which suits the cyber strategies mentioned above. According to him, the enablers are: 1. offensive freedom of action, 2. significant vulnerability to attack, 3. prospects of effective retalation and escalation are minimized and 4. vulnerabilities can be identified, targeted, and damage can be assessed' (Rattray, 2001: 99-100). In terms of cyber operations, it might be difficult to assess the damage they do as well as the minimization of escalation and

[62] This definition can be derived from Nye's framework 'Targets of Cyberpower', see: Nye, J. S. (2003) The Information Revolution and the Paradox of American Power, *Proceedings of the Annual Meeting (American Society of International Law)*, 97.

retaliation risks. Most of the strategies mentioned risk escalation and thus retaliation at some point, or as Stiennon put it: '[t]here is real and present danger that these skirmishes [cyber operations] could boil over into network outages that impact everyone' (Stiennon, 2010: 77). This very important issue will be addressed in the chapter on game theory (see chapter V).

7.6 Towards an Anti-War Era

The *going dark* strategy, as well as the supplementary function of cyber operations within the *cyber war* strategy, is neither new nor surprising. Disconnecting networks and using available cyber operations capabilities to supplement a conventional war are less complex than those strategies in between: *deterrence*, *sub rosa* and *shashou jian* as well as the potential of cyber-cyber-war within the *cyber war* strategy. Those strategies mark the real potential of cyber operations and provide different options for states to solve conflicts. At the same time, the application of those strategies carries the genuine potential of another Cold War like state of international relations through adding a variety of tools to the traditional means of cloak and dagger activities. The cyber strategies in question have the potential to achieve political objectives without involving any other domain. Though this too carries the risk of escalation, most of the strategies actually aim at preventing conflicts from turning into a war or at least keeping the conflict inside the cyber domain and deciding it there through decisive strikes.

During the Cold War, the nuclear weapon was the Sword of Damocles. Activities during the Cold War, therefore limiting the sphere of influence of the opposed superpower without risking or using nuclear weapons, and hence triggering Armageddon. Somehow, the new cold war seems to go further. Cyber strategies are implemented in order to prevent conflicts from turning into a war or if so, keeping it inside the cyber domain (for example cyber-cyber-war). Therefore, they try to prevent the use of conventional and nuclear forces, while allowing the different stakeholders to engage in a conflict to achieve their respective political aims (see chapter IV, the *Olympic Games*

case study). Sulek and Moran compared cyber operations to the Cold War. They state that:

> *'[t]he cyber as a Cold War analogy is ripe with similarities. The most obvious parallel between the Cyber and Cold War eras is the central role of espionage. [...] This appears to parallel efforts during the Cold War, where the Superpowers each invested resources into the creation and maintenance of rival spy networks. These networks were primarily designed to gather intelligence in an effort to gain a competitive advantage in diplomatic, economic, informational, and military confrontations'* (Sulek and Moran, 2009: 8).

A heavy reliance of extraction operations gives a first clue of what Anti-War might look like. Sulek and Moran discuss another similarity between the Cold War and cyber operations. According to them, '[t]he Cold War offers a powerful image that of a protracted struggle between powers for political, military, and ideological supremacy. There are obvious similarities—the cat-and-mouse game of espionage that boils below the geopolitical surface; the proxy wars that may suddenly break out in cyberspace; and the importance of retaining technological superiority' (Sulek and Moran, 2009: 9). Dipert paints a similar picture, stating that:

> *'[...] what we are likely to see in the next years, perhaps decades, is something like the Cold War between the Allied Forces and the Soviet Union. The espionage 'cat and mouse games' of the Cold War are well known, and there was also extensive probing of each other's territorial defenses, by the incursion of small numbers of air, sea, and ground forces, never giving sufficient reason to believe that a large-scale attack was imminent. What we are likely to see is the informal development of a similar 'equilibrium' in the accepted quantity and seriousness of cyberattacks'* (Dipert, 2010: 403).

This *cat-and-mouse* game can be played via *sub rosa*, deterrence or *shashou jian* strategies in cyberspace directly between the two adversaries or in the framework of

proxy wars/ conflicts. In addition to the analysis above that 'cyberwarfare qua warfare is soaked in intelligence' (Libicki, 2009: 155), another indicator is important for the Anti-War debate. Janczewski and Colarik state that cyber attacks might follow certain physical events with political impact as response (Janczewski and Colarik, 2008: xiv). Dearth, Williamson and Stiennon state that cyber only attacks are more likely to provoke response than a conventional attack (Dearth and Williamson, 1996: 28 and Stiennon, 2010: 103). Anti-War therefore reflects a state responding to internal political pressure by the adoption of cyber means or the support of allied stakeholders in a proxy war.

This new setting resembles much of what Heidi and Alvin Toffler called *Anti-War*. Toffler and Toffler describe Anti-War as '[...] actions taken by politicians, and even by warriors themselves, to create conditions that deter or limit the extent of war' (Toffler and Toffler, 1993: 4). They went further explaining how this could be implemented by stating that: '[k]nowledge weapons alone, even including the use of the media, may never suffice to prevent war or to limit its spread. But the failure to develop systematic strategies for their use is inexcusable. Transparency, surveillance, weapons monitoring, the use of information technology, intelligence, interdiction of communication services, propaganda, the transition from mass lethality to low-lethal or non-lethal weapons, training, and education are all elements of a peace-form for the future' (Toffler and Toffler, 1993: 239). Anti-War therefore includes strategies which allow for political necessities as a response to a hostile action but stay below a potentially escalating threshold in order to prevent war by allowing to figuratively blow a certain amount of political steam, thus releasing tension out of a conflict, subsequently cooling it down.

The Anti-War framework however allows for direct contact of the opposing powers with a potential, but not a guarantee, for escalation, depending on the level of communication and signalling. New opportunities come with new challenges. Apart from the signalling, Adams identified another problem, stating that the Cold War had rules and boundaries which are missing in cyber-aggressions, thus leading to a '[...] free-for-all, with more and more players hurrying to join scrimmage' (Adams, 2001: 102).

Herein lies another difference between the Cold War period and the current developments. Due to the low costs of entry and the potentially asymmetrical advantage of cyber operations, the cyber operations arena portrays the world as a multi-stakeholder coliseum and not a traditional bi-stakeholder playing field. Though different levels of resources are likely to result in different degrees of sophistication, every state can virtually participate in the cyber struggle. Gross pinpoints the latter challenge, stating that '[m]uch, perhaps most, information about cyber conflict of all types is classified, which creates tremendous practical problems of communication' (Gross, 2011).

In addition to the complexity and frictions of cyber operations discussed earlier, escalation cannot be excluded. Especially so because cyber strategies tempt to comparatively high degree of intensity, based on Geers levels of intensity for strategic information warfare (Geers, 2011: 26). At the same time, escalation is to be avoided. For the special relationship between the People's Republic of China and the United States, Inkster argued that '[t]he reality is that for both, China and the United States, cyber warfare in its more apocalyptical portrayal seem far from an immediate prospect since such conflict would inevitable be a function of a more general war between the two countries – something which, at present, clearly neither side wants' (Inkster, 2013: 22). The Anti-War era is subsequently marked by:

1. a dominance of intelligence operations (according to the definition of cyber operations),
2. comparatively low rate of lethality of actions (if cyber operations are an option),
3. multi-stakeholderism with power centres (for example United States, China, Israel) and periphery (for example India, United Kingdom, Australia),
4. international conflict resolution rather than conflict escalation,
5. higher friction and complexity in terms of strategic challenges,
6. a need for clear signalling and proper communication channels and
7. affecting a geographical location (networks making up the Internet) which no stakeholder wants to see destroyed or crippled.

The description of cyber operations as Anti-War means coincides with Rid's assunption that '[…] in several ways, cyber attacks are not creating more vectors of violent interaction; rather they are making previously violent less violent' (Rid, 2013: viii). If Anti-War is the description of the current era where strategy finds itself in – through the advent of cyber weapons, operations and strategies – then the according stratagem would be to *break the cauldrons and sink the boats* (Tung and Tung, 2010: 230-233). If there is no going back, the options are fewer and the motivation to pursue those which remain increases. This signal goes out to all stakeholders demanding a careful consideration of actions and the possible implications and fallout.

8. Case Study: The 'Olympic Games' Operation

8.1 Framework and Methodology

The last section focussed on various cyber strategies, their indicators and implications. This part presents the case study of the 'Olympic Games' operation and analyses it within the framework of cyber strategies. In 2001, Adams mentioned that the United States had highly destructive cyber weapons (Adams, 2001: 111). Their use within Olympic Games therefore was surprising but not without precedent. The cyber campaign dubbed Olympic Games was a number of cyber activities planned and conducted against Iran's nuclear enrichment facility in Natanz which started in 2006 (DuRaul, 2012). Commonly, this operation is only referred to as Stuxnet which is one of the core cyber weapons used during this campaign. There are several cyber weapons which are inter-related and are linked through several operations, presented here. The campaign was based on inflicting damage to the target facility by manipulating and sabotaging the Supervisory Control and Data Acquisition (SCADA) controls. 'SCADA systems are used to control and monitor a variety of processes. Such processes can be industrial, infrastructure, or facility based meaning power, mining or water systems' (Andrees and Winterfield, 2011: 123)[63].

Despite the high complexity of the Olympic Games campaign, it has been selected as a case study for this research for several reasons. First, the information which are publicly available due to technical reports (for example see: Falliere, Nicolas; Murchu, Liam O. and Chien, Eric, 2012; Rodionov, 2012 or Gostev, 2012) and political publications (Sanger, 2012) offer valuable discussion as a basis for analysis. Secondly, Olympic Games have been named the start of an international cyber arms race, a milestone for highly sophisticated cyber operations. Campaigns such as Ghostnet, Night Dragon and

[63] For more details on SCADA, see Sherif, A. (2012) SCADA Hacking, *The Hacker News*, 10, pp. 13-18.

Aurora would have also made solid case studies but are by far not as sophisticated. In addition, less information about those campaigns is publicly available[64].

The primary sources, as mentioned above, are mostly technical reports as well as the political dossier published by David Sanger in 2012. The technical reports are analyses conducted by some of the major anti-virus software companies such as Kaspersky and Symantec as well as smaller companies. The analyses took apart the different kinds of attack vectors and malicious software used during the Olympic Games campaign. Though they were not able to analyse the entire landscape (for example, the Gauss payload still needs to be decrypted, most attack vectors are suspected but unknown), most of the technical details are available. Sanger's account is believed to be retrieved through insider information. Even though there are questions whether this account is completely reliable, most authors ascribe to its veracity (for example through comparison with the technical details). For the secondary sources, this work relies on a constant media review and informal discussions with experts from January 2011 – March 2014 within the information and cyber security environment.

The first part introduces and distinguishes between the cyber weapons which can be summarized under the 'Flame Operation' - Flame, miniFlame, and Gauss. The distinction of this operation from the Olympic Games seems prudent as it is an entirely different campaign – though links exist. As the current literature and subsequent discussions mostly evolve around the particular kinds of cyber weapons and their individual implications it is important to overcome these micro-perspectives. This case study therefore categorizes the cyber weapons into the two mentioned campaigns and explains what the differences are. The second part then focuses on the Tilded platform (which is the technical platform for the Olympic Games), discussing the cyber weapons with emphasis on Stuxnet, as it presents the core of the operation. This analysis translates the technical components of the malicious software into a political

[64] The Red October and the Careto campaigns would have also made good case studies, but they were only revealed in January 2013 and February 2014 respectively, when this chapter was already drafted.

framework. After Tilded's technical landscape has been translated into a political analysis, the subsequent section embeds the analysis in an overall strategic framework.

8.2 The Technical Platforms

8.2.1 'Flame'

Flame

The Flame cyber weapon was discovered in 2012, after the discovery of Stuxnet. Several authors agree however, that Flame had been programmed and used prior to Stuxnet, with estimates ranging from 2007 to 2010 (for example Dunn, 2012 and Boldizsár *et al*., 2012: 980). The targets of Flame were the critical facilities such as oil-terminals in the Middle East including Iran, Lebanon, Syria, Israel and others (Dunn, 2012, Gostev, 2012 and Thomas, 2012). 'It [Flame] appears to be designed for general espionage and not targeted at any particular industry' (Mills, 2012). After Flame infected a system through one of its attack vectors:

> *'[i]t gathers intelligence in multiple ways, including logging key strokes, saving screen shots, switching on the microphone and the web camera (if available) to record audio and video, and browsing through the storage devices attached to the infected computer. It also switches on the Bluetooth radio if available on the infected computer, and saves information about neighboring Bluetooth enabled devices. In addition, it can also use the Bluetooth radio to send information about the victim system to a nearby device (possibly controlled by the attackers). [...] Similar to Stuxnet and Duqu, Flame uses compression and encryption to obfuscate its files' (Boldizsár et al., 2012: 980). The collected information 'is available to the operators through the link to Flame's command-and-control servers'* (Gostev, 2012).

Thus, Flame is a highly complex modular cyber weapon which main operation is to steal information.

Boldizsár *et al*. state that 'researchers found identical code segments in an early Stuxnet variant and Flame, making us believe that Flame belongs to the same cyber espionage operation and it is indeed member of the Stuxnet family' (Boldizsár *et al*., 2012: 972). Glenny and DuRaul state that based on the latest research, Flame is clearly linked to Stuxnet's creators (Glenny, 2012 and DuRaul, 2012). It therefore seems reasonable that Stuxnet and Flame are linked in their origins, the 'factory' or people which created them. There is however no proof that the information collected by Flame were used for the implementation of Stuxnet – neither do they share the same technical platform. Boldizsár *et al*. argue that that Stuxnet and Flame belong to 'the same cyber espionage operation' simply means a similar origin (supposedly the United States) and roughly the same target (Middle Eastern countries). From a strategic perspective though, those facts do not put Stuxnet and Flame in the same campaign or operation. For all we know, they might both be created by the United States to achieve information superiority over countries in the Middle East – without being further connected to each other. While Stuxnet was designed to disrupt services in a very specific environment, Flame aimed at a rather broad range of targets. Flame is able to download further malicious software modules on the infected computers as well as siphoning off documents and information. It might have provided some basic information for the development of Stuxnet among other things but it does look to be a standalone cyber weapon for the conduct of espionage.

Gauss

The Gauss cyber weapon was also uncovered in 2012 and its use has been traced back to September 2011 (Mills, 2012 and Kaspersky Lab Global Research & Analysis Team, 2012a: 48). This new cyber weapon or 'espionage or surveillance toolkit' (Mills, 2012) 'was found on computers mostly in Lebanon, Israel, and Palestine, followed by the U.S. and the United Arab Emirates' (Mills, 2012). 'With an infection count from 2,500 to tens of thousands of computers, Gauss' reach is roughly in the mid-range of its state-sponsored peers. Stuxnet infected more than 100,000 machines, mostly in Iran, while Duqu is estimated to have infected just 50 computers in a variety of countries. Flame is

believed to have infected some 1,000 systems in Iran and elsewhere in the Middle East' (Goodin, 2012). Though the numbers give the impression that Gauss was a larger operation, this is misleading. While it spread fairly far, Gauss was programmed in a way that its payload was only triggered if the cyber weapon hit the right target. For all other targets, it did not trigger the payload. Boldizsár *et al.* conclude that 'it is intended to be executed only on one or a few specific systems where the decryption key can be successfully recovered' (Boldizsár *et al*., 2012: 986). This is also the reason why an analysis of Gauss could not be completed. The technical teams evaluating the cyber weapon did establish any decrypted payload. The decryption in laboratories is ongoing (Boldizsár et al., 2012: 972). What can be said about Gauss however is that it uses a modular structure similar to Flame, and collects information about the infected system. In addition to the kind of information, Flame and Duqu targeted, Gauss focused on stealing credentials for online banking, targeting inter alia Citibank and Paypal among Lebanese banks (Mills, 2012; Boldizsár *et al*., 2012: 986; Kaspersky Lab Global Research & Analysis Team, 2012a: 3 and Goodin, 2012). The command-and-control servers of Gauss where shut down in July 2012, while the internationally known anti-virus company Kaspersky was already conducting its research and analysis of Gauss incidents (Kaspersky Lab Global Research & Analysis Team, 2012a: 4).

Gauss is believed to be created by the same factory as Stuxnet, Duqu and Flame (Goodin, 2012; Kaspersky Lab Global Research and Analysis Team, 2012a: 48 and Boldizsár *et al*., 2012: 972). It uses a similar exploit for proliferation as Stuxnet but in general, Gauss is more sophisticated and stealthier (Kaspersky Lab Global Research & Analysis Team, 2012a: 4). Even though the link to Stuxnet, Duqu and Flame is clear, it is not clear if Gauss is based on the same platform as Stuxnet, as some authors argue (for example Kaspersky Lab Global Research & Analysis Team, 2012a: 3), although this is far from unanimous (for example Rodionov, 2012)[65]. The strong focus on

[65] For a detailed comparison between Gauss and Flame, see Kaspersky Lab Global Research & Analysis Team (2012a) *Gauss: Abnormal Distribution*. Moscow: Kaspersky Lab, pp. 10-11.

Lebanon, geographically as well as targeting Lebanese banks, allow the assumption that Gauss is not connected to Stuxnet in a strategic framework. While the Tilded platform cyber weapons as well as Flame mainly targeted Iran, Gauss targeting Lebanon makes it appear to be a standalone operation.

miniFlame

The cyber weapon dubbed miniFlame was discovered in 2012 and its development can be traced back to 2010 so far – while it is estimated that its first version was programmed well before 2010 (Kaspersky Lab Global Research & Analysis Team, 2012b). As miniFlame came in several versions, Kaspersky believes that every version focused on a different region in the Middle East (for example Lebanon, Palestine, Iran or Kuwait), concluding that, 'SPE [miniFlame] does not have a clear geographical bias' (Kaspersky Lab Global Research & Analysis Team, 2012b). Compared to the other cyber weapons, miniFlame only infected a very small number of targets (Menn, 2012 and Kaspersky Lab Global Research & Analysis Team, 2012b). It can be therefore deduced that it was a highly targeted attack against very specific targets across the Middle East. The weapon itself designed to open a backdoor on the infected machines for the attacker. They could then retrieve data or upload further malicious software to the infected machines (Zetter, 2012). As compared to Gauss and Flame, miniFlame is a smaller cyber weapon – like a module in the modular structure of Flame or Gauss.

As a module, MiniFlame links to Gauss. The Gauss cyber weapon actually has the ability to work with miniFlame – demonstrating at once its character and their common origins (Paganini, 2012). While miniFlame and Gauss are technically related (Kaspersky Lab Global Research & Analysis Team, 2012b) – miniFlame is potentially an optional module of the latter - miniFlame was discovered during an analysis of Flame's command-and-control server (a process called *sinkholing*). Therefore, miniFlame links Flame to Gauss. As discussed, Flame is related to Stuxnet, thereby linking miniFlame and Gauss to Stuxnet as well. As there is no direct link between miniFlame and Stuxnet (or Duqu and Wiper), miniFlame does not seem to be part of the Tilded platform.

8.2.2 'Tilded'

The name Tilded is derived from the common platform that was used to create both Stuxnet and Duqu (Kaspersky Lab Global Research & Analysis Team, 2012a: 3).

> *'The Tilded platform is modular in nature and is designed to conceal the activities of malicious software by employing techniques such as encryption, thereby evading detection by anti-virus solutions. By utilising the Tilded platform developers of cyber weapons can simply change the payload, encryption techniques or configuration files in order to launch any number of exploits against a range of targets'* (McGuire, 2012: 9).

The first version of Stuxnet however was based on the Flame platform, according to an analysis of the much later discovered sample of Stuxnet's earliest found version 0.5. McDonald *et al*. state that, 'Stuxnet 0.5 is partly based on the Flamer platform whereas 1.x versions were based primarily on the Tilded platform. Over time, the developers appear to have migrated more towards the Tilded platform. The developers actually re-implemented Flamer-platform components using the Tilded platform in later versions' (McDonald et al., 2013: 3). Grauman states that, 'Duqu and Stuxnet were invented by the same software company and that they struck far and wide - Duqu stole information which Stuxnet was equipped with to target Iran's centrifuges and it has been operating for four years' (Grauman, 2012: 10-11). Boldizsár *et al*. also agree saying that 'our analysis results suggest that Duqu is very closely related to the infamous Stuxnet worm, while Flame and Gauss appear to be more distant cousins of Stuxnet' (Boldizsár *et al*., 2012: 999). The link between Stuxnet and Duqu therefore is comparatively obvious. Not only are they based on the same technical platform with a modular design – suggesting at least a shared *factory* – but Duqu's potential role as a precursor to Stuxnet's design. The third cyber weapon which this work assumes to be part of the Tilded platform is Wiper. According to Kaspersky, Wiper 'may have been related to Duqu and Stuxnet, given the common filenames, but we cannot be sure of this' (Kaspersky Lab, 2012). Wiper is not based on the Tilded platform as Stuxnet and Duqu are. It does however not only use similar common filenames, but also focuses its main

function (wiping systems clean) on files which are associated with Stuxnet and Duqu. 'Interesting enough, on some systems we noticed that all PNF files in the INF Windows folder were wiped with a higher priority than other files. Once again, this is a connection to Duqu and Stuxnet, which kept their main body in encrypted PNF files' (Kaspersky Lab, 2012). This work therefore assumes that the Tilded platform consists of three cyber weapons, which utilized different tools and attack vectors. Those cyber weapons are Duqu, Stuxnet and Wiper. In terms of cyber operations, Duqu carried out extraction of information, Stuxnet implemented disruption of industrial controls and Wiper conducted deception and degradation to obfuscate Duqu's and Stuxnet's operations.

8.3 Cyber Weapons of the 'Olympic Games'

8.3.1 Duqu

Duqu was discovered in late 2011 (Mills, 2012), but '[t]he exact start of the Duqu operation is still unsure today, but the stealthy period of the malware spans several months, maybe years' (Boldizsár *et al*., 2012: 977). Due to the nature of gathering intelligence, for example on industrial control systems which were targeted by Stuxnet, a common assumption would be that Duqu served as a reconnaissance tool for Stuxnet. Grauman for example states that '[...] Duqu stole information which Stuxnet was equipped with to target Iran’s centrifuges [...]' (Grauman, 2012: 10-11). However, 'no similar precursor files have been recovered that date prior to the Stuxnet attacks' (Symantec Security Response, 2011: 3). Duqu infected only a very limited number of systems which it chose deliberately – each of those systems it could have used different modules (Gostev, 2011). The attack vector of Duqu is not entirely clear. In one case, it could be traced back and the evaluation was that '[...] the attackers used a specifically targeted email with a Microsoft Word document. The Word document contained a currently undisclosed 0-day kernel exploit that was able to install Duqu' (Symantec Security Response, 2011: 2).

Duqu and Stuxnet are both based on the same technical framework, the ~d (read: Tilded) platform (Boldizsár et al., 2012: 971). According to DuRaul, 'the framework may have

become the blueprint for the next big cyber weapon, Duqu, has striking similarities to Stuxnet**.** According to researchers 50% of the source code and 99% of the software rules for Duqu are the same as Stuxnet' (DuRaul, 2012). Another author concludes that 'Duqu shares a great deal of code with Stuxnet; however, the payload is completely different. Instead of a payload designed to sabotage an industrial control system, it has been replaced with general remote access capabilities. The creators of Duqu had access to the source code of Stuxnet, not just the Stuxnet binaries' (Symantec Security Response, 2011: 3). Despite those similarities, as mentioned, Duqu had a different target than Stuxnet[66]. The cyber weapon was designed to infect a specific target system and then siphon off information. It was also able to download other modules to the infected system (Gostev, 2011 and Boldizsár et al., 2012: 979). As compared to Stuxnet, Duqu was 'an information stealer rootkit targeting MS Windows based PCs' (Boldizsár et al., 2012: 973). Linking this feature to Grauman's assumption, an author explains that 'Duqu's purpose is to gather intelligence data and assets from entities such as industrial infrastructure and system manufacturers, amongst others not in the industrial sector, in order to easily conduct a future attack against another third party. The attackers are looking for information such as design documents that could help them mount a future attack on various industries, including industrial control system facilities' (Symantec Security Response, 2011: 1). Duqu also used obfuscation by disguising the transmitted information and data as *.jpg picture files to deceive observers and security mechanisms (Symantec Security Response, 2011: 2). There is another anomaly within the Duqu source code. It is common for programmers to leave comment in the source code of a program (or cyber weapon). Usually, those comments help to debug it during the evaluation stage and are removed before the program is launched. In the case of Duqu, researchers found some comments which were intentionally left in the source code. In this case it was a picture of colliding stars. On a different occasion, programmers can chose random number sets called 'magic numbers' which can for example help a

[66] For a technical comparison of Stuxnet and Duqu, see McGuire, C. (2012) Digital Apocalypse: The Artillery of Cyber War, *PenTest Magazine*, 2(6), p. 9.

program see if a system has been already infected. In case of Duqu, Kaspersky's team came up with some links between the magic number, the picture and a possible involvement of the United States and Israel. Those, however, are only hunches and could also just have been used as a deception[67].

Even though Duqu was actually capable of carrying out virtually any task (through its backdoor function to download further malicious software), it served to implement two different cyber operations: extraction and deception. Its part towards the extraction operations is fairly obvious. The cyber weapon targeted specific systems to gain access to particular information and data. This data has likely been used to configure and adapt Stuxnet and the latter needed technical details to function well. Duqu targeted systems that could potentially hold the needed intelligence and extracted the information. In terms of deception, Duqu's task was two-fold. First of all, it used obfuscation techniques in order to deceive the enemy and stay effectively covered within the infected systems. When discovered, Duqu's source code contained bits and pieces of information which themselves are a deception – or a political message with built-in plausible denial as anyone could have left it there. Drawing a connection to other forms of warfare, Duqu shows resemblance to Unmanned Aeriel Vehicles (UAV). One of the main missions for UAVs is to penetrate adversarial airspace and deliver deep reconnaissance for future strategic decisions (for example target planning) while essentially staying hidden while doing so. While UAVs could have only covered so much (outside pictures and videos, infrared masks etc.), Duqu was able to make its way deep inside the targeted structures and systems.

8.3.2 Stuxnet

It is highly likely that Stuxnet was developed by the National Security Agency with some support from Unit8200 Sigint National Unit (Sanger, 2012: 195; Stark, 2011 and

[67] For more information on the magic numbers and picture included in Duqu, see Boldizsár, B., Pék, G., Buttyán, L. and Félegyházi, M. (2012) The Cousins of Stuxnet: Duqu, Flame, and Gauss, *Future Internet*, 4(6), pp. 974-977.

SPIEGEL, 2013), making it 'a joint U.S.-Israeli collaboration' (Ackermann, 2011). This would coincide with Williams' assumption that Stuxnet was created by one organization and then adapted by another one for propagation (Williams, 2011). It looks however like the key work was done by the American counterpart while smaller parts where created and adapted by the Israelis. Stuxnet was discovered in June 2010, although it had been active since 2009 (Falliere; Murchu and Chien, 2010: 2), and carrying out its main task in late 2009 or early 2010 (Albright; Brannan and Walrond, 2011: 1). Stuxnet's target was the nuclear enrichment facility in Natanz, Iran. Stuxnet's geographic distribution, analysed by Symantec, is as follows: 58,31% Iran, 17,83% Indonesia, 9,96% India, 3,40% Azerbaijan rest below 1,5% of in total 40.000 unique IP addresses (Falliere; Murchu and Chien, 2010: 6). The Natanz facility used air-gaped networks (going dark), so Stuxnet infected the systems and networks of the facility via an infected universal serial bus (USB) thumb drive (Arthur, 2011). It remains unclear however if this was brought in by a Russian supplier of software, a Siemens employee, or a Mossad agent.

While Stuxnet was only employed within an air-gaped network, it somehow infected computers in other parts of the world as well. This allowed international security experts and companies to analyse the cyber weapon (Sanger, 2012: 205). This is noteworthy because the cyber weapon itself did not contain any propagation mechanism to spread beyond local networks - even if the infected computer would have connected to the Internet (Cherry, 2012). It remains unclear if this was a flaw in the design of the propagation mechanism, or instead if Stuxnet infected the systems in Indonesia, among other countries, by other means. An earlier version of Stuxnet, version 0.5, was in fact able to propagate itself via E-Mail (McDonald et al., 2013: 3). This was not, however the version found on computer systems around the world.

Stuxnet itself is said to be a combination of existing and unknown exploits, an 'amalgam of components' (Farwell and Rohozinski, 2011: 27) or 'Frankenstein patchwork' (Farwell and Rohozinski, 2011: 25), which might have been designed specifically to impair affiliation attempts. Similar to Duqu, Stuxnet contains magic numbers and other

clues which might point to dates or people of historical relevance (Falliere; Murchu and Chien, 2010: 14-20). Similar to the conclusion above, Schneier states that '[s]ure, these markers could point to Israel as the author. On the other hand, Stuxnet's authors were uncommonly thorough about not leaving clues in their code; the markers could have been deliberately planted by someone who wanted to frame Israel. Or they could have been deliberately planted by Israel, who wanted us to think they were planted by someone who wanted to frame Israel' (Schneier, 2010).

The cyber weapon first mapped its environment[68] and then targeted the 'process control systems manufactured by Siemens that were running inside an Iranian uranium enrichment center. [...] The goal of the initiative was to destroy or delay Iran's ability to build nuclear weapons, which by all means it did by up to five years' (Mimoso, 2011). The destruction of the centrifuges running in Natanz was achieved by 'slowing down or speeding up the motor to different rates at different times' (Falliere; Murchu and Chien, 2010: 40). The process was designed to stay under the radar and look like random system flaws to avoid arousing Iranian suspicions and undermining their confidence in the project by making it look like accidents (Sanger, 2012: 198-199 and Albright; Brannan and Walrond, 2011: 4)[69]. Stuxnet's task was to limit the success of the Iranian nuclear projects, and ultimately drive the Iranians to abandon the project altogether.

Weighing the options, Ackermann compares Stuxnet's use to the air warfare. He argues that '[t]he mission of an aerial bombardment of Iran would be to set Iran's nuclear program back; to at least some degree, Stuxnet has done precisely that. Only Stuxnet did not kill anyone, and it did not set off the destabilizing effect in the region that a bombing campaign was likely to reap' (Ackermann, 2011). Betz and Stevens argue

[68] For more details on what Stuxnet recorded, see Dominguez, K. (2011) *Keeping tabs on the Stuxnet* [online], Shibuya: Trend Micro. Available: http://blog.trendmicro.com/keeping-tabs-on-the-next-stuxnet/ [Accessed 28 December 2011].

[69] For an overview over Stuxnet's technical details, see Sherif, A. (2012) SCADA Hacking, *The Hacker News*, 10, p. 18.

similarly, stating that '[t]he Stuxnet virus may have accomplished relatively cleanly what a large air force might have struggled to do messily but, rightly, much attention has been paid to the virus's remarkable sophistication' (Betz and Stevens, 2011: 131). Mentioning the similarity between an air strike and *Operation Opera/ Babylon* of the Israeli Air Force against Iraqi's nuclear reactor in Osirak. Kirschbaum states that ' [t]he effect of Operation Opera was one of delay — precisely how many years it is difficult to say — but not of insuperable impediment' (Kirschbaum, 2010: 56) leading to several casualties and an increased diplomatic tensions for Israel (Bishara, 1982: 59 and Kirschbaum, 2010: 57).

Stuxnet, the cyber weapon, destroyed roughly 1000 centrifuges which are critical to generate uranium for nuclear weapons but it did not lead to a complete halt in Iran's nuclear ambitions. For the Iranians, Stuxnet was a setback rather than the end. However, '[...] we may look at it [Stuxnet] as the Zeppelin bomber of its day: expensive and complex to operate, a foreshadow of yet more expense and complexity' (Betz and Stevens, 2011: 131). In short, Stuxnet was a non-kinetic cyber weapon, used in an air-gaped network, causing kinetic impact (Gragido and Pirc, 2011: 118-120).

The Stuxnet 0.5 version which has not been used against Natanz would have caused a much more significant kinetic impact. McDonald *et al.* state that it '[…] contains an alternative attack strategy, closing valves within the uranium enrichment facility at Natanz, Iran, which would have caused serious damage to the centrifuges and uranium enrichment system as a whole' (McDonald et al., 2013: 1). It remains unclear why this version was not ultimately used against the target.

In terms of cyber operations, Stuxnet's main mode of operation was disruption. It aimed at disrupting the enrichment process in order to make the centrifuges spin out of control. This led to the physical destruction of those centrifuges. At the same time, Stuxnet was a deceptive operation. First, the way Stuxnet operated aimed to disguise itself and in doing so trick the adversary into believing the faults were coming, not from Stuxnet, but from the adversary's own systems. At the same time, in case of discovery, the source

code of Stuxnet included magic numbers and other indicators of origin which could politically coerce, but did not threaten plausible deniability.

8.3.3 Wiper

Even though Kaspersky conducted an in-depth analysis of Wiper, not a lot was found out about the origin of the cyber weapon. The Kaspersky team states that '[t]he creators of Wiper were extremely careful to destroy absolutely every single piece of data which could be used to trace the incidents. So, in every single case we have analysed, almost nothing was left after the activation of Wiper. It's important to stress *almost nothing* here because some traces did remain that allowed us to get a better understanding of the attacks' (Kaspersky Lab Global Research & Analysis Team, 2012c). What can be confirmed however is that Wiper's activity can be dated back to April 2012 even though there were similar events taking place in December 2011 already (Kaspersky Lab Global Research & Analysis Team, 2012c). All discovered incidents related to infected system in the Iran (Gostev, 2012).

Wiper had one task, it 'wipes data from hard drives, placing high priority on those with a .pnf extension [...]' (Kumar, 2012). The file extension 'PNF' was used for by both cyber weapons, Stuxnet and Duqu. It was the extension for the encrypted body of those cyber weapons (Kaspersky Lab Global Research & Analysis Team, 2012c). When activated, Wiper wiped the entire data from all hard drives of the infected systems. It did so with high precision and complex tweaks in order to make sure that all data is wiped entirely without taking too much time to do so (Kaspersky Lab Global Research & Analysis Team, 2012c). It is not likely that Wiper was associated with either Flame, miniFlame or Gauss as the acitivities of Wiper, subsequently its discovery and analysis, led to the discovery of both Flame and Gauss (Kaspersky Lab Global Research & Analysis Team, 2012c). While Flame had the ability to download additional modules, it would not have required Wiper. It could have just downloaded a custom module to wipe the infected system. In addition to the priority of deleting files which were used by both, Duqu and Stuxnet, there are further similarities which are stated in Kaspersky's report. It therefore

leaves the assumption that Wiper was associated with Duqu as well as with Stuxnet and functions as a cleaner to remove all traces. This did not work out too well, as Duqu and Stuxnet could both be discovered, retrieved and analysed.

Wiper runs in the framework of two cyber operations: degradation and deception. First off, its only task was to degrade systems, wipe all data on the infected systems. While doing so, it covered the traces of itself and potentially other cyber weapons, Duqu and Stuxnet in particular according to its design. This can be regarded as deception, denying the enemy from retrieving information about what hit them.

8.4 Implications of the Olympic Games

8.4.1 Olympic Games and *Shashou Jian*

Substituting *Stuxnet* with *Tilded platform*, Ackermann summarizes these cyber operations well, saying that '[...] Stuxnet [the Tilded platform] may represent the so-called “high end” of cyberwarfare: a stealthy, stand-alone capability to oust an opponent’s Queen, without the need to laboriously trap the King in Mate with traditional military hostilities. It wouldn't be taking out a particular ship’s radar system or even a command-and-control satellite. All of that could still happen. But this would be the first instance of cyberwarfare aimed at a truly strategic target' (Ackermann, 2011). Milevski adds that 'Stuxnet was operating entirely in unknown territory' (Milevski, 2011: 69). Until this point, it is still questionable if the Tilded platform was truly a *standalone capability* or if traditional intelligence operations helped to deliver the cyber weapons to their destination. Apart from that, Ackermann and Milevski make valid points referring to the stealth, uniqueness and decisiveness of the operations, aiming at a strategic target – also including a potential traditional military option. In this case, the Tilded operations aimed at avoiding or at least postponing a traditional military strike, rather than the leveling the playing field.

To locate the case study within the framework of the presented cyber strategies, it is imperative to have a look at the cyber operations indicators. First, the Tilded platform

was utilizing a wide variety of cyber operations and multiple weapons (see figure 11). Extraction of information was carried out by Duqu, disruption of services was aimed at by Stuxnet and degradation of data was Wiper's task. All of those cyber weapons included their own share of deception. To pinpoint a particular cyber security behavior which coincides with those operations it difficult to do. As the *factory* which produced those cyber weapons is aware of the dangers however, it is fairly safe to argue that at least a reactive if not planned cyber security behavior was implemented – also with reference to the American and Israel cyber security strategies overall. It does not seem like the Tilded platform went along with a proactive cyber security behavior as American systems are susceptible to similar attacks based on the published code of the cyber weapons (Mulrain, 2011). A proactive cyber security behavior would have led to closing those vulnerabilities before the weapons are discovered and analysed even if that might have given the information about some of the vulnerabilities away. The Tilded platform operations took place during peace times but were carrying a genuine risk of escalation. The reason for this is not only the current environment in international relations, more specifically the political tensions between the United States and Israel on one side and Iran on the other side but also its intensity. The Tilded platform, particularly Stuxnet, had the ability to cause physical damage to a nuclear enrichment facility, therefore not only violating the territorial integrity of Iran (through its CNII) but also endangering the life of people. Broadly speaking, Tilded platform's the main objective was to avoid a conventional war but making sure that the Iranian nuclear program would suffer a (major) setback. Apart from the proactive cyber security behavior, the Tilded platform resembles entirely the strategic framework of *shashou jian*. The strategic implications which can be derived from choosing *shashou jian* are its use as surrogate for conventional warfare was well as the destruction of system confidence. The next sections will elaborate on those points further. Figure 11 shows *shashou jian's* role as a cyber strategy, the cyber operations it is composed of and the cyber weapons used to carry out those operations.

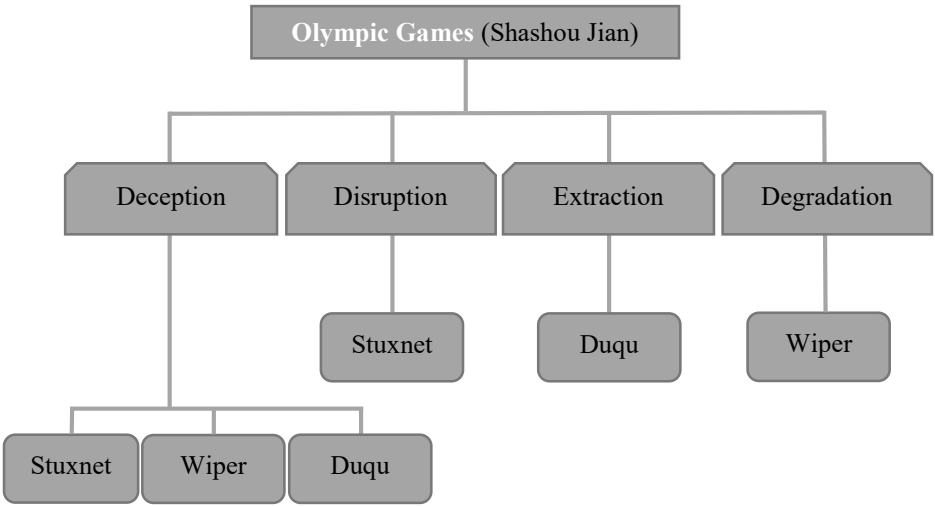

Figure 11

8.4.2 Olympic Games and Cyber Strategy

Transitioning from the plane of the individual strategy to a more general framework of strategy in the cyber domain, the Tilded platform shows some remarkable strategic indicators. The campaign shows that cyber operations can be conducted as standalone activity in order to realise political objectives. Though it remains unclear if other intelligence elements where involved in planting Stuxnet weapon inside the Natanz facility, it is reasonable to define it as standalone warfare rather than as supplementary to other traditional forms of warfare. All cyber weapons used by the Tilded platform reflect the points mentioned about the genuine covertness and ability to scale the tools (compare to sub-section 7.2). Though details about the operations were made public, and samples of Stuxnet where found outside Natanz, the weapons were able to complete their mission while staying covert and without causing collateral damage. Four of the ten strategic dimensions which were dubbed as important for strategy of cyber operations (compare to sub-section 7.2.3) these too can be identified as crucial to the Tilded platform. The people that coded the weapons, the sophistication of the technology used, information and intelligence needed to create and implement those

custom-tailored weapons, as well as the geography of Natanz (the air-gaped nature of the networks), were vital elements of the entire campaign.

In term of geography, the Tilded platform also accomplished a striking operational success in bridging the air-gaped nature of the networks. Referring to section 7.2.4, this action resembles the *Maginot Line* or in the case of cyber security *candy security*. The networks were secured by not connecting them to broader networks, and thus the Internet. Once this first line of defence was overcome, Stuxnet was apparently unstoppable. A defence-in-the-depth approach with additional security updates, firewalls, anti-malware tools and cyber security in general, might have been able to limit the success of the operation. At the same time, the air-gaping was also the only friction in the strategic sense (compare to sub-section 7.2.6), the amorphousness of the networks reflected by a non-connection to the Internet.

On the tactical level, the Tilded platform was very well executed. Duqu and Stuxnet were used in a way that they could accomplish their goals while staying covert. The autonomy and sophistication with which they worked, and especially Stuxnet, was unparalleled. It is arguable if the campaign achieved the political objective entirely (by sending a strong political message and delaying the nuclear research) or only partially. Given that this was the first major campaign relying entirely on cyber operations however, the tactical level can be regarded as a success.

8.4.3 Olympic Games and Strategic Implications

Regarding the strategic implications on a macro-level, a first conclusion can be deduced from the comparison of the Tilded platform activities as opposed to a potential conventional military assault. Sanger argues that bombing Iran would have had a unifying effect (for the region) and might not have been effective given the complexities in attacking secret facilities in Natanz (Sanger, 2012: 220-225). Additionally, Farwell and Rohozinski argue that '[...] a [conventional] strike poses risks. A single strike might not succeed, and it is not clear how many over-flights Saudi Arabia or the United States might permit. Israel could sustain significant losses. Iran would hold the United States

responsible, and could attack US installations and troops in Iraq, Afghanistan or elsewhere. It might disrupt the flow of oil out of the Gulf and oil prices could escalate. Air strikes might unite a currently divided Iran and enable Ahmadinejad and his allies to consolidate power' (Farwell and Rohozinski, 2011: 29). Geers supports this view of the possible impact of a conventional strike on the international relations arena, stating that '[...] Stuxnet may have been more effective than a conventional military attack and may have avoided a major international crisis over collateral damage' (Geers, 2011: 13). The strategic implication which can be derived from this discussion is that cyber operations are now a viable military option for striking an adversary's centres of gravity – even as standalone option. Estimates see the nuclear programme setback an estimated 6 months to 18 months. Though, it is difficult to anticipate what damage and delay a conventional strike would have caused, the fact that cyber operations had an impact with zero causalities on the attacker's side makes it a viable option for future operations.

One of the key advantages which cyber operations are supposed to have over other forms of warfare is the lack of collateral damage. In the case of the Tilded platform, this issue is a tricky one. Stuxnet, the cyber weapon which actually did the most damage, was found on computer systems around the world. There are also rumours that due to a Stuxnet infection, an Indian satellite was destroyed and that a Russian nuclear power plant was severely affected (Kaspersky, 2013). All of this 'creates a potentially serious risk of political blowback if the attacking parties are identified' (Farwell and Rohozinski, 2011: 35). However, a system infected with Stuxnet will not necessarily sustain any damage at all. Gervais points this out, saying that, '[...] while the Stuxnet worm did infect civilian industrial control systems around the world, the harmful effect was triggered only by the conditions present in Iran's nuclear program. The Stuxnet worm satisfies the criteria of distinction because the worm was designed for a specific military target – assuming the Natanz plant is not a civilian nuclear energy program – and it could not indiscriminately destroy civilian computer systems' (Gervais, 2011: 38). Though several systems not targeted were infected, no damage has been done to those systems. Save for the Natanz incident, no others were reported and traced back to

Stuxnet. Other targets in Iran were reportedly hit by Wiper but those also appeared to be intended targets (Kaspersky Lab Global Research & Analysis Team, 2012c). So beyond the potential impact on the Indian satellite and the mere infection of systems[70], there seems to be no further collateral damage – and this potential collateral damage was only economical. No person became a victim of collateral damage of the Tilded platform activities.

It should however be kept in mind that cyber weapons such as Stuxnet are created with a high potential of functioning autonomously, especially when used in air-gaped systems. Healey therefore concludes that 'details on Olympic Games are difficult to come by but it appears Stuxnet was just such an exception, set loose with only algorithms, rather than a human, to tell it whether to unleash Hell' (Healey, 2013). A bug in the programming could have changed that and might have had serious impact on industrial controls worldwide. No state could be interested in carrying out cyber operations resulting in the (temporary) break down of the worldwide Internet or even worse, multiple nuclear power plants going haywire. The potential collateral damage of cyber operations therefore is immense.

The second strategic implication from the Olympic Games case study therefore is that causalities on the attacker's side as well as collaterals on the target's side are very low – in terms of people's lives even non-existent. In the case of the Tilded platform, cyber operations qualify as having physical impact without being lethal and reducing the causalities of the own forces. Though the operations might not be over yet (Richardson, 2011: 10), another strategic implication is the existence of a genuine game changer nature within cyber operations. Andrees and Winterfield discuss certain possible game changers in the field of cyber security such as an international arms treaty (Andrees and Winterfield, 2011: 269-270). Sanger also uses the term *game changer* in his description

[70] Not taking into account the discussion that Stuxnet was actually not able to spread itself to systems over the Internet and some other party might be at fault for the wide infection of systems outside the intended target, Iran (see 8.3.3).

of Obama's hopes that the Olympic Games would function as such in regard to the Iranian nuclear program (Sanger, 2012: 187). At this point, it is difficult to definitively state whether the Tilded platform was a game changer or not. It helped to delay the Iranian nuclear program and therefore possibly postponed a conventional strike. The fact that Iran continues to pursue their enrichment shows that Olympic Games' impact did not extent to successfully achieving its ultimate aim in permanently halting Iran's nuclear programme. That said, it equally cannot be state that cyber operations do not represent a serious departure from the status quo. Here, it was impactful but it did not change the entire game. In other cases, it might do so, therefore it has the potential to be a game changer.

In summary, a *shashou jian* has been implemented through the use of the cyber weapons based on the Tilded platform framework. It implies that cyber operations can have a strategic impact as standalone, physical, non-lethal option with low to none collateral damage and casualties. It also shows however, that it is no game changer *per se* though is carries that potential. The case of Olympic Games viably portrays the underlying Anti-War era. The activities of the Tilded platform were stealthy and aimed to achieve strategic goals while trying to avoid human casualties, and especially aim to avoid further escalation. Those implications leave cyber operations in an interesting position. In the semantics of conflict escalation, cyber operations sort themselves after political pressure and economic sanctions, and before special operations and armed conflict. It is however not quite so straightforward. Compared to economic sanctions, which – in terms of resources – can backfire on one's own economy or allies, cyber operations offer a more attractive option. As mentioned above in the case of Natanz, the Olympic Games operation seemed very interesting to the decision-makers because it left all other options on the table; a military attack could have still been carried out. It was also obvious at this point that economic sanctions and political pressure would not be sufficient to convince the Iran to stop its nuclear research programme. The comparatively low costs of the cyber attack added to its vitality and appeal. Due to the *problem of attribution*, cyber operations also allow for plausible denial, which is not

something political pressure, economic sanctions and armed conflict can claim. Lastly, the flexibility and precision which cyber weapons can offer – if programmed correctly – might elevate it to the strategist's preferred options.

CHAPTER V

9. Game Theory in Cyber Operations

9.1 Introduction

Game theory provides an analytical tool in appreciating the strategic relevance of cyber operations for states. This chapter adopts the methods of game theory to illustrate the pay-offs and dominant strategies of cyber operations. It is divided into four sections outlining the premises, arguments, and scenarios of game theory as applied in cyber operations. The first section discusses the validity and criticism of game theory as a tool in social sciences and particularly in strategic studies. It provides reasons why the tools of game theory can be applied to this research to deepen the analysis of strategic implications for the state.

The second section demonstrates how these tools are applied to analyse concepts and indicators in the cyber domain. A straightforward application of game theory, as a methodology, to analyse cyber operations is discussed, starting with its formal structure. First, the players are discussed and defined. Then, pay-offs and sums are discussed. The correct incorporation of the variables that define the pay-off is crucial for the analysis presented here. Following this premise, the pay-off is adapted to cyber operations, the core of this application stemming from risk valuation, strategy consideration and the calculation of results. Third, strategy and utility are discussed and defined. The strategies, which also play an important role, are adapted from the previous chapters where they have already been analysed thoroughly. Fourth, information and forms are presented as they are vital for the formal setup of the scenarios. Lastly, the game theory representation of iteration is mapped to the cyber domain.

The penultimate section illustrates the resulting strategies for cyber operations from the analysis and applies it to two hypothetical states. Seven scenarios with varying preconditions are illustrated in order to analyse the strategic implications for the states. The aim of analysing these scenarios is not to showcase an ongoing or past event in

particular, but to create a framework which enables strategists to calculate the outcome of a future conflict in the cyber domain. First, the simple form is applied to every scenario in order to create a general overview and wherever more complex tools of game theory are needed in order to find a stable equilibrium; those tools are applied as well. This includes, *inter alia,* the complex form and probability distribution. When the right structure has been identified, the scenario is solved using standard computation methods of game theory to pinpoint the dominant strategy(ies)- a Nash Equilibrium.

The conclusion summarizes and thoroughly analyses the outcomes of the scenarios. It formulates lessons drawn from these outcomes and levels the playing field for the ultimate conclusion in the next chapter. This chapter finally proposes where cyber operations place in the strategies of states and points to areas where further studies are needed owing to the limited scope of this research. Together with the rest of the developed framework, states should be enabled to improve their calculations of the implications before engaging in such a conflict.

9.2 The Methodology

9.2.1 Validity

Choosing game theory as a method owes partly to its origins as a method in the study of nuclear warfare. Similar to cyber operations, nuclear warfare is also part of the strategies studies domain. To facilitate strategic assessments for decision-makers, game theory has been applied to nuclear warfare (e.g. Kaplan, 1983). Research and review by the author of this work highlighted its potential for cyber operations.

The application of game theory to cyber operations serves as a tool to improve the analytical understanding of the strategic implications for the state. As Snidal presents: '[t]he theoretical use of game models allows us to adapt them directly to the most salient aspects of international politics' (Snidal, 1985: 44). While the description and analysis of cyber operations and their strategies have been completed in the past chapters, only some strategic implications were presented. The analysis has concluded that cyber

means as tool for conflict resolution enables the evolution of an Anti-War era in the international relations environment. This era is marked by states engaging in non-escalatory cyber activities. The ultimate aim of the states is achieving information dominance. The assumptions which have been drawn so far regarded cyber operations in a vacuum. Tools, approaches and strategies have been developed in the past chapters on the basis of a single state. In order to increase its validity, game theory introduces the arena of international relations by adding an opposing state to the equation. Game theory methods are applied in this chapter to verify the validity of those outcomes and to discover the inherent strategic implications.

According to von Neumann[71], one of the fathers of game theory, game theory is defined as 'a mathematically precise method of determining rational strategies in the face of critical uncertainties' (Kaplan, 1983: 65). The core points are the formal, mathematical nature of the method, rational decision-makers and an analysis of how those decision-makers will act in conflict situations – and the subsequent logical implications to and reactions of the other stakeholders included in the conflict (Evans and Newnham, 1998: 189; Camerer, 1991: 149 and Shubik, 1972: 37). However, the approach used here focuses on qualitative analysis. Leonard's argument supports this approach, stating that '[g]ames, [...] are in reality highly complex, so that mathematical calculation can be, at best, a supplement to strategic cunning' (Leonard, 2010: 61). He points out that: '[i]ts [Game Theory] value, rather, was that it helped structure thinking in a qualitative, conceptual way, highlighting the importance of strategic interaction, threats, credibility, and similar factors' *(ibid*: 299). A quantitative analysis can then follow the results of the qualitative research. Once the latter has been completed, quantitative analysis can be pursued, e.g. with the help of computer simulations (Hamilton *et al.*, 2001: 1). This work applies game theory indicators to embed the developed cyber strategies into a framework. This framework is then used as a model for analysis and to derive general

[71] For an overview over the history of game theory, see Kormann, G. and Klapper, M. (1978) Game Theory's Wartime Connections and the Study of Industrial Conflict, *Industrial and Labor Relations Review*, 32(1), pp. 24-39.

conclusions about the strategic implications of cyber operations for the state from it based on abstract numbers. A truly quantitative approach would need to be based on actual empirical numbers of a real-life case study which would be used to convert the abstract numbers into tangible ones.

Game theory helps to model the logical implications of conflicts with more than one player and more than one strategy. This is a requirement which is fulfilled by the outcome of the previous analysis on cyber operations in this work, defining five strategies for at least two involved conflict parties. The application aims to create a model which allows decision-makers to foresee (by computation) the implications of their strategies *vis-à-vis* a reasonable opponent, allowing them to choose the most advantageous strategy. Brams and Kilgour describe the benefits from applying game theory to conflict scenarios:

> *'[t]o paraphrase an old saying, national security is too important to leave to game theorists or political scientists, especially those who build abstract models. Yet if game theory does not provide an immediate solution to the next crisis, it does, we believe, help greatly in thinking carefully about national security policy, especially its seeming paradoxes'* (Brams and Kilgour, 1988: 196).

9.2.2 Criticism

Game theory is not, however, without its shortcomings. An often discussed flaw in game theory is the underlying assumption (and requirement) that every stakeholder acts in a perfectly rational way (e.g. Morton, 1983: 9 and Camerer, 1991: 138) and that their decision-making mirrors this. Once an opponent deviates from the most logical (perfect) response to an opponent's strategy, the (game theory) model's computations risk jeopardy. It is of course an assumption of the model that all actors are equally vested in achieving the highest possible pay-off. Game theory has also been applied to strategic deliberations on nuclear warfare, where the same concern has been raised. Brodie responds by arguing that such a rationality of the opponent can be assumed as they have

no other interest than maximizing their own outcome by not risking an escalation of the conflict (Brodie, 1965: v, 78-79, 22-23). Thus, by choice, and with perfect information, every stakeholder would always strive to play flawlessly and achieve the highest possible pay-off. A situation where stakeholders do not choose the most rewarding strategy can, for example, occur if one or more player lack perfect information. For decision-makers, this risk can be reduced if they not only have perfect information about their own pay-offs and strategies, but also about those of the adversary. The information needed to conduct a precise analysis is the offensive and defensive capabilities of each state, as well as vulnerabilities and the strategic value that is put on the targets of the conflict. An analyst of either state would therefore require information about their own capabilities as well as those for the adversary, for example, through intelligence.

Subsequently, the impact of this valid criticism can be mitigated by pointing towards comprehensive intelligence for all stakeholders. In order to prevent an accidental escalation of the conflict through imperfect information, the Cold War saw the establishment of the *hot line*, a telephone line between Washington and Moscow which aimed at preventing the Cold War from turning hot, especially nuclear hot. By enabling direct communications, e.g. in the event of a possibly fatal misperception, the aim of the *hot line* was to facilitate information exchange. Interestingly, such a telephone line has been set up in 2013 for similar events concerning cyber war (Gallagher, 2013). Those needing information can be gathered through traditional espionage as well as through cyber operations. The latter, however might lead to a catch-22 where gathering information through cyber means to avoid escalation inadvertently sparks an escalation. Perfect information through comprehensive intelligence and information on one side (A) does not solve the challenge. The other stakeholder (B) might not obtain perfect information and be unable to act as rationally as stakeholder (A). In fact, every stakeholder tries to deny its adversary perfect information (for example, through counter-intelligence) thereby actively contributing to the potential inaccuracy of an analysis. Furthermore, even if all involved stakeholders possess perfect information, the decision-makers are still human. And human judgment might err at times. Ultimately,

it constitutes a valid criticism of game theory which, in the context of strategic studies, can be subsumed under *friction, chance, and uncertainty* (see sub-section 7.2.3).

Game theory enables the creation of models which work with numbers. Those numbers have to be derived from quantitative but also qualitative data. Quantitative data does not necessarily need a translation and can be directly transferred to the corresponding model. Qualitative data, however is more difficult to transfer to a model which works with numbers (e.g. Kaplan, 1983: 88 and Leonard, 2010: 250). Kaplan stated that 'the analyst had to have some way of calculating what numbers should go in the matrices' (Kaplan, 1983: 67). Quantification of indicators in conflict scenarios is undoubtedly a great challenge. The works of the 'Wizards of Armageddon'[72] took into account human lives, destroyed cities and dollars needed to build military equipment. During their analysis, they had to also quantify the worth of human lives in monetary terms in order to be able to conduct computations about the spending on nuclear weapons and shelters. Being aware of this challenge is a first step to overcome it. Thus, a lot of effort has to be put in the translation of all available data into numbers which can be used to ultimately calculate the pay-offs. A particular case study can only be solved by attribution of empirical numbers through decision-makers. This conclusion is in no way tautological. Academia (e.g. this research) provides a framework to derive general guidelines by using sample data, while a real-life application can only be conducted with the support of the involved decision-makers. With no framework, decision-makers would be left with no tools to base their decisions. Outcomes would only be based on a mere hunch. Without the involvement of decision-makers however, academia would only be able to provide a framework without any apparent use.

More specific criticism on the application of game theory to cyber operations comes from Libicki. He states that game theory's application to cyber operations is even more difficult than its application to nuclear warfare – due to the problems of calculating responses and impact down to the n^{th} level (Libicki, 2007: 42). Libicki argues forcefully

[72] See Kaplan, F. (1983) *The Wizards of Armageddon*. New York: Simon & Schuster.

that calculating theoretical responses to an action where the impact is unclear is certainly challenging, particularly if those responses are reactions to reactions to reactions – on the n^{th} level. It is also true that: '[i]t is easier to forecast the outcome of a chess game because at least the board and the pieces do not change as the game is played' (Libicki, 2007: 93). This should not discourage researchers from trying to do so. After all, it can be argued that the underlying technology has been well analysed, hence the impact of a power-grid going offline for an hour is quite foreseeable and its expected outcome can be computed and simulated. Furthermore, developing a framework does not end with its first appearance. Its added value is derived from a constant probing and adaptation through, for example, the aforementioned computer simulations.

Those criticisms have their *raison d'être*. Therefore, this work acknowledges their validity by offering the development of a qualitative and flexible game theoretical framework on the strategic implications of cyber operations for the decision-makers of a given state. A key means through which some of these criticisms can be negated, however is the development of the – relative – pay-off value z. This pay-off factors in offensive and defensive elements of cyber operations, conventional and cyber capabilities of a state as well as the risk of conflict escalation. Rather than referring to absolute numbers (e.g. the number of tanks or cyber soldiers) it sets the adversary's capacities in relation (e.g. double as strong), thereby being very flexible and allowing for the inclusion of different factors.

9.3 Translation of Indicators

9.3.1 Players

Players is the game theory term for stakeholders, in this work, players are states. Based on the definition of the state used in this research (see chapter I), it is regarded as an independent decision-making entity. The actual decision-making process leading to the choice of the preferred cyber strategy might account for a number of voices from the political and military arena, but the state will carry out the decisions made as a single entity. The internal decision-making process might add to the reasonability which is

said to be required for players in game theory models[73]. Every game needs players – therefore, the conceptualization of a model has to take the number of players into account as a game always depends on the actions of all players (Leonard, 2010: 62).

Part of the added value provided by applying this method is the conclusion that can be derived from embedding these observations and analysis into game theory. The research so far focused on the general implications of cyber operations, independent from the number and nature of the stakeholders. In order to derive implications which are more specific to a particular empirical situation, the general framework needs to be tailored to reality. To do so, this requires the inclusion of more than one player into the model. Therefore, the number of players considered here is 2. In formal language this is written as N = 1, 2. As international cooperation in cyber operations or even cyber security issues seems far-fetched now (compare to chapter III), the limitation to two player seems sufficient. Nye argues that '[s]tates are caught in a zero-sum game where it is rational to fend for themselves because they cannot trust others' (Nye, 2011: 27-28). In the years to come, an extension of this theory by an N>2 multi-stakeholder or multi-player approach might be worth exploring. This extension would allow for a concise inclusion of the cooperation factor of cyber security as well as incorporate training and other offensive cooperation (FireEye, 2013: 9).

Players are considered reason-driven (see 9.1.2). The assumption is therefore, that the players in this model behave rationally. By rational, the literature refers to maximizing their own pay-off with a disregard for their opponent's outcomes. It usually disregards the compared pay-off of the adversarial player. If players appear to act irrationally, it might be because they are not in possession of perfect information (see 9.2 for more details). It is therefore necessary to judge a situation from the perspective of the particular player.

[73] A point that is well-discussed in the framework of the *Diskursethik* by Jürgen Habermas. See for example Habermas, J. (1991) *Erläuterungen zur Diskursethik*. Frankfurt am Main: Suhrkamp.

9.3.2 Pay-off and Sum

The pay-off in a game theory model represents the gain or loss of one player's strategy *vis-à-vis* the other player and his chosen strategy. The pay-off therefore incorporates both the costs and gains of a strategy and describes its output numerically. In this paper, the variable z has been chosen to represent the pay-off.

Defining costs in the cyber domain is a comparatively difficult task. While literature on game theory and nuclear warfare utilized absolute numbers, either referring to deaths and injured human beings or million US dollar in economic costs. Cyber operations can adopt neither of these well, although economic costs can be included to a certain degree. The economic considerations of cyber operations are rather straight-forward. If a state plans on setting up cyber forces, it will have to invest a certain amount of resources. Those resources suffice in order to implement cyber security as well an offensive cyber operations unit. The costs for securing the state as well as developing or using cyber weapons have been discussed in the previous chapters. Compared to the development and deployment of nuclear weapons, or conventional forces such as destroyers, the costs to setup cyber forces are not significant. On the other hand, costs can be defined by the losses in case of an adversarial cyber attack. Here again, the pure numbers are not that important. Considering the stolen blue prints of the American joint strike fighter in development (Gorman et al., 2009), the loss of US dollars paid for the development was not as significant as was the loss of information superiority. The adversary which was able to leverage that information was not only able to leapfrog technological development but also gained strategic intelligence about potential vulnerabilities and weaknesses. Hence, the resources that matter are not money but the strategic value of information (stolen, deleted etc.) and how it can be used to achieve political objectives.

In the end, it is about the value of information. Information can be stolen or corrupted and its flow can be disrupted or misdirected. In the case of the Olympic Games operations, what was significant was not the economic loss but the political and strategic gains for the United States and allies. The extent to which the US and allies set back the

Iranian nuclear program was more significant than the simple costs involved. Information being stolen does not necessarily mean that a change in ownership takes place- the result of copying a file from a computer is that two copies with equal information exist. What can be lost is the significance of this piece of information. It might lose its significance, and hence value, for the original owner if its value is linked to the uniqueness of ownership. If state A plans a surprise attack against state B, the knowledge and information about the surprise attack only has a value for state A as long as state B is not also in possession of this information. Decision-makers are the only ones who can put a number value on pieces of information. Letting the attacker as well as the defender rate the strategic value of a piece of information allows for a more objective absolute quantification on an arbitrary scale. However, the same piece of information must not have the same value for both sides (Denning, 2000: 23). Keeping that in mind, quantity (in terms of size) is irrelevant. A gigabyte of information can have less value than fifty megabyte of information, assuming the latter is rated higher on the value scale than the other. The login name and administration password to a confidential database consists of a few bytes while the president's vacation videos might take up several gigabytes of disc space.

The variable to determine the pay-off z of a certain cyber strategy for a particular player is defined as v, the strategic value which the players attribute to the information and the CNII tampered with. v is defined as $1 \geq v_n \geq 0$ whereas 1 means 'of critical value' and 0 means 'no value at all'. For example, player 1 chooses a *shashou jian* strategy which in effect disrupts the power grid of player 2 to prepare for an air strike. The pay-off for player 1 would depend on the strategic value player 1 and 2 attribute to the disruption of the power grid. Assuming that both players would rate the strategic value as *critical*, one part of the pay-off calculation would be $v_{total} = v_1 + v_2 = 2$.

The net gain for the player is therefore the sum of the strategic value attributed by the player (v_1) and the strategic value attributed by the adversaries (v_2 to v_n). The mere fact that something is targeted does not point to the necessity of its success. Additional to this equation, the cyber capabilities, c of the player *vis-à-vis* the other player have to be

factored in. The cyber capabilities (strength) are included as a simple multiplier with 1 being similarly strong as the opponent. Assuming that the attacker has only half the cyber capabilities compared to the defender, the resulting equation then is $c * v_{total} = c * (v_1 + v_2) = 0.5 * (1 + 1) = 1$.

Similar to the value of information, cyber capabilities have to be estimated by decision-maker. The decision-maker has to calculate the cyber capabilities of its own forces and of the adversarial forces in order to derive an accurate c.

Section 7.6 identified the Anti-War era as the underlying framework for cyber operations. Thus, the issue of escalation, more precisely the lack thereof, is vital to the conduct of cyber operations. By definition, all players would want to avoid the escalation of a conflict into a fully-fledged deadly conventional or nuclear war. While escalation can be avoided by limiting the intensity of cyber operations, it can also be avoided by possessing the superior conventional military force. For instance, an adversary is eager to escalate a conflict due to high intensity cyber attacks against it, it might choose not to do so because it is intimidated by the adversary's conventional military strength. Instead of fighting two losing battles (cyber and conventional), the inferior power might opt for not escalating the high intensity cyber conflict in order to avoid higher casualties. Thus, controlled escalation is an option. Therefore, escalation dominance is factored in through the difference in conventional military capabilities (m).

While all players aim at maximizing their pay-off, escalation is (theoretically) out of the question. Thus, the variable r is defined as the risk of escalation inherent to the strategy linked to the pay-off. The higher the intensity of a cyber strategy, the higher the risk of escalation. While a going dark cyber strategy does not exert any coercion/ intensity towards the adversary, the *sub rosa* cyber strategy does. The pay-off of a certain strategy equals 0 if it triggers an escalation – as an escalation to be avoided above all else. The risk of escalation is defined as $1 \geq r > 0$ where 1 means no risk of escalation at all and 0 means a definite escalation, following an equal distribution over all applicable cyber

strategies. If there is no risk of escalation (1), the value ($c * v_{total}$) gained, can be viewed as entire net gain. If the strategy caused a medium risk of escalation (0.5), the net value ($c * v_{total}$) gained is only half of what it would be worth if no risk of escalation would have been caused. Thus, as r approaches 0, the net gain vanishes entirely, as the premise is that escalation recedes. Incorporating r in the calculation for the pay-off leaves $z = (c * v_{total}) * r$.

Coming back to the value of conventional military forces (m), the risk of escalation for a player is not only linked to the intensity of the conflict, but also to the conventional military forces he can back up a potential escalation with. A player which has a much stronger non-cyber military capability, m, than its opponent will more likely increase the intensity of a conflict - even though it would still try to avoid complete escalation. The player with lower, non-cyber, warfare military capabilities, on the other hand will rate the risk of escalation of a certain strategy more highly. Similar to c, m is factored in as a multiplier *vis-à-vis* the adversary. This means that if the adversarial non-cyber military capabilities are only half of the player's, the player's risk of escalation is subsequently also only half – as the adversary is less likely to escalate the conflict. Incorporating m into the equation, the final equation for the calculation of pay-off for a player's strategy is the following:

$$Pay\text{-}off_{cyber\ strategy}: z = (c * v_{total}) * (r * m)$$ [74]

9.3.3 Strategy and Utility

In game theory terms, a strategy is referred to as a player's plan of action, motivated towards a specific pay-off. Every player has at least two strategies which he can choose from. He does not necessarily know his own pay-offs or the pay-offs of the other players. Furthermore, the final outcome (in terms of pay-off) does not only depend on his own strategy, but also on the strategy of the other player. In game theory, A_i refers

[74] The round brackets are merely utilised to highlight the two main components in this formula: 'gain' and 'escalation'.

to all possible strategies while the single strategies are referred to as a_1, a_2 ... a_n. The player can also choose to not play one pure strategy but rather mixed strategies. Mixed strategies are the decision of the player and might be used if there is no dominant strategy. The player can announce a certain probability, p, with which a strategy is played, or else use a randomizing device such as a die to decide on the strategy. This would allow players to minimize vulnerabilities or pattern detection by the opposing side (Niou and Ordeshook, 1994: 171). Taking mixed strategies into account allows the mathematical ability to find equilibrium (Niou and Ordeshook, 1994: 171) where there is no dominant strategy. This theorem, proven by von Neumann and Morgenstern in 1944, allows a rational choice for every decision-maker.

The definition for 'strategy' in game theory varies from its definition in strategic studies. Shubik describes the difference as follows:

> *'[t]he game theory definition of a strategy contains all of the minute details of tactics as well as the overall plan. The typical or military usage of the concept of a strategy or an overall plan sketches out the main aspects and leaves a certain amount of freedom of action to improvise for those entrusted with the task of carrying out the plan. It is extremely difficult to translate this far less precise but more operational concept of strategy into a formal mathematical model'* (Shubik, 1972: 41).

This paper already identified five cyber strategies: going dark, deterrence, *sub rosa*, *shashou jian* and cyber war. Those strategies are adapted to game theory as the following:

a_1 = going dark

a_2 = deterrence

a_3 = sub rosa

a_4 = shashou jian

a_5 = cyber war

In order to translate them into game theory strategies, they have to be simplified by reducing them to their pay-off z. The pay-off has been extensively discussed and defined in this chapter in order to represent the differences in the cyber strategies.

The utility function u is, according to Morton, '[a] utility function, if it does anything, must reflect a person's preferences accurately; it serves no other purpose' (Morton, 1983: 68). It represents the utility of all strategies that a certain player has, hence incorporating what players care about and what their overall aim is (Shoham, 2012b). It therefore assumes a strict reasoning on the basis of the knowledge available to the players in relation to potential pay-offs and their own motivation, or in short 'players maximize their expected pay-offs given their beliefs' (Shoham, 2012a). Player n's utility function therefore would be u_n: (a_1, a_2 ... a_n).

9.3.4 Information and Form

A game with perfect information means that all players have all the information about the game. Chess is an example of this. All the pieces and their utility is known to both players. A game of imperfect information, or *Bayesian game,* limits the information that one or both players have. A real-world game representing the Bayesian logic is the Games of the Generals, where both players know what pieces the other has but lack the knowledge of where the pieces are situated. The ability to deduce the missing information by the moves that the other players makes is called the Bayesian rule (Jackson and Shoham, 2012). Subsequently, in a game of imperfect information, one player has private information that the other player does not have[75]. In the case of competition, hence strategic/conflict studies made by decision-makers, it can be

[75] For more information and the application of imperfect information, see Alastair, S. and Stam, A. C. (2004) Bargaining and the Nature of War, *The Journal of Conflict Resolution*, 48(6), pp. 783-813 and Frihberg, M. and Jonsson D. (1968) A Simple War and Armament Game, *Journal of Peace Research*, 5(3), pp. 233-247.

assumed that other players (decision-makers of other states) are not supposed to know details of each other's strategies insofar as it disadvantages the player that offers their information. It can be further acknowledged that through the introduction of the strategic value of information v_{total}, the ability of one player to achieve a state of perfect information is virtually impossible as it is difficult to know exactly which level of strategic value the adversary places on individual pieces of information. The calculation of the pay-off defined in 9.3.2 shows that for most factors (e.g. m and c), not only information about the own capabilities, but also information about the adversarial capabilities are needed. Thorough intelligence therefore plays a vital part in creating a state of perfect information.

Furthermore, game theory allows models to be presented in various ways. The simple form and the extensive form are different ways to visualize a model. While the simple form allows for an easier analysis of a given game, the extensive form helps to visualize games with imperfect information better. Shubik argues that

> *'[i]f the stress is on strategy and payoffs, the strategic form as illustrated by the matrix game will be used. If interest is on detail, information, and fine structure, then the extensive form of a game will be employed'* (Shubik, 1972: 40).

The simple form allows for an easier overview; the application of the extensive form enhances the analytical depths in games with imperfect information or non-synchronized turns. As discussed, imperfect information and non-synchronized turns are very well possible in cyber operations, this method is applied to show if there are significant differences in the outcomes.

9.3.5 Repetition

A repeated game refers to an extensive form game that takes into account future actions and their outcomes as a basis for decision-making. In a repeated game, a one-time large gain (high pay-off) with subsequent significant losses (very low pay-offs) will not be

chosen over a steady gain (mediocre pay-offs) because it performs poorly in the long-run (repeated game). Even though cyber operations are thought of as 'speed of light' attacks, the game theory adaptation does not treat cyber strategies as simultaneous moves. This might be true for the tactical and operational level, but it is certainly not the case at the strategic level. The strategic level, which is discussed here, is a non-simultaneous setup of games. States' strategic considerations can be pro-active or reactive, responding to the strategy of another state. Strategies can be changed over the course of a conflict. Even if there are no clear moves visible, the players can for example choose to apply deterrence up to a certain point and then shift to *sub rosa* and at some point shift back to deterrence, if that means a higher overall pay-off.

A repeated game might also lead to strategy change owing to unforeseen issues with the initial strategy. In cyber operations, this could happen if the estimate for the strategic value z for the stolen information was far from reality. Calculations have to be re-done, strategies adjusted. In that case, one stakeholder might surrender rather than face a disaster, despite their previous positive assumptions about the state of play. As the current assumption is that cyber operations cannot, on their own, lead to the conquest of another country, a conflict in the cyber domain will be repeated infinitely until it either reaches escalation or mutually enforced cooperation, a *Nash Equilibrium*. However, the result of mutually enforced cooperation can represent a successful coercion of one state.

Stone introduces an interesting idea when arguing that:

> *'[i]n fact, one might say that the objective of game theory is to determine how the structure of games, together with the preferences and beliefs of the actors, determines strategic interaction. This does not mean, however, that decisions about "who moves first" cannot be left up to the actors. The model can specify that one player has a choice to move first or second or can introduce a random device, vote, or any other mechanism one wishes to propose. Game theory simply insists that these modeling choices have important consequences, so they must be made explicit'* (Stone, 2001: 227).

The introduction of a doomsday-machine-like device which automatically shuts down major parts of the Internet seems technically feasible for some greater powers, but can be disregarded for the purposes of this research. Due to the decentralized nature of the Internet, even the shutdown of major optic fiber connections will only slow down the traffic, or regionalize it, but not bring down the whole Internet. While the Spamhaus attack in 2013 (Arthur, 2013) showed that it might be possible to temporarily halt Internet services it seems far-fetched for a state to do so. Arguably, those major powers which actually would have the ability to shut down the Internet - partially or completely for some time – are too dependent on it to do so. Thus, such a move would result in potential self-destruction. If smaller states, which are not too connected and Internet-dependent, would be able to have the credible ability to threat an Internet take-down, this discussion might become relevant. Until then, the 'what if' question can be, if not neglected, postponed.

At first glance, it seems inappropriate to ask the question *who moved first* as the cyber domain enables communication at a very high speed. At all levels however, tactical, operational and strategic, moves are visible in their order. Administrators can tell you to the millisecond when an attacker tried to gain access to a certain CNII. While it takes some time to conclude all the details, as it was the case with the late discovery of the earliest Stuxnet version (McDonald et al., 2013), cyber operations campaigns which reflect certain strategies can be tracked *a posteriori* in terms of timing. Thus, the sequence of moves cannot be neglected *per se*.

9.4 Modelling

9.4.1 Framework

The following sub-section illustrates different scenarios of cyber conflicts and calculate their outcome. They will vary in strength of conventional and cyber capabilities and, in general, the overall military power of the two participating states (players). The scenarios are being created and their outcome computed in order to derive some more general lessons from cyber operations for the states' strategies towards the cyber domain

(as mentioned in the introduction to this chapter). At the same time, those scenarios serve as examples to teach decision-makers how to create and compute their own cyber operations case studies, based on the available empirical data. The first scenario assumes two symmetrically strong adversaries (in terms of m and c) mirroring the pay-off of each strategy. The second scenario presents two states which have equal non-cyber capabilities (m) but one state is twice as strong in terms of cyber capabilities (c) as the other. The third scenario matches the second, distinguished by the stronger player is now four-times as strong, in terms of cyber capabilities. The fourth scenario presents two states where one state is twice as strong in terms of cyber capabilities but the other state is twice as strong in terms of non-cyber capabilities. The fifth scenario matches the fourth but instead of the states possessing twice the respective power, here they are four-times as superior. The sixth scenario presents a state with very high cyber capabilities facing off with a state with only slightly higher non-cyber capabilities. The last scenario presents a state with very high non-cyber capabilities facing off with a state with only slightly higher cyber capabilities. Each scenario is based on the search for equilibrium. Equilibrium shows the final outcome of the conflict the two players are engaged in.

9.4.2 Scenario 1: Symmetrical Adversaries

For this scenario, the military capabilities (m and c) are equal for both players, therefore 1 resulting in:

$m = 1$

$c = 1$

The strategies are linked to each other as they represent an increasing level of risk of escalation with going dark having no risk of escalation and cyber war (*qua* definition) represents the full risk of escalation (see section 9.3). For the other three strategies, the assumption is an equally proportional, increasing likelihood of escalation. The resulting risk of escalation for both states is:

$r_{\text{Going Dark}} = 1$

$r_{\text{Deterrence}} = 0.75$

$r_{\text{Sub Rosa}} = 0.5$

$r_{\text{Shashou Jian}} = 0.25$

$r_{\text{Cyber War}} = 0$

In order to identify v_{total}, the first arbitrary assumption is that $v_1 = v_2$. The second assumption follows the logic from before, calculating an equally proportional increasing v_{total}. The higher the intensity of a strategy, the more likely is the increase in the strategic value. Going Dark will not result in pay-off gains, resulting in $v_{total} = 0$. Based on the equally proportional distribution, this would result in the following strategic value for both states: Strategic value indicates the strategic gain that can be derived from the information stolen or infrastructure disrupted by implementing the respective strategies and is proportional to the intensity of the strategy.

$v_{\text{total (Going Dark)}} = 0$

$v_{\text{total (Deterrence)}} = 0.5$

$v_{\text{total (Sub Rosa)}} = 1.0$

$v_{\text{total (Shashou Jian)}} = 1.5$

$v_{\text{total (Cyber War)}} = 2.0$

The resulting pay-off for both states is therefore:

$z_{\text{Going Dark}} = 0$

$z_{\text{Deterrence}} = 0.375$

$z_{\text{Sub Rosa}} = 0.5$

$z_{\text{Shashou Jian}} = 0.375$

$z_{\text{Cyber War}} = 0$

Mapped in a simple form, the matrix would look like this:

		State B				
		Going Dark	Deterrence	Sub Rosa	Shashou Jian	Cyber War
State A	Going Dark	0 / 0	0 / 0.375	0 / 0.5	0 / 0.375	0 / 0
	Deterrence	0.375 / 0	0.375 / 0.375	0.375 / 0.5	0.375 / 0.375	0.375 / 0
	Sub Rosa	0.5 / 0	0.5 / 0.375	0.5 / 0.5	0.5 / 0.375	0.5 / 0
	Shashou Jian	0.375 / 0	0.375 / 0.375	0.375 / 0.5	0.375 / 0.375	0.375 / 0
	Cyber War	0 / 0	0 / 0.375	0 / 0.5	0 / 0.375	0 / 0

Table 4

The matrix (see table 4) shows that both states would choose the *sub rosa* strategy above other available strategies, as this strategy leaves them with the highest pay-off. *Sub rosa* is the dominant strategy for both players, including the highlighted Nash Equilibrium. If both states conduct *sub rosa* cyber strategies none of them would deviate from it because it can only result in a lower pay-off.

In order to convert this game into a game with imperfect information, the assumption is that state A conduct a cyber operation against state B without knowing the strategies, pay-offs or general preferences of it. This application is better shown using the extensive form. This presentation assumes that state A moves first. Due to the symmetrical nature of their pay-offs and strategies, the choice of player at this point is irrelevant. At the root node, the player has to decide which cyber strategy to engage in, without knowledge of the adversary's choice of strategy. This can either mean that the adversary has not yet chosen a strategy, or that the player at the root node does not know which strategy the adversary has chosen. Hence, in the latter case they operate with only imperfect information. When it is state B's turn to choose a strategy, state A will still not know which strategy has been chosen by state B. Without all this information, state A can already see, that *sub rosa* is the most rewarding strategy, thus it would choose this strategy.

Concluding, even if state A does not have perfect information, it would make the same choices it would in the case of perfect information. In this case, it would implement *a*

sub rosa cyber strategy. The reason for this is first, that both states in this example are symmetrically strong. Additionally, and most importantly, one player's pay-off is independent on the other player's pay-off, thus excluding counter-strategies. Due to the existence of a stable equilibrium, there is no need to apply further tools from game theory, such as mixed strategies.

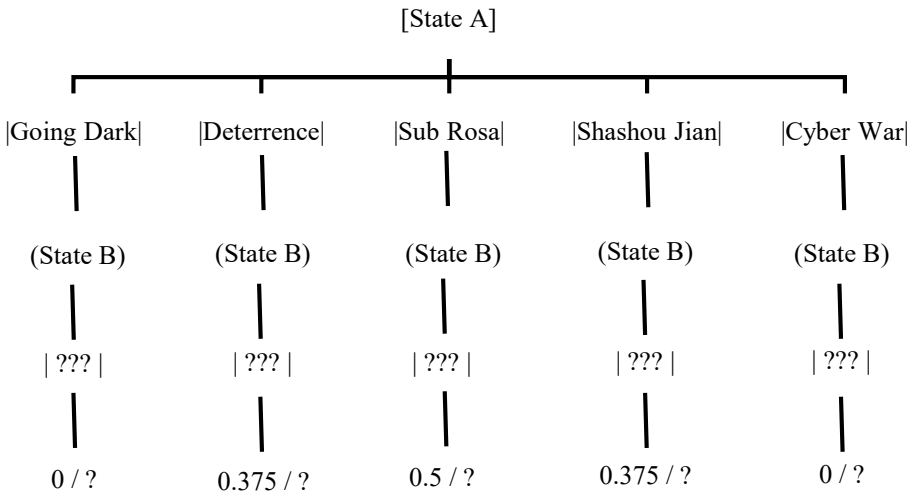

Figure 12

[] indicates the root node, () subsequent nodes and || the chosen strategies at a preceding node and x / x the pay-off for the players at the nodes [] / (). The three question marks (???) represent the imperfect information state A has about state B: the chosen strategy of the adversary as well as the pay-off from those strategies unknown to state A.

9.4.3 Scenario 2: Asymmetrical Adversaries

This scenario assumes that one player is twice as strong as the other player. In more specific terms, this means that state A has twice the military strength (m and c) of its adversary. That aspect directly influences the risk of escalation, and hence the pay-off. Assuming that one state has twice the military capabilities as its opponent, it will value the risk of escalation less because it is well equipped for a possible escalation (escalation dominance). Bearing in mind that this discussion assumes a two-player international arena as a setting, the state will not only value the risk of escalation less, but also include the cyber war strategy in its list of possible strategies. Knowing its superiority ta state will assume that its opponent will be unlikely escalate the conflict due to the lack of non-cyber military capabilities (m).

In numerical terms, the risk of escalation for going dark is still non-existent- therefore - 1. The risk of escalation is distributed over the other four strategies with cyber war being >0, and no strategy having a definite risk of escalation (escalation control). The risk of escalation and strategic options for the weaker state are analogous to the scenario above, as the difference in conventional military strength is already factored in the risk of escalation for the stronger state. Thus, going dark remains at 1 and cyber war at 0 with the risk of escalation equally distributed over the three remaining strategies.

risk of escalation for state A (strong)	risk of escalation for state B (weak)
$r_{\text{Going Dark}} = 1$	$r_{\text{Going Dark}} = 1$
$r_{\text{Deterrence}} = 0.8$	$r_{\text{Deterrence}} = 0.75$
$r_{\text{Sub Rosa}} = 0.6$	$r_{\text{Sub Rosa}} = 0.50$
$r_{\text{Shashou Jian}} = 0.4$	$r_{\text{Shashou Jian}} = 0.25$
$r_{\text{Cyber War}} = 0.2$	$r_{\text{Cyber War}} = 0$

Table 5

Due to the asymmetrical nature of non-cyber capabilities, factoring m into the equation from the weaker state's perspective, the risk of escalation will be double as much (m = 0.5). The state is now twice as risk-averse as before. The factor non-cyber capabilities

m for the stronger state remains 1 (twice as strong as the adversary). Including them on both sides would lead to an over-valuation as the result would be quadruple instead of double.

$m_{weak\ state} = 0.5$

$m_{strong\ state} = 1.0$

m * r for state A (strong)	m * r for state B (weak)
$m * r_{Going\ Dark} = 1$	$m * r_{Going\ Dark} = 0.5$
$m * r_{Deterrence} = 0.8$	$m * r_{Deterrence} = 0.375$
$m * r_{Sub\ Rosa} = 0.6$	$m * r_{Sub\ Rosa} = 0.25$
$m * r_{Shashou\ Jian} = 0.4$	$m * r_{Shashou\ Jian} = 0.125$
$m * r_{Cyber\ War} = 0.2$	$m * r_{Cyber\ War} = 0$

Table 6

Concerning the strategic values, the numbers for the stronger state will remain. It follows an equal distribution from the maximum value of information derived from conducting cyber war to the minimum of strategic value derived from conducting going dark. The assumption that one state has twice the cyber military capabilities (c) as the other is represented here from the weak states perspective. Similar to the inclusion of m before, the factor cyber capabilities, c for the stronger state remains 1 (twice as strong as the adversary).

$c_{weak\ state} = 0.5$

$c_{strong\ state} = 1.0$

The strategic value of information gained remains the same, as the influence based on the difference in strengths is factored in through the application of c. Based on the equal distribution, this would result in the following strategic value for both states:

$v_{total\ (Going\ Dark)} = 0$

$v_{total\ (Deterrence)} = 0.5$

$v_{total\ (Sub\ Rosa)} = 1.0$

$v_{total\ (Shashou\ Jian)} = 1.5$

$v_{total\ (Cyber\ War)} = 2.0$

The strategic value that a state gains from conducting a strategy depends on the cyber capabilities in existence. The weaker state only has half the military capabilities *vis-à-vis* the adversary and can subsequently derive only half the strategic value from the operations it conducts. Going dark does not produce any strategic value and cyber war produces the highest strategic value. The rest is equally distributed over the other three strategies.

$c * v_{total}$ for state A (strong)	$c * v_{total}$ for state B (weak)
$c * v_{total\ (Going\ Dark)} = 0$	$c * v_{total\ (Going\ Dark)} = 0$
$c * v_{total\ (Deterrence)} = 0.5$	$c * v_{total\ (Deterrence)} = 0.25$
$c * v_{total\ (Sub\ Rosa)} = 1.0$	$c * v_{total\ (Sub\ Rosa)} = 0.5$
$c * v_{total\ (Shashou\ Jian)} = 1.5$	$c * v_{total\ (Shashou\ Jian)} = 0.75$
$c * v_{total\ (Cyber\ War)} = 2.0$	$c * v_{total\ (Cyber\ War)} = 1.0$

Table 7

The resulting pay-offs are then calculated accordingly.

Pay-offs for state A (strong)	Pay-off for state B (weak)
$z_{Going\ Dark} = 0$	$z_{Going\ Dark} = 0$
$z_{Deterrence} = 0.4$	$z_{Deterrence} = 0.09375$
$z_{Sub\ Rosa} = 0.6$	$z_{Sub\ Rosa} = 0.125$
$z_{Shashou\ Jian} = 0.6$	$z_{Shashou\ Jian} = 0.09375$
$z_{Cyber\ War} = 0.4$	$z_{Cyber\ War} = 0$

Table 8

The resulting matrix is as follows:

		State B (weak)				
		Going Dark	Deterrence	Sub Rosa	Shashou Jian	Cyber War
State A (strong)	Going Dark	0 / 0	0 / 0..9375	0 / 0.125	0 / 0.09375	0 / 0
	Deterrence	0.4 / 0	0.4 / 0.09375	0.4 / 0.125	0.4 / 0.09375	0.4 / 0
	Sub Rosa	0.6 / 0	0.6 / 0.09375	0.6 / 0.125	0.6 / 0.09375	0.6 / 0
	Shashou Jian	0.6 / 0	0.6 / 0.09375	0.6 / 0.125	0.6 / 0.09375	0.6 / 0
	Cyber War	0.4 / 0	0.4 / 0.09375	0.4 / 0.125	0.4 / 0.09375	0.4 / 0

Table 9

The matrix shows that state A would either choose *sub rosa* or *shashou jian* strategy. Between those two strategies, the state is at liberty to decide, given that both strategies offer the same pay-off. There is no single dominant strategy for state A. It could either choose one of those strategies or choose both strategies each with the probability (p) 0.5. As for state B, it would always prefer the *sub rosa* strategy as it offers the single highest pay-off and therefore becomes the state's dominant strategy. Subsequently, there are two Nash Equilibria: *sub rosa / sub rosa* and *shashou jian / sub rosa* (highlighted).

Analogous to the scenario above, the extensive forms (see figure 13 and figure 14) portray the same situation but with imperfect information and the assumption that a certain state moves first (or without the knowledge of the prior moves of the other state). For state B, the choice of strategies, even with imperfect information, is obvious – it will always choose the *sub rosa* cyber strategy. For state A, the situation is more complex. Without prior information on the adversaries pay-off and chosen strategy, it is undecided between *sub rosa* or *shashou jian* as both pay-offs are equal. A logical, risk-averse choice would be to apply both strategies each with a probability of p = 0.5. This way, the adversary would get the average pay-off of both strategies with neither the chance of having a distinctively high pay-off or distinctively low pay-off. The result does not, however differ from the assumption above, that state A will have a guaranteed pay-off of 0.6 while state B's pay-off will be 0.125. Subsequently, state A will mix *sub rosa* and *shashou jian* cyber strategies while state B will conduct a *sub rosa* cyber strategy.

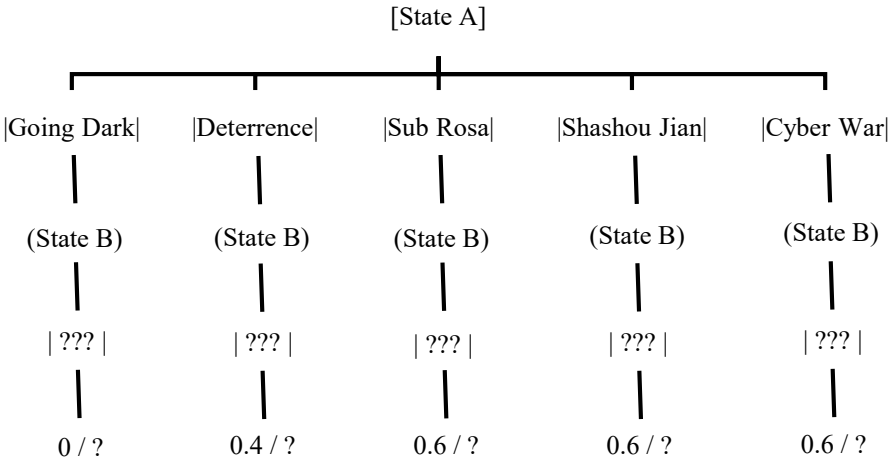

Figure 13

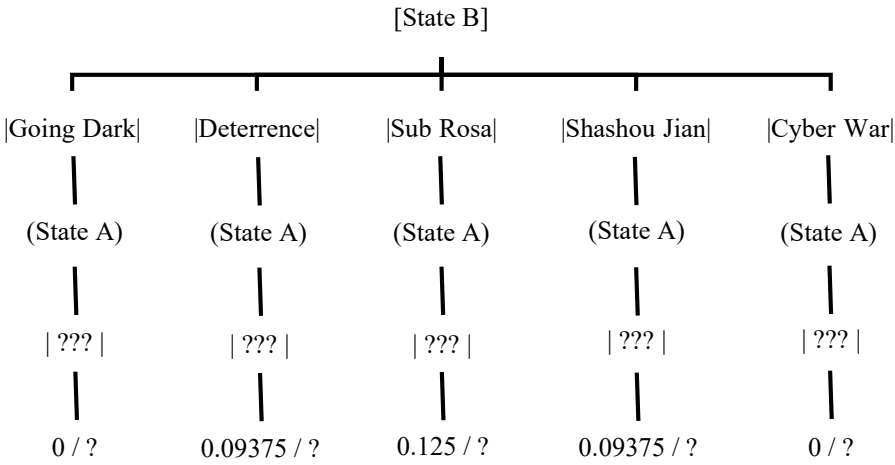

Figure 14

9.4.4 Scenario 3: Highly Asymmetrical Adversaries

This scenario is similar to 9.4.3 with the difference that the assumption is that the strong state is four times as strong as other state (in terms of m and c). The scenario has been chosen to analyse the consequences of a higher degree of difference in capabilities between the two states. As in 9.3.3, this means that the pay-off for the stronger state is higher (multiplied by c) and the value put to the risk of escalation by the weaker state is higher (multiplied by m).

$m_{weak\ state} = 0.25$

$m_{strong\ state} = 1.00$

$c_{weak\ state} = 0.25$

$c_{strong\ state} = 1.00$

Numerically, the risk of escalation for going dark is still 1. The risk of escalation is equally distributed over the other four strategies with cyber war being >0, with no strategy carrying a definite risk of escalation (as explained above). The risk of escalation for the weaker state is analogous to the scenario above. It will still not consider cyber war as a strategic option, while going dark is not considered to bear escalating potential at all, putting going dark at 1 and cyber war at 0. The risk of escalation is then equally distributed over the three remaining strategies.

risk of escalation for state A (strong)	risk of escalation for state B (weak)
$r_{Going\ Dark} = 1$ $r_{Deterrence} = 0.8$ $r_{Sub\ Rosa} = 0.6$ $r_{Shashou\ Jian} = 0.4$ $r_{Cyber\ War} = 0.2$	$r_{Going\ Dark} = 1$ $r_{Deterrence} = 0.75$ $r_{Sub\ Rosa} = 0.50$ $r_{Shashou\ Jian} = 0.25$ $r_{Cyber\ War} = 0$

Table 10

m * r for state A (strong)	m * r for state B (weak)
$m * r_{Going\ Dark} = 1$	$r_{Going\ Dark} = 0.25$
$m * r_{Deterrence} = 0.8$	$r_{Deterrence} = 0.1875$
$m * r_{Sub\ Rosa} = 0.6$	$r_{Sub\ Rosa} = 0.125$
$m * r_{Shashou\ Jian} = 0.4$	$m * r_{Shashou\ Jian} = 0.0625$
$m * r_{Cyber\ War} = 0.2$	$m * r_{Cyber\ War} = 0$

Table 11

The strategic value is similar to 9.4.3. It follows an equal distribution from the maximum value of information derived from conducting cyber war to the minimum of strategic value derived from conducting going dark. Based on the equal distribution, this would result in the following strategic value for both states:

$v_{total\ (Going\ Dark)} = 0$

$v_{total\ (Deterrence)} = 0.5$

$v_{total\ (Sub\ Rosa)} = 1.0$

$v_{total\ (Shashou\ Jian)} = 1.5$

$v_{total\ (Cyber\ War)} = 2.0$

The resulting values, including the cyber capabilities are:

$c * v_{total}$ for state A (strong)	$c * v_{total}$ for state B (weak)
$c * v_{total\ (Going\ Dark)} = 0$	$c * v_{total\ (Going\ Dark)} = 0$
$c * v_{total\ (Deterrence)} = 0.5$	$c * v_{total\ (Deterrence)} = 0.125$
$c * v_{total\ (Sub\ Rosa)} = 1.0$	$c * v_{total\ (Sub\ Rosa)} = 0.25$
$c * v_{total\ (Shashou\ Jian)} = 1.5$	$c * v_{total\ (Shashou\ Jian)} = 0.375$
$c * v_{total\ (Cyber\ War)} = 2.0$	$c* v_{total\ (Cyber\ War)} = 0.5$

Table 12

The resulting pay-offs are:

Pay-offs for state A (strong)	Pay-off for state B (weak)
$z_{\text{Going Dark}} = 0$	$z_{\text{Going Dark}} = 0$
$z_{\text{Deterrence}} = 0.4$	$z_{\text{Deterrence}} = 0.0234375$
$z_{\text{Sub Rosa}} = 0.6$	$z_{\text{Sub Rosa}} = 0.03125$
$z_{\text{Shashou Jian}} = 0.6$	$z_{\text{Shashou Jian}} = 0.0234375$
$z_{\text{Cyber War}} = 0.4$	$z_{\text{Cyber War}} = 0$

Table 13

The resulting matrix is as follows:

		State B (weak)				
		Going Dark	Deterrence	Sub Rosa	Shashou Jian	Cyber War
State A (strong)	Going Dark	0 / 0	0 / 0.0234375	0 / 0.03125	0 / 0.0234375	0 / 0
	Deterrence	0.4 / 0	0.4 / 0.0234375	0.4 / 0.03125	0.4 / 0.0234375	0.4 / 0
	Sub Rosa	0.6 / 0	0.6 / 0.0234375	0.6 / 0.03125	0.6 / 0.0234375	0.6 / 0
	Shashou Jian	0.6 / 0	0.6 / 0.0234375	0.6 / 0.03125	0.6 / 0.0234375	0.6 / 0
	Cyber War	0.4 / 0	0.4 / 0.0234375	0.4 / 0.03125	0.4 / 0.0234375	0.4 / 0

Table 14

The result is exactly the same as in 9.4.3, albeit with differing pay-offs. The dominant strategies for both states, as well as the Nash Equilibrium, remain the same. Thus, there is no need for the extensive form to be applied. When simply multiplying the strategic value and the risk of escalation with the same number, no other outcome was expected. One implication that is worth analysing is the effect to which the stronger state's pay-off has been increased. In 9.4.3 state A (strong) was twice as strong as state B (weak) and the pay-off subsequently was four times as much (0.6 to 0.125). In 9.4.4 state A (strong) was four times as strong as state B (weak) and the pay-off was more than 25 times as much (0.6 to 0.0234375). Cyber operations subsequently do not only serve as a force multiplier but as an exponential force multiplier.

9.4.5 Scenario 4: Equally Asymmetrical Adversaries

The earlier scenarios assumed that conventional military power and cyber capabilities are related with each other. While the non-cyber military capabilities influence the risk of escalation, the cyber capabilities influence the strategic value as a result of conducting different strategies. This scenario assumes that state A is superior in terms of non-cyber military strength while it is inferior in terms of cyber capabilities. To allow comparisons to the earlier scenario, the scenario assumes that state A's non-cyber military power is twice that of state B and its cyber capabilities are only half as much as state B's.

m_{state} A = 1.0

m_{state} B = 0.5

c_{state} A = 0.5

c_{state} B = 1.0

The risk of escalation is calculated analogous to 9.3.3 and 9.3.4, whereas cyber war is an option for state A but not for state B for the same reasoning.

risk of escalation for state A	risk of escalation for state B
$r_{Going\ Dark}$ = 1 $r_{Deterrence}$ = 0.8 $r_{Sub\ Rosa}$ = 0.6 $r_{Shashou\ Jian}$ = 0.4 $r_{Cyber\ War}$ = 0.2	$r_{Going\ Dark}$ = 1 $r_{Deterrence}$ = 0.75 $r_{Sub\ Rosa}$ = 0.50 $r_{Shashou\ Jian}$ = 0.25 $r_{Cyber\ War}$ = 0

Table 15

Subsequently, the table for m * r is calculated.

m * r for state A	m * r for state B
$m * r_{Going\ Dark} = 1$	$m * r_{Going\ Dark} = 0.5$
$m * r_{Deterrence} = 0.8$	$m * r_{Deterrence} = 0.375$
$m * r_{Sub\ Rosa} = 0.6$	$m * r_{Sub\ Rosa} = 0.25$
$m * r_{Shashou\ Jian} = 0.4$	$m * r_{Shashou\ Jian} = 0.125$
$m * r_{Cyber\ War} = 0.2$	$m * r_{Cyber\ War} = 0$

Table 16

For the strategic value, the calculations are analogue to 9.4.3 and 9.4.4.

$v_{total\ (Going\ Dark)} = 0$

$v_{total\ (Deterrence)} = 0.5$

$v_{total\ (Sub\ Rosa)} = 1.0$

$v_{total\ (Shashou\ Jian)} = 1.5$

$v_{total\ (Cyber\ War)} = 2.0$

The strategic value is then multiplied with the strength in cyber capabilities.

$c * v_{total}$ for state A	$c * v_{total}$ for state B
$c * v_{total\ (Going\ Dark)} = 0$	$c * v_{total\ (Going\ Dark)} = 0$
$c * v_{total\ (Deterrence)} = 0.25$	$c * v_{total\ (Deterrence)} = 0.5$
$c * v_{total\ (Sub\ Rosa)} = 0.5$	$c * v_{total\ (Sub\ Rosa)} = 1.0$
$c * v_{total\ (Shashou\ Jian)} = 0.75$	$c * v_{total\ (Shashou\ Jian)} = 1.5$
$c * v_{total\ (Cyber\ War)} = 1.0$	$c * v_{total\ (Cyber\ War)} = 2.0$

Table 17

The resulting pay-offs are then calculated accordingly.

Pay-offs for state A	Pay-off for state B
$z_{\text{Going Dark}} = 0$	$z_{\text{Going Dark}} = 0$
$z_{\text{Deterrence}} = 0.2$	$z_{\text{Deterrence}} = 0.1875$
$z_{\text{Sub Rosa}} = 0.3$	$z_{\text{Sub Rosa}} = 0.25$
$z_{\text{Shashou Jian}} = 0.3$	$z_{\text{Shashou Jian}} = 0.1875$
$z_{\text{Cyber War}} = 0.2$	$z_{\text{Cyber War}} = 0$

Table 18

The resulting matrix looks like this:

		State B				
		Going Dark	Deterrence	Sub Rosa	Shashou Jian	Cyber War
State A	Going Dark	0 / 0	0 / 0.1875	0 / 0.25	0 / 0.1875	0 / 0
	Deterrence	0.2 / 0	0.2 / 0.1875	0.2 / 0.25	0.2 / 0.1875	0.2 / 0
	Sub Rosa	0.3 / 0	0.3 / 0.1875	0.3 / 0.25	0.3 / 0.1875	0.3 / 0
	Shashou Jian	0.3 / 0	0.3 / 0.1875	0.3 / 0.25	0.3 / 0.1875	0.3 / 0
	Cyber War	0.2 / 0	0.2 / 0.1875	0.2 / 0.25	0.2 / 0.1875	0.2 / 0

Table 19

The resulting choice of strategies for the states is the same as in 9.4.3, therefore an additional drafting of the corresponding extensive form is not required. The table shows that the Nash Equilibrium are *sub rosa / sub rosa* and *shashou jian / sub rosa*. For state A, there is no single dominant strategy as both, *sub rosa* and *shashou jian,* lead to the same pay-off. For state B, *sub rosa* is the dominant strategy, as it offers the single highest pay-off among all strategies. Subsequently, imperfect information would lead to state A choosing both strategies with the probability of p = 0.5 each and resulting in a total pay-off of 0.3. State B would always choose the *sub rosa* strategy (p = 1) and therefore would acquire the outcome of the pay-off being 0.25.

At first glance, it seems like the changed superiority in cyber capabilities (c) did not affect the choice of strategies at all, with the conventionally superior (m) state A still attaining a higher pay-off than its counterpart and still choosing the *sub rosa* and

shashou jian strategies half of the time (both with p = 0.5). State B, correspondingly still has a lower pay-off than state A and only one dominant strategy, *sub rosa*. Generally speaking, there is no difference at the macro level. Yet, a very important difference can be found in the numbers. The gap between the pay-offs for both states decreases vastly and is nearly equalized. When state A was superior in cyber and conventional military capabilities, the difference in the pay-offs for both state was significant with a total of 0.475 (0.6 compared to 0.125). In other words, state B's pay-off was 20.83% of state A's pay-off. In this scenario, where a state is still superior in conventional military capabilities, but not in cyber military capabilities, the difference in the pay-offs for both states is only 0.05 (0.3 compared to 0.25). In other words, state B's pay-off is now 83.3% of state A's pay-off. While the superiority of each state in its respective field is equal, the outcome is that the states are not on par with neither the strategic choices nor the outcomes (pay-off).

Comparing the outcomes of this, and the earlier scenario lead to a pivotal conclusion: cyber capabilities can make up for the lack of conventional capabilities – but not entirely. In the setting where two states enjoy relative superiority in one or the other field, the state with the conventional superiority will have a higher pay-off and more strategic options. Despite that, the very narrow gap between the states in this example cannot be ignored for a simple reason: if a state is more likely to achieve a superiority in cyber capabilities (e.g. due to the needed resourced or access), it should aim for it rather than running the risk of being inferior in both domains.

9.4.6 Scenario 5: Highly Equally Asymmetrical Adversaries

This scenario is analogous to 9.4.5, but assumes that state A is four times as strong in non-cyber capabilities as state B while state B is four times as strong in cyber capabilities as state A.

m_{state} A = 1.0

m_{state} B = 0.25

c_{state} A = 0.25

c_{state} B = 1.0

The risk of escalation follows the same logic as in 9.4.4, resulting in the following:

Table 20

risk of escalation for state A	risk of escalation for state B
$r_{Going\ Dark} = 1$ $r_{Deterrence} = 0.8$ $r_{Sub\ Rosa} = 0.6$ $r_{Shashou\ Jian} = 0.4$ $r_{Cyber\ War} = 0.2$	$r_{Going\ Dark} = 1$ $r_{Deterrence} = 0.75$ $r_{Sub\ Rosa} = 0.50$ $r_{Shashou\ Jian} = 0.25$ $r_{Cyber\ War} = 0$

The calculation including the non-cyber military capabilities leads to the following table.

m * r for state A	m * r for state B
$m * r_{Going\ Dark} = 1$ $m * r_{Deterrence} = 0.8$ $m * r_{Sub\ Rosa} = 0.6$ $m * r_{Shashou\ Jian} = 0.4$ $m * r_{Cyber\ War} = 0.2$	$m * r_{Going\ Dark} = 0.25$ $m * r_{Deterrence} = 0.1875$ $m * r_{Sub\ Rosa} = 0.125$ $m * r_{Shashou\ Jian} = 0.0625$ $m * r_{Cyber\ War} = 0$

Table 21

For the strategic value, the calculations match to 9.4.3 and 9.4.4.

$V_{total\ (Going\ Dark)} = 0$

$V_{total\ (Deterrence)} = 0.5$

$V_{total\ (Sub\ Rosa)} = 1.0$

$v_{total\ (Shashou\ Jian)} = 1.5$

$v_{total\ (Cyber\ War)} = 2.0$

The strategic value is then multiplied with the strength in cyber capabilities.

$c * v_{total}$ for state A	$c * v_{total}$ for state B
$c * v_{total\ (Going\ Dark)} = 0$	$c * v_{total\ (Going\ Dark)} = 0$
$c * v_{total\ (Deterrence)} = 0.125$	$c * v_{total\ (Deterrence)} = 0.5$
$c * v_{total\ (Sub\ Rosa)} = 0.25$	$c * v_{total\ (Sub\ Rosa)} = 1.0$
$c * v_{total\ (Shashou\ Jian)} = 0.375$	$c * v_{total\ (Shashou\ Jian)} = 1.5$
$c * v_{total\ (Cyber\ War)} = 0.5$	$c * v_{total\ (Cyber\ War)} = 2.0$

Table 22

The resulting pay-offs are then calculated accordingly.

Pay-offs for state A	Pay-off for state B
$z_{Going\ Dark} = 0$	$z_{Going\ Dark} = 0$
$z_{Deterrence} = 0.1$	$z_{Deterrence} = 0.09375$
$z_{Sub\ Rosa} = 0.15$	$z_{Sub\ Rosa} = 0.125$
$z_{Shashou\ Jian} = 0.15$	$z_{Shashou\ Jian} = 0.09375$
$z_{Cyber\ War} = 0.1$	$z_{Cyber\ War} = 0$

Table 23

The resulting matrix looks like this:

		State B				
		Going Dark	Deterrence	Sub Rosa	Shashou Jian	Cyber War
State A	Going Dark	0 / 0	0 / 0.09375	0 / 0.125	0 / 0.09375	0 / 0
	Deterrence	0.1 / 0	0.1 / 0.09375	0.1 / 0.125	0.1 / 0.09375	0.1 / 0
	Sub Rosa	0.15 / 0	0.15 / 0.09375	0.15 / 0.125	0.15 / 0.09375	0.15 / 0
	Shashou Jian	0.15 / 0	0.15 / 0.09375	0.15 / 0.125	0.15 / 0.09375	0.15 / 0
	Cyber War	0.1 / 0	0.1 / 0.09375	0.1 / 0.125	0.1 / 0.09375	0.1 / 0

Table 24

The results are comparable to the results of 9.4.5. State A still has more strategic choices, it can choose *sub rosa* or *shashou jian* and state B only *sub rosa.* Additionally, state A's pay-off is higher than the pay-off for state B. While both states are similarly strong in their respective fields (four times as much), state B's pay-off remains 83.3% of state A's pay-off (0.15 to 0.125). Thus, an increased cyber capability can be countered by an increased non-cyber military capability – and the other way around. This also means that an equal advantage in the opposing field will always leave the conventionally stronger power with a higher pay-off and more strategic options.

9.4.7 Scenario 6: Cyber Superiority

This scenario is analogous to 9.4.5 and 9.4.6. It assumes that state A is twice as strong in non-cyber capabilities as state B while state B is four times as strong in cyber capabilities as state A.

m_{state} A = 1.0

m_{state} B = 0.50

c_{state} A = 0.25

c_{state} B = 1.0

The risk of escalation follows the same logic as in 9.4.4, resulting in the following:

risk of escalation for state A	risk of escalation for state B
$r_{Going\ Dark} = 1$ $r_{Deterrence} = 0.8$ $r_{Sub\ Rosa} = 0.6$ $r_{Shashou\ Jian} = 0.4$ $r_{Cyber\ War} = 0.2$	$r_{Going\ Dark} = 1$ $r_{Deterrence} = 0.75$ $r_{Sub\ Rosa} = 0.50$ $r_{Shashou\ Jian} = 0.25$ $r_{Cyber\ War} = 0$

Table 25

The calculation including non-cyber military capabilities leads to the following table:

m * r for state A	m * r for state A
$m * r_{Going\ Dark} = 1$	$m * r_{Going\ Dark} = 0.5$
$m * r_{Deterrence} = 0.8$	$m * r_{Deterrence} = 0.375$
$m * r_{Sub\ Rosa} = 0.6$	$m * r_{Sub\ Rosa} = 0.25$
$m * r_{Shashou\ Jian} = 0.4$	$m * r_{Shashou\ Jian} = 0.125$
$m * r_{Cyber\ War} = 0.2$	$m * r_{Cyber\ War} = 0$

Table 26

For the strategic value, the calculations match 9.4.3 and 9.4.4.

$v_{total\ (Going\ Dark)} = 0$

$v_{total\ (Deterrence)} = 0.5$

$v_{total\ (Sub\ Rosa)} = 1.0$

$v_{total\ (Shashou\ Jian)} = 1.5$

$v_{total\ (Cyber\ War)} = 2.0$

The strategic value is then multiplied with the strength in cyber capabilities.

$c * v_{total}$ for state A	$c * v_{total}$ for state B
$c * v_{total\ (Going\ Dark)} = 0$	$c * v_{total\ (Going\ Dark)} = 0$
$c * v_{total\ (Deterrence)} = 0.125$	$c * v_{total\ (Deterrence)} = 0.5$
$c * v_{total\ (Sub\ Rosa)} = 0.25$	$c * v_{total\ (Sub\ Rosa)} = 1.0$
$c * v_{total\ (Shashou\ Jian)} = 0.375$	$c * v_{total\ (Shashou\ Jian)} = 1.5$
$c * v_{total\ (Cyber\ War)} = 0.5$	$c * v_{total\ (Cyber\ War)} = 2.0$

Table 27

The resulting pay-offs are then calculated accordingly.

Pay-offs for state A	Pay-off for state B
$z_{\text{Going Dark}} = 0$	$z_{\text{Going Dark}} = 0$
$z_{\text{Deterrence}} = 0.1$	$z_{\text{Deterrence}} = 0.1875$
$z_{\text{Sub Rosa}} = 0.15$	$z_{\text{Sub Rosa}} = 0.25$
$z_{\text{Shashou Jian}} = 0.15$	$z_{\text{Shashou Jian}} = 0.1875$
$z_{\text{Cyber War}} = 0.1$	$z_{\text{Cyber War}} = 0$

Table 28

The resulting matrix looks like this:

		State B				
		Going Dark	Deterrence	Sub Rosa	Shashou Jian	Cyber War
State A	Going Dark	0 / 0	0 / 0.1875	0 / 0.25	0 / 0.1875	0 / 0
	Deterrence	0.1 / 0	0.1 / 0.1875	0.1 / 0.25	0.1 / 0.1875	0.1 / 0
	Sub Rosa	0.15 / 0	0.15 / 0.1875	0.15 / 0.25	0.15 / 0.1875	0.15 / 0
	Shashou Jian	0.15 / 0	0.15 / 0.1875	0.15 / 0.25	0.15 / 0.1875	0.15 / 0
	Cyber War	0.1 / 0	0.1 / 0.1875	0.1 / 0.25	0.1 / 0.1875	0.1 / 0

Table 29

The results are similar to those of the past scenarios. State B is left with only one option, the *sub rosa* strategy. State A, however has the opportunity to decide if it wants to either conduct *sub rosa* warfare or *shashou jian* warfare and will apply both strategies with the probability of $p = 0.5$ as long as it does not have perfect information. The difference to the other scenarios is, that state B's pay-off is higher than state A's pay-off (0.25 to 0.15). Subsequently, superiority in cyber capabilities can help a state to have a higher pay-off than its adversary as long as the superiority in this field is higher than the superiority of the adversary in the non-cyber capabilities.

9.4.8 Scenario 7: Non-Cyber Superiority

This scenario is analogous to 9.4.7, but assumes that state A is four times as strong in non-cyber capabilities as state B while state B is only two times as strong in cyber capabilities as state A.

m_{state} A = 1.0

m_{state} B = 0.25

c_{state} A = 0.5

c_{state} B = 1.0

The risk of escalation follows the same logic as in 9.4.4, resulting in the following:

risk of escalation for state A	risk of escalation for state B
$r_{Going\ Dark}$ = 1 $r_{Deterrence}$ = 0.8 $r_{Sub\ Rosa}$ = 0.6 $r_{Shashou\ Jian}$ = 0.4 $r_{Cyber\ War}$ = 0.2	$r_{Going\ Dark}$ = 1 $r_{Deterrence}$ = 0.75 $r_{Sub\ Rosa}$ = 0.50 $r_{Shashou\ Jian}$ = 0.25 $r_{Cyber\ War}$ = 0

Table 30

The calculation including the non-cyber military capabilities leads to the following table.

m * r for state A	m * r for state B
m * $r_{Going\ Dark}$ = 1 m * $r_{Deterrence}$ = 0.8 m * $r_{Sub\ Rosa}$ = 0.6 m * $r_{Shashou\ Jian}$ = 0.4 m * $r_{Cyber\ War}$ = 0.2	m * $r_{Going\ Dark}$ = 0.25 m * $r_{Deterrence}$ = 0.1875 m * $r_{Sub\ Rosa}$ = 0.125 m * $r_{Shashou\ Jian}$ = 0.0625 m * $r_{Cyber\ War}$ = 0

Table 31

For the strategic value, the calculations match to 9.4.3 and 9.4.4.

$v_{total\ (Going\ Dark)} = 0$

$v_{total\ (Deterrence)} = 0.5$

$v_{total\ (Sub\ Rosa)} = 1.0$

$v_{total\ (Shashou\ Jian)} = 1.5$

$v_{total\ (Cyber\ War)} = 2.0$

The strategic value is then multiplied with the strength in cyber capabilities.

$c * v_{total}$ for state A	$c * v_{total}$ for state B
$c * v_{total\ (Going\ Dark)} = 0$	$c * v_{total\ (Going\ Dark)} = 0$
$c * v_{total\ (Deterrence)} = 0.25$	$c * v_{total\ (Deterrence)} = 0.5$
$c * v_{total\ (Sub\ Rosa)} = 0.5$	$c * v_{total\ (Sub\ Rosa)} = 1.0$
$c * v_{total\ (Shashou\ Jian)} = 0.75$	$c * v_{total\ (Shashou\ Jian)} = 1.5$
$c * v_{total\ (Cyber\ War)} = 1.0$	$c * v_{total\ (Cyber\ War)} = 2.0$

Table 32

The resulting pay-offs are then calculated accordingly.

Pay-offs for state A	Pay-off for state B
$z_{Going\ Dark} = 0$	$z_{Going\ Dark} = 0$
$z_{Deterrence} = 0.4$	$z_{Deterrence} = 0.09375$
$z_{Sub\ Rosa} = 0.3$	$z_{Sub\ Rosa} = 0.125$
$z_{Shashou\ Jian} = 0.3$	$z_{Shashou\ Jian} = 0.09375$
$z_{Cyber\ War} = 0.2$	$z_{Cyber\ War} = 0$

Table 33

The resulting matrix looks like this:

		State B				
		Going Dark	Deterrence	Sub Rosa	Shashou Jian	Cyber War
State A	Going Dark	0 / 0	0 / 0.09375	0 / 0.125	0 / 0.09375	0 / 0
	Deterrence	0.4 / 0	0.4 / 0.09375	0.4 / 0.125	0.4 / 0.09375	0.4 / 0
	Sub Rosa	0.3 / 0	0.3 / 0.09375	0.3 / 0.125	0.3 / 0.09375	0.3 / 0
	Shashou Jian	0.3 / 0	0.3 / 0.09375	0.3 / 0.125	0.3 / 0.09375	0.3 / 0
	Cyber War	0.2 / 0	0.2 / 0.09375	0.2 / 0.125	0.2 / 0.09375	0.2 / 0

Table 34

The Nash Equilibrium of this scenario is deterrence / *sub rosa*. The non-cyber superior state A tries to deter the cyber superior state B from launching cyber operations against it. State B on the other hand will conduct *sub rosa* cyber operations against state A. As compared to the previous scenario, the strategic options for both players are limited as there only is but one dominant strategy for each state. The scenario differs from the aforementioned. It presents a deterring state A which faces-off with *a sub rosa* conducting state B.

The outcome provides a valuable insight as compared with the finding in 9.4.7, because in this scenario, state A is even stronger in conventional terms and less weak in cyber capabilities. Analysing all the other scenarios, this will lead to the assumption that state A would adopt a more offensive cyber strategy. State A is equipped with more strategic options and has cyber war as an available strategy with the highest pay-off. The scenario's calculation however shows that the opposite is the case. State A has only one dominant strategy – a defensive one. Taking the setup and results of 9.4.6 into account, it can be deduced that cyber capabilities c seems to be the trigger for this unexpected outcome. As compared to 9.4.6 and 9.4.7, the state A in 9.4.8 is half as strong in cyber capabilities instead of quarter as strong as the opposing state. The increase in its own cyber capabilities (still not matching the adversary's), leads to a more defensive strategy. However, the pay-off for state is higher than in 9.4.6 and 9.4.7 as well as the difference of the pay-offs of the dominant strategies between state A and state B.

9.5 Conclusion

9.5.1 Remarks and Further Studies

This chapter has developed the game theory representation of cyber war strategies. This is not to say, however, that the issue is exhausted. Before discussing options for further studies, some remarks should be made about the methodology. First, the definition of the pay-off indicates independence of the players' strategies from each other. This presents the concept of dominant strategies. The dependence and outcome of the choice of strategies is only displayed in the final matrix. Established game theory models include dependence factored in on the level of strategies and therefore allow for counter-strategies. For example, player A acts giving player B choices, and non-deviation is reached because of the dependence of the other players' strategies. The dependence in the developed model is on the level of pay-offs with regard to the strategic value the adversary allocates to the information gathered, as well as cyber and non-cyber capabilities. This issue constitutes a minor snare which has to be kept in mind when continuing work with this framework.

A second point is the extension to an n-player game with additional stakeholders. This might also require the use of advanced game theory calculations, including but not limited to probability distribution and the application of the Grimm-Trigger effect. Third, the inclusion of threats, commitments, and credibility of such threats and commitments to a certain strategy is another area for further studies as exemplified by Stone (Stone, 2001: 218-220). Stone asked how it would change a game, if one of two people playing chicken – steering their cars into each other and whoever swerves first loses – would deconstruct the steering wheel and throw it out of the window, so that the other driver could see it. This therefore changes the strategy since it creates the advantage of having the first move and establishing a credible threat to the other player. A similar situation comes to mind when several US officials announced that a cyber attack against their critical information infrastructure might be retaliated against with by the use of nuclear weapons. The earlier-mentioned doomsday-machine falls in the

same category. All of these factors were not exhausted in this research but by no means indicates this that this research failed to answer the crucial questions about the strategic implications for the state. It is rather how Shubik described it by saying that:

> *'[t]he relationship between game theory and gaming goes in both directions. Game theory provides an extremely useful background for the structuring, the building and analysis of games. Yet at the same time gaming provides important evidence for the construction of new solution concepts for games and for the isolation of sociological, psychological and other variables which are not taken into account in the game theoretic model'* (Shubik, 1972: 53).

9.5.2 Leveling the Playing Field

The use of the game theory model as the tool of analysis on the strategic implications of cyber operations is both pragmatic and valuable. First, the analysis shows that the choice of an offensive option (excluding cyber war) almost always (with the exception 9.4.8) leads to a higher pay-off than a defensive strategy. Thus, all but one model indicated that the state's best option is to conduct offensive cyber operations in order to achieve the highest possible pay-off. This is contradictory to Lindsay's argument that there exists no categorical offense dominance in the cyber domain (Lindsay, 2013: 394-397). As the risk of escalation is included in the models, this outcome highlights the observation made in this research that there is a current era of Anti-War where states will conduct offensive cyber operations against each other rather than only focusing on the defensive capabilities.

Second, the analysis showed that cyber capabilities can make up for the lack in non-cyber capabilities to a limited extent. A very strong cyber force remains at the mercy of superior traditional forces, insofar as those traditional forces continue to outstrip the cyber forces by the same margin. If the adversary however does not increase the non-cyber forces by the same margin, the state focusing on cyber capabilities, thus achieving cyber superiority will reach a tipping point and subsequently end up with a higher pay-off than the adversary (see 9.4.7). In other words, increased cyber capabilities can be

countered by increased conventional capabilities of the opponent – and the other way around (compare 9.4.5 and 9.4.6).

Third, as shown, non-cyber superiority does not only lead to an edge over the adversary but can also allow the state to choose from more strategic options. While the non-cyber inferior state has only the option to conduct *sub rosa* cyber operations, the non-cyber superior state was able to choose between *sub rosa* and *shashou jian* cyber operations (see 9.4.6 and 9.4.7). This means that an equal advantage in the opposing field will always leave the non-cyber power with a higher pay-off- and more strategic choices. Interestingly, this strategic advantage did not hold true for the non-cyber superiority case. When the non-cyber superiority is asymmetrically higher than the cyber superiority of the adversary, the state is only left with the strategy to deter the adversary (see 9.4.8). As a result, offensive cyber operations will be conducted but non-cyber capabilities cannot be dismissed and in fact will give the stronger state the edge.

Fourth, comparing the results of 9.4.3 and 9.4.4 shows that cyber capabilities are by no means unimportant. The numbers show that cyber operations are a force multiplier *par excellence*, leading to an exponential growth of the pay-off.

Lastly, the almost complete absence of the more defensive strategies - going dark and deterrence – demands further acknowledgement. Only one scenario outcome saw deterrence as the dominant strategy and none saw going dark as a viable option for the state. This does not mean that the defensive approaches ought to be neglected. As shown in chapter IV, every cyber strategy is complemented by a one or more possible cyber security behaviors precisely because protecting itself in the cyber domain is *sine qua non*. Protective action is the defensive foundation that enables offensive action. Thus, choosing deterrence does not necessarily mean that the state is more protected in the cyber domain as when choosing offensive strategies. It simply means that fewer resources are needed in the implementation of a strategy along with a lower intensity of offensive operations and thus risk for retaliation and escalation. Second, deterrence *qua* definition includes offensive elements to make deterrence work. Additionally, going

dark can be regarded as passive rather than defensive, while all the other strategies are active.

Concluding, the distinction should not be made between defensive and offensive strategies but between less offensive (for example deterrence) and more offensive (for example *shashou jian*) strategies. This has taken into consideration the design of the scenarios. The calculation of the pay-offs values offensive success more than defensive success. In the long run however, less offensive strategies can only lose, as their aim is to prevent a disadvantage *vis-à-vis* an opponent, rather than creating an advantage (as in information superiority) over the said adversary. Simply put: a more offensive strategy has the ability to make up losses with wins, whereas a less offensive strategy only has the ability to prevent losses. From a game theory perspective, less offensive strategies are therefore genuinely weaker. This outcome is demonstrated repeatedly in the scenarios. The scenario which results in one player adopting cyber deterrence is inherently logical, but a paradox outcome in relation to the other scenarios. It suggests that there are exemptions from the rule(s) that have been concluded here.

The strategic implications derived from this analysis for the state posit that cyber operations are to be conducted in a more offensive, non-escalating manner against adversaries[76]. To implement offensive but non-escalatory actions against an adversary, it is pertinent to avoid attribution and focus on deception and *sub rosa*. At the same time, a backing with non-cyber military capabilities will allow cyber operations to gain the edge over the adversary, potentially enabling more strategic options and an exponentially increased pay-off.

[76] The activities of the American intelligence agencies against e.g. France and Germany, which were published by Edward Snowden starting in June 2013, are indicators that the term 'adversary' might be blurred when used to analyse cyber operations. In this framework it might be interesting to research on the validity of Kant's democratic peace theory derived from his work *Perpetual Peace*.

CONCLUSION

10. Conclusion

In 2011, Nye stated that

> *'[i]n comparison to the nuclear revolution in military affairs, strategic studies of the cyber domain are chronologically equivalent to 1960 but conceptually more equivalent to 1950. Analysts are still not clear about the lessons of offense, defense, deterrence, escalation, norms, arms control, or how they fit together into a national strategy'* (Nye, 2011: 19).

Not much progress has been made in the years that have passed something which contributed to the inspiration and motivation for this research. Several fields within the strategic domain of cyber operations have yet to be developed and this research aims to develop a part of that. This research has primarily concerned itself with contributing to the analysis and understanding of the strategic implications derived from offensive cyber activities of the state, embedded in its national strategy. The goal has been to form a comprehensive study of the strategic implications of cyber operations for the state, and hence contribute to supporting the decision-making process. In order to answer the questions posed by this dissertation, it was vital to explore several issues and analyse them in accordance to the research framework. This section structures and concludes the individual research outcomes and divides them into the three key areas for cyber operations: stakeholder, strategy and environment (see figure 15). The first part presents the strategic implications derived from the state as a stakeholder in the cyber domain and its interaction with other stakeholders. The second part covers the implications of cyber strategies, including their definitions, adaptation of strategic concepts and further strategic discussions within the cyber operations framework. The last part outlines the strategic implications for the state based on the environment in international relations, the Anti-War era. Those three key indicators mutually affect one another and are connected through cyber operations, forming the *cyber triangle*. The cyber triangle can therefore be regarded as the visual representation of the important strategic factors that influence cyber operations and are influenced by it.

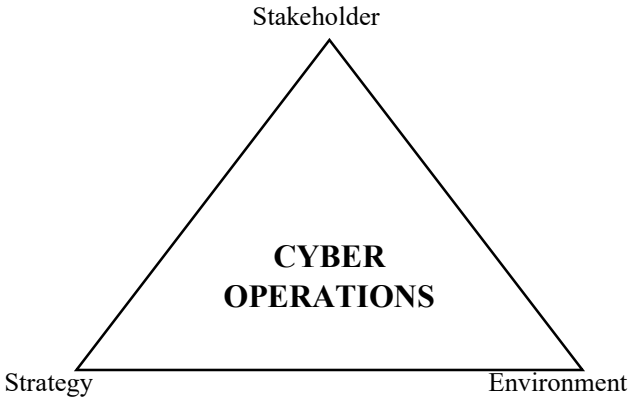

Figure 15

First, in order to analyse the strategic implications of any kind, one has to define the state in accordance to the respective domain by applying a theoretical framework to it. Focusing on the implications for one state, and leaving aside potential cooperation and internal struggles, and its pursuit of power, Georg Jellinek's state-teachings have been applied, attributing territory, citizens and the legitimate monopoly of power to the state (see chapter I). For operations in other domains, this definition is readily applied to them, something which has not so far extended to cyber operations. Cyber operations, as their partial liberation from traditional geographical borders, poses an additional challenge. Therefore, the need to translate a traditional reading of Jellinek's work onto the cyber domain, digitalizing the state, arose. To achieve this, the notion of a Critical National Information Infrastructure has been adopted and adapted to as a concept to represent the state in the cyber domain (see chapter II). The Critical National Information Infrastructure is composed in a way which demonstrates that attacks launched against it directly translate into an attack against people, territory or monopoly of power, and hence ultimately the state itself. Protecting the state from cyber operations therefore requires securing the Critical National Information Infrastructure, and the establishment of national cyber security. National cyber security is based on various actions and driven by an overarching strategy, the cyber security behaviour, which can be reactive, planned or proactive (see chapter III). The research identified the proactive

approach as most beneficial in terms of security and as a platform for potentially offensive actions or reactions, while requiring the most in terms of resources for proper implementation. It is the only approach with the potential to inflict damage on an attacker in return. Thus, while the Critical National Information Infrastructure represents the state in the cyber domain, the national cyber security ought to protect it, adopting proactive cyber security behaviour (see table 35).

The state's security in the cyber domain is ultimately measured in its ability to secure its Critical National Information Infrastructure. As outlined in the chapter on cyber security, international cooperation still proves a major challenge. The potential information advantage which can be derived from international cooperation can be substantial however. Sharing information on attack patterns or vulnerabilities can prove to be a large security gain. At the same time, cooperation can be exploited through information superiority over the cooperating partner and using information to prepare for a custom attack. Thus, another implication which can be derived from the analyses of this paper is that the state's approach towards the cyber domain should be self-focused at the outset while imbuing international cooperation and coordination in the long-run, as this presents opportunities to further strengthen existing strategy. This also provides challenges, which if handled wisely, is an opportunity to shed light on the existing weaknesses.

Stakeholder-Level	**State**
Conceptualization	**People, Territory and Legitimate Monopoly of Power**
Digitization	**Critical National Information Infrastructure**
Protection	**National Cyber Security**
Driving Force	**Proactive Cyber Security**
Foundation	**Cyber Security Pillars**

Table 35

Second, the academic discussions around cyber conflict, cyber war, information warfare, cyber operations and similar terms appear incoherent due to the lack of widely accepted definitions, and the implications they have. This research therefore analysed the different definitions and concluded chapter II with a definition of cyber operations on which the succeeding chapters are based. Cyber operations are defined as *the targeted use and hack of digital code by any individual, group, organization or state using digital networks, systems and connected devices, which is directed against Critical National Information Infrastructure in order to steal, alter, destroy information or disrupt and deny functionality with the ultimate aim to weaken and/ or harm the targeted political unit* (see chapter II).

This definition is the outcome of looking beyond the military use and including academic discourse on espionage, crime and civil disobedience in order to describe the precise activity which, targeted at the Critical National Information Infrastructure, is regarded as an attack against a state. Cyber operations evolved in different stages. It started in the late 90s with activities mainly focusing on data theft, progressed towards the use for political statements at the dawn of the millennium. Cyber operations transformed into long-term *sub-rosa* operations which peaked during the discovery of Stuxnet, Red October, Careto or Uroburos, as fully-blown virtual cloak-and-dagger games ten years later (see chapter II). It is not yet clear if a further acceleration of the ubiquity of cyber operations should be expected, or if the extent of its scope has been reached already.

The goal of this dissertation is to advance the literature on cyber operations from the conceptual to the strategic through a thorough discussion and analysis of concepts and to translate it to an operational language. The outcome depicts cyber operations as a unique kind of operations. Speaking in Gray's dimensions of strategies, the dimensions *people, technology, information and intelligence* as well as *friction* and *geography* deserve special attention and are distinctively different to other forms of warfare. Additionally, the lack of proper *attribution*, its *amorphousness* as well as its *ubiquity*, are distinct features of cyber operations, making them at once extremely complex and

highly volatile. Those indicators apply not only to the strategic but also to the political, operational and tactical levels. At the same time, cyber operations enable various strategic approaches such as coercion, deterrence and *sub-rosa* operations (see section 3.4). Cyber strategy has been defined as *the development and employment of cyber operations, potentially integrated and coordinated with other operational domains and forms of information operations, to achieve or support the achievement of political objectives* (see chapter IV). The research identified and scrutinized five different cyber strategies which are 1. going dark, 2. deterrence, 3. *sub rosa*, 4. *shashou jian* and 5. cyber war. The strategic choices that the cyber strategies offer in general can be regarded as intentionally stealthy, while unintentionally prone to escalation. The mode of implementation shows a strong *sub rosa* design, while the impact might lead to conflict escalation. The risk of the latter is mitigated by the aforementioned lack of proper attribution. Despite cyber operations' distinctiveness as a form of operations, the strategies are comparable to traditional strategies with certain variations (see section 7.4).

From a stakeholder's perspective, there are certain requirements which have to be fulfilled in order to make prudent decisions in implementing cyber operations. A deep understanding for the nature and impact of cyber operations is required alongside a constant monitoring of the situation and an awareness of the cross-domain implications and opportunities of said form of warfare (see section 7.3). All these findings contribute substantially to the current literature on offensive strategic operations in the cyber domain, going some way towards the possibility of political-level conclusions. Based on Nye's model of national power, these strategies contribute to military and information power in respect of the theory's national power indicator. Thus, the strategies contribute to achieving the political objectives of a given state within this framework (see section 7.4). Specifically, the strategies allow the achievement of certain political objectives without involving other warfare domains, therefore potentially keeping conventional and nuclear warfare at arm's length (see section 7.6). This precise point has been highlighted through the analysis of the case study Olympic

Games. It allowed the pursuit of a certain political objectives without more lethal forms of warfare. At the same time, this strategy leaves other options on the table, implying '[…] that cyber operations can make a strategic impact as stand-alone, physical, non-lethal option with low to none collateral damage and casualties' (see sub-section 8.4.3). Thus, cyber operations have been identified as a valuable addition to the state's menu of conflict responses. The last chapter utilized game theory in order further probe the results of the analytical sub-chapters on strategic cyber operations and Anti-War. Therefore, a customised approach within a game theory framework has been developed, based on the outcomes of the descriptive chapters on the state, cyber operations and national cyber security. While game theory has a rich history within strategic studies, especially relating to nuclear war, there is only limited literature applying the same methods to cyber operations. Subsequently, the use of game theory concluded the analysis of the strategic implications of cyber operations for the state while also serving as a proof of concept for its applicability of cyber operations issues. This method provided valuable insights into the necessity and vitality of cyber capabilities being developed by the state.

Cyber capabilities can potentially compensate for the lack in conventional warfare capabilities to a certain degree, but without traditional backing, an advanced cyber power would still be an inferior force, meaning that '[...] increased cyber capabilities can be countered by increased conventional capabilities of the opponent – and the other way around' (see section 9.5). Thus, stronger cyber capabilities have been determined to give equally conventionally strong adversaries the edge, while often also offering to choose from more strategic options. Those outcomes do not highlight the importance of cyber operations well, however. The analysis showed that cyber operations are a very strong force multiplier, meaning that states will be able to increase their total military strength efficiently by pouring resources into the development of cyber capabilities (see section 9.5). The analysis also showed that better outcomes can be achieved by the implementation of more offensive strategies. All strategies include a strong defensive element (see chapter IV) in order to uphold the crucial protection of the Critical National

Information Infrastructure. In the chapter on cyber security (chapter III) concludes that the most viable cyber security behaviour (proactive cyber security) includes offensive elements alongside with strong defensive ones. The conclusion of this game theory application is that to be most profitable, '[…] cyber operations are to be conducted in a more offensive, non-escalating manner against its adversaries. At the same time, a backing with non-cyber military capabilities will allow cyber operations to gain the edge over the adversary […]', meaning that cyber operations can be conducted as stand-alone but is by far more effective when being conducted as supplement (see section 9.5).

An additional implication from the use of game theory for strategic analysis of cyber operations, is their significance for symmetrical and asymmetrical conflict settings. This is one of crucial discourses on the strategic value of cyber operations. While some scholars argue that cyber operations have a significant impact on asymmetrical conflicts, favouring the weak, others argued that only symmetrical conflicts can be decided by cyber operations. This paper's analysis aligns with the latter position. Cyber operations allow the conventionally inferior stakeholder to recover a degree of military strength. At this point however it follows Gartzke's rationale that '[c]yberattacks are unlikely to prove particularly potent in grand strategic terms unless they can impose substantial, durable harm on an adversary' (Gartzke, 2013: 43). While cyber capabilities can make up for the lack in conventional warfare capabilities, they cannot sufficiently compensate for inferior traditional capacities. Cyber capabilities serve as a force multiplier and can therefore possibly deter the stronger adversary from pursuing further action but will not allow the weaker state to gain the upper hand without proper conventional support. The weaker state can only hope to coerce the superior adversary into withdrawal. If all stakeholders are aware of the circumstances, cyber operations have an impact in an asymmetrical conflict, but not a decisive one. In symmetrical settings however, cyber capability can, in fact, be decisive. For states, this conclusion points to the necessity of maintaining traditional forces rather than splitting expenditure with cyber capacities, if the state is to maintain a constant level strength. Cyber

capabilities have to be established in addition to, not as a substitution of traditional forces.

Adding cyber capabilities rather than substituting conventional forces leads to another area in the existing literature. While the main schools of thought mentioned in the introduction present both assumptions, (both standalone and supplementary approaches to cyber operations) this research suggests that both options are viable, depending on the political and strategic imperatives. Derived from the game theory discussion, supplementary cyber operations work effectively as a force multiplier of existing conventional capabilities. Considering the definition of cyber operations which has been used in this research, this also means that traditional forms of espionage and sabotage can be efficiently supported by cyber means. Cyber operations remain viable as standalone approach. Albeit the case that cyber strategies are less intense as a standalone force, cyber approaches are more subtle- a useful tool when secrecy is tantamount. The standalone approach can be utilized in special operations based on its affinity to non-escalation and plausible deniability. By developing cyber capabilities, states stand to gain a powerful new tool to be used in conflicts in a variety of ways.

Third, as more and more states - and potentially other stakeholders - enter the cyber domain and equip themselves with cyber capabilities, partially based on the aforementioned assumptions, the field of strategic studies will experience a new period, the Anti-War era. This era has been identified and discussed as one of the prime outcomes of this research. It is marked by a dominance of information operations, a comparatively low lethality in conflicts, a multi-stakeholder environment with power centres and an aspiring peripheries as well as a common desire among decision-makers to resolve rather than escalate conflicts. One of the reasons for this is the international reliance on the Internet. The Anti-War period requires clear signaling and the setup of proper communication channels in order to deal with the high complexity of cyber operations and the subsequent frictions which arise through the strategic conduct of operation in the cyber domain (see chapter IV). The game theory based analysis suggests that stakeholders will aim to equip themselves with cyber capabilities and

subsequently join by conducting offensive operations in the cyber domain to avoid being put at a disadvantage from an overtly defensive approach (see chapter V). For this very reason, the Anti-War era seems to be gaining momentum and is still far from its peak. Based on the outcomes of the first four chapters, the research identified the existence of an Anti-War era, similar to the Cold War era. This finding counters Lewis' statement that '[w]e can reject statements that America is in a new cold war or a covert cyberwar, as these characterizations are inaccurate and often self-serving' (Lewis, 2013a: 9). Not only the United States, but all countries inadvertently find themselves in the period which Lewis named *covert cyberwar* and has been identified as Anti-War in this research.

While the strong *sub rosa* character of Anti-War has been covered already, another crucial indicator is escalation. Within this framework, it is noteworthy that the advent of cyber operations was hailed as the new dimension of war. The direct connection between critical cyber attacks with nuclear retaliation is interesting. The basic logic of conflict is not changed by the inclusion of the cyber domain into the dimensions of military strategy. An escalation will still be an escalation, leading to more physical casualties. In the case of cyber operations, traditional warfare might hopefully come before nuclear warfare. Thus, cyber operations constitute another level in the escalation ladder, enabling states to carry out conflicts in an even more complex way. This leaves the question of the potential of an additional layer of non-physical conflict to the lower likelihood of escalation. As Brodie states with regard to the nuclear option, '[c]learly the Soviets are as keenly alive as we are to the catastrophic nature of general war' (Brodie, 1965: v). For states, having an additional conflict resolution tool at their disposal could contribute to a lower likelihood of escalation. The precondition for this would be the restriction of cyber operations to be carried out with a specific intensity in order to be as non-escalatory as possible while still attempting to coerce the adversary. With that restriction in mind, cyber operations will stay below the escalation radar unless an *accidental war* takes place.

Brodie states that accidental wars did not happen (Brodie, 1965: 22-23), pointing to a foreseeable escalation as the culmination of smaller conflicts (Brodie, 1965: 1). Thus, there are means to mitigate the effects of smaller conflicts before a cold war turns hot, or an Anti-War turns into war. In a frictionless setting, non-escalating cyber operations exist in equilibrium without escalating a conflict. However, the strategic conduct of cyber operations faces many challenges such as the lack of proper attribution or the difficulty of signaling. Thus, it can be doubted that a frictionless setting, and hence a non-escalating equilibrium, can persist for a longer period of time. This coincides with Rid's *danger paradox*. The paradox explains that cyber espionage is not an act of war, non-violent and yet most dangerous (Rid, 2013: 82). As it has been concluded, the definition of cyber operations partially includes cyber espionage; Rid's paradox might as well apply to cyber operations as it is applied in this research.

The answer to the main question posed by this research, about the strategic implications of cyber operations for the state, is outlined in the *cyber triangle* (see figure 15), consisting of *environment*, *strategy* and *stakeholder*. The *environment* for the state in connection with cyber operations has been defined as Anti-War, succeeding the Cold War era. During the latter, most states were, to a certain extent, affiliated with this state of international relations, either by treaties or through spillover effects of related conflicts. For the reason that every state is represented in the cyber domain, it will inevitably become a stakeholder in the Anti-War environment as well. Thus, as a first step, every state has to realise this and subsequently prepare for it. As far as the cyber *strategy* is concerned, the state's first aim would be to adopt a holistic, self-centered, proactive cyber security approach as foundation for subsequent cyber strategies. Within this framework, a more offensive cyber strategy must be implemented in a non-escalatory manner. While this research offers contributions to both basic research as well as strategic adaptation, scholarly discourse on the strategic application of cyber operations (especially in the field of offense) remains rare and should still be pursued and extended. The state as the core *stakeholder* has to ensure that the requirements for the development of offensive and defensive capabilities, which are derived from the

specific strategies, can be achieved. This includes financial and human resources in the education, research and development of the required technologies. Furthermore, the state has recognise its role, and that it is likely become a preferred target due to the lack of proper attribution, plausible deniability and the *sub rosa* nature of cyber operations. Lastly, in order to achieve certain policy objectives, the state has to realise that information superiority is the key element; and that it can only be obtained by conducting offensive cyber operations against adversaries.

BIBLIOGRAPHY

Ackermann, S. (2011) *With Stuxnet, Did The U.S. And Israel Create a New Cyberwar Era? [Updated]* [online], New York: Wired. Available: http://www.wired.com/dangerroom/2011/01/with-stuxnet-did-the-u-s-and-israel-create-a-new-cyberwar-era/ [Accessed 17 January 2011].

Adams, J. (2001) Virtual Defense*, Foreign Affairs*, 80(3), pp. 98-112.

Adams, T. and Scolland, S. (2006) *Internet Effectively. A Beginner's Guide to the World Wide Web.* London: Pearson Education Inc..

Ahrari, M. E. (1997) U.S. Military Strategic Perspectives on the PRC: New Frontiers of Information-Based War, *Asian Survey,* 37(12), December 1997, pp. 1163-1180.

Alastair, S. and Stam, A. C. (2004) Bargaining and the Nature of War, *The Journal of Conflict Resolution*, 48(6), pp. 783-813.

Albright, D., Brannan, P. and Walrond, C. (2011) *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report*. Washington: Institute for Science and International Security (ISIS).

Aljazeera (2010) *Fault Lines – Cyberwar* [online video], 16 December 2010. Available: http://english.aljazeera.net/programmes/faultlines/2010/04/2010421152728872905.html [Accessed:5 January 2012].

Alperovitch, D. (2011) *Revealed: Operation Shady RAT. White Paper, Version 1.1*. Santa Clara: McAfee.

Amores, R. (2011) *Cyber China Spy Threat | Cyber Espionage and Influence* [online], USCyberLabs. Available: http://uscyberlabs.com/blog/2011/09/22/cyber-china-spy-threat-cyber-espionage-influence/ [Accesed 15 December 2011].

Andrees, J. and Winterfield, S. (2011) *Cyber Warfare. Techniques, Tactics and Tools for Security Practitioners.* Waltham: Syngress.

Ang, P. W. and Nadarajan, B. (2002) *Censorship and Internet: a Singapore Perspective.* New York: United Nations Public Administration Network.

Arquilla, J. (2013) Twenty Years of Cyberwar, *Journal of Military Ethics*, 12(1), pp. 80-87.

Arquilla, J. and Ronfeldt, D. (1993), Cyberwar is Coming!. In Arquilla, J. and Ronfeldt, D. (Eds.) *In Athena's Camp: Preparing for Conflict in the Information Age. Santa Monica: RAND Corporation, pp. 23-60.*

Arquilla, J. and Ronfeldt, D. (1996) Information, Power, and Grand Strategy: In Athena's Camp'. In Schwartzstein, S. J. D. (Ed.) *The Information Revolution and National Security: Dimensions and Directions.* Washington D.C.: Center for Strategic and International Studies (CSIS), pp. 132-180.

Arquilla, J. and Ronfeldt, D. (1997) *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica: RAND Corporation.

Arquilla, J. and Ronfeldt, D. (2001) *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica: RAND Corporation.

Armond, P. (2001) Netwar in the Emerald City: WTO Protests Strategy and Tactics. In Arquilla, J. and Ronfeldt, D. (Eds.) *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica: RAND Corporation, pp.: 201-235.

Arreguín-Toft, I. (2001) How the weak win wars. A Theory of Asymmetric Conflict, *International Security,* 26(1), pp. 93-128.

Arthur, C. (2013) *Internet slows down after DNS attack on Spamhaus* [online], London: The Guardian. Available:

www.theguardian.com/technology/2013/mar/27/cyber-attack-spamhaus-slows-down-internet/ [Accessed 28 March 2013].

Arthur, C. (2011) *Iran should investigate Stuxnet virus, says atomic chief* [online], London: The Guardian. Available: http://www.guardian.co.uk/world/2011/feb/04/iran-stuxnet-virus/ [Accessed 4 February 2011].

Australian Government (2009), *Cyber Security Strategy.* Canberra: Commonwealth of Australia.

Avri, D. and Kleinwächter, W. (2008*) Internet Governance Forum: The First Two Year.* Geneva: IGF Secretariat.

Ball, D. (2011) China's Cyber Warfare Capabilities, *Security Challenges*, 7(2), pp. 81-103.

Barletta, G. A., Barletta, W. A. and Tsygichko, V. N. (2011) Cyber Conflict & Geo-Cyber Stability. In Touré, H. (Ed.) *The Quest for Cyber Peace*. Geneva: International Telecommunication Union & World Federation of Scientists, pp. 53-65.

Baumgartner, K. and Raiu, C. (2014) *The 'Penquin' Turla* [online], Moscow: Kaspersky Lab. Available: https://securelist.com/blog/research/67962/the-penquin-turla-2/ [Accessed 18 February 2015].

Baylis, J., Wirtz, J., Cohen, E. and Gray, C. S. (2002) *Strategy in the Contemporary World. An Introduction to Strategic Studies.* Oxford: Oxford University Press.

BBC News (2001) *'Truce' in US-China hacking war* [online], London: British Broadcasting Corporation (BBC). Available: http://news.bbc.co.uk/2/hi/asia-pacific/1322839.stm/ [Accessed 10 June 2011].

Berners-Lee, T. (2000) *Weaving the Web. The Past, Present and Future of the World Wide Web by its Inventor.* London and New York: Texere.

Betz, D. J. and Stevens, T. (2011) *Cyberspace and the State: Toward a Strategy for Cyber-power.* New York: Routledge.

Bhagyavati, B. (2008) Social Engineering. In Janczewski, L. J. and Colarik, A. M. (Eds.) *Cyber Warfare and Cyber Terrorism*. Hershey and New York: IGI Global, pp. 182-190.

Billo, C. and Chang, W. (2004) *Cyber Warfare. An Analysis of the Means and Motivations of Selected Nation States*. Hanover: Institute for Security Technology Studies, Darthmouth College.

Bishara, G. (1982) The Political Repercussions of the Israeli Raid on the Iraqi Nuclear Reactor, *Journal of Palestine Studies*, 11(3), pp. 58-76.

Bluth, C. (1995) *Britain, Germany, and Western Nuclear Strategy.* Oxford: Oxford University Press.

BMI (2011) *Cyber-Sicherheitsstrategie für Deutschland.* Berlin: Ministry of Interior of the Federal Republic of Germany.

Boldizsár, B., Pék, G., Buttyán, L. and Félegyházi, M. (2012) The Cousins of Stuxnet: Duqu, Flame, and Gauss, *Future Internet*, 4(6), pp. 971-1003.

Boldt, H. (2004), Staat, Recht und Politik bei Georg Jellinek. In Anter, A. (Ed.) *Die normative Kraft des Faktischen. Das Staatsverständnis Georg Jellineks.* Baden-Baden: Nomos, pp. 13-36.

Brams, S. J. and Kilgour, M. (1988) National Security Games, *Synthese*, 76(2), pp. 185-200.

Broad, W. J., Markoff, J. and Sanger, S. E. (2011), *Israeli Test on Worm Called Crucial in Iran Nuclear Delay* [online], New York: New York Times. Available: https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0 [Accessed 21 January 2011].

Brodie, B. (1946) War in the Atomic Age. In Chaliand, G. (Ed.)(1994) *The Art of War in World History. From Antiquity to the Nuclear Age*. London: University of California Press.

Brodie, B. (1965) *Escalation and the Nuclear Option*. *Memorandum RM-4544-PR*. Santa Monica: RAND Corporation.

Bronk, C. (2008) Hacking the Nation-State: Security, Information Technology and Policies of Assurance, *Information Security Journal: A Global Perspective,* 17, pp. 132-142.

Brown, M. A. (2009), Navy Operations to Achieve Military Power in Cyberspace: A Draft Concept for Navy Computer Network Operations. In Wentz, L. K.; Barry, C. L. and Starr, S. H. (Eds.) *Military Perspectives on Cyberpower*. Washington D.C.: Center for Technological and National Security Policy at the National Defense University, pp. 73-86.

Brown, M. L. (1996) The Revolution in Military Affairs: The Information Dimension. In Campen, A. D., Dearth, D. H. and Goodden, T. R. (Eds.) *Cyberwar: Security, Strategy, And Conflict In The Information Age.* Fairfax: AFCEA International, pp. 267-285.

Bull, H. (1977) *The Anarchical Society: A Study of Order in World Politics.* New York: Columbia University Press.

Bush, G. W. (2002) *The National Security Strategy of the United States of America*. Washington D.C.: The White House.

Bush, G. W. (2006) *The National Security Strategy of the United States of America*. Washington D.C.: The White House.

Cabinet Office of the United Kingdom (2008) *The National Security Strategy of the United Kingdom. Security in an Interdependent World.* London: Cabinet Office.

Cabinet Office of the United Kingdom (2011) *The UK Cyber Security Strategy. Protecting and promoting the UK in a Digital World.* London: Cabinet Office.

Camerer, C. F. (1991) Does Strategy Research Need Game Theory?, *Strategic Management Journal*, 12, pp. 137-152.

Campen, A. D. (1996) Coming To Terms With Information War. In Campen, A. D., Dearth, D. H. and Goodden, T. R. (Eds.) *Cyberwar: Security, Strategy, And Conflict In The Information Age.* Fairfax: AFCEA International, pp. 251-255.

Campen, A. D. (1996) Uncommon Means for the Common Defense. In Campen, A. D., Dearth, D. H. and Goodden, T. R. (Eds.) *Cyberwar: Security, Strategy, And Conflict In The Information Age.* Fairfax: AFCEA International, pp. 71-75.

Campen, A. D., Dearth, D. H. and Goodden, T. R. (1996) *Cyberwar: Security, Strategy, And Conflict In The Information Age.* Fairfax: AFCEA International.

de Caro, C. (1996) SOFTWAR. In Campen, A. D., Dearth, D. H. and Goodden, T. R. (Eds.) *Cyberwar: Security, Strategy, And Conflict In The Information Age.* Fairfax: AFCEA International, pp. 203-218.

Carr, J. (2010) *Inside Cyber Warfare. Mapping the Cyber Underworld.* Sebastopol: O Reilly.

Cavelty, M. D. (2007) Critical information infrastructure: vulnerabilities, threats and responses, *ICTs and International Security*, 3, pp. 15-22.

Chadwick, A. (2006) *Internet politics. States, Citizens, and New Communication Technologies.* New York and Oxford: Oxford University Press.

Chaliand, G. (1994) *The Art of War in World History. From Antiquity to the Nuclear Age*. Berkeley: University of California Press.

Cheng, J. (2011) *Anonymous to security firm working with FBI: "You've angered the hive"*" [online], New York: Ars Technica. Available: http://arstechnica.com/tech-

policy/news/2011/02/anonymous-to-security-firm-working-with-fbi-youve-angered-the-hive.ars [Accessed 1 March 2011].

Cherry, S. (2012) *Stuxnet: Leaks or Lies?* [podcast], 4 September 2012. Available: http://spectrum.ieee.org/podcast/computing/embedded-systems/stuxnet-leaks-or-lies? [Accessed 6 September 2012].

Cheswick, W. R. and Bellovin, S. M. (1994) *Firewalls and Internet Security. Repelling Wily the Hacker.* Boston: Addison-Wesley Professional Computing, Pearson Education.

People's Republic of China (2002) *China's National Defense in 2002*. Beijing: Information Office of the State Council.

Cebula, J. J. and Young, L. R. (2010), *A Taxonomy of Operational Cyber Security Risks. CMU/SEI-2010-TN-028.* Pittsburgh: Carnegie Mellon University.

Cerf, V. G. (2008) The Scope of Internet Governance. In Avri, D. and Kleinwächter, W. (Eds.*) Internet Governance Forum: The First Two Year.* Geneva: IGF Secretariat, pp. 51-56.

Cilluffo, F. J. and Nicholas, P. J. (2006) Cyberstrategy 2.0, *The Journal of International Security Affairs*, 10.

Clark, D. (2003) *Computer security officials discount chances of 'digital Pearl Harbor'* [online], Washington: Government Executive Media Group. Available: http://www.govexec.com/dailyfed/0603/060303td2.htm/ [Accessed 22 April 22 2011].

Clark, R. (1995) *Information Infrastructure* [online], Chapman: Xamax Consultancy Pty Ltd. Available: http://www.rogerclarke.com/II/ [Accessed 10 July 2011].

Clark, W. P. (1982) *National Security Strategy* [online], Washington D.C.: Center for Strategic and International Studies (CSIS). Available: http://www.disam.dsca.mil/pubs/Vol%205-1/Clark.pdf [Accessed 30 June 2011].

Clarke, D. C. (2012), *Crime* [online], London: Encyclopaedia Britannica. Available: https://www.britannica.com/EBchecked/topic/142953/crime/ [Accessed: 3 February 2012].

Clarke, R. A. and Knake, R. K. (2010) *Cyber War. The Next Threat To National Security And What To Do About It*. New York: Harper-Collings Publisher.

von Clausewitz, K. (1997) *On War.* Hertfordshire: Wordworth Edition Limited.

von Clausewitz, K. (2003) *Vom Kriege.* München: Ullstein Verlag.

Cohen, E. A. (2002) *Supreme Command. Soldiers, Statesmen, and Leadership in Wartime.* New York: Anchor Books.

Cohen, E. A. (2002) Technology and Warfare. In Baylis, J., Wirtz, J., Cohen, E. and Gray, C. S. (Eds.) *Strategy in the Contemporary World. An Introduction to Strategic Studies.* Oxford: Oxford University Press, pp. 235-253.

Cooney, M. (2013) *Calling all security gods – DARPA has $2 million cyberthreat challenge for you* [online], Framingham: Network World. Available: http://www.networkworld.com/community/blog/calling-all-security-gods-%E2%80%93-darpa-has-2-million-cyberthreat-challenge-you/ [Accessed: 30 November 2013].

Cordesman, A. C. (2000) *Critical Infrastructure Protection and Information Warfare. Final Review Draft for Comment, Revision: 8 December 2000*. Washington D.C.: Center for Strategic and International Studies (CSIS).

Cordesman, A. H. (2000) *Defending America. Redefining The Conceptual Borders of Homeland Defense. Critical Infrastructure Protection and Information Warfare*. *Final Review Draft for Comment.* Washington D.C.: Center for Strategic and International Studies (CSIS).

Cornell University (2011) *Emergence of Cyberwar Game Theory* [online], Ithaca: Cornell University. Available: http://blogs.cornell.edu/info2040/2011/10/23/emergence-of-cyberwar-game-theory/ [Accessed 3 January 2012].

Craig, G. A. and Gilbert, F. (1991) Reflections on Strategy in the Present and Future. In Paret, P. (Ed.) *Makers of Modern Strategy. From Machiavelli to the Nuclear Age.* Oxford: Clarendon Press, pp. 863-872.

Curran, K., Concannon, K. and McKeever, S. (2008) Cyber Terrorism Attacks. In Janczewski, L. J. and Colarik, A. M. (Eds.) *Cyber Warfare and Cyber Terrorism*. Hershey and New York: IGI Global, pp. 1-6.

Curran, K., Smyth, N. and Mc Grory, B. (2008) Cryptography. In Janczewski, L. J. and Colarik, A. M. (Eds.) *Cyber Warfare and Cyber Terrorism*. Hershey and New York: IGI Global, pp. 57-64.

Davis, M. D. (1983) *Game Theory. A Nontechnical Introduction*. New York: Dover Publications, Inc..

Dearth, D. H. and Williamson, C. A. (1996) Information Age/ Information War. In Campen, A. D., Dearth, D. H. and Goodden, T. R. (Eds.) *Cyberwar: Security, Strategy, And Conflict In The Information Age.* Fairfax: AFCEA International, pp. 14-29.

Delio, M. (2001) *It's (Cyber) War: China vs. U.S*. [online], New York: Wired. Available: http://archive.wired.com/politics/law/news/2001/04/43437 [Accessed 24 May 2014].

Denning, D. E. (2000) *Information Warfare and Security.* Oxford: Association for Computer Machinery (ACM) Press.

Denning, D. E. (2001) Activism, Hacktivism, and Cyberterrorism: The Internet As A Tool For Influencing Foreign Policy. In Arquilla J. and Ronfeldt D. (Eds.) *Networks*

and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica: RAND Corporation, pp. 239-288.

Denning, D. E (2003) The US key escrow encryption technology, *Computer Communications*, 17(7), pp. 453-457.

DHS (2003) *Critical Infrastructure Identification, Prioritization, and Protection* [online], Washington D.C.: Department of Homeland Security. Available: http://www.dhs.gov/homeland-security-presidential-directive-7#1 [Accessed 24 May 2014].

DHS (2010) *Preventing and Defending Against Cyber Attacks* [online], Washington D.C.: Department of Homeland Security. Available: http://www.dhs.gov/xlibrary/assets/defending-against-cyber-attacks-september-2010.pdf [Accessed 24 May 2014].

Dipert, R. R. (2006) Preventive War and the Epistemological Dimension of the Morality of War, *Journal of Military Ethics*, 5(1), pp. 32-54.

Dipert, R. R. (2010) The Ethics of Cyberwarfare, *Journal of Military Ethics*, 9(4), pp. 384-410.

Dipert, R. R. (2013) Other-Than-Internet (OTI) Cyberwarfare: Challenges for Ethics, Law, and Policy, *Journal of Military Ethics*, 12(1), pp. 80-87.

Disterer, G., Alles, A. and Hervatin A. (2008) Denial-of-Service (DoS) Attacks: Prevention, Intrusion Detection, and Mitigation. In Janczewski, L. J. and Colarik, A. M. (Eds.) *Cyber Warfare and Cyber Terrorism*. Hershey and New York: IGI Global, pp. 254-272.

DoD (2002) *Future of Warfighting Concept.* Canberra: Department of Defence.

DoD (2011) *Department of Defense Strategy for Operating in Cyberspace*. Washington D.C.: Department of Defense.

Dominguez, K. (2011) *Keeping tabs on the Stuxnet* [online], Shibuya: Trend Micro. Available: http://blog.trendmicro.com/keeping-tabs-on-the-next-stuxnet/ [Accessed 28 December 2011].

Donath, M. (2001) *Demokratie und Internet, Neue Modelle an der Bürgerbeteiligung an der Kommunalpolitik – Beispiele aus den USA*. Frankfurt am Main: Campus Verlag.

Dunn, J. E. (2012) *Flame was intelligence-gathering tool for Stuxnet* [online], Framingham: Network World. Available: https://www.networkworld.com/news/2012/062112-flame-was-intelligence-gathering-tool-for-260391.html (Accessed 24 May 2014).

Dunning, W. A. (1902) *A history of political theories in ancient and medieval*. New York: Macmillan.

DuRaul, N. (2012) *Stuxnet: The New Face of 21st Century Cyber Warfare Infographic* [online], Burlington: Veracode Application Security. Available: https://www.veracode.com/blog/2012/08/stuxnet-the-new-face-of-21st-century-warfare-infographic/ [Accessed 7 October 2012].

Elisan, C. C. (2013) *Malware, Rootkits & Botnets: A Beginner's Guide.* Columbus: McGraw-Hill.

Elixmann, D. and Scanlan, M. (2002) *The Economics of IP Networks: Market, Technical and Public Policy Issues Relating to Internet Traffic Exchange.* Brussels and Luxembourg: European Commission.

Elliot, S. (2010) *Cyber Warfare and the Conflict in Iraq* [online], New York: Wired. Available: https://www.infosecisland.com/blogview/6750-Cyber-Warfare-and-the-Conflict-in-Iraq.html/ [Accessed 10 February 2012].

Enconado, B. (2011) *TDL 4. A Sophisticated Fraudster's Rootkit* [conference presentation], Rootcon5 Hacker and Security Conference, 9 September 2011.

EPIC (2001) *Filters and Freedom 2.0: Free Speech Perspectives on Internet Content Controls.* Washington D.C.: Electronic Privacy Information Center (EPIC).

Evans, G. and Newnham, J. (1998) *The Penguin Dictionary of International Relations*. London: Penguin Group.

Fagerland, S. (2012) *Systematic cyber attacks against Israeli and Palestinian targets going on for a year*. Lysaker: Norman AS.

Fagerland, S. (2013) *The Hangover Report.* Lysaker: Norman AS:

Falliere, N, Murchu, L. O. and Chien, E. (2010) *W32.Stuxnet Dossier, Version 1.3, Number 2010*. Mountain View: Symantec Corporation.

Farivar, C. (2013) *Finland's Foreign Ministry gets pwned by worse- than-Red October malware* [online], New York: Ars Technica. Available: http://arstechnica.com/tech-policy/2013/10/finlands-foreign-ministry-gets-pwned-by-red-october-malware/ [Accessed 10 November 2013].

Farwell, J. P. and Rohozinski, R. (2011) Stuxnet and the Future of Cyber War, *Survival: Global Politics and Strategy*, 53(1), pp. 23-40.

Federation of American Scientists (1998) *Nuclear Weapon EMP Effects* [online], Washington D.C.: Federation of American Scientists (FAS). Available: https://www.fas.org/nuke/intro/nuke/emp.htm/ [Accessed 6 March 2012].

FireEye (2013) *World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks.* Milpitas: FireEye Inc..

Fleming, R. (2010) *4chan-based group 'Anonymous' targets PayPal to support WikiLeaks* [online], Portland: Digital Trends. Available: http://www.digitaltrends.com/computing/4chan-based-group-anonymous-targets-paypal-to-support-wikileaks/ [Accessed 30 September 2011].

Fogarty, K. (2012) *NATO launches disturbingly relaxed-sounding 'rapid reaction' cyberwar team'* [online], Framingham: International Data Group (IDG). Available: http://www.itworld.com/security/258466/nato-launches-disturbingly-relaxed-sounding-rapid-reaction-cyberwar-team/ [Accessed 20 March 2012].

Forward-Looking Threat Research Team (2012) *LUCKYCAT REDUX. Inside an APT Campaign with Multiple Targets in India and Japan. Trend Micro Research Paper 2012.* Shibuya: Trend Micro.

FORWARD Consortium (2010) *Managing Emerging Threats in ICT Infrastructures. D3.1: White book: Emerging ICT threats.* Vienna: FORWARD Consortium.

Foster, W. and Goodman, S. E. (2000) *The Diffusion of the Internet in China*. Stanford: Center for International Security and Cooperation.

Freedman, L. (2002) Conclusion: The Future of Strategic Studies. In Baylis, J., Wirtz, J., Cohen, E. and Gray, C. S. (Eds.) *Strategy in the Contemporary World. An Introduction to Strategic Studies.* Oxford: Oxford University Press, pp. 254 – 338.

Freedman, L. (2003) *The Evolution of Nuclear Strategy.* Hampshire: Palgrave Mcmillan.

Frihberg, M. and Jonsson D. (1968) A Simple War and Armament Game, *Journal of Peace Research*, 5(3), pp. 233-247.

Fritsche, K.-D. (2011) *Cyber-Sicherheit, Die Sicherheitsstrategie der Bundesregierung*. *Analysen & Argumente*, 89, pp. 3-6.

Fritz, J. (2008) How China will use Cyber Warfare To Leapfrog In Military Competitiveness, *Culture Mandala*, 8(1), pp. 28-80.

Gallagher, S. (2013) *US, Russia to install "cyber-hotline" to prevent accidental cyberwar* [online], New York: Ars Technica. Availanle:

http://arstechnica.com/information-technology/2013/06/us-russia-to-install-cyber-hotline-to-prevent-accidental-cyberwar/ [Accessed 30 June 2013].

Gardner, H. (2009) War and the media paradox. In Karatzogianni, A. (Ed.) *Cyber Conflict and Global Politics.* New York: Routledge, pp. 13-30.

Gartzke, E. (2013) The Myth of Cyberwar. Bringing War in Cyberspace Back Down to earth's, *International Security*, 38(2), pp. 41-73.

G DATA SecurityLabs (2014) *Uroburos. Highly complex espionage software with Russian roots.* Bochum: G Data Software AG.

Geers, K. (2011) *Strategic Cyber Security*. Talinn: NATO Cooperative Cyber Defence Centre of Excellence (CCD COE).

Gerson, M. S. (2009) Conventional Deterrence in the Second Nuclear Age, *Parameters*, Autmn 2009, pp. 32-48.

Gertz, B. (2012) *Chinese Hackers Suspected in Cyber Attack on Council on Foreign Relations* [online], Washington D.C.: The Washington Free Beacon. Available: http://freebeacon.com/chinese-hackers-suspected-in-cyber-attack-on-council-on-foreign- relations/ [Accessed 19 February 2013].

Gervais, M. (2011) Cyber Attacks and the Laws of War, *Yale Law School* [online]. Available: http://ssrn.com/abstract=1939615/ [Accessed 15 February 2012].

Gibson, W. (1984) *Neuromancer*. New York: Ace.

Gibson, S. (2004) Open Source Intelligence. An Intelligence Lifeline, *RUSI Journal*, February 2014, pp. 16-23.

Glabus, E. M. (2000) Metaphors and Modern War:Biological, Computer, and Cognitive Viruses. In Copeland, T. E. (Ed.) *The Information Revolution and National Security.* Carlisle: Strategic Studies Institute (SSI), pp. 81-84.

Glenny, M. (2012) *A Weapon We Can't Control* [online], New York: New York Times. Available: https://www.nytimes.com/2012/06/25/opinion/stuxnet-will-come-back-to-haunt-us.html/ [Accessed 24 June 2012].

Global Research & Analysis Team (2012) *The Madi Campaign – Part I* [online], Moscow: Kaspersky Lab. Available: https://www.securelist.com/en/blog/208193677/The_Madi_Campaign_Part_I/ [Accessed 28 July 2012].

Global Research & Analysis Team (2013a) *"NetTraveler is Running!" - Red Star APT Attacks Compromise High-Profle Victims* [online], Moscow: Kaspersky Lab. Available: http://www.securelist.com/en/blog/8105/ [Accessed 28 October 2013].

Global Research & Analysis Team (2013b) *The Icefog APT: A Tale of Cloak and Three Daggers* [online], Moscow: Kaspersky Lab. Available: http://www.securelist.com/en/blog/208214064/The_Icefog_APT_A_Tale_of_Cloak_and_Three_Daggers/ [Accessed 28 October 2013].

Global Research & Analysis Team (2013c) *The "Red October" Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies* [online], Moscow: Kaspersky Lab. Available: https://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies [Accessed 19 February 2013].

Global Research & Analysis Team (2013d) *The TeamSpy Crew Attacks - Abusing TeamViewer for Cyberespionage* [online], Moscow: Kaspersky Lab. Available: https://www.securelist.com/en/blog/208194185/The_TeamSpy_Crew_Attacks_Abusing_TeamViewer_for_Cyberespionage/ [Accessed 28 October 2013].

Global Research & Analysis Team (2014a) *Regin: nation-state ownage of GSM networks* [online], Moscow: Kaspersky Lab. Available:

https://securelist.com/blog/research/67741/regin-nation-state-ownage-of-gsm-networks/ [Accessed 19 February 2014].

Global Research & Analysis Team (2014b) *'Unveiling "Careto" The Masked APT*. Moscow: Kaspersky Lab.

Global Research & Analysis Team (2015a) *Equation: The Death Star of Malware Galaxy* [online], Moscow: Kaspersky Lab. Available: https://securelist.com/blog/research/68750/equation-the-death-star-of-malware-galaxy/ [Accessed 18 February 2015].

Global Research & Analysis Team (2015b) *The Desert Falcons targeted attacks* [online], Moscow: Kaspersky Lab. Available: https://securelist.com/blog/research/68817/the-desert-falcons-targeted-attacks/ [Accessed 19 February 2015].

Goldsmith, J. L. (2003) Against Cyberanarchy. In Thierer, A. and Wayne Crews Jr., C. (Eds.) *Who Rules the Net? Internet Governance and Jurisdiction.* Washington: CATO Institute, pp. 31-70.

Goldsmith, J. L. (2011) *Cybersecurity Treaties. A Skeptical View*. Stanford: Hoover Institution.

Goldsmith, J. L. and Wu, T. (2008) *Who Controls the Internet? Illusions of a Borderless World.* Oxford: Oxford University Press.

Goodin, D. (2012) *Nation-sponsored malware with Stuxnet ties has mystery warhead* [online], New York: Ars Technica. Available:http://arstechnica.com/security/2012/08/nation-sponsored-malware-has-mystery-warhead/ [Accessed 11 August, 2012].

Gorman, S., Cole, A. and Dreazen, Y. (2009) *Computer Spies Breach Fighter-Jet Project* [online], New York: The Wall Street Journal. Available:

http://online.wsj.com/article/SB124027491029837401.html/ [Accessed 18 August 2012].

Gostev, A. (2011) *The Mystery of Duqu: Part One* [online], Moscow: Kaspersky Lab. Available: https://www.securelist.com/en/blog/208193182/The_Mystery_of_Duqu_Part_One/ [Accessed 21 January 2013].

Gostev, A. (2012) *The Flame: Questions and Answers* [online], Moscow: Kaspersky Lab. Available: https://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers/ [Accessed 31 May 2012].

Gragido, W. and Pirc, J. (2011) *Cybercrime and Espionage. An Analysis of Subversive Multivector Threats*. Burlington: Elsevier.

Graham, D. R. (2012) *Bogus story: no Chinese backdoor in military chip* [online], Atlanta: Errata Security. Available: http://erratasec.blogspot.co.uk/2012/05/bogus-story-no-chinese-backdoor-in.html/ [Accessed 28 May 2012].

Graham, P. (2004) *Great Hackers* [online], Paul Graham. Available: http://www.paulgraham.com/gh.html/ [Accessed 31 July 2011].

Grauman, B. (2012) *Cyber-security: The vexed question of global rules*. Brussels: Secure & Defence Agenda.

Gray, C. S. (1999) *Modern Strategy*. Oxford: Oxford University Press.

Gray, C. S. (2009) *Schools for Strategy: Teaching Strategy for the 21st Century Conflict*. Carlisle: Strategic Studies Institute (SSI).

Gross, M. J. (2011) *Enter the Cyber-dragon* [online] Greensboro: Vanity Fair. Available: http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109/ [Accessed January 11, 2012].

Habermas, J. (1991) *Erläuterungen zur Diskursethik.* Frankfurt am Main: Suhrkamp.

Habiger, E. E. (2010) *Cyberwarfare and Cyberterrorism: The Need For A New U.S. Strategic Approach. Provoking Cybersecurity Change White Paper Series, White Paper 1:2010*. Washington D.C.: Cyber Secure Institute.

Hachigian, N. (2001) China's Cyber-Strategy, *Foreign Affairs*, 80(2), pp. 118-133.

Haeni, R. E. (1997) *Information Warfare. An Introduction*. Washington D.C.: Cyberspace Policy Institute, George Washington University.

Hamilton, S. L., Miller, W. L., Ott, A. and Saydjari, S. O. (2001) *The Role of Game Theory in Information Warfare* [online], Maxwell AFB: The Air University. Available: http://www.au.af.mil/au/awc/awcgate/afrl/hamilton-31-08-b-1.pdf/ [Accessed 24 May 2014].

Hare, F. B. and Zimmerman, G. (2009) The Air Force in Cyberspace: Five Myths of Cyber Superiority. In Wentz, L. K., Barry, C. L. and Starr, S. H. (Eds.) *Military Perspectives on Cyberpower*. Washington D.C.: Center for Technological and National Security Policy, National Defense University, pp. 87-96.

Harwit, E. and Clark, D. (2001) Shaping the Internet in China. Evolution of Political Control over Network Infrastructure and Content, *Asian Survey*, 41(3), pp. 377-408.

Healey, J. (2013) *Stuxnet and the Dawn of Algorithmic Warfare* [online], New York: Huffington Post. Available: http://www.huffingtonpost.com/jason-healey/stuxnet-cyberwarfare_b_3091274.html/ [Accessed 24 May 2014].

Hedberg, N. (2012) *China: 40.000 Police Officers Monitor the Internet* [online], Jarl Stockholm: Hjalmarson Foundation. Available: http://www.hjalmarsonfoundation.se/2012/03/china-40-000-police-officers-monitor-the-internet/ [Accessed 30 January 2013].

Herpig, S. (2009), *Is the Nation-State fit for governing the Internet.* Unpublished thesis (MA), University of Hull.

Hjortdal, M. (2011) China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence, *Journal of Strategic Security*, 4(2), pp. 1-24.

HMGovernment (2010) *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. London: Her Majesty's Government.

Hoffman, B. (1998) *Inside Terrorism.* London: Victor Golancz.

Hogben, G. (2011) *Botnets: Detection, Measurement, Disinfection & Defence*. Brussels: European Network and Information Security Agency (ENISA).

Howard, M. (1979) The Forgotten Dimensions of Strategy, *Foreign Affairs*, 57(5), pp. 975-986.

Hubbard, Z. P. (2007) Information Operations in the Global War on Terror: Lessons Learned From Operations in Afghanistan and Iraq. In Armistead, L. (Ed.) *Information Warfare. Separating Hype from Reality.* Washington D.C.: Potomac Books Inc., pp. 45-72.

Hughes, C. R. (2003) Fighting the smokeless war: ICTs and international security. In Hughes, C. R. and Wacker G. (Eds.) *China and the internet: politics of the digital leap forward.* London: Routledge, pp. 139-161

Hughes, R. (2007) Bits, Bytes and Bullets, *The World Today*, 63(11), pp. 20-22.

Hutchinson, W. (2006), Information Warfare and Deception, *Informing Science,* 9, pp. 213-223.

IEEE Security (2014) *GAO Reports DoD SBU Computer Security Inadequate* [online], University Park: IEEE Security. Available: http://www.ieee-security.org/Cipher/Newsbriefs/1996/960522.GAOrept.html [Accessed: 10 June 2011].

IGF Secretariat (2006) *The Internet Governance Forum (IGF) Inaugural Meeting, Background Paper*, *Athens.* Geneva: IGF Secretariat.

Information Warfare Monitor and Shadowserver Foundation (2010) *Shadows in the Cloud: Investigating Cyber Espionage 2.0, Joint Report of the Information Warfare Monitor and the Shadowserver Foundation (JR03-2010).* Ottawa: The SecDev Group.

Inkster, N. (2013) Conflict Foretold: America and China, *Survival: Global Politics and Strategy*, 5, pp. 7-28.

Jackson, M. O. and Shoham, Y. (2012) *Bayesian Games* [online course material], Mountain View: Coursera Inc.. Available: https://www.coursera.org/course/gametheory/ [Accessed 19 March 2012].

Jackson Higgins, K. (2013) *The Long Shadow Of Saudi Aramco* [online], San Francisco: Dark Reading. Available: http://www.darkreading.com/attacks-breaches/the-long-shadow-of-saudi-aramco/d/d-id/1140664 [Accessed 28 October 2013].

Janczewski, L. J. and Colarik, A. M. (2008) Cyber Warfare and Cyber Terrorism, *Information Science Reference.* Hershey and New York: IGI Global.

Janet, P. and Picot, G. (1887) *Histoire de la science politique dans ses rapportes avec la morale*.

Jeffers, D. (2012) *A Sinister Breed of Malware is Growing* [online], Framingham: CSO Online. Available: http://www.csoonline.com/article/2132141/data-protection/a-sinister-new-breed-of-malware-is-growing.html [Accessed 20 August 2012].

Jellinek, G. (1959) *Allgemeine Staatslehre.* Darmstadt: Wissenschaftliche Buchgesellschaft.

Jomini, A.-H. (1811) *Traité Des Grandes Opérationes Militaires, Contenant L'Histore Des Campagnes De Frédéric II, Comparées à Celles De L'Empereur*

Napoléon; Avec Un Recueil Des Principes Généreaux De L'Art De La Guerre. Paris: Magimel.

Jomini, A.-H. (1868), *The Art of War.* Philadelphia: J. B. Lippincott & Co..

Kahn, H. (2007) *On Thermonuclear War.* London: Transaction Publishers.

Kant, I. (2007) *Perpetual Peace.* Minneapolis: Filiquarian Publishing LLC.

Kaplan, D. (2011) *Anonymous takes over security firm in vengeful hack* [online], New York: SC Magazine. Available: http://www.scmagazine.com/anonymous-takes-over-security-firm-in-vengeful-hack/article/195837/ [Accessed 24 May 2014].

Kaplan, F. (1983) *The Wizards of Armageddon.* New York: Simon & Schuster.

Kaspersky Lab (2012) *Securing Critical Information Infrastructure: Trusted Computing Base* [online], Moscow: Kaspersky Lab. Available: https://www.securelist.com/en/analysis/204792248/Securing_Critical_Information_Infrastructure_Trusted_Computing_Base [Accessed 31 October 2012].

Kaspersky Lab Global Research & Analysis Team (2012a) *Gauss: Abnormal Distribution*. Moscow: Kaspersky Lab.

Kaspersky Lab Global Research & Analysis Team (2012b) *miniFlame aka SPE: Elvis and his friends* [online], Moscow: Kaspersky Lab. Available: https://www.securelist.com/en/blog/763/miniFlame_aka_SPE_Elvis_and_his_friends [Accessed 12 February 2013].

Kaspersky Lab Global Research & Analysis Team (2012c) *What was that Wiper thing?* [online], Moscow: Kaspersky Lab. Available: https://www.securelist.com/en/blog/208193808/What_was_that_Wiper_thing [Accessed 15 February 2013].

Kellerman, T. (2012) *Peter the Great versus Sun Tzu*. Shibuya: Trend Micro.

Kello, L. (2013) The Meaning of the Cyber Revolution: Perils to Theory and Statecraft, *International Security*, 38(2), pp. 7-40.

Kersten, J. (2004) Warum Georg Jellinek? Jelliknek und die Staats- und Europarechtslehre der Gegenwart. In Anter, A. (Ed.) *Die normative Kraft des Faktischen. Das Staatsverständnis Georg Jellineks.* Baden-Baden: Nomos, pp. 175-199.

Kilroy Jr., R. J. (2008) The U.S. Military Response to Cyber Warfare. In Janczewski, L. J. and Colarik, A. M. (Eds.) *Cyber Warfare and Cyber Terrorism*. Hershey and New York: IGI Global, pp. 439-445.

Kiltz, S., Lang, A. and Dittmann, J. (2008) Malware: Specialized Trojan Horse. In Janczewski, L. J. and Colarik, A. M. (Eds.) *Cyber Warfare and Cyber Terrorism*. Hershey and New York: IGI Global, pp. 155-160.

Kirschbaum, J. (2010) Operation Opera: an Ambiguous Success, *Journal of Strategic Security*, 3(4), pp. 49-62.

Klare, M. T. (2001) Waging Postindustrial Warfare on the Global Battlefield, *Current History*, 100, pp. 433-437.

Kleinwächter, W. (2005) De-Mystification of the Internet Root: Do We Need Governmental Oversight?. In Drake J. (Ed.), (2005) *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance (WGIG)*. New York: The United Nations Information and Communication Technologies Task Force, pp. 209-225.

Klimburg, A. and Healey, J. (2012) Strategic Goals & Stakeholders. In Klimburg, A. (Ed.) *National Cyber Security. Framework Manual.* Talinn: NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), pp. 66-107.

Knapp, K. J. and Boulton, W. R. (2008) Ten Information Warfare Trends. In Janczewski, L. J. and Colarik, A. M. (Eds.) *Cyber Warfare and Cyber Terrorism*. Hershey and New York: IGI Global, pp. 17-25.

Knecht, R. J. (1996) Thoughts About Information Warfare. . In Campen, A. D., Dearth, D. H. and Goodden, T. R. (Eds.) *Cyberwar: Security, Strategy, And Conflict In The Information Age.* Fairfax: AFCEA International, pp. 161-174.

Kormann, G. and Klapper, M. (1978) Game Theory's Wartime Connections and the Study of Industrial Conflict, *Industrial and Labor Relations Review*, 32(1), pp. 24-39.

Kramer, F. D. (2009) Cyberpower and National Security: Policy Recommendations for a Strategic Framework. In Kramer, F. D., Starr, S. H. and Wentz, L. K. (Eds.) *Cyberpower and National Security*. Washington D.C.: National Defense University, pp. 3-23.

Kramer, F. D. (2012) *Achieving International Cyber Stability*. Washington D.C.: Atlantic Council.

Krekel, B., Bakos, G. and Barnett, C. (2009) *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*. McLean: Northrop Grumman.

Krekel, B., Adams, P. and Bakos, G. (2012) *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*. McLean: Northrop Grumman.

Kristensen, H. (2008) Counterproliferation and US Nuclear Strategy, *International Journal*, 63(4), 803-820.

Kuehl, D. T. (2007) Brother, Can You Spare Me a DIME?. In Armistead, L. (Ed.) *Information Warfare. Separating Hype from Reality.* Washington D.C.: Potomac Books Inc., pp. 1-4.

Kuehl, D. T. (2009) From Cyberspace to Cyberpower: Defining the Problem. In Kramer, F. D., Starr, S. H. and Wentz, L. K. (Eds.) *Cyberpower and National Security*. Washington D.C.: National Defense University, pp. 24-42.

Kuehl, D. and Armistead, L. (2007) Information Operations: The Policy and Organizational Evaluation. In Armistead, L. (Ed.) *Information Warfare. Separating Hype from Reality.* Washington D.C.: Potomac Books Inc., pp. 5-26.

Kugler, R. L. (2009) Deterrence of Cyber Attacks. In Kramer, F. D., Starr, S. H. and Wentz, L. K. (Eds.) *Cyberpower and National Security*. Washington D.C.: National Defense University, pp. 309-342.

Kumar, M. (2012) *Wiper, destructive Malware possibly connected to Stuxnet and Duqu* [online], Gurgaon: The Hacker News. Available: http://thehackernews.com/2012/09/wiper-destructive-malware-possibly.html [Accessed 10 January 2012].

Lam, W. (2010) Beijing Bones Up Its Cyber-Warfare Capacity, *China Brief*, 10(3), pp. 2-4.

Lammle, T. (2006) *CCNA Intro. Introduction to Cisco Networking Technologies. Study Guide.* Indianapolis: Wiley Publishing.

Lan, T. and Xin, Z. (2010) Can Cyber Deterrence Work?. In Nagorski, A. (Ed.) *Global Cyber Deterrence, Views from China, the U.S., Russia, India, and Norway.* New York: EastWest Institute, pp. 1-3.

Langlois, C. C. and Langlois, J.-P. P. (1996) Rationality in International Relations: A Game-Theoretic and Empirical Study of the US-China Case, *World Politics*, 48(3), pp. 358-390.

Laquer, W. (1996) Postmodern Terrorism: New Rules for an Old Game*, Foreign Affairs*, 75(5), pp. 24-36.

Lee, D. (2012) *Israel tops cyber-readiness poll but China lags behind* [online], London: British Broadcasting Corporation (BBC). Available: http://www.bbc.co.uk/news/technology-16787509 [Accessed 15 February 2012].

Leggewie, C. (1998) Demokratie auf der Datenautobahn. In Leggewie, C. and Maar, C. (Eds.) *Internet & Politik. Von der Zuschauer- zur Beteiligungsdemokratie?.* Köln: Bollmann Verlag GmbH.

Leiner, B. M. (2000), *A Brief History of the Internet* [online], Geneva: Internet Society. Available: http://www.isoc.org/internet/history/brief.shtml [Accessed 25 June 2011].

Leonard, R. (2010) *Von Neumann, Morgenstern, and the Creation of Game Theory. From Chess to Social Science, 1900-1960*. Cambridge: Cambridge University Press.

Lessig, L. (1999) *Code and other Laws of Cyberspace.* New York: Basic Books.

Lessig, L. (2002) *The Future of Ideas. The Fate of the Commons in a Connected World.* New York: Vintage Books.

Lessig, L. (2006) *Code. Version 2.0.* New York: Basic Books.

Lewis, J. A. (2002) *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Washington D.C.: Center for Strategic and International Studies (CSIS).

Lewis, J. A. (2010) *Cross-Domain Deterrence and Credible Threats*. Washington D.C.: Center for Strategic and International Studies (CSIS).

Lewis, J. A. (2011) *Cybersecurity Two Year Later, A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*. Washington D.C.: Center for Strategic and International Studies (CSIS).

Lewis, J. A. (2013a) *Conflict and Negotiation in Cyberspace, A Report of the Technology and Public Policy Program*. Washington D.C.: Center for Strategic and International Studies (CSIS).

Lewis, J. A. (2013b) Cybersecurity and cyberwarfare: assessment of national doctrine and organization. In United Nations *The Cyber Index. International Security Trends and Realities.* New York and Geneva: United Nations Institute for Disarmament Research, pp. 9-90.

Libicki, M. C. (1994) The Small and the Many. In Arquilla, J. and Ronfeldt, D. (1997) *In Athena's Camp*. Santa Monica: RAND Corporation, pp. 191-216.

Libicki, M. C. (1996) Protecting the United States in Cyberspace. In Campen, A. D., Dearth, D. H. and Goodden, T. R. (Eds.) *Cyberwar: Security, Strategy, And Conflict In The Information Age.* Fairfax: AFCEA International, pp. 91-105.

Libicki, M. C. (2007) *Conquest in Cyberspace. National Security and Information Warfare*. Cambridge: Cambridge University Press.

Libicki, M. C. (2009a) *Cyberdeterrence and Cyberwar.* Santa Monica: RAND Corporation.

Libicki, M. C. (2009b) Sub Rosa Cyber War. In Czosseck, C. and Geers, K. (Eds.) *The Virtual Battlefield: Perspectives on Cyber-Warfare*. Amsterdam: IOS Press, pp. 53-65.

Liddell-Hart, B. (1929) The Decisive Wars of History. In Chaliand, G. (1994) (Ed.) *The Art of War in World History. From Antiquity to the Nuclear Age*. Berkeley: University of California Press, pp. 927-931.

Lindsay, J. R. (2013) Stuxnet and the Limits of Cyber Warfare, *Security Studies*, 22, pp. 365-404.

Lischka, K. and Rosenbach, M. (2011) *Hacker klauen Daten von Zoll Server* [online], Hamburg: SPIEGEL Online GmbH. Available: http://www.spiegel.de/netzwelt/web/0,1518,773189,00.html [Accessed 14 July 2011].

Lonsdale, D. J. (2004) *The Nature of War in the Information Age. A Clausewitzian Future*. Frank Class: London.

Lonsdale, D. J. (2007), *Alexander the Great. Lessons in Strategy.* Oxon: Routledge.

Luiijif, E. and Healey, J. (2012) Organisational Structures & Considerations. In Klimburg, A. (Ed.) *National Cyber Security. Framework Manual.* Talinn: NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), pp. 108-145.

Luttwak, E. N. (1980) The Operational Level of War, *International Security*, 5(3), pp. 61-79.

Luttwak, E. N. (1987) *Strategy. The Logic of War and Peace.* Cambridge: Havard University Press.

Luttwak, E. N. (1995) Toward Post-Heroic Warfare, *Foreign Affairs*, 74(3), pp. 109-122.

Lynn, W. J. (2010) Defending a New Domain: The Pentagon's Cyber Strategy, *Foreign Affairs*, 89(5), pp. 97-108.

Lyons, D. (2009) *China's Golden Shield Project: Myths, Realities and Context* [online], Dave Lyon. Available: http://www.scribd.com/doc/15919071/Dave-Lyons-China-s-Golden-Shield-Project [Accessed 5 January 2012].

Mac William, B. (2006) China's Cyberwarriors, *Foreign Policy*, 156, p. 93.

Malawer, S. S. (2010) Cyber Warfare: Law and Policy Proposals for U.S. And Global Governance, *Virginia Lawyer*, 58, pp.: 28-31.

Mandel, R. (1994) *The Changing Face of National Security.* Westport, CT: Greenwood.

MANDIANT (2013) *APT1. Exposing One of China's Cyber Espionage Units* [online], Milpitas: FireEye Inc.. Available: https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/ [Accessed 14 March 2013].

Markentin, M., Schmidt, M. B. and Bekkering, E. (2008) Steganography. In Janczewski, L. J. and Colarik, A. M. (Eds.) *Cyber Warfare and Cyber Terrorism*. Hershey and New York: IGI Global, pp. 50-56.

Marquand, R. and Arnoldy, B. (2007) *China emerges as leader in cyberwarfare* [online], Boston: The Christian Science Monitor. Available: http://www.csmonitor.com/2007/0914/p01s01-woap.html [Accessed 15 February 2012].

Mathews, J. T. (1997) Power Shift, *Foreign Affairs,* 76(1), pp. 50-51.

Mathiason, J. (2009) *Internet Governance. The new frontier of global institutions.* Oxon: Routledge.

McAfee Foundstone Professional Services and McAfee Labs (2011) *Global Energy Cyberattacks: 'Night Dragon'*. Santa Clara: McAfee.

McCurry, J. (2009) *North Korean hackers may have stolen US war plans* [online], London: The Guardian. Available: http://www.guardian.co.uk/world/2009/dec/18/north-south-korea-hackers [Accessed 17 July 2011].

McDonald, G., Murchu, L. O., Doherty, S. and Chien, E. (2013) *Stuxnet 0.5: The Missing Link*. Mountain View: Symantec.

McGuire, C. (2012) Digital Apocalypse: The Artillery of Cyber War, *PenTest Magazine*, 2(6), pp. 6-10.

Meikle, G. (2009) Electronic civil disobedience and symbolic power. In Karatzogianni, A. (Ed.) *Cyber Conflict and Global Politics.* New York: Routledge, pp. 177-187.

Menn, J. (2012) *New 'miniFlame' Virus In The Middle East: 'A Scalpel For A Focused Surgical Dissection'* [online], New York: Huffington Post. Available: http://www.huffingtonpost.com/2012/10/15/miniflame-virus_n_1967077.html [Accessed 18 October 2012].

Microsoft (2009) *What is antivirus software?* [online], Redmond: Microsoft Corporation. Available: https://www.microsoft.com/canada/protect/protect-your-computer/antivirus-software/article.aspx?article=what-is-antivirus-software [Accessed 25 May 2014].

Mills, E. (2012) *A who's who of Mideast-targeted malware* [online], New York: CNET Networks. Available: http://news.cnet.com/8301-1009_3-57503949-83/a-whos-who-of-mideast-targeted-malware/ [Accessed 1 September 2012].

Milevski, L. (2011) Stuxnet and Strategy. A Special Operation in Cyberspace?, *Joint Force Quartlery (JFQ)*, 63(4), pp. 64-69.

Mimoso, M. S. (2011) *Schneier on Stuxnet malware analysis* [online], Newton: SearchSecurity.com. Available: http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1528091,00.html [Accessed 15 June 2011].

Minemura, K. (2011) *China bolstering cyber defenses for modern-day warfare* [online], Tokyo: The Asahi Shimbun. Available: http://ajw.asahi.com/article/asia/china/AJ2011110716782 [Accessed 30 March 2012].

Mitnick, K. D. and Simon, W. L. (2002) *The Art of Deception. Controlling the Human Element of Security.* Indianapolis: Wiley Publishing.

Moran, N. and Oppenheim, M. (2014) *A Detailed Examination of the Siesta Campaign* [online], Milpitas: FireEye Inc.. Available: http://www.fireeye.com/blog/technical/targeted-attack/2014/03/a-detailed-examination-of-the-siesta-campaign.html [Accessed 14 April 2014].

Moran, N. and Villeneuve, N. (2013) *Operation DeputyDog: Zero-Day (CVE-2013-3893) Attack Against Japanese Targets* [online], Milpitas: FireEye Inc.. Available: http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html [Accessed 20 February 2014].

Morgenthau, H. J. (1985) *Politics among Nations*. New York: McGraw-Hill.

Mueller, M. L., Mathiason, J. and Klein, H. (2007) The Internet and Global Governance: Principles and Norms for a New Regime, *Global Governance*, 13, pp. 237-254.

Mueller, M. and Tan, Z. (1997) *China in the Information Age. Telecommunications and the Dilemmas of Reform*. London: Praeger Publishers.

Mulrain, M. (2011) *DHS: Stuxnet Clones May Target US Infrastructures* [online], Tysons Corner: ExecutiveBiz. Available: http://blog.executivebiz.com/2011/07/dhs-stuxnet-clones-may-target-us-infrastructures/ [Accessed 25 May 2014].

Nagpal, R. (2002) *Cyber Terrorism in the Context of Globalization* [online], Pune: Asian School of Cyber Laws. Available: http://www.asianlaws.org/aboutus/spain.pdf [Accessed 26 May 2014].

Navrozov, L. (2005) *Chinese Geostrategy: 'Assassin's Mace'* [online], West Palm Beach: Newsmax. Available: http://archive.newsmax.com/archives/articles/2005/10/20/172811.shtml [Accessed 7 July 2011].

Neuneck, G. (2013) Assessment of international and regional organizations and activities. In United Nations *The Cyber Index. International Security Trends and Realities.* New York and Geneva: United Nations Institute for Disarmament Research, pp. 91-109.

Newmann, W. (2002) Reorganizing for National Security and Homeland Security, *Public Administration Review*, 62, pp. 126-137.

Niou, E. M. S. and Ordeshook, P. C. (1994) A Game-Theoretic Interpretation of Sun Tzu's The Art of War, *Journal of Peace Research*, 31(2), pp. 161-174.

Nugent, J. H. and Raisinghani, M. (2008) Bits and Bytes vs. Bullets and Bombs: A New Form of Warfare. In Janczewski, L. J. and Colarik, A. M. (Eds.) *Cyber Warfare and Cyber Terrorism*. Hershey and New York: IGI Global, pp. 26-34.

Nye, J. S. (2003) The Information Revolution and the Paradox of American Power, *Proceedings of the Annual Meeting (American Society of International Law)*, 97, pp. 67-75.

Nye, J. S. (2011) Nuclear Lessons for Cyber Security?, *Strategic Studies Quarterly*, 5(4), pp. 18-38.

Obama, B. (2008) *Barack Obama's Speech at the University of Purdue* [online], New York: Council on Foreign Relations. Available: http://www.cfr.org/elections/barack-obamas-speech-university-purdue/p16807 [Accessed 24 May 2014].

Obama, B. (2010) *National Security Strategy*. Washington D.C.: The White House.

Osiander, A. (2001) Sovereignty, International Relations, and the Westphalian Myth, *International Organization*, 55 (2), pp. 251-287.

Owen, B. (2000) *Lifting the Fog of War.* New York: Farrar, Straus and Giroux.

Owen, R. S. (2008) Infrastructures of Cyber Warfare. In Janczewski, L. J. and Colarik, A. M. (Eds.) *Cyber Warfare and Cyber Terrorism*. Hershey and New York: IGI Global, pp. 35-41.

Paganini, P. (2012) *Flame, miniFlame, the mystery of an ongoing cyber espionage campaign* [online], New York: Wired. Available: http://www.infosecisland.com/blogview/22586-Flame-miniFlame-the-mystery-of-an-on-going-cyber-espionage-campaign.html [Accessed 18 October 2012].

Paganini, P. (2013) *Operation Beebus, another chinese cyber espionage campaign* [online], Pierluigi Paganini. Available: http://securityaffairs.co/wordpress/12216/hacking/operation-beebus-another-chinese-cyber-espionage-campaign.html [Accessed 19 February 2013].

Page, L. (2007) *Israeli sky-hack switched off Syrian radars countrywide* [online], London: The Register. Available: http://www.theregister.co.uk/2007/11/22/israel_air_raid_syria_hack_network_vuln_intrusion/ [Accessed 28 October 2011].

Pandey, S. N. (2010) *Hacktivism of Chinese Characteristics and the Google Inc. Cyber Attack Episode*. Berlin: Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung.

Panetta, L. E. (2012) *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security* [online], Washington D.C.: U. S. Department of Defense. Available: http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136 [Accessed 13 April 2013].

Payne, K. B. and Walton C. D. (2002) Deterrence in Post Cold-War World. In Baylis, J., Wirtz, J., Cohen, E. and Gray, C. S. (Eds.) *Strategy in the Contemporary World. An Introduction to Strategic Studies.* Oxford: Oxford University Press, pp. 161-182.

Peace Treaty between the Holy Roman Emperor and the King of France and their respective Allies. Treaty of Westphalia (1648) [online]. Available: http://avalon.law.yale.edu/17th_century/westphal.asp [Accessed 17 June 2009].

Pernet, C. and Lu, K. (2015) *OPERATION WOOLEN-GOLDFISH. When Kittens Go Phishing. Trend Micro Research Paper.* Shibuya: Trend Micro.

Pironti, J. P. (2006) Key Elements of a Threat and Vulnerability Management Program, *Information Science Control Journal*, 3, pp. 1-5.

Pisanti, A. (2009) The Key to Trust and Growth of the Internet. In Drake, W. (Ed.) *Internet Governance: Creating Opportunities For All, The Fourth Internet Governance Forum, Sharm el Sheikh, 15 – 18 November 2009*. New York: United Nations, pp. 46-56.

Pollock, F. (1890) *An Introduction to the history of the science of politics*. London and New York: Macmillan.

Public Broadcasting Service (2003) *The Warnings?* [online], Arlington: Public Broadcasting Service. Available: http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/ [Accessed 10 June 2011].

Qiu, J. L. (1999) Virtual Censorship in China: Keeping the Gate between the Cyberspaces, *International Journal of Communications Law and Policy,* 4, pp. 1-25.

Raduege, H. D. Jr. (2010) Fighting Weapons of Mass Disruption: Why America Needs a 'Cyber Triad'. In Nagorski, A. (Ed.) *Global Cyber Deterrence, Views from China, the U.S., Russia, India, and Norway.* New York: EastWest Institute, pp. 3-5.

Raiu, C., Soumenkov, I., Baumgartner, K. and Kamluk, V. (2013) *The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor*. Moscow: Kaspersky Lab.

Ramachandran, A., Feaster, N. and Dagon, D. (2006) *Revealing Botnet Membership Using DNSBL Counter-Intelligence.* Atlanta: Georgia Institute of Technology.

Rascagnères, P. (2015) *Babar: espionage software finally found and put under the microscope* [online], Bochum: G DATA SecurityBlog. Available: https://blog.gdatasoftware.com/blog/article/babar-espionage-software-finally-found-and-put-under-the-microscope.html [Accessed 19 February 2015].

Rattray, G. J. (2009) An Environmental Approach to Understanding Cyberpower. In Kramer, F. D., Starr, S. H. and Wentz, L. K. (Eds.) *Cyberpower and National Security*. Washington D.C.: National Defense University, pp. 253-274.

Rattray, G. J. (2001) *Strategic Warfare in Cyberspace.* Cambridge: The MIT Press.

Rawls, J. (1971) *A Theory of Justice*. Cambridge: Harvard University Press.

Rawnsley, G. D. (2005) Old Wine in New Bottles: China-Taiwan Computer-Based 'Information Warfare' and Propaganda, *International Affairs*, 81(5), pp. 1061-1078.

Rawnsley, G. D. (2009) The laws of the playground: information warfare and propaganda across the Taiwan Strait. In Karatzogianni, A. (Ed.) *Cyber Conflict and Global Politics.* New York: Routledge, pp. 79-94.

Reitinger, P. (2011) *Enabling Distributed Security in Cyberspace. Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action*. Washington D.C.: Department of Homeland Security.

Rhodes, K. A. (2001) *Code Red, Code Red II,and SirCam Attacks Highlight Need for Proactive Measures, GAO-01-1073T.* Washington D.C.: United States General Accounting Office.

Richards, J. (2009) *Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security* [online], Washington D.C.: Elliott School of International Affairs. Available: http://www.iar-gwu.org/node/65 [Accessed 3 September 2011].

Richardson, J. (2011) *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield* [online], JMR Portfolio Intelligence. Available: http://ssrn.com/abstract=1892888 [Accessed 20 November 2012].

Rid, T. (2012) Cyber War Will Not Take Place, *Journal of Strategic Studies*, 35(1), pp. 5-32.

Rid, T. (2013), *Cyber War Will Not Take Place.* London: Hurst & Company.

Rietveld, P. and Perk, D. (2014) *Crimean Cyber Troubles are Ramping Up* [online], Portland: Tripwire Inc.. Available: http://www.tripwire.com/state-of-security/security-data-protection/crimean-cyber-troubles-ramping/ [Accessed 22 June 2014].

Riley, M. and Vance A. (2011) *Cyber Weapons: The New Arms Race* [online], New York: Businessweek. Available: http://www.businessweek.com/printer/magazine/cyber-weapons-the-new-arms-race-07212011.html [Accessed 22 July 2011].

Rios, B. K. (2009) Sun Tzu was a Hacker: An Examination of the Tactics and Operations from a Real World Cyber Attack. In Czosseck, C. and Geers, K. (Eds.) *The Virtual Battlefield: Perspectives on Cyber-Warfare.* Amsterdam: IOS Press, pp. 143-155.

Ripsman, N. M. and Paul, T. V. (2005), Globalization and the National Security State: A Framework for Analysis*, International Studies Review*, 7(2), pp. 199-227.

Robotis, K. and Tzouramanis, T. (2008) Electronic Money Management in Modern Online Business. In Janczewski, L. J. and Colarik, A. M. (Eds.) *Cyber Warfare and Cyber Terrorism*. Hershey and New York: IGI Global, pp. 129-137.

Rodionov, E. (2012) *Interconnection of Gauss with Stuxnet, Duqu & Flame* [online], Bratislava ESET. Available: http://blog.eset.com/2012/08/15/interconnection-of-gauss-with-stuxnet-Duqu-flame [Accessed 14 January 2013].

Rollins, J. and Henning, A. C. (2009) *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations, 7-5700, R40427*. Washington D.C.: Congressional Research Service for Congress.

Ronfeldt, D. and Arquilla, J. (2001) What Next For Networks and Netwars?. In Arquilla, J. and Ronfeldt, D. (Eds.) *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica: RAND Corporation, pp. 311-361.

del Rosso, S. J. Jr. (1995) The Insecure State: Reflections on 'The State' and 'Security' in a Changing World, *Daedalus*, 124(2), pp. 175-207.

Röttgen, N. and Koschyk, H. (2008) *Eine Sicherheitsstrategie für Deutschland* [online], Berlin: CDU/CSU Parliamentary Group. Available: https://www.cducsu.de/sites/default/files/Sicherheitsstrategie_Bechluss_080506_1.pdf [Accessed 25 May 2014].

Rowe, N. C. (2008) Deception in Defense of Computer Systems from Cyber Attacks. In Janczewski, L. J. and Colarik, A. M. (Eds.) *Cyber Warfare and Cyber Terrorism*. Hershey and New York: IGI Global, pp. 97-104.

Rowe, N. C. and Custy, J. E. (2008) Deception in Cyber Attacks. In Janczewski, L. J. and Colarik, A. M. (Eds.) *Cyber Warfare and Cyber Terrorism*. Hershey and New York: IGI Global, pp. 91-96.

Saich, T. (2004) *Governance and Politics of China.* New York: Palgrave Macmillan.

Sanger, D. E. (2012) *Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power.* New York: Crown Publishers.

Sanson, M. (2008) *International Law and Global Governance.* London: Cameron May Ltd..

Schmitt, M. N. (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press.

Schneier, B., Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Neumann, P. G., Rivest, R. L. and Schiller, J. I. (1997) *The Risks of Key Recovery, Key Escrow , and Trusted Third – Party Encryption*. *Final Report* [online], Bruce Schneier. Available: http://www.schneier.com/paper-key-escrow.pdf [Accessed 10 October 2010].

Schneier, B. (2004) *Secrets and Lies. Digital Security in a Networked World.* Indianapolis: Wiley Publishing Inc..

Schneier, B. (2008a) *America's Dilemma: Close Security Holes, or Exploit Them Ourselves* [online], Bruce Schneier. Available: http://www.schneier.com/essay-216.html [Accessed 20 April 2011].

Schneier, B. (2008b) *Chinese Cyberattacks: Myth or Menace* [online], Bruce Schneier. Available: http://www.schneier.com/essay-227.html [Accessed April 20, 2011].

Schneier, B. (2009) *So-called Cyberattack Was Overblown* [online], Bruce Schneier. Available: http://www.schneier.com/essay-280.html [Accessed 20 April 2011].

Schneier, B. (2010) *Stuxnet* [online], Bruce Schneier. Available: http://www.schneier.com/blog/archives/2010/10/stuxnet.html [Accessed 7 October 2010].

Schwartau, W. (1996) Ethical Conundra of Information Warfare. In Campen, A. D., Dearth, D. H. and Goodden, T. R. (Eds.) *Cyberwar: Security, Strategy, And Conflict In The Information Age.* Fairfax: AFCEA International, pp. 243-249.

SC Magazine (2013) *Eugene Kaspersky Press Club* [online video], 8 November 2013. Available: http://www.youtube.com/watch?v=6tlUvb26DzI&feature=youtu.be [Accessed 10 November 2013].

Sharma, A. (2009) Cyber Wars: A Paradigm Shift from Means to Ends. In Czosseck, C. and Geers, K. (Eds.) *The Virtual Battlefield: Perspectives on Cyber-Warfare.* Amsterdam: IOS Press.

Shawnna, R. and Rault C. (2012) *The state of Cyberwar in the U.S.* [online] DiploNews. Available: http://www.diplonews.com/reports/2012/20120205_L_CyberWar.php [Accessed 6 February 2012].

Sherif, A. (2012) SCADA Hacking, *The Hacker News*, 10, pp. 13-18.

Shimeall, T., Williams P. and Dunlevy, C. (2002) Countering Cyber War, *NATO Review*, Winter 2001/ 2002, pp. 16-18.

Shoham, Y. (2012a) *Dominance* [online course material], Mountain View: Coursera Inc.. Available: https://www.coursera.org/course/gametheory/ [Accessed 19 March 2012].

Shoham, Y. (2012b) *Normal Form Definition* [online course material], Mountain View: Coursera Inc.. Available: https://www.coursera.org/course/gametheory/ [Accessed 19 March 2012].

Siegel, P. C. (2007) Perception Management: IO's Stepchild. In Armistead, L. (Ed.) *Information Warfare. Separating Hype from Reality.* Washington D.C.: Potomac Books Inc., pp. 27-44.

Singh, C. (2012) *Analyzing The Great Firewall Of China Or The Golden Shield* [online], Sikh Archives. Available: http://www.sikharchives.com/?p=2604 [Accessed 9 February 2012].

Skoudis, E. (2009a) Evolutionary Trends in Cyberspace. In Kramer, F. D., Starr, S. H. and Wentz, L. K. (Eds.) *Cyberpower and National Security*. Washington D.C.: National Defense University, pp. 147-170.

Skoudis, E. (2009b) Information Security Issues in Cyberspace. In Kramer, F. D., Starr, S. H. and Wentz, L. K. (Eds.) *Cyberpower and National Security*. Washington D.C.: National Defense University, pp. 171-205.

Snidal, D. (1985) The Game Theory of International Politics, *World Politics*, 38(1), pp. 25-57.

Snow, G. M. (2011) *Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism*. Washington D.C.: Federal Bureau of Investigation.

Snyder, G. (1961) *Deterrence and Defense: Toward a Theory of National Security.* Princeton: Princeton University Press.

Sohmen, P. (2001) Taming the Dragon: China's Efforts to Regulate the Internet, *Stanford Journal of East Asian Affairs*, 1, pp. 17-26.

Sosmeňa, G. C. Jr. (2009) *Local Governance and National Security.* Pasay City: Local Government Development Foundation (LOGODEF).

SPIEGEL (2013) *Edward Snowden Interview: The NSA and Its Willing Helpers* [online], Hamburg: SPIEGEL Online GmbH. Available: http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html [Accessed 8 July 2013].

Stark, H. (2011) *Mossad's Miracle Weapon* [online], Hamburg: SPIEGEL Online GmbH. Available: http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html [Accessed 16 January 2013].

Starr, S: H. (2009) Towards an Evolving Theory of Cyberpower. In Czosseck, C. and Geers, K. (Eds.) *The Virtual Battlefield: Perspectives on Cyber-Warfare.* Amsterdam: IOS Press, pp. 18-52.

Steele, R. D. (1996) Creating a Smart Nation: Information Strategy, Virtual Intelligence, and Information Warfare. In Campen, A. D., Dearth, D. H. and Goodden, T. R. (Eds.) *Cyberwar: Security, Strategy, And Conflict In The Information Age.* Fairfax: AFCEA International, pp. 77-89.

Stein, G. J. (1996) Information Warfare. In Campen, A. D., Dearth, D. H. and Goodden, T. R. (Eds.) *Cyberwar: Security, Strategy, And Conflict In The Information Age.* Fairfax: AFCEA International, pp. 175-183.

Stewart, W. (2009) *TCP/IP Internet Protocol* [online], Living Internet. Available: http://www.livinginternet.com/i/ii_tcpip.htm [Accessed: 3 July 2011].

Stiennon, R. (2010) *Surviving Cyber War*. Plymouth: Government Institutes.

Stone, R. W. (2001) The Use and Abuse of Game Theory in International Relations: The Theory of Moves, *The Journal of Conflict Resolution*, 45(2), pp. 216-244.

Stolleis, M. (1992) *Geschichte des öffentlichen Rechts in Deutschland. Band 2: Staatsrechtslehre und Verwaltungswissenschaft 1800 bis 1914.* Nördlingen: C. H. Beck.

Struck, P. (2002), *Pressekonferenz mit Minister Struck zur Weiterentwicklung der Bundeswehr* [online], Berlin: Bundesministerium der Verteidigung. Available: http://www.bmvg.de/portal/a/bmvg/!ut/p/c4/NY3BCsIwEET_KGkOFetNUUEPetR6KWmypItNUjabevHjTYXOwBzmDYx8yeKgZ3SaMQY9yqdsDe76j-j97ITHgImBMHvhIJkBzcDQ_dkMxIAWXQ4urcMuAXKnmroWliYoTWLK5i0fy5MFYWIAXpIhMJZ0pDmSmCLxuJBMVIhAK9tKHQ-Vqlap72bbXk9NqS63811O3u9_-L2Ycw!!/ [Accessed 24 May 2014].

Sulek, D. and Moran, N. (2009) What Analogies Can Tell Us About the Future of Cybersecurity. . In Czosseck, C. and Geers, K. (Eds.) *The Virtual Battlefield: Perspectives on Cyber-Warfare.* Amsterdam: IOS Press, pp. 118-131.

Symantec Security Response (2011) *W32.Duqu. The precursor to the next Stuxnet.* Mountain View: Symantec Corporation.

Szafranski, R. (1996) A Theory of Information Warfare: Preparing for 2020. In Campen, A. D., Dearth, D. H. and Goodden, T. R. (Eds.) *Cyberwar: Security, Strategy, And Conflict In The Information Age.* Fairfax: AFCEA International, pp. 231-242.

Szor, P. (2011*) Duqu - Threat Research and Analysis.* Santa Clara: McAfee.

Tarakanov, D. (2013) *The "Kimsuky" Operation: A North Korean APT?* [online], Moscow: Kaspersky Lab. Available: http://www.securelist.com/en/analysis/204792305/The_Kimsuky_Operation_A_North_Korean_APT [Accessed 28 October 2013].

Taylor, J. (1997) The Emerging Geographies of Virtual Worlds, *Geographical Review*, 87(2), pp. 172-192.

The Guardian (2010) *Inside 'Anonymous': tales from within the group taking aim at Amazon and Mastercard* [online], London: The Guardian. Available: http://www.guardian.co.uk/technology/blog/2010/dec/13/hacking-wikileaks [Accessed 15 December 2010].

The Guardian (2013) *THE NSA FILES* [online], London: The Guardian. Available: http://www.theguardian.com/world/the-nsa-files/ [Accessed 28 October 2013].

The Economist (2014) *Predictions for 2014. The Final Countdown* [online], London: The Economist. Available: http://www.economist.com/blogs/theworldin2014/2013/12/predictions-2014 [Accessed 11 January 2014].

The SecDev Group (2009) *Tracking GhostNet: Investigating a Cyber Espionage Network*. *JE02-2009.* Ottawa: The SecDev Group.

Thomas, B. (2012) *McAfee Working To Protect Critical Infrastructure Against Stuxnet Type Viruses* [online], Dehli: DefenseWorld.net. Available: http://www.defenseworld.net/news/7189/McAfee_Working_To_Protect_Critical_Infrastructure_Against_Stuxnet_Type_Viruses (Accessed 17 July 2012).

Thomas, T. L. (2000) *Like Adding Wings To The Tiger: Chinese Information War Theory and Practice* [online], Fort Leavensworth: Foreign Military Studies Office. Available: http://www.iwar.org.uk/iwar/resources/china/iw/chinaiw.htm [Accessed 6 January 2012].

Thomas, T. L. (2009) Nation-State Cyber Strategies: Examples from China and Russia. . In Kramer, F. D., Starr, S. H. and Wentz, L. K. (Eds.) *Cyberpower and National Security*. Washington D.C.: National Defense University, pp. 465-488.

Tkakic, J. (2007) *Trojan Dragons: China's International Cybewarriors* [online], Washington D.C.: The Heritage Foundation. Available: http://www.heritage.org/research/reports/2007/12/trojan-dragons-chinas-international-cyber-warriors [Accessed 12 December 2012].

Toffler, A. and Toffler H. (1993) *War and Anti-War. Survival at the Dawn of the 21st Century.* London: Little Brown and Company.

Tordilla, P. (2011) *Cyber Warfare* [online], Percival Tordilla. Available: http://www.scribd.com/doc/50081543/cyberwarfare [Accessed 9 November 2012].

Touré, H. I. (2011a) Cyberspace and the Threat of Cyberwar. In Touré, H. I. and the Permanent Monitoring Panel on Information Security (Eds.) *The Quest for Cyber Peace*. Geneva: International Telecommunication Union & World Federation of Scientists, pp. 7-13.

Touré, H. I. (2011b) ITU's Global Cybersecurity Agenda. In Touré, H. I. and the Permanent Monitoring Panel on Information Security (Eds.) *The Quest for Cyber*

Peace. Geneva: International Telecommunication Union & World Federation of Scientists, pp. 104-109.

Touré, H. I. (2011c) The International Response to Cyberwar. In Touré, H. I. and the Permanent Monitoring Panel on Information Security (Eds.) *The Quest for Cyber Peace*. Geneva: International Telecommunication Union & World Federation of Scientists, pp. 86-103.

TrendLabs Security Intelligence Blog (2011) *Web Threatmorphosis* [online], Shibuya: Trend Micro. Available: http://blog.trendmicro.com/threat-morphosis [Accessed 12 February 2012].

Trend Micro (2013) *How Deep Discovery Protected Against The Korean Cyber Attack* [Online], Shibuya: Trend Micro. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/how-deep-discovery-protected-against-the-korean-mbr-wiper/ [Accessed 21 March 2013].

Trites, G. D. (2008) *Data-Centric Security, White Paper*. Toronto: Chartered Accountants of Canada.

Troiani, G. (2012) *NSA Director: Defense Network Not 'Defensible'* [online], Tysons Corner: ExecutiveBiz. Available: http://blog.executivebiz.com/2012/01/nsa-director-defense-network-not-defensible/ [Accessed 1 February 2012].

Tse-Tung, M. (1967) *Selected Military Writings of Mao Tse-Tung.* Peking: Foreign Language Press.

Tung, D. S. and Tung, T. K. (2010) *36 Stratagems Plus: Illustrated by International Cases.* Victoria: Trafford Publishing.

Tuysuz, G. and Watson, I. (2014) *Turkey blocks YouTube days after Twitter crackdown* [online], Atlanta: Cable News Network (CNN). Available: http://edition.cnn.com/2014/03/27/world/europe/turkey-youtube-blocked/ [Accessed 28 March 2014].

Griffith, S. B. (1963) *Sun Tzu The Art of War*. Oxford: Oxford University Press.

United Nations (2013) *The Cyber Index. International Security Trends and Realities. UNIDIR/2013/3.* New York and Geneva: United Nations Institute for Disarmament Research.

Villeneuve, N.; Bennett, J. T.; Moran, N.; Haq, T.; Scott, M. and Geers, K. (2014) *Operation "Ke3chang" Targeted Attacks Against Ministries of Foreign Affairs* [online], Milpitas: FireEye Inc.. Available: https://www.fireeye.com/content/dam/legacy/resources/pdfs/fireeye-operation-ke3chang.pdf [Accessed 18 February 2015].

Wacker, G. (2003) Internet censorship in China. In Hughes, C. R. and Wacker G. (Eds.) *China and the Internet. Politics of the digital leap forward.* London and New York: Routledge Curzon, pp. 58-82.

Wall, D. S. (2003) Mapping out Cybercrimes in a Cyberspatial Surveillant Assemblage. In Ball, K. and Webster, F. (Eds.) *The Intensification of Surveillance. Crime, Terrorism and Warfare in the Information Age.* London: Pluto Press, pp. 112-136.

Walter, J. (2012) *'Flame Attacks': Briefing and Indicators of Compromise, White Paper*. Santa Clara: McAfee.

Walton, G. (2001) *China's Golden Shield. Corporations and Development of Surveillance Technology in the People's Republic of China.* Québec: International Centre for Human Rights and Democratic Development.

Waltz, K. N. (1979) *Theory of International Politics.* Reading: Addison-Wesley.

Warschauer, E. (1911) *Schopenhauers Rechts- und Staatslehre.* Kattowitz.

Weber, S. (2004) Target of Opportunity: Networks, Netwar, and Narratives, *Grey Room*, 15, pp. 6-27.

Webster, F. (2003) Information Warfare, Surveillance and Human Rights. In Ball, K. and Webster, F. (Eds.) *The Intensification of Surveillance. Crime, Terrorism and Warfare in the Information Age.* London: Pluto Press, pp. 90-111.

Wegener, H. (2011) A Concept of Cyber Peace. In Touré, H. I. and the Permanent Monitoring Panel on Information Security (Eds.) *The Quest for Cyber Peace*. Geneva: International Telecommunication Union & World Federation of Scientists, pp. 77-85.

Westby, J. R. (2011a) *Global Cyber Security* [podcast], 28 February 2011. Available: https://csis.org/multimedia/audio-inteview-jody-westby-global-cyber-security [Accessed 6 March 2011].

Westby, J. R. (2011b) Introduction. In Touré, H. I. and the Permanent Monitoring Panel on Information Security (Eds.) *The Quest for Cyber Peace*. Geneva: International Telecommunication Union & World Federation of Scientists, pp. 1-6.

Wilkinson, C. (2011) *Cyber opportunities are hot in 2012* [online], Vienna: Washington Technology. Available: http://washingtontechnology.com/articles/2011/11/28/cybersecurity-opportunities.aspx? [Acessed 29 November 2011].

William, P. (2001) Transnational Criminal Networks. In Arquilla, J. and Ronfeldt, D. *Networks and Netwars: The Future of Terror, Crime, and Militancy.* Santa Monica: RAND Corporation, pp.: 61-98.

Williams, C. (2011) *Stuxnet: Cyber attack on Iran 'was carried out by Western powers and Israel* [online], London: The Telegraph. Available: http://www.telegraph.co.uk/technology/8274009/Stuxnet-Cyber-attack-on-Iran-was-carried-out-by-Western-powers-and-Israel.html [Acessed 22 January 2011].

Wilson, C. (2004) *Information Warfare and Cyberwar: Capabilities and Related Policy Issues, RL31787.* Washington D.C.: Congressional Report Service for Congress.

Wilson, C. (2009) Cyber Crime. In Kramer, F. D., Starr, S. H. and Wentz, L. K. (Eds.) *Cyberpower and National Security*. Washington D.C.: National Defense University, pp. 415-436.

Wilson, T. (2013) *Move Over, APTs -- The RAM-Based Advanced Volatile Threat Is Spinning Up Fast* [online], San Francisco: Dark Reading. Available: http://www.darkreading.com/advanced-threats/167901091/security/vulnerabilities/240149192/move-over-apts-the-ram-based-advanced-volatile-threat-is-spinning-up-fast.html/ [Accessed 17 March 2013].

Winkler, I. (2005a) *Guard against Titan Rain hackers* [online], Framingham: Computer World. Available: https://www.computerworld.com/s/article/105585/Guard_against_Titan_Rain_hackers?taxonomyId=017 [Accessed 23 March 2012].

Winkler, I. (2005b) *Spies Among Us. How to stop the spies, terrorists, hackers, and criminals you don't even know you encounter every day.* Indianapolis: Wiley Publishing Inc..

Winkler, I. (2007) *Zen and the Art of Information Security.* Rockland: Syngress.

Winkler, T. H., Ebnöther, A. H. and Felberbauer, E. M. (Eds.) (2004) 6th International Security Forum. Proceedings of the Conference, *Studies in Contemporary History and Security Policy,* 14.

Winton, H. R. (2006) *An Imperfect Jewel* [presentation]. Washington D.C.: National Defense University.

Wohlstetter, A. (1959) The Delicate Balance of Terror, *Foreign Affairs,* 37(1), pp. 211-234.

Wolf (2012) *THREAT FROM HUAWEI* [online], Washington D.C.: The Library of Congress. Available: http://thomas.loc.gov/cgi-bin/query/z?r112:H19MR2-0028:/ [Accessed 7 June 2012].

Wu, G. (2011) China in 2010, *Asian Survey*, 51(1), pp. 18-32.

Yang, G. (2003) The Co-evolution of the Internet and Civil Society in China, *Asian Survey,* 43(3), pp. 405-422.

Yoshihara, T. (2001) *Chinese Information Warfare: A Phantom Menace or Emerging Threat?*. Carlisle: Strategic Studies Institute (SSI).

Zanini, M. and Edwards, S. J. A. (2001) The Networking of Terror in the Information Age. In Arquilla, J. and Ronfeldt, D. *Networks and Netwars: The Future of Terror, Crime, and Militancy*, pp. 29-60.

Zetter, K. (2012) *State-Sponsored Malware 'Flame' Has Smaller, More Devious Cousin* [online], New York: Wired. Available: http://www.wired.com/threatlevel/2012/10/miniflame-espionage-tool/ [Accessed 18 October 2012].

Zimet, E. and Barry, C. L. (2009) Military Service Overview. In Kramer, F. D., Starr, S. H. and Wentz, L. K. (Eds.) *Cyberpower and National Security*. Washington D.C.: National Defense University, pp. 284-308.

APPENDIX

Appendix I

Year	Cyber Incident/ Attack	More Information/ Source
2015	Operation Woolen-Goldfish	Pernet and Lu, 2015
2015	Babar	Rascagnères, 2015
2015	Desert Falcon	Global Research & Analysis Team, 2015b
2015	Equation (e. g. Fanny)	Global Research & Analysis Team, 2015a
2014	Regin	Global Research & Analysis Team, 2014a
2014	Penquin Turla	Baumgartner and Raiu, 2014
2014	Operation Ke3chang	Villeneuve *et al.*, 2014
2014	Crimea/ Ukraine Crisis	Rietveld and Perk, 2014
2014	Siesta Campaign	Moran and Oppenheim, 2014
2014	Uroburos/ Snake/ Turla	G Data SecurityLabs, 2014
2014	Careto	Global Research & Analysis Team, 2014b
2013	Finnland	Farivar, 2013
2013	Icefog	Global Research & Analysis Team, 2013b
2013	Operation Kimusk	Tarakanov, 2013
2013	Operation Deputy Dog	Moran and Villeneuve, 2013
2013	National Security Agency	The Guardian, 2013
2013	Net Traveler	Global Research & Analysis Team, 2013a
2013	Operation Hangover	Fagerland, 2013
2013	MiniDuke	Raiu, Soumenkov, Baumgartner and Vitaly, 2013
2013	TeamSpy	Global Research & Analysis Team, 2013d
2013	MBR Wiper	Trend Micro, 2013
2013	APT1 / Comment Crew	MANDIANT, 2013
2012	Operation Beebus	Paganini, 2013

2012	Red October	Global Research & Analysis Team, 2013c
2012	Lucky Cat	Forward-Looking Research Team, 2012
2012	Council of Foreign Relations	Gertz, 2012
2012	Xtreme RAT	Fagerland, 2012
2012	Shamoon	Jeffers, 2012
2012	Gauss	Goodin, 2012
2011	Mahdi	Global Research & Analysis Team, 2012d
2010	CENTCOM	Lynn, 2010
2010	Flame	Walter, 2012
2010	Duqu	Szor, 2011
2010	Stuxnet	Rid, 2012, 14-16
2009	Night Dragon	McAfee Foundstone Professional Services and McAfee Labs, 2011
2009	Korea	Malawer, 2010: 28-31
2009	Ghosnet	Clarke and Knake, 2010: 58-62
2009	Aurora	Andrees and Winterfield, 2011: 14
2008	Caucasian Cyberwar	Clarke and Knake, 2010: 17-21
2008	Buckshot Yankee	Andrees and Winterfield, 2011: 13
2007	Operation Orchard	Rid, 2013: 42-43
2007	Middle-East	Malawer, 2010: 28-31
2007	First Cyberwar in Estonia	Bronk, 2008: 132-134
2006	Operation Shady Rat	Alperovitch, 2011
2003	Titan Rain	Clarke and Knake, 2010: 58-62
2001	Code Red'	Public Broadcasting Service, 2003
2001	Honker Union	Public Broadcasting Service, 2003
1999	Belgrade Embassy Bombing	Billo and Chang, 2004: 14-15
1999	Taiwan	Denning, 2000: 276
1999	Legion of the Underground	Denning, 2000: 274

1998	Free East Timor	Denning, 2000: 272
1998	Bhabha Atomic Research Center (milw0rm)	Denning, 2000: 272-273
1998	Internet Black Tigers	Denning, 2000: 268-272
1998	Kosovo Crisis	Denning, 2000: 239-250
1998	Solar Sunrise	Cordesman, 2000
1998	Moonlight Maze	Public Broadcasting Service, 2003
1994	Rome Labs Incident	IEEE Computer Society's Technical Committee on Security and Privacy, 2011