UiA University of Agder

Master

Back to the Future? Planning for uncertainty
A call for bridging the security and development communities

MAGNUS STAVENES

SUPERVISOR

Prof. Oddgeir Tveiten

University of Agder, 2020
Faculty of Social Sciences
Department of Global development and planning

Back to the Future? Planning for uncertainty

A call for bridging the security and development communities

Table of Contents

Preface

This work has been a culmination of the author's academic venture through both the MA program in development studies at UiA and a MA at the Centre for International Studies and Diplomacy at SOAS, University of London.

It was clear to the author that there was a gap that existed within the development literature. This gap consists of the theoretical underpinnings of international relation and international security in terms of thinking about relationships of national interests, conflict and its real-world applications. It is this that the author wants to shed light on, primarily how an understanding of international relations and security will benefit from assessing different challenges that are currently unfolding in the international community.

As the world becomes increasingly digital, it seemed like the right place to start was to put a significant focus on what the digital space will mean for contemporary societies going into the future. How we plan for, and what is implemented, will have consequences going forward. Thus, creating awareness of some issues, like how the digital realm could be used for malicious intents are highlighted in this thesis.

The questions then, is what now and where do we go from here? That is for the policymakers to decide. However, academia does have a role to play. One area, as the author sees it, is to incorporate some of the elements that are addressed in this thesis into the development literature as these respective fields have overall common goals. That is a focus on human security.

The author would like to extend my gratitude to professor Oddgeir Tveiten. We have known each other outside of the academic world for a time. Furthermore, I was delighted to have Oddgeir as my supervisor. Though we did not always see eye to eye, and our relationship with this thesis at specific points could be described as rawkus. I would not have had it any other way. The work was ostensibly premature before we got to work in the early stage of 2020. After this, the work got the editorial composition needed. And are now ready to be presented as a coherent thesis, arguing a credibly presented point.

I would also like to thank Ewan Lawson. Lawson, who was my professor in international security at SOAS. Lawson served in the RAF for over three decades. His ability to combine practical

elements in conjunction with academic rigor made his lectures and tutorials highly sought after. His diplomatic approach made me and my peers engage in new ways. Leading to real constructive in-depth discussions, but he never let anyone get away with shortcuts or shallow conclusions.

Furthermore, I would like to extend a sincere appreciation to friends and family. For too long, they have had to listen, engage, and discuss topics of my interests. Having sparing partners on points of interest have been instrumental in shaping my own arguments. As these have been laid out over time. Their feedback has proven most useful.

Abstract

We currently see a foreign policy environment that is becoming more complex and volatile. Cyber is now established as a frequently used tool in foreign policy. Its disruptive qualities are concerning in terms of its implications on contemporary established economic and political structures. Cyber capabilities are cheap, accessible, omnipresent, and the domain from which it operates, namely that of cyberspace, is an inherent unregulated space. The concept of the security dilemma has resurged into cyberspace, and actors on a national and international level, are currently engaged in a digital arms race. Cyber capacity building was created as a tool by the cybercommunity to mitigate some of these challenges. Due to the impact that ICTs have on a societal scale, its implementation into a development context is inescapable.

Nevertheless, the development community has been hesitant to implement security issues in its literature and is thus failing to engage on security-related matters sufficiently. One of the problems is the existence of silo mentalities. Hindering academic cross-pollination is limiting both communities in terms of creating mutually beneficial policies, which is a relatively stable foreign policy environment—described as an environment where sustainable political solutions can take root.

The need to further develop the security/development nexus into a strategic partnership to critically engage contemporary security and development challenges will be critical going forward. There cannot be development with the absence of security, and there cannot be security without development. To create robust, long-term development, and security strategies, the security/development nexus must be further addressed. The creation of norms, international laws, and regulation in cyberspace is imperative moving forward. This includes an understanding of the operating environment by understanding the actors who occupy the said environment. If not, the experience will be that of tactics without strategies implemented in ad hoc solutions that will ultimately fail in its objectives of creating sustainable solutions with tolerated levels of conflict.

Keywords: Security dilemma, CCB, Hybrid Warfare, Cybersecurity.

List of Abbreviations

Acronyms:

A2AD	Anti Access/Area Denial
AFR	Automatic Facial Recognition
ARAMCO	Saudi Arabia´s national oil company, formerly known as Arabian-American Oil Company
AU	The African Union
AUF	Authorization on the Use of Force
CCB	Cyber Capacity Building
CIA	Central Intelligence Agency
CAN	Computer Network Attack
CO	Cyber Operations
CSIS	Centre for Strategic and International Studies
CT	Counter Terrorism
DDoS	Distributed Denial of Service
DoS	Denial of Service
DOD	US Department of Defense
DSB	Norwegian Directorate for Civil Protection
EU	The European Union
ESS	European Security Strategy
FBI	Federal Bureau of Investigation
FDI	Foreign Direct Investment
FPA	Foreign Policy Analyses
GCHQ	Government Communications Headquarters
GWoT	the Global War on Terror
GNA	Government of National Accord (International recognized governing body in Libya)
GRU	Russian Military Intelligence (Glavnoje Razvedyvatel´noje Upravlenije)
GPS	Global Positioning System
HCSEC	Huawei Cyber Security Evaluation Centre
HDI	Human Development Index
IDF	Israeli Defense Forces
ICRC	International Committee of the Red Cross
ICT	Information Computer Technology

ICWC	International Cyberwar Convention
IHL	International Humanitarian Law
IMF	International Monetary Fund
INF	The Intermediate-Range Nuclear Forces Treaty (the 1987 treaty on the elimination of US and Soviet/Russia intermediate, and short-range missiles)
IR	International Relations
IS	International Security
IRA	Russian Internet Research Agency (Агентство интернет-исследований)
ISC	Intelligence and Security Committee of Parliament
ITU	International Telecommunications Union´s
JCPOA	Joint Comprehensive Plan of Action (the Iran Nuclear Deal)
JIT	Joint Investigation Team
KRG	The Kurdistan Regional Government
KRIPOS	The Norwegian National Criminal Investigation Service
LNA	Libyan National Army
MAD	Mutually Assured Destruction
MENA	The Middle East and North Africa
NATO	North Atlantic Treaty Organization
NATO CCD COE	NATO Cooperative Cyber Defense Centre of Excellence
New START	Strategic Arms Reduction Treaty
NIS	The Norwegian Intelligence Service
NSA	National Security Agency
NSM	Norwegian National Security Authority
OECD	Organization for Economic Co-Operation and Development
P5	The five permanent members of the UNSC
PKK	The Kurdistan Workers Party (Partiya Karkerên Kurdistanê)
PLA Unit 61398	Peoples Liberation Army – Unit 61398 – Chinas military cyber operation
POTUS	the President of the United States
PST	The Norwegian Police Security Service
QAP	Al-Qaeda on the Arabian Peninsula
R2P	Responsibility to Protect
SDG	Sustainable Development Goals
START	Strategic Arms Reduction Treaty
Stuxnet	The computer virus that was used to sabotage the Iranian The nuclear facility at Natanz
UiA	University of Agder
UK	The United Kingdom

UN	United Nations
UN GGE	United Nations Group of Governmental Experts
UN HRC	United Nations Human Rights Council
UNGA	United Nations General Assembly
UNSC	United Nations Security Council
Unit 8200	Israel´s military cyber operations unit
US	The United States of America
USSR	The Union of Soviet Socialist Republics
WWI	World War I
WWII	World War II
WB	The World Bank
YPG	The Peoples Defense Units (*Yekîneyên Parastina Gel*)

1. Introduction

Nation-states such as the US, UK, Israel, China, and Russia (but not limited to), are increasingly utilizing ´cyber` as a tool of international engagement with hostile intent. This tool is an integral implication in a foreign policy environment that is becoming more complex and volatile (ISC, 2017; NATO, 2019b; NIS, 2019; NSM, 2019; RUSI, 2019). It seems increasingly clear that the West in the 21st century is struggling to cope with a return of complex inter-state competition that does not fit neatly in a simple peace-war dichotomy (Lawson, 2019).

As the ISC (2017, p. 31) notes, ´State actors are [now] highly capable of carrying out advanced cyber-attacks.` While the geopolitical and diplomatic consequences historically restricted cyber-attacks if the use of such methods would be uncovered, recent Russian activities suggest, however, that this is no longer the case (ibid).

Cyber is also becoming a standard tool in terms of foreign policy.[1] Its disruptive qualities are problematic as a national security issue, as well as a catalyst for security competition. This is in considerable respect due to concerns relating to cyber and its impact on contemporary economic and political structures. Cyber capabilities are cheap, accessible, and omnipresent (Egel, Robinson, Cleveland, & Oates, 2019; D. Hollis, 2020). Also, cyber as a domain is an inherently unregulated space, at least on the international level (Henriksen, 2019).

The concept of the security dilemma has resurged into cyberspace. Actors on both the national and international level, are currently engaged in a digital arms race (Buchanan, 2016; Henriksen, 2019; Jervis, 1978; NIS, 2019; Sanger, 2018). The cybercommunity created cyber capacity building as a tool to mitigate some of these challenges (Pawlak, 2014). Due to the impact that ICTs have on a societal scale, its implementation into a development context is inescapable (Utenriksdepartementet, 2017). Nevertheless, the development community has been hesitant to implement security issues in its literature. Moreover, because of this, there exists a vacuum to sufficiently engage with highly relevant security issues (Beall, Goodfellow, & Putzel, 2006; Benjaminsen & Svarstad, 2009, p. 314; Pawlak, 2014; P. Williams, 2008, p. 247). One of the issues

[1] List of significant cyber incidents between 2006 and 2019 provided by CSIS, link in bibliography (CSIS, 2020).

is the existence of a silo mentality hindering the benefits of cooperation.[2] There cannot be development with the absence of security, and there cannot be security without development (OLA, 2010). To create robust, long-term development and security strategies, this must be addressed. In this respect, the creation of norms, international laws, and a regulated cyberspace is an imperative moving forward (Schmitt, 2013, 2017; UNGA, 2013; UNODA, 2019). If not, we will experience that of tactics without strategies implemented in ad hoc solutions that will ultimately fail in its objectives. The need to develop the security/development nexus into a strategic partnership, to critically engage contemporary challenges will be critical going forward.

The concept of the security dilemma is currently driving a digital arms race, as it once stimulated nuclear proliferation (Booth & Wheeler, 2007; Buchanan, 2016).[3] The concepts utility to explaining security competition is substantial. Thus, it transfers as a concept integral in defining security competitions and great-power rivalries. This is classically done in the manner of how states interact in the international system. Such explanations often accompany nuclear posture as this is in the heart of deterrence theory. Security competition then is often characterized by nuclear proliferation and classic deterrence, with mutually assured destruction (MAD). This has then gone on to include cyberspace (Barkawi & Laffey, 2006; Buchanan, 2016; Jervis, 1989; Mearsheimer, 2001).

Conflict of interests diverges national interests. This includes the methods and tools that are used in order to pursue those interests. In lieu of such circumstances, we are currently engaged in more complicated theatres of conflict. As witnessed by a divergence from a US-centric geopolitical model. A model that came to be with the demise of the bipolar world of the Cold War era, and the unipolar moment that followed this period. Now there are significant pressures building on this geopolitical model. State actors such as China and Russia are testing the limits for what would normative constitutes acceptable state behavior (NIS, 2019; RUSI, 2019).

Previous operating environments have been more easily defined with distinguishable lines between war and peace; these clear lines are now replaced with new grey-zone dimensions. These

---

[2] The author offers synopsis on this point in the Appendixes. Security and Development perspectives to Winkel and Aase (2008). This will include some major points on the required need to incorporate matters of international relations, and security into the development literature.

[3] The two categories of cyber and nuclear arms races are categorically different. Both in terms of implementation and consequences. Though there have been drawn comparisons between the two in strategic thinking (Stone, 2013). They are however comparable as products of systems of analysis, if so in different spheres or theatres. The security dilemma works as the catalyst in driving processes linked to arms races which are used as examples throughout this thesis.

grey-zone dimensions are characterized by its complicated nature that lacks definitional clarities. Both in terms of no clear beginnings or ends. Though grey-zone, hybrid, or threshold warfare, can still easily be regarded as detecting those activities that are just shy of any defined threshold (Lawson, 2019, p. 8). A significant component is how cyber as a new domain is also providing new challenges.

Furthermore, due to its obfuscating characteristics, the cyber domain works as a significant catalyst in terms of proliferating uncertainties and conflict both in and outside of cyberspace. Giving way to such a new dimension, warfare is now characterized as multi-layered and multi-faceted. These new multi-dimensional modes include a wide range of methods. Such methods include political influence, economic coercion, use of proxies, and cyber along with conventional military forces. This also means that the different modes are highly operational. Not just in a specific theatre, but on a broader array of campaigns on both local and global scales. Moreover, it is initiated by various state and non-state actors. It is, therefore, a necessity to address this on the strategic, as well as the tactical level (RUSI, 2019).

When conflict is addressed in this thesis, it is not just state-on-state conflict. Conflict is as much a conflict of interests between non-state- as well as between state actors. This carries significant security implications. Those implications arise from the blurring of distinctions on how war, or conflict, is classically understood. Such actors involved are state (understood as violence between organized political entities for political gains); non-state actors such as organized crime organizations (violence undertaken by private enterprises, primarily for monetary gains); and large-scale violations of human rights (violence by states or other political motivated groups against individuals) (Kaldor, 2013, p. 2).

It is these implications that carry significant consequences for people who occupy specific regions. In terms of cybersecurity and development processes, digital domains can be significantly disrupted through a state- or non-state actor targeting government systems. Also, the reason why security implications are so important to incorporate into the development discourse is that ´extreme difference in values and ideologies exacerbates international conflict` (Jervis, 1978, p. 174).

There are now severe strains put on the current established international liberal, rules-based order. What this means specifically is that the international system that has been built up under US leadership is now witnessing a US in retreat. This is happening simultaneously with state-actors such as China and Russia seek to challenge these systems. This establishment which is

under stress is so due to a decline of US leadership (Bulmer-Thomas, 2018). Which have been greatly accelerated under the current Trump administration. There are evident signs that point towards trends that would indicate shifts in both global and regional hegemonic positions (Mearsheimer, 2010, pp. 381-382; NIS, 2019). Most often today addressed through the rise of China and the effects this carries vis-à-vis the position of the US as the world's leading superpower (Mearsheimer, 2010).

During the Cold War, great power competition between the two superpowers of the time, namely that of the US and the Soviet Union, shaped the geopolitical agenda. The Cold War era is thus often characterized through the bipolarity positions of the US and the USSR. The diametrically opposed positions that these political entities subscribed to quickly and drastically changed following the collapse of the Soviet Union. Signified by the fall of the Berlin wall and the subsequent dissolution of the Soviet Union. This is the unipolar moment, where Washington now the proprietor of geopolitical affairs. Due to its status as the world´s sole superpower (Krauthammer, 1990). Even though this position of "superpower" was semi-global in scale, namely, because it never included Russia or China (Bulmer-Thomas, 2018). The current global political system, which is based in Washington, is now being challenged, primarily by a rising China and a resurgent Russia. There are now legitimate challenges to the existing international economic and political systems. With indicative shifts towards favoring a *realpolitik* approach, as a principal tool to analyze geopolitical affairs. Though this is viewed and analyzed through different theoretical prisms (Frazier & Stewart-Ingersoll, 2010; Kurowska & Pawlak, 2009; Maurer, 2018; Mearsheimer, 2010; NIS, 2019, 2020; Waltz, 2000).

Information warfare is a component in this renewed competition for regional and global spheres of influence. The Russian Federation worked as a catalyst in bringing information warfare tactics in vogue. Predominantly as information warfare, as a topic of interest, soared since the Russian invasion of Ukraine in 2014 (Giles, 2016, p. 3; Pomerantsev, 2019; RUSI, 2019).

By looking closer at the security dilemma´s incorporation into cyberspace, it will be possible to identify some of the broader implications of this kind of state-on-state competition (ibid).

This will also provide the opportunity to address some of the implications of globalization, particularly in terms of economic and political interconnectedness. As these processes are greatly facilitated by ICTS, highlighting specific parts of the threat landscape will contribute to a clearer image of some of the complications we are currently facing. Due to Chinese and Russian practices, along with their cyber capabilities (not to exclude western ones), there should be a real

concern for a conflagration of conflict in cyberspace. As the world once again falls under spheres of influences, or great power competition (Giles, 2016; Mearsheimer, 2010), this will attribute to new fragmented constellations of political and ideological entities, that will most likely be followed by a continuing proliferation of conflict in and outside of cyberspace.

A significant part of this problem is the existence of different conceptualizations of cyberspace. These differences are then based on the fragmented political entities and their different definitions and understandings of cyberspace. Which then are a significant source for the increased complexities in the current operating environment. The West regards cyberspace as an enabling domain of information sharing, and therefore a catalyst for economic growth and education. The Eastern view does not necessarily contradict this but also sees the *internet of things* as a threat to regime stability (Giles, 2016; RUSI, 2019).

First and foremost, the state can no longer easily control the flow of information. As information can spread in real-time, controlling political narratives can be done on scales that have not previously been possible. Also, due to security competition in an increasingly hostile foreign policy environment different conceptions of cyber fuels this concerto. It is these different perceptions that lead to different attitudes and approaches taken to offensive/defensive cyber capabilities. The increased use of cyber capabilities in international relations has made the UN significantly increased its efforts into reaching a consensus on what would be considered acceptable state behavior in the digital domain. The UN seeks to bring stability to this digital domain primarily through a robust regulatory framework to the international political system (Atzori, Iera, & Morabito, 2010; Giles, 2016).

In addition to these challenges posed to existing political structures. Some states are creating alternative institutions, principally concerning the already established Bretton Wood institutions. By creating a separate system for global development initiatives, these alternative institutions seek to promote alternative eastern perspectives on development processes. Furthermore, it seeks to change future trajectories. Some of the principal components to these alternative institutions are that there are no preconditions needed. Such as a focus on democratic governance. Which is a typical Western approach. The traditional Western theme of development is rooted in the notion of democracy, the rule of law, and human rights. Though the concept of promoting democracy and liberalism as a western tool in a core/periphery setting has often worked on the brink of hypocrisy. This has been particularly noticeable when economic restructuring programs have

been implemented,[4] as a part of promoting western-style governance structures in the periphery/ global south (Easterly, 2003; Konadu-Agyemang, 2000; Rodrik, 1990).

Ultimately, this thesis is about the role the development community can play in shaping future security strategies. There is a sincere acknowledgment in the security discourse of how an understanding of the operating environment and the people who occupy this environment is crucial in current and future conflict scenarios. This is an essential area where the development community can aid in the reappraisal of present strategies as these strategies need an understanding of the cultural, social, political, and historical setting of all actors involved in this increasingly complex foreign policy ecosystem. The goal of this thesis is then a call to bridge the security and development community to better address future digital challenges under the principles of sustainable development.

1.1 Problem Statemen

This thesis will take a theoretical approach to address what the author views as limitations in mainstream development literature. This is not a critique of development literature in general.

It is a critique in terms of highlighting what the author regards as a gap in the literature, which does not include security elements which will be highlighted in this thesis. Even though security elements are deeply embedded in key multilateral bodies such as the UN and the EU - the development body of literature is still lacking in addressing the importance that security studies offer. Which, in classical terms, concentrates on the analyses of the causes of war and the conditions of peace. Included in this thesis is the study of the use of force by state and non-state actors and its real-world implications (Dunne, Kurki, & Smith, 2016, p. 1). Highlighting how intimately security issues are interlinked with the development discourse. Security strategies created to address security challenges would benefit from incorporating social anthropological elements from the development community. Primarily concerning a quest for a more profound and intimate understanding of culture and the people who occupy the specific environment that the strategy would address. By tackling some of the challenges posed in this increasingly complex security environment, it is the authors hope to shed light on some of these issues.

[4] For the WB and IMF, SAPs have been under long-standing scrutiny. Particularly from the political left, who views the policies as disproportionately hurting the poor.

Cyber related operations or computer network attacks are the ´employment of cyber capabilities where the overall purpose is to achieve objectives in or through cyberspace.` These are actions taken to ´disrupt, deny, degrade, or destroy information. This is also categorized as a type of cyber-attack (Cartwright & James, 2010, p. 8; NATO, 2019e, p. 30). Such operations are threatening to undermine development processes at both local, regional, and macro levels. Spanning a range from cybercrime to more substantial political destabilizing operations, the control of information and abilities to infiltrate foreign networks, including domestic security perspectives, have created significant new challenges as a by-product of globalization processes (Giles, 2016; Pawlak & Barmpaliou, 2017). Thus, the double-edged sword of cyber that is both the benefits and subsequent threats is significant. There are considerable resources devoted to the acts of mitigating foreign intrusion efforts as well as offensive/defensive capabilities. However, though there is an awareness of this, it still seems that cyber in itself is treated as an elusive concept. Primarily, as it is located in a hypothetical periphery, not touching upon one´s own reality. This thesis states that there is a need to move on from such a narrow understanding. Moreover, the development discourse needs to incorporate security elements better, if development processes (as is classically understood) are to function in the 21st century.

1.2 Thesis outline

This thesis is divided into seven parts. The first section will include the introduction and a brief summary of how different theoretical schisms are used in the analysis of world affairs. This thesis will be a literature study. It will be a critical theoretical review, where the authors´ analysis will be the main driver. The data collection is based on the literature chosen to provide this thesis with a satisfactory conclusion. There was an initial use of informants who provided insights to highlight and map key areas of interest. These informants range from the academic to the practical side of international security, foreign policy, development studies, and cyber.[5] This will not be expanded upon as this was only used preliminary in the research phase and do not constitute the makeup of this thesis.

Next will be the primary theoretical foundation, detailing the importance of the security dilemma and how security competition has been and continues to be influential in shaping historical and contemporary development processes. Also, this thesis discusses why this proven concept ought to be incorporated into the development fold as this has severe and direct consequences in terms

[5] The informants are presented in full in the appendixes´ (informants).

of human security. This 70-year-old concept is critical in thinking on how and why states act the way that they do, in the physical as well as the digital terrain. The concept will thus establish a structural framework of analysis. It will describe some of the complications that ICTs provide on an international level, as well as being a national security issue. By examining current and possible future trends. To do this, it will highlight current tendencies in thinking about what grey zone or hybrid threats are and how this will shape the future conflict environment. Furthermore, it emphasizes why getting it right matters in the steps taken today can better shape tomorrow.

It will then describe how different strategies are shaping current conflicts, both in cyberspace as well as the physical terrain. It will have the empiric sections incorporated throughout the text as it will then have the ability to continually reference both security and development topics and how this applies in a foreign policy environment, which is growing more fragmented and conflict oriented.

It will then go on to highlight some of the problems we are currently facing, with the difficulties in creating sound regulatory frameworks for responsible state behavior in cyberspace.

Lastly, it will address some of the critiques and limitations to the contents in this thesis. It will also include the author´s afterthoughts on the project, before concluding that development and security are inexorably linked. That security is not just peace or a lack of conflict. It is about how to create an environment where sustainable political solutions can take hold. One of the core issues is definitional that intersubjective interpretations provide grounds for conflict. Principally through communicating past each other as individuals, as a conflict of interests manifests into an operating environment, characterized by an increasing confrontational raison d´état dynamic.

2. Theorizing security

IR scholarship is very much divided in terms of methodologies used to explain world affairs. Political science, in this respect, is divided into terms between the application of a positivist (problem-solving approach) and critical theory (Dunne et al., 2016, p. 25).

Traditional scientific approaches, or *problem-solving theory,* takes the world as self-evident or ´as it is` (Browning, 2013, p. 13). It is a neutral exercise to determine the objective nature of a particular object. This is a positivistic approach, which means it can be tested against an empirical reality with a set of a priori conditions (ibid). Cox (1981, p. 128) applies this to international relations with the ´prevailing social and power relationships` as natural. Furthermore, since they are perceived as natural, the theory on which they are based need not come into question. Instead, the point is to make these ´relationships and institutions` work as efficiently as possible (ibid).

On the other side is *critical theory*. This approach uses theory as ´potentially constituting our experience of the world,` which arguably gives it a more dynamic view (Browning, 2013, p. 15; Grimen, 2004, pp. 75-77). Though its origins stem from the enlightenment, it is through the Frankfurt school that critical theory came into place. This unorthodox critique of society was an intriguing contradiction; ´rather than liberating man from oppression, technology, market forces (e.g., consumerisms), liberal tenets of individual freedom had conspired to suppress the political consciousness of man` (Dunne, et al., 2016, p. 147). What this means is what Walter Benjamin referred to as a ´jargon of authenticity` - that the owner of the system (in this case a strict adherence to problem-solving theory) has the capacity of producing and reproducing the *truth* about the essence of society (Benjamin in Dunne, et al., 2016, p. 147).

An understanding of the different theoretical approaches is essential to recognize different approaches used in this thesis as it carries a significant element of different IR and IS theoretical underpinnings including Foucault's discursive formations. Constituted in that perceptions, or discourses produces our experienced reality. As one considerable premise in this thesis is grounded in the intersubjectivity of man. Namely that it is the definitional question of cyber and what this constitutes, which is one of the significant factors in increasing threat perceptions in the foreign policy environment.

The principal position of US scholarship in IR makes it non-avoidable. Also, even though positivist accounts are predominant in American IR. This does not mean that US IR scholarship per definition is based on positivistic approaches. There is an excellent variety of US scholarship. It is, however, a reflection that it carries a significant element of this type of methodology. Thus many of the sources used in this thesis will be grounded in problem-solving theory (Dunne et al., 2016, p. 25). The critique against this approach is based on the notion that the positivist position is too simplistic (Hopf, 1998; Weldes, 1996; Wendt, 1992). The critique is rooted in how things, narratives, and perceptions are relative to the different referent objects. This is important to address as the same position will have a different meaning to different actors since there are always two stories to tell about world political events, which cannot be converted into a single narrative (M. Hollis & Smith, 1990). It is, therefore, central to understand the crux of the issue by the separation of different theoretical approaches. By this divergence, it is possible to divide the theory (broadly speaking) into the two more specific camps, namely problem-solving and critical theory (Cox, 1981, p. 128). Because of this, there will be an emphasis on collecting a wide arrange of primary and secondary sources from several schools of thought to create an overall more nuanced argument.

One example of the diametrically opposed positions of realism and constructivism lies in how IR is addressing nuclear weapons and proliferation. According to a realist approach, states act in fundamental self-interest throughout time and space. Realism classically does not adhere to domestic politics. States are black boxes and regard all other states the same in this sense. Constructivism's critique of this preposition is how security is a socially constructed issue. That the state has an idea of "self." States see themselves as a product of historical political, cultural, and socioeconomic factors (Hopf, 1998). From a realist perspective, nuclear weapons should have the same a priori meaning, regardless of the state who possesses these weapons. However, according to constructivism, this is not the case. And is certainly not reflected on an operational basis in the international community. The US response to Western powers' nuclear capabilities is not equal to its perception of the DPRK nuclear capabilities (Farago, 2016). Nor does it equate to Iran´s quest for such capabilities. Concerning nuclear weapons being de facto the same, they represent *radically* different meanings to different actors.

It is, however, out of the scope of this thesis to address all approaches to both development and security studies. This includes processes on the application of practice and theory in different contextual environments. It is still essential to address some of the critiques connected to the

issues which are discussed in this thesis. It is still recognized that this will be limited, as to fit with the scope of this project.

The methodology will be laid out with the distinct aim of giving a clear, transparent, and convincing argument. This thesis will be first and foremost, a literature study, where the author´s analysis will be the main driver.

2.1 Research questions

It was made efforts into formulating the research questions early on in the research phase. The following list then proved for the overarching architecture of the thesis.

i. Does the security dilemma transmit to cyberspace?
ii. Do digital capabilities provide nation-states with the ability to project coercive force in a geopolitical context?
iii. Is cyber contributing to growing complexities in the foreign policy environment?
iv. Are matters of security and development inexorably linked?
v. Is CCB proliferating conflict in cyberspace
vi. Does cyber contribute as a threat to the established liberal rules-based order?
vii. How can liberal democracies defend themselves against cyberattacks without triggering escalations?

The primary premise will be that the security dilemma as a concept central to how states interact in a geopolitical context, outlined in an international security framework (Baylis, Smith, & Owens, 2017; Dunne et al., 2016; Norheim-Martinsen et al., 2019).

Three of the underlying premises are that there are definitional differences on what cyber is. That the security dilemma has traversed into cyberspace as another domain of war (Buchanan, 2016), the other domains being sea, air, land, and space (Crowther, 2017, p. 63). Furthermore, that ICTs are integral to current and future sustainable development processes (Utenriksdepartementet, 2017). The Norwegian foreign service defines the internet as the ´superstructure on which all other infrastructures depends`(ibid).

Cyber challenges conventional approaches in the social sciences. This is due to the multiple levels of cyberspace (Deibert, Rohozinski, & Crete-Nishihata, 2012, p. 6). By investigating how international power relations both in and outside of cyberspace are shaping security and

development strategies. The thesis concludes that there is a need to bridge the security/development communities further to create better security strategies for long term solutions in both local, regional, and global contexts.

The research questions were formulated early in the process to steer the initial research phase better. However, the research question and the following sub-questions were not fixed at the start of the project. They were allowed to be fluid throughout the research and writing process with the intent that the questions could evolve as the work progressed. They continued to serve as useful guidelines throughout the entirety of the project. However, like the main title of this work, they have changed throughout this project (Bryman, 2012).

The leading case will be Russia´s broader information warfare (threshold warfare) campaign against the West. Russia´s threshold warfare campaign is designed to use asymmetrical means to combat, destabilize, and seed mistrust against western political and military alliances. Who is characterized by Russian military doctrine as a conventional stronger enemy (Giles, 2016). Threshold or hybrid warfare are both terms used to describe actions taken by a state that does not directly give the justification of jus ad bellum (RUSI, 2019). Following this will be a set of selected exemplifying cases. These cases carry the ´objective to capture the circumstances and conditions of everyday situations` concerning the research questions (Bryman, 2012, p. 62). Some of these will be the Russian attacks on Estonia in 2007 and Georgia in 2008, the case of Stuxnet, and the Russian involvement in the US 2016 presidential election. All of this will be addressed at further length at a later stage.

By supplementing and combining methods and cases, the project will have increased flexibility. By utilizing the potential of having different approaches complementing each other, the overall argument will be better served (Thagaard, 2013, p. 18). This combination of multi- or mixed-method is a well-established and popular style of supplementing different research methods (Gerring, 2017, p. 144).

Sources will be provided by different theoretical and institutional schemes. These different theoretical approaches will vary both within and between disciplines. This will be reflected in the data collection. The literature is not based strictly on academic sources, but also from key state and non-state actors. This includes multilateral bodies such as the UN, EU, NATO, US, and the UK. Also, secondary sources, predominantly through academic journals, books, and web-based sources, will provide a critical addition. In conjunction, these factors will help overall, providing a

positive effect in terms of confidence in the inclusive findings of the thesis (Bryman, 2012, p. 386; Thagaard, 2013).

Reflexivity will be an essential issue (Bryman, 2012, p. 388). It is primarily coupled through the emphasis on transparency by a clear methodology, research process, and data usage. This will be of critical importance to ensure the overall reliability and validity of the thesis (Bryman, 2012, p. 62; Gerring, 2017, pp. 208-211; Thagaard, 2013, pp. 22-23). Some of the steps taken to ensure this will be to clarify the theory relating to the security dilemma while simultaneously having a clear, consistent, and coherent argument through this thesis. Also, by providing a case selection that will give detailed practical examples to work in parallel with the theory to provide a more coherent argument, ultimately strengthening the conclusion and thus the hypothesis. A thorough and extensive data-collection will be vital, which includes the ability to re-visit and re-trace any steps that have led the argument to its ultimate conclusion (Gerring, 2017, pp. 209-210).

The thesis will be limited in latitude. Thus, it is acknowledged that it will be out of the scope of this thesis to thoroughly address all critiques of different subjects that will come up throughout this thesis. Such critiques can be typically critical theoretical approaches, such as a post-colonial, -structural, or -modern take on the security-development nexus. The concept of the security dilemma, which will carry significant weight through the thesis, is often linked to the realist conceptions of international relations. This thesis is not a realist theoretical conception. It will, therefore, not spend significant time critiquing the conceptual standpoint of realism. It does, however, carry properties of an eclectic approach to achieve its primary goal. That is to connect the development and security community better to adequately address security issues vital for both camps, on how to manage digital risks and opportunities with tolerated levels of conflicts. The data collected is then fused and analyzed in an interdisciplinary manner between international relations, security, and development studies. By doing so, a wide arrange of sources is needed, including the need not to adhere to one specific dogma (Barnett & Duvall, 2005, p. 45). Though the thesis statement is an interdisciplinary question, the research question is *concretely* rooted in development practices for human security - facilitating both local, regional and global development through strengthening digital infrastructure and the regulatory space that ought to govern it. The security-development nexus is a well-established concept based on the inextricably linked relation between security and development (Ferguson, 2011; Keukeleire & Raube, 2013; Stern & Öjendal, 2010).

On the other hand, this dissertation will, in some respect, be conceptual. By placing the argument in both historical and contemporary settings. It will make limited attempts at making predictions

on future trends and directions. This puts increased weight on the need for a rigorous process to shore up the validity of this thesis.

2.2 Thesis summary

The following section will provide a brief summary of the main premises and the literature to support it. It should be read as a condensed version of the thesis with its primary literary sources.

The observation that there is an information revolution is something of the past. The revolution is over, and we are now inhabitants of a world where we rely (from the ground up) on all things digital. This has, however, brought challenges with it in terms of how we think about development processes in both contemporary and future settings (Egel et al., 2019). From a security/development standpoint, the UK's 2010 National Security Strategy sums this up by stating that ´Britain is both more secure and more vulnerable than in most of her long history.` Mainly due to its open society being more networked than ever before (Cameron, 2010).

The security dilemma is a crucial concept in the analysis of explaining how states act in the international system; it is thus a fundamental part of international relations theory (Baylis et al., 2017; Booth & Wheeler, 2007; Browning, 2013; Dunne et al., 2016). What this entails is that as a state seeks to increase its security, it effectively undermines the security of its neighboring states (Booth & Wheeler, 2007; Herz, 1950; Jervis, 1978, 1989; Mearsheimer, 1990; G. Snyder, 1984). The concept of the security dilemma is now digitalized, and we are currently experiencing digital security competitions (Buchanan, 2016, 2020; Cavelty, 2014; Deibert & OpennetInitiative, 2010).

Within this new domain of cyber, the security dilemma plays a part in a current ongoing information war, which is a part of the security/military doctrine on cyber (Cameron, 2010; Macron, 2017; NIS, 2019; Trump, 2017). On the role of cyber and warfare, the concept of cyberwar has different schools of thought. Some, like Arquilla and Ronfeldt (1997, 2001); R. A. Clarke and Knake (2014); Schwartau (1995, 2000) think that cyberwar *will* take place. Not only that, it will take place, but it is also currently ongoing, by emphasizing the revolutionary power of the digital domain. Other, more conservative voices, Gray (1999); Lonsdale (2016); Rid (2012) focuses on a more strict Clausewitzian historical analysis. Here the central premise is that cyberwars have never happened and are also unlikely ever to occur. Mainly as the conditions of war are not met in cyberspace (ibid).

However, while it is not constructive to warn of a ´cyber Pearl Harbor` (Stavridis, 2017), in a current complex and volatile security environment, where escalatory measures are a distinct characteristic, the intensity of cyber-attacks as tools in inter-state conflict is increasing (DSB, 2019b; NIS, 2019).

The creation of Cyber Capacity Building came as a tool to mitigate some of the digital challenges posed by an increasingly digital world. This digital world also provides challenges related to its uneven distribution of what has been labeled technological maturity (ITU, 2016; Muller, 2015; Pawlak, 2014; Pawlak & Barmpaliou, 2017). Technological maturity is the level of sophisticated technological integration in society. CCB is connected to how we traditionally understand capacity building, as mechanisms to achieve acceptable levels of state capacity to deliver core functions (Donais, 2009; Hameiri, 2009; Pouligny, 2005; Wilén, 2009). Thus these concepts play an integral part in terms of playing a dynamic role in sustaining national sustainable developing processes (UN, 2019a).

In terms of norms building, regulation, and customary law, with the application of international law to cyber warfare. The Tallinn manual, and subsequent Tallinn manual 2.0 along with the UN GGE process, are the best and most robust attempt to establish set of a regulatory framework to this inherent unregulated digital space (Giles, 2016; GIP, 2019; Schmitt, 2013, 2017; UNGA, 2013; Venkataramakrishnan, 2019). Today, there are no international ratified agreements regarding state behavior in cyberspace (Henriksen, 2019; Singh, 2019).

However, the development community has not addressed how it will benefit by incorporating security studies into its body of literature, which makes in large parts up the silo mentality that needs to be addressed. Development studies, in general, have classically been reluctant to address security issues (Beall et al., 2006; Benjaminsen & Svarstad, 2009; Chandler, 2007; Pawlak & Barmpaliou, 2017; P. Williams, 2008).

There exists an entire body of literature referring to the security-development nexus. Much of which sees the bridging security and development as a potential for a more coherent and well-managed policy on many of the complex issues we face today, such as conflicts, peacekeeping operations, fragile states and societies, great power rivalries and politics. With the development communities´ strong ties with the NGO sector as a primary example (Allen & Thomas, 2000; Benjaminsen & Svarstad, 2009; Rigg, 2007; Shannon, 2009). As the role of NGO´s has a strong presence in conflict zones, connecting development and security concepts is imperative in areas where the need for human security is at its highest (Beall et al., 2006; Chandler, 2007). The

development community´s intimate knowledge of certain specific geographical locations should make them a highly valued partner in the creation of security strategies. Having a more comprehensive understanding of the people who occupy the space on which one is formulating said strategies are critical.

It then requires a stronger push towards creating bridges between the communities, who have overall shared interests and goals in mind. By focusing on such shared interests, more coherent strategies can be formulated. These are that security is first and foremost political. Meaning peace (security) is not just the absence of conflict, but about creating an environment where sustainable political solutions can flourish.

3. Back to the Future? a Digital Security Dilemma

This chapter will lay the foundational premise of this thesis. That is to extrapolate how the security dilemma is thought of, its theoretical underpinnings and real-world applications. It will highlight how security competitions works as an underlying premise in state interactions in the international community, and that the national interests are a key driver in terms of foreign policy. It will briefly discuss sovereignty, the Cold War and development institutions as working concepts which have been created through the idea of the national interest and security competition. It will go on to highlight some of the implications that comes from societies being more technological integrated, in terms of vulnerabilities that work in conjunction with ICTs. As the digital domain remains fundamentally an ungoverned space. There exists latitude for actors to conduct actions that though would not constitute jus ad bellum, it is certainly characterized as acts of aggression. It will also devote space to the term hybrid warfare, which is a terminology used to exemplify some of the modern challenges that security competitions has brought forth. That is that acts of aggression can be done to a larger extent without the fear of retaliation. This is due to the opaque nature of the digital realm. Lastly it will conclude with the importance that the elements that have been addressed in this chapter relates to human security. Including how important it is to maintain a continued focus on fundamental rights to ´life, liberty, and the pursuit of happiness.

3.1 Security competition

The security dilemma entails that when a state increases its security, it effectively decreases the security of other states (Jervis, 1978). It was first articulated by Herz (1950), who wrote of the bipolar world driven by cold-war logic in the 1950s. In which constellations of interconnected social groups, forms the ultimate unit of political life – even though groups are organized into societies, there still exists no higher authority to exert order (in Weber´s terms ´a monopoly on violence`) onto those groups. Thus, with the absence of a leviathan, the structure of the international is, therefore, inherently anarchic. This condition of anarchy then is understood as the Greeks framed it, not as chaos, but as ´without a ruler` (Dunne et al., 2016, p. 68). The

security dilemma is manifested through such political entities, as they seek security concerning other (possibly hostile) entities (Booth & Wheeler, 2007; Jervis, 1978; Sørensen, 2007, p. 359).

This seeming paradox manifests itself when a state seeks security and takes the necessary precautions to achieve this. Through increased defense spending with the overall aim to increase its offensive/defensive military capabilities, it effectively decreases the security of the neighboring state. Who then sees the increased threat levels corresponding to the former states increase in such capabilities, and thus regards their capabilities vis-à-vis the first state in question diminished in a zero-sum calculus. The response, in this case, would be for the latter state to match or supersede the capabilities of the former state (Herz, 1950; Jervis, 1978). This is now entering an escalatory dynamic, most often characterized as an arms race.[6]

Sun Tzu opens his Art of War by declaring that ´war is a matter of vital importance to the state; the province of life or death; the road to survival or ruin. It is mandatory that it be thoroughly studied` (SunTzu, 2005, p. 91). For the state that is increasing its security potential, providing assurances to neighboring states that the security apparatus put in place are not offensive tools, is not plausible. This is for the specific purpose that defensive and offensive measures most often are interlinked and can be used for both purposes (Browning, 2013, p. 20; Jervis, 1978; Mearsheimer, 1990; Walt, 1998; P. Williams, 2008, p. 21). Its core emphasis lies in the notion that it is impossible to know intentions, especially future ones. It is thus the duty of the state to ensure that its sovereignty and integrity is safeguarded against external/internal threats, as well as to ensure both the political freedom and action for its civilian population (Forsvarsdepartementet, 2015). In terms of a state´s modus operandi, it is perhaps most clearly articulated by Lord Palmerston´s remarks in the House of Commons in 1841, where he noted that; ´we have no eternal allies, nor do we have perpetual enemies. Our interest is eternal and perpetual, and those interests it is our duty to follow` (Palmerston in D. Brown, 2011, p. 312). Put plainly; it will be directly irresponsible to base national security on the goodwill of other nations.

The security dilemma then suggests that the world consists of independent states, and there is no higher authority to govern them. This leads to an inherent state of anarchy, or uncertainty, which means that states are dependent only upon themselves for survival. Because of the ever-present possibility that a potential state will at one point in time project some form of coercive force onto another state (Buchanan, 2016, pp. 3-4; Clark, 1989, p. 145; Halperin, 2004, pp. 230-231;

[6] Where a ´race between hostile nations to accumulate or develop weapons, in an ever escalating race or competition` (Merriam-Webster, 2019).

Mearsheimer, 1990, p. 12). By creating an ever-present state of readiness to mitigate such power projections are, therefore, essential for the state to ensure its integrity and survival (ibid). The defense of its territorial borders and the safety of its citizens are thus the state´s most important tasks. Its ability to ´deal with and handle crises, armed conflicts, in both its own and neighboring allied areas must be given utmost priority` (Forsvarsdepartementet, 2015, p. 1).

The foundational reality of the concepts lies in its engagement with the ´existential condition of uncertainty` which characterizes all human relations. From micro to macro levels, these human relations, because of insecurities described through the security dilemma, often shapes the interactions on the most significant and most violent of stages – which are central themes in international politics (Booth & Wheeler, 2007). The core tenet of the security dilemma as a principle has ´proven robust,` and as a concept are continuously applicable in contemporary settings from discussing cyberspace, nuclear war, or non-state ethnic conflict (Booth & Wheeler, 2007; Buchanan, 2016; Herz, 1950; Jervis, 1978; Posen, 1993).

Though *it is not deterministic*, states fall into security competition by trying to ensure its safety and thereby decreasing the relative security of its neighboring states, leading to what is better known as security competitions. These can exist on multiple levels, with the mainstream depiction being arms races. Typically explained through nuclear proliferation and MAD deterrence theory, using the Cold War as the classic backdrop (Browning, 2013, p. 20; Buchanan, 2016, p. 3; Jervis, 1989; Mearsheimer, 1990). This is oriented explicitly between the bipolar political reality that existed between the two superpowers of the Cold War, namely the US and the Soviet Union. With the newly developed atomic bomb, showcased individually with its dual usage, and the ultimate conclusion of its destructive power on the Japanese cities of Hiroshima and Nagasaki in 1945, in the closing stages of WWII. The Soviet Union, now the Russian Federation, responded with its first test of an atomic weapon in 1949, which raised significant levels of fear in Western Europe. This led to a domino effect prompting western countries such as Britain in 1952, and France in 1960 to produce a nuclear arsenal of their own. Later, China, India, and Pakistan would also procure a nuclear arsenal, followed then by Israel.[7] North Korea[8] is the latest installment in the club of countries that possess nuclear capabilities (ACA, 2019b; SIPRI, 2019a). With the end goal

[7] Israel has not publicly admitted possessing nuclear weapons. It is estimated that Israel have possession of around a hundred nuclear warheads (SIPRI, 2019a).

[8] North Korea has an estimate of twenty to thirty nuclear warheads (SIPRI, 2019a).

of achieving "security" through deterrence, which states, ´if you annihilate us, we will have time to annihilate you,` or mutually assured destruction (MAD) (Browning, 2013; Jervis, 1989).

Similar to the arms race, which was a defining characteristic of the Cold War, we are now witnessing security competition unfolding both, in and outside, of cyberspace which is taking place in both conventional and unconventional spaces and weaponry—illustrated in the same way as described through nuclear proliferation and deterrence theory. Now, states have added its engagements to the digital domain, causing a *digital* arms race, and a digital security competition (Buchanan, 2016; Jervis, 1978). This is important when discussing CCB and the security/development nexus. This will, however, be addressed at a later stage.

In the digital age, the security dilemma does not just account for specific regions or geographically fixed locations, and it does not only affect a neighboring or regional located state but is genuinely global in scale. This is not to say that power projections were not global before the rise of the internet. However, the digital element has brought forth a new domain or dimension to consider – as the levels of interconnectedness experienced today caused by globalization have effectively changed how and the speed in which information travels (Castells, 2000; Cerny & Prichard, 2017, p. 379).

The digital security dilemma is now at a point that has caused both state and non-state actors to take severe steps to try and make their systems more resilient to mitigate external influence. Through compromising critical infrastructure and maliciously influencing domestic political agendas, cyber threats and related challenges have come as a consequence of the information revolution which arguably weakens sovereignty and, consequently, the security of the state (Deibert & OpennetInitiative, 2010, p. 3; Egel et al., 2019; Herrera, 2010, p. 17). In the policy world, this transmutes to practices of the type of arms races described by Jervis (1978).[9]

---

[9] This kind of rank-ordering is not entirely an analyst's invention, as is shown by the following section of a British army memo of I903 dealing with British and Russian railroad construction near the Persia-Afghanistan border:

The conditions of the problem may . . . be briefly summarized as follows:
a) If we make a railway to Seistan while Russia remains inactive, we gain a considerable defensive advantage at considerable financial cost;
b) If Russia makes a railway to Seistan, while we remain inactive, she gains a considerable offensive advantage at considerable financial cost;
c) If both we and Russia make railways to Seistan, the defensive and offensive advantages may be held to neutralize each other; in other words, we shall have spent a good deal of money and be no better off than we are at present on the other hand, we shall be no worse off, whereas under alternative (b) we shall be much worse off. Consequently, the theoretical balance of advantage lies with the proposed railway extension from Quetta to Seistan.

Explained through converging the security dilemma with such concepts as Rousseau´s stag hunt, and the prisoner´s dilemma, to explain how the security dilemma came to fruition (Jervis, 1978, pp. 167-172). During the Cold War, there was a consensus among national leaders that nuclear weapons had changed the dynamics of the national security environment, though how to manage it remained disputed.

> The lack of an international sovereign not only permits wars to occur, but also makes it difficult for states that are satisfied with the status quo to arrive at goals that they recognize as being in their common interest. Because there are no institutions or authorities that can make and enforce international laws, the policies of cooperation that will bring mutual rewards may bring disaster if they do not. (Jervis, 1978, p. 167).

So, in the act of ensuring one's security, it creates in effect the potential of insecurity, as this happens at the expense of others. The response for the pressured state is to do what is considered necessary, which is to react too, and counter the threat posed, and to respond in kind. At this point, all roads lead to a ´perpetual security competition` (Mearsheimer, 2016, p. 54; G. Snyder, 1984, p. 461). Due to the inherent a lack of trust in the international state-system where at the core lies the notion that security is a *relative concept* - ´all actors cannot have more of it` (Baylis et al., 2017, p. 102; Dunne et al., 2016, p. 353; Kassab, 2014, p. 65).

Thus sovereignty and security competition has been a central contentious issue in a world structured by a Westphalian definition of sovereignty - created after the thirty years war, and the subsequent peace at Westphalia in 1648 (Croxton, 1999; L. Gross, 1948; Heller & Sofaer, 2001; Maurer, 2018, p. 3). Herein lies the concept of sovereignty as it was first defined, and the notion of the state had, in effect, a new meaning. In this Westphalia definition, ´sovereignty` is defined as ´a political entity´s externally recognized right to exercise final authority over its affairs` (C. Brown et al., 1996, p. 2; Croxton, 1999, p. 570). This is the prelude to how we interpret and conduct our analysis of international relations with its European/Westphalian system of state organization, and its definition of sovereignty (Holmes & Rofe, 2016). Today, Article 2(7) of the UN Charter is that of non-interference - in matters ´within the domestic jurisdiction of any State` (UNSC, 2020). The Westphalian definition of sovereignty is arguably not a reflection of the modern state system and contemporary understandings of sovereignty as there was no sense of

W. G. Nicholson, "Memorandum on Seistan and Other Points Raised in the Discussion on the Defense of India," (Committee of Imperial Defence, March 20, I903). It should be noted that the possibility of neither side building railways was not mentioned, thus strongly biasing the analysis (Jervis, 1978, p. 167-168).

international law, which means, for example, that integral sovereignty was severely restricted in any modern terms (Biersteker, 2002; Chandler, 2001). It is, however, essential to address the concept of sovereignty due to the paramount position it holds in the international system (C. Brown et al., 1996, pp. 1-2; Krasner, 2004), and how the world is structured in such an image - through a series of political entities of sovereign states. The concept of sovereignty, therefore, cannot be detached from the international state-system. Alongside with how national interests shape the foreign policy of individual states.

Developmental policies cannot escape how foreign policy shapes outcomes on both the micro and macro levels. Thus, with an emphasis on sovereignty, its ensuing governance processes and the importance of the concept´s foundation seems meaningful. This also comprises of how the states of medieval Europe transformed the continent, and later the rest of the world – this includes how sovereignty was the initial prelude to the age of colonization (C. Brown et al., 1996; Chandler, 2001). As European empires respected (to a certain extent) the notion of sovereignty amongst each other while infringing with impunity on the sovereignty of others (Strang, 1990).

This is not to say that the European powers did not fight amongst themselves, quite to the contrary. Tilly (1990) argued the notion of the war-making state-making concept, through early European state-making processes and the subsequent bellicose literature. Tilly´s famous aphorism ´war made the state, and the state made war,` are an influential argument in comparative macrosociology (Brian D. Taylor & Botea, 2008, p. 27). The competition between the fragmented warring kingdoms of medieval Europe, initiated the winners in Europe to become global-reaching empires (Ferguson, 2011).

This, however, did not happen in isolation. Brian D. Taylor and Botea (2008) takes this *crucial* fact into account, explaining that the political development of 15th century Europe is also linked with the failure of the states that did not survive. A strong sense of social Darwinism can be used to describe the process of Europe´s ´war-centric account of state development` (Centeno in Brian D. Taylor & Botea, 2008, p. 29). For a war centric account to be valid in a contemporary state-making enterprise, certain vital factors need to be present, that is, a ´reasonable level of social cohesion` prior to a war. Also, a ´unification around a national ideology.` There is a specific need for political and national coherence, which in Europe came as a consequence of war. Tilly's aphorism should thus instead read as *the state made war, and war made the state* (Brian D. Taylor & Botea, 2008, pp. 28-29).

Finally, in relation to the security dilemma the classic point of the Thucydides Trap should be mentioned. If only in passing. Allison (2017) portrays the account of Thucydides and the Peloponnesian War and applies the concept of the Thucydides Trap. Particularly with the rise of China, and how this will affect the dominant position that the US holds in the international system. Here he elaborates on how the security dilemma echoes through the ages through the concept of Thucydides trap. The trap is a depiction of where a ´rising power threatens to displace a ruling power` (ibid, p. 6). Thucydides describes, not the trap in itself, which is a product of IR. However, what Thucydides described was that *´it was the rise of Athens, and the fear this instilled in Sparta that made war invadable`* (Allison, 2017, p. 7; Thucydides, 2009, p. xiv).

What Thucydides describes, is the Peloponnesian war between Sparta and Athens 2500 years ago. Thucydides, an Athenian general, and historian details the 27-year long war, and his seminal work is still widely utilized (Cartledge, 2016; Jackson, 2013). What this trap describes is that the "ruling power" have a *difficult* time relinquishing power peacefully to the displacing power (Allison, 2017). Thucydides trap in a contemporary setting is used in the analysis of how US-Sino relations will dominate the international arena in the foreseeable future. Exploring the possibilities of armed confrontation between the US and China as China´s military, economic and political power grows, threatening to undermine US supremacy (ibid).

3.2 The creation of "development" institutions

The history of the colonial mission also shrouded the multilateral institutions set forth after the end of WWII, such as the Bretton Woods institutions and the United Nations. These institutions both made and governed what constituted international law, norms, and practices, ought to be viewed as predominantly western products. Moreover, serving the interests of its creators, primarily being western countries lead from Washington. Again the Bretton Woods institutions and the UN were set up to promote such interests, more than its (perceived) foundational multilateral mission (Bulmer-Thomas, 2018, p. 140) – The victors of WWII got a permanent seat at the UNSC, also known as the P5. To exemplify just how adjusted the new institutions were to western interests is to call attention to how the US did not have to use its veto in the UNSC until the 1970s. During the ongoing Cold War, the US found ways of circumnavigating the Soviet veto by using procedure rulings in the General Assembly, rather than in the Security Council. With a safe majority secured in both the general assembly and in the security council (through France and Britain). Through such factors, the US essentially did not have to exercise its veto. Due to

this specific political reality, the US had strong incentives, backed by its national interest, to prevent any new nations, who might be sympathetic to the Soviet cause, from joining the UN. However, with the proliferation of new states emerging in a post-colonial world, this was beyond any direct US control. Subsequently, the US could no longer dictate the UN members list (Bulmer-Thomas, 2018, p. 144).

Escobar (1995) critique of classical development thought was founded in how the US consolidated its power after WWII to control international economic and political output, for what was labeled security necessities. This analysis, based on Foucault's power relations, emphasizes the world as constructed of actors seeking to utilize their relative political power capabilities to shape desired political outcomes (Barnett & Duvall, 2005; Benjaminsen & Svarstad, 2009, p. 316; Bulmer-Thomas, 2018; Escobar, 1995).

What this describes is how the intricacies of the security dilemma function in practical terms. Through the UN, the US was able to achieve several of its strategic goals, articulated by their contemporary national interest, through both diplomatic channels and military means. The security dilemma is then not something that always is explained through guns, bullets, bombs, and aircraft carriers. Though such a framework most often reflects a *realpolitik* approach and understanding of international politics. That is, coercion is often the most effective mean of exerting one's will, and thus, the largest military has the principal capacity to extend its coercive capabilities - while simultaneously being (in no small extent) immune to external pressures. In large part, because it would be considered suicidal for anyone to directly confront a significantly superior force (state) in such terms (Frazier & Stewart-Ingersoll, 2010; Mearsheimer, 2001). However, in taking such an approach, we need only to discuss the Vietnam war to see that this perception is severely skewed. Vietnam is a classic example of asymmetric warfare, where the dominant power did not achieve victory. When the North Vietnamese army engaged US forces in conventional open battle, they often suffered severely, as early encounters in the war during 1965 testified. However, when the Vietcong kept to guerilla tactics and prepared for a long-term engagement, the Americans were vexed and frustrated` (Freedman, 1998, p. 58), ultimately losing the war. In retrospect, lessons identified are highlighted. Petraeus (1986, p. 46) draws as a principal component that the experience of Vietnam provided the US with the ability to see the ´limits of what military power was able to accomplish in world affairs`[10] with more contemporary examples being Afghanistan and Iraq.

[10] Coercion theory details how coercion might be thwarted, even by material weaker opponents (Biddle, 2020).

The security dilemma does not echo such a limiting approach. That is, the largest military force is secured victory in all aspects. Military dominance does not alone secure desired outcomes. And therefore, a single prism of conventional military dominance is not adequate to deal with complex political challenges. Actions to ensure the most optimal outcomes need not always be through confrontation between states and their armed forces. Alternatively, how states interact on the international stage with the following consequences, through a perceived security competition (real or not) in and a zero-sum political reality – are achieved just as well though incremental steps taken through diplomatic channels, to ensure more optimal outcomes in this perceived zero-sum game. Such actions taken were highlighted by US practices concerning the UN´s formative years.

Furthermore, exemplifying how the national interests and the security dilemma works in practice. This principle of statecraft was also the modus operandi of the US foreign policy of Soviet containment during the Cold War, ultimately based on Kennan´s *long telegram* (Bulmer-Thomas, 2018, p. 147).[11] This is not to say that US-Soviet relations only turned hostile in the aftermath of WWII. Both the ´power-political` and the ´ideological` bases for the US-Soviet hostilities originated in the 1914-1918 period - in the immediate moments of the Soviet conception springing from the 1917 Bolshevik revolution. The Cold War has its origins in the opposing formations of what the international order should look like, be it in Lenin´s or Wilson´s framework with each respective base located either in Washington or Petrograd (Clark, 1989, p. 147).

Just as Kennan´s telegram laid out the strategy of Soviet containment post-1945, it is still hardwired into the modus operandi of US foreign policymaking. In the 2017 US national security strategy, there is a quite remarkable section that states that

> Authoritarian actors have long recognized the power of multilateral bodies and have used them to advance their interests and limit the freedom of their own citizens. If the United States cedes leadership of these bodies to adversaries, opportunities to shape developments that are positive for the United States will be lost. All institutions are not equal, however. The United States will prioritize its efforts in those organizations that

[11] Kennan (1946) long telegram was a telegram sent through diplomatic cables from the US embassy in Moscow to Washington. In this telegram, security analyst George Kennan proposed the policy of containing the USSR in economic, military and spheres of influence, which led the US to seek its main foreign policy objective of containment against the USSR. Which meant in all terms to minimize Soviet external influence, including undermining domestic Soviet policies.

> serve American interests, to ensure that they are strengthened and supportive of the United States, our allies, and our partners (Trump, 2017, p. 40).

Thus far, the emphasis has been on how the security dilemma exists between states. From this, it falls naturally also to include the elements from where those states came. For this reason, the colonial and post-colonial era needs to be addressed, for the purpose of the contentious and precarious nature that this topic entails. This relates to how security issues are framed, including how these issues are viewed through the prism of intersubjective national interests (Baylis et al., 2017; P. Williams, 2008). Primarily on the topics of the nation-state and sovereignty.

When Weber defined states' legitimate monopoly on the use of force - this was effectively a by-product of the concept of sovereignty as defined in 1648. That is that the legitimate use of force is linked to the European emergence of the nation-state. This Westphalian notion of the state and sovereignty is the one that today defines our concept of the nation-state and became ´codified globally` after WWII, through the UN Charter (Croxton, 1999; Maurer, 2018). Sovereignty signifies the legitimization of a state's control of a specific territory. In the international state system, states recognize other states final legitimate authority in this given territory, and only they are the actors who can act with that legitimacy within this system (Croxton, 1999, p. 570; PCA, 1928, p. 838; Schmitt, 2013, 2017).

The security dilemma exists when an increase in security, often through military preparations in one state, create an ´unresolvable uncertainty in the mind of another.` Also, it is essential to acknowledge that the uncertainty lies in the fact that there is no guarantee that the preparations are defensive or offensive. That is to change the status quo in order to pursue an advantage (Wheeler & and Booth in Baylis et al., 2017, p. 102).

As stated previously, this thesis focuses on the core concept of the security dilemma – an axiom, to international relations theory (Booth & Wheeler, 2007; G. Snyder, 1984, p. 461; Sørensen, 2007, p. 357). It is critical to stress that this specific concept *definitely* transmits to the realm of cyberspace (Buchanan, 2016; Kiggins, 2013, p. 170; Sanger, 2018), where the contemporary reality is, that cybersecurity institutions remain highly underdeveloped (Kiggins, 2013, p. 170; Nissenbaum, 2005, p. 62). Shortly after the internet was developed and commercialized in the mid-1990s, states saw the potential that the internet provided. Not only in its development and communication abilities but as a ´platform to project coercive power, with an exponentially increasing range` (Maurer, 2018, p. 4).

A fundamental continuum to the international state order has been how to counteract this security dilemma (Buchanan, 2016, p. 7; Cerny, 2000, p. 623). Since there is no supra-national government that can provide any guarantees for security, in a Weberian sense, there are no guarantees that if conflict were to break out, anyone would come to aid the state in question. In this inherently anarchic structure, a self-help mentality is continuously being addressed (Jervis, 1978; Mearsheimer, 1994).

> Hereby it is manifest, that during the time men live without a common power to keep them all in awe, they are in that condition which is called war; and such a war, as is of every man, against every man … Whatsoever, therefore, is consequent to a time of war … and which is worst of all, continual fear, and danger of violent death; and the life of man, solitary, poor, nasty, brutish, and short.[12]

What Hobbes describes is a verbal social account of a *homo homini lupus* condition, that does not necessarily preclude social cooperation. However, the terms of solidarity and cooperation are rather elements in a conflict situation. Elements with specific functions for the ´purpose of the consolidation and strengthening of particular groups in their competition with other groups` (Buchanan, 2016, p. 18; Herz, 1950, p. 157). Though being a pessimistic, realist view on the international arena, it is still a core element in theories of international relations (Browning, 2013, p. 14; Hopf, 1998; Jervis, 1978; Machiavelli, 2013; Mearsheimer, 2001; Weldes, 1996).

Why is it then that we do not see an even more violent or conflict-ridden operating environment? States are not as fragile as the state of man, which Hobbes described (Jervis, 1978, p. 178). Also, in an environment poised with insecurities, it creates foundations for cooperation. Cooperation can take the form of bilateral or multilateral agreements that are meant to serve the interests of the state concerning fellow states, and in doing so, are in the continuous interests to regulate agreements facilitating a continuum of the treaties in question that serves mutual interests. Other examples are the creation of international bodies such as the UN, EU, NATO, and the AU. These are multilateral organizations that see integration and cooperation between states as a primary conduit for international peace and security (Biscop, Francioni, Graham, & Ortega, 2005; Forman & Segaar, 2006). NATO is a security organization created to balance state interests in security competition vis-à-vis the USSR and its (at the time) parallel organization, the Warsaw Treaty Organization, or the Warsaw Pact. NATO is also a political organization, as well as a military alliance. In classic Clausewitzian terms, war is just politics by different means (Clausewitz,

[12] Hobbes (1996, p. 84).

1832). NATO is a continuation of this idea. With the principal premise that it is security in our daily lives that are the key to current and future well-being. It is promoting trust-building between nations with the credibility to back up political agendas with military means (NATO, 2019d). It is still vital to stress that in underlying theories on alliance diplomacy and game theory on the international level. The ultimate defeat relating to the security dilemma is the loss of sovereignty and the possible demise of the state (Jervis, 1978).

THE COMPOSITE SECURITY DILEMMA IN A MULTIPOLAR SYSTEM

Strategies	*Possible Consequences*	
	Alliance game	*Adversary game*
I ALLIANCE C: Support, strengthen commitment ADVERSARY D: Stand firm.	"GOODS" 1. Reassure ally, reduce risk of abandonment 2. Enhance reputation for loyalty "BADS" 1. Increase risk of entrapment 2. Reduce bargaining power over ally 3. Foreclose realignment option 4. Solidify adversary's alliance	"GOODS" 1. Deter, or prevail over, adversary 2. Enhance reputation for resolve "BADS" 1. Provoke adversary; increase tension; insecurity spiral
II ALLIANCE D: Withhold support, weaken commitment ADVERSARY C: Conciliate	"GOODS" 1. Restrain ally, reduce risk of entrapment 2. Increase bargaining power over ally 3. Preserve realignment option 4. Divide adversary's alliance "BADS" 1. Increase risk of abandonment 2. Reduce reputation for loyalty	"GOODS" 1. Resolve conflict; reduce tension "BADS" 1. Encourage adversary to stand firmer 2. Reduce reputation for resolve

(G. Snyder, 1984, p. 469).

On the other side, we are currently witnessing the withdrawal from international agreements such as the JCPOA and the INF treaty. New START will continue until February of 2021. New START can be superseded by succeeding agreements (ACA, 2019a), but in lieu of recent developments in terms of arms control, it is the author´s pessimistic view that also New START will be dismantled. The parties involved being the US and Russia can withdraw from the

agreement by citing that ´extraordinary events related to the subject matter of this treaty have jeopardized its supreme interests.` All the examples mentioned above are considered a direct threat to the directive of the UNSC as being international peace and security.

3.3 Alarmism, or cautionary measures

Today there is no established regulatory framework on state behavior in cyberspace. There are, however, significant potential and common interests in norms building and judicial structures that effectively govern cyberspace. However, national interests often get in the way of this happening, as states see their interests change regarding how geopolitical realities evolve. As of today, cyberspace continues to be a frontier, characterized as a lawless space (Henriksen, 2019; Singh, 2019). This still gives the potential to find new grounds for state interaction, norms building, and customary law. It is essential to assert the importance of multilateral bodies such as the UN and the role it serves as a platform for constructive dialogue on the international level. This includes the position that such a multilateral organization holds on mitigating ´collective action problems in the face of challenges relating to development` (Pike, Rodríguez-Pose, & Tomaney, 2017, p. 161). Also, that cooperation does exist alongside lines of conflict or disagreements, and that in such a context' politics mediate the relationship between institutions and economic performance` (Dellepiane-Avellaneda (2009) in Pike et al., 2017, p. 161). However, Pike et al. (2017, p. 161) acknowledge that history does matter, moreover, that ´critical junctures` exists. This means that those significant events, which include a combination of factors, can disrupt existing ´economic and political institutions.`

Concerning cyberspace and how to administer this new source of technological advancement is challenging. Mainly as it runs parallels in its civilian and military applications, how this technology now is changing global power structures, is not fully grasped (Sanger, 2018, p. xiv).

While analogical cries of an imminent ´cyber Pearl Harbor` (Stavridis, 2017) are unhelpful, it is true that as the prevalence and intensity of cyber-attacks as a tool of inter-state conflict increases, so does the likelihood that such attacks seriously and negatively impact civilians. Former GCHQ director Robert Hannigan has continually called for international agreements and norms building. With the critical premise that there needs to be put in place real regulatory systems to mitigate current illicit behavior from both states and non-state actors in cyberspace. This includes setting up agreements on how to conduct cyberwarfare and hacking by nation-states. Thus, furthermore emphasizing the immense challenges for creating such regulatory systems (Burgess, 2018).

> Now is a particularly difficult time to get any kind of international agreement through because there is so much tension between the major powers. The significant danger is that you end up with a treaty that one side implements and the other does not. That would make things' worse than ever`, further emphasizes that ´it seems inevitable, that physical injury will happen,` when critical infrastructure is attacked. When power and water supplies are tampered with, or air traffic controls, the increased risk for civilians to get hurt are substantial (ibid).

One example of where this could have a dangerous effect is in relation to the usage of the GPS systems. The GPS is a US military developed system initially used to support navigation but is now used amongst civilians for personal purposes in addition to its military use. Currently, both military and civilian parties are dependent on GPS systems (Stickings, 2019) and it is a fundamental component of all types of infrastructures (NASA, 2017). Furthermore, GPS is vital for maritime navigation, missile targeting, and other autonomous systems. They are essential for the ´precision upon which Western warfighting capabilities are based (Stickings, 2019, p. 49). The dependency of the GPS can cause various parties in the use of the system to lean too strongly on it, leaving them vulnerable to outside influence. Since 2017, GPS usage in Scandinavia has frequently been disrupted in conjuncture with military exercises, such as the NATO´s Trident Juncture, during which GPS signal loss was recorded. These disruptions stem from Russian attacks. Additionally, Kirkenes airport is amongst the airports which have frequently experienced GPS disruptions. Though civilian passenger planes carry backup navigation instruments, such disruptions of GPS signals carries dangerous potential as pilots can lose their ability to verify precise positions which is a direct threat to the safety of people on board an inflight airplane (Coultrup, 2019; NIS, 2019, p. 8). In terms of bilateral and multilateral relations, such breaches of sovereignty are not taken lightly (Forsvarsdepartementet, 2015, 2017; NIS, 2019; Singh, 2019; Utenriksdepartementet, 2017).

Today, Russia is devoting sizeable resources to destabilize Europe and the US politically - in Putin´s view of a zero-sum power play (Covington, 2015; Giles, 2019). Fueling polarization is a critical tactic in Russian information warfare campaigns conducted against the West. However, such destabilization efforts work by the use of disinformation carried out through ICTs. As another example, in the Brexit campaign, the targeted advertisement was a vital component where falsified information on how England´s economic and political landscape was undermined and destroyed by foreigners. This had a significant political effect on voters´ decision-making process and turnout. Also, this had an overarching effect that was an influential element behind the Brexit or leave campaign. This does not just have a severe impact on domestic policies but carries significant implications internationally (Giles, 2016; Hobolt, 2016; McGaughey, 2018).

In addition, Russian interference in the US 2016 presidential election was a severe step in terms of its agenda of destabilizing the West politically. Aimed at, and successful in its mission, to further polarize the American populace, the Russian interference was substantial. Through a multipronged ambitious and aggressive CO, Russian operators showcased how controlling and shaping information and narratives can have dire political consequences (Buchanan, 2020, p. 213; R. Mueller, 2019; Sanger, 2018, p. xv). This was done by the ´spread of false information, manipulation of media sources, the creation of propaganda that aligned with preexisting narratives.` The case of Russia's interference in the 2016 election has become a textbook case example of CO (Buchanan, 2020, p. 213). It also included breaching the DNC computer network. Russian entities "directed recent compromises of e-mails from US persons and institutions, including US political organizations," and, "[t]hese thefts and disclosures are intended to interfere with the US election process (Buchanan, 2020; K. P. Mueller, Castillo, Morgan, Pegahi, & Rosen, 2006). Not just targeted attempts at US persons, but also US critical infrastructure.

> In 2016, cybersecurity for electoral infrastructure at the state and local level was sorely lacking; for example, voter registration databases were not as secure as they could have been. Aging voting equipment, particularly voting machines that had no paper record of votes, were vulnerable to exploitation by a committed adversary (SCI, 2019, p. 4)

If this interference was significant enough to change the electoral outcome is hard to say. What is certain is that the current US administration has been destabilizing for the international community for several reasons. In terms of developmental processes specific key issues such as pulling out of the Paris climate accord, the US trade war with China, withdrawing from the Joint Comprehensive Plan of Action, re-imposing strict economic sanctions on Iran, had a significant emphasis on maximum pressure campaigns, including forcing its European to follow suit (Regjeringen, 2018).

With the US retracting from several multilateral agreements, not just in terms of trade deals such as the TPP and NAFTA but also in its involvement within the UN system, severe economic cuts have been made to the UN, as aid has not been a priority to the current US administration. The geopolitical implications are real in the sense of the longevity and repercussions they carry. They are not dissociated as something that is not related to developmental processes but is explicitly connected and needs to be addressed as such. What happens on the macro-level dictates much of what happens at the micro-level and vice-versa. For instance, a lack of cohesion in terms of multilateral responses not just in terms of the JCPOA, but to Russia´s annexation of Crimea is

disturbing. In terms of the international security environment, Ukraine now serves as a test-bed for the Russian armed forces who are currently getting valuable experience in running conventional, as well as unconventional military operations (Giles, 2016). An interesting side note to exemplify the lack of responses to the Russian invasion of Ukraine lies in how the tech giants, Apple and Google, have seeded to Russian pressure campaigns. This is done by these companies who now are recognizing Crimea as Russian territory (Higgins, 2019).[13] These are significant developments in terms of legitimizing the Russian annexation of said territories. Similar pressure campaigns are currently conducted by China to get formal recognition of the South China Sea by using ´speech acts`[14] amongst other means as a wide arrange of methods in order to incorporate the South China Sea into legitimate Chinese controlled waters (Miyoshi, 2012). It is, however, out of the scope of this thesis to adequately address the current situation in the South China Sea in any meaningful way.[15]

On the point of challenges addressing the regulation of international treaties - recent political developments have caused the INF agreement to be dismantled (Kramer, 2019; Manson, 2018; Rose, 2019). For an international community which is dependent on a certain level of cohesion to implement structural frameworks, the new US policies of unilateral actions, and on a broader focus on bilateral partnerships are discouraging. What this explicitly refers to is;

- The US withdrawal from the JCPOA,
- Russian and the US withdrawal from the INF treaty,
- The US withdrawal from the Paris climate agreement,

[13] Apple and Google Maps now show the annexed Ukrainian territories by Russia as Russian sovereign territory.

[14] Language does more than simply say things; rather, we do things with words, hence the term "speech acts." (Anderson, 2018).

[15] The Chinese are constructing artificial islands in the South China Sea with the explicit function to exert military influence and control these waters. For China, the South China Sea are regarded as a core interest. The South China Sea is a strategic waterway that carries more than half of the worlds merchant tonnage. And are an important transit routes for several navies. The example of the escalatory dynamics of the current security competition that is unfolding in the South China Sea are significant. This thesis will *not* address this. But it will stress upon the importance that this development carries in local, regional and international terms. With a particular reference to security competition between the state-actors involved in said region. Including the role of the US both in terms as being a security guarantor for others, and what this means the position that the US holds in terms of military primacy.

- The US tearing up the two-state solution in Palestine by recognizing Jerusalem as the capital of Israel

Such erratic state behaviour comes in a time where political cohesion is needed in terms of how to achieve more stability, not less. Particularly to the processes for creating sustainable norms and legal framework for cyberspace are issues that need continued devotion (ibid). Furthermore, the US withdrawal from the JCPOA (Fitzpatrick, 2017), has severe impacts on Iran´s ability for financial transactions, as well as hitting its energy sector hard. This will mean a severe economic impact for ordinary Iranians who already suffer from worsening economic conditions, and this will also be further accelerated, by the US, re-imposing strict economic sanctions (Davenport, 2019; Dempsey, 2018). From a development perspective, often framed in the light of creating economic opportunities for people, the geopolitical implications of decisions, such as the US withdrawal from the JCPOA, is enormous (van Bergeijk, 2015). For Iran, this will tighten its ability to move and operate in the international arena, thus providing grounds for potential future political tensions. In terms of planning processes, indigenous development approaches have had a significant impact on development discourse and practices with utilities that are highly valuable for local and regional development processes. With a focus on bottom-up solutions grounded in stakeholders on the ground (Pike et al., 2017; Tödtling, 2011). By not sufficiently addressing the external forces pushing on these processes, in this case, highlighted by security-related questions like the JCPOA, it seems hard to create any coherent and robust long-term strategy to promote real, sustainable political and economic solutions in Iran; at least from a development and planning perspectives.

Before the JCPOA was negotiated, there have been several instances where attempts have been made by states in the Middle East to acquire nuclear weapons. In the cases of both Iraq and Syria[16], it ended with Israeli aerial bombardment of these facilities before becoming operational (Follath & Stark, 2009; K. P. Mueller et al., 2006). This is in strict adherence to Israeli defense strategies and its Begin doctrine (Brom, 2005). In the case of Iran, there have been several assassinations of Iranian nuclear scientists (Tobey, 2012), and one of the most notorious cyber-attacks to date, Stuxnet. Stuxnet is the classic example of the application of digital capabilities to conduct offensive military operations. It refers to the malicious computer code that was created to slow the Iranian uranium enrichment program at the Natanz nuclear facility (Bulmer-Thomas, 2018, p. 243). This operation led by the US and Israel attacked Iran´s nuclear facility at Natanz.

[16] The nuclear facility in Iraq was bombed in 1981. The facility in Syria was bombed in 2007.

The cyber worm was smuggled into the facility´s computer systems, where it targeted the operating system, causing over one thousand centrifuges processing nuclear materials, to spin out of control and explode. The operation was conducted to hinder, or at least slow, Iran´s ambition of procuring nuclear weapons by enriching uranium (Buchanan, 2016, p. 31; Bulmer-Thomas, 2018, p. 243; Sanger, 2018).

The JCPOA became a historic agreement in 2015, between the P5+1 (UNSC + Germany) and Iran on its nuclear program. The deal had strict restrictions on Iranian enrichment processes, limiting it to strict civilian purposes, which included a substantial reduction of fissile material. Overall this would remove any possibilities for Iranian break-out capabilities.[17] In return, sanctions that were put in place on Iran due to its nuclear program would, in great detail, be lifted (Bulmer-Thomas, 2018, p. 327). With the US withdrawal from the JCPOA in 2018 and the subsequent reinstatement of sanctions, Iran has resumed its uranium enrichment program (ACA, 2019c), which has seeded grounds for renewed heightened tensions in the Persian Gulf. Being given access to international markets, are critical to any petroleum focused exporting economy and OPEC member, and regarded as a vital necessity for all commercial purposes.

There is no question that international security and development are inexorably linked. Also, climate change is another essential component that affects the dynamic between the aforementioned. Climate change is a substantial part of the development body of literature as its consequence are immensely destructive to people already living in challenging environments (Allen & Thomas, 2000; Benjaminsen & Svarstad, 2009; Jonas, McCann, & Thomas, 2015; Aarsæther, Falleth, Nyseth, & Kristiansen, 2015). This thesis has laid a significant focus on the effect of global leadership roles, and the formative role of the US since WWII. Recent developments with the current US administration seem to withdraw from such leadership roles. One of which is on the climate debate. President Trumps' decision to enact executive powers in respect of withdrawing from the Paris climate accord gives space for alternative leadership roles (Carin & Mehlenbacher, 2010), which seems to contradict the current US national security strategy (Trump, 2017). This also creates uncertainty on the international level in terms of inconsistencies in combating the forces of climate change.

As a final example to emphasize this point, is again the POTUS´s use of executive power to tear up the two-state solution for the middle east (Bulmer-Thomas, 2018). In the case of moving their

[17] Break-out capabilities refer to where the state has the possibility within a short amount of space to develop nuclear weapons.

Israeli embassy from Tel Aviv to Jerusalem. This is a process that will need substantial efforts and will take years; by the time, a different administration will be in the White House. That being said, it is still official US policy, in terms of Palestine, that Jerusalem now is the capital of Israel.

What these examples highlight is the fluid nature of national interests influencing world affairs with consequences that can shape both constructive, as well as destructive outcomes. It does also showcase the possibilities that cooperation between states carries with it and that a retreat from multilateralism should not be the desired outcome in terms of systems in global sustainable developmental processes.

3.4 Hybrid, Grey zone or Threshold Warfare

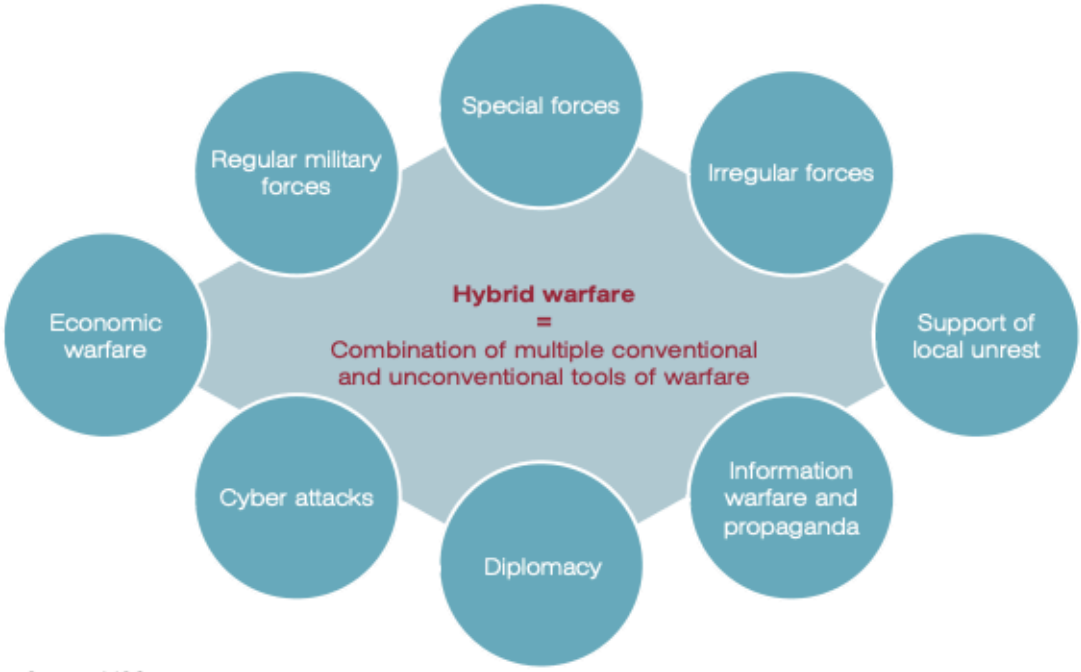
With the changing complexities to our foreign policy environment (Mattis, 2018), the term hybrid, grey zone, threshold, asymmetric warfare, and threats, have gotten significant traction. What this refers to is the ability to strike at an opponent using a myriad of capabilities. Though the concept of hybrid warfare became vogue after the Russian annexation of Crimea, the term hybrid and its effects were coined by Hoffman (2007). Here Hoffman (2007) notes how ´potential adversaries were likely to combine non-conventional forms of warfare – from irregular warfare to terrorism in sequence or simultaneously – to target the vulnerabilities of those militaries` (Hoffman, 2007; Lawson, 2019).

In a contemporary setting, it often refers to being the ability to be engaged in a conflict scenario, and acting within this scenario with means that are considered just under the threshold of what would constitute Jus ad Bellum.[18] Alternatively, potential adversaries have seen that the best way to counter Western conventional military strength is to ensure that it is not used (Lawson, 2019, p. 7). This is showcased by the Obama administration´s failure to respond to the use of chemical weapons in Syria. Specifically, after the Obama administration drew a red line concerning the use of such chemical weapons, this is now put extensively into practice. Such as Russia´s operations in both Georgia and Ukraine, and China´s occupation of islands in the South China Sea (ibid). According to NATO, ´hybrid threats are those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their

[18] ´*Jus ad bellum* refers to the conditions under which one may justifiably resort to war, or the use of force in general; *jus in bello* governs the conduct of belligerents during a war, and in a broader sense comprises the rights and obligations of neutral parties as well` (CUP, 2019).

objectives` (NATO-lib, 2019). Hybrid threats have changed in recent years from predominantly entailing non-state actors and unconventional tactics, to now include state-actors, like the US, UK, Russia, China, Israel, and Iran.

Visualized model of hybrid warfare components (MSC, 2015, p. 35).



This modus operandi is not new per se. That is the employment of conventional and unconventional means to an operating environment. However, the conflagration of coordinated use of security apparatuses, military and non-military institutions are perceived as new, as it is diverging from classical perspectives on warfare. Hence the terminology conventional and unconventional. This concept carries several different strains of language, obfuscating an already cloudy area which does not help to clarify existing complex and multi-dimensional issues (Cormac & Aldrich, 2018; RUSI, 2019). These different explanations, however, tends to mean the same thing. That ´asymmetric` war is;

> when two combatants are so different in their characters, and in their areas of comparative strategic advantage, that a confrontation between them comes to turn on one side's ability to force the other to fight on their own terms…. The strategies that the weak have consistently adopted against the strong often involve targeting the enemy's domestic political base as much as his forward military capabilities. Essentially, such

> strategies involve inflicting pain over time without suffering unbearable retaliation in return (Freedman, 1998).

The absence of an agreement to an appropriate response regarding the employment of such techniques also poses challenges between the US, EU, and NATO (Bredesen & Reichborn-Kjennerud, 2016). This evolving character of conflict is described as *convergence*, which means the merging of the "physical and psychological, the kinetic and non-kinetic, and combatants and non-combatants. So, too, we see the convergence of military force and the interagency community, of states and non-state actors, and the capabilities they are armed with" (Hoffman, 2009, p. 34).

A 2016 study, conducted by CSIS, concluded that the Kremlin had developed a sphere of ´malign economic influence in Europe ´by cultivating what was described as an ´opaque network of patronage,` that is used to ´influence and direct` decision making processes. This political and economic network thrives on and exploits corruption, including gaps in governments and their service deliveries with the primary objective of ´weakening and destroy democratic systems from within`(Conley, Ruy, Stefanov, & Vladimirov, 2019, p. 1). In accordance with Hoffman (2007), hybrid warfare is the ability to use a myriad of techniques to inherently weaken and exploit adversaries' vulnerabilities. State actors like Russia have then adopted such tactics as its approach to counter western dominant military might. One of which is that a political opponent, that being another state, generally requires governmental approval to employ its military as a response to a problem (Lawson, 2019, p. 8). This is particularly important in open democratic societies where the political will of the people, is instrumental in selecting its political leadership. As Clausewitz defined war as a continuation of politics by other means, so did Fanon (1963). ´The art of politics is simply transformed into the art of war; the political militant is the rebel. To fight the war and to take part in politics: the two things become one and the same` (Fanon & Sartre, 1963, p. 105).

As previously stated, hybrid warfare is not something new. The employment of methods such as propaganda, deception, sabotage, and non-military tactics have always been a part of any effort to destabilize adversaries. The concept of hybrid warfare is then rather simple; it is detecting those activities that are just shy of any defined threshold (Lawson, 2019, p. 8). All warfare is based on deception (SunTzu, 2005). These concepts are as old as war itself. However, what is new with what we now have labeled hybrid warfare, is the speed, scale, and intensity. This is greatly facilitated by the exponential scale of ICTs and the global interconnectedness that now exists (Giles, 2016; NATO, 2019c).

> A new type of war has emerged, in which armed warfare has given up its decisive place in the achievement of the military and political objectives of war to another kind of warfare - information warfare (Kvachkov in Giles, 2016, p. 3).

The role of ICTs in hybrid conflicts involves multi-layered efforts to destabilize a functioning state, polarizing the society, and the aggressor most often makes it a priority to be anonymous. It is, therefore, primarily coming to terms with how such processes represent tremendous challenges for open democratic societies (NIS, 2019).

In the Russian construct, there is no difference between the notions of times between war and peace. The information war that we are currently witnessing is in this construct is one component of a much broader information warfare campaign (Brantly & Collins, 2018; Giles, 2016; Lawson, 2019). There are apparent definitional differences between Russian and Western views on conflict. In Russia, warfare is a constant continuum, and the Russian state is constantly maneuvering in a battlespace. Information warfare is thus not something that is confined to a formally declared conflict, or even the initial phases leading into one. Information warfare[19] is an ´ongoing activity regardless of the state of the relations with the opponent` (Giles, 2016, p. 4). The definition used by the Russian Military Academy of the General Staff highlights its own clear definitional difference with its western counterparts. In that, the Russian definition is ´broad, and not limited to wartime` - and the Western on, which is described as ´limited, tactical information operations carried out during hostilities (ibid).

Still, the cyber domain provides ample opportunities to change rapidly, create, and to use information; information operations are, for example, the use of disinformation and misinformation. The creation of narratives that are used (in terms of this thesis by ICTs, but not confined to this specific space) with the main agenda of being politically destabilizing. When countries are at the receiving end of these kinds of operations, it can prove challenging for several reasons. This can be difficult for states to counteract, mainly when there is a concern to ensure that the response is based on purely accurate information. It allows adversaries to get inside states' OODA loop[20] in this area. Much of these operations are targeted at public opinion

[19] Information warfare is not the same as cyberwar. It is the author´s view that describing conflict in cyberspace as a cyberwar is an inadequate idle attempt to describe a very complex phenomenon. The characteristics of the cyber domain are multi-dimensional, meaning that there exists space for multiple accounts to happen simultaneously. Also, the terminology of war in cyberspace is in itself meaningless in terms of how it is used to describe phenomena´s in the physical world

[20] The OODA loop is the cycle observe-orient-decide-act. The approach explains how agility can overcome raw power in dealing with human opponents. It is especially applicable to cyber security and

for political reasons, as highlighted throughout this thesis. It can also be targeting states and states' engagement abroad in aims of impacting moral cohesion (RUSI, 2019). To (Clausewitz, 1832), the ´fog of war` is limiting the abilities for sound decision-making due to the onset of uncertainties

> War is the province of uncertainty: three-fourths of those things upon which actions in War must be calculated, are hidden more or less in the clouds of great uncertainty. Here, then, above all, a dine and penetrating mind is called for, to search out the truth by the tact of its judgment (Clausewitz, 1832, Book one, Chapter three).

Russia does not see *war* or conflict as something that one either engage in or not. Instead, it is a *continuous* process of engagement with adversaries. The terms of war and peace are not meaningless, but they work on a scale where Russia is engaged in an endless "battle" with its adversaries - ´In the Russian construct, information warfare is not an activity limited to wartime … It is an ongoing activity regardless of the state of relation with the opponent - to be waged constantly in peacetime`(Connell & Vogler, 2017; Giles, 2016, p. 4; 2019; Heickerö, 2010, pp. 18-20). Reiterating Clausewitz, war is a continuation of politics with other means (Clausewitz, 1832, p. 87).

There is a real concern that if cyberweapons are used in aggressive terms, spillover effects to civilian systems will be among the externalities (CEA, 2018; McKenzie, 2017; Sanger, 2018). This can cause harm as critical infrastructure is affected both directly and indirectly, such as hospitals or disrupting power supplies. The attacks do not, however, need to be on such a severe level, but can still be significantly damaging due to sheer volume. Information warfare from a Russian perspective includes a vast array of different activities and processes to achieve its goals of undermining its political adversaries through such asymmetrical means. These activities include, but are not limited to, ´steal, plant, interdict, manipulate, distort or destroy information.` The methods for accomplishing this are equally broad in range and includes ´computers, smartphones, real or invented news media, statements by leaders or celebrities, online troll campaigns, text messages, vox pops by concerned citizens, YouTube videos, or direct approaches to individual human targets` (Giles, 2016, p. 4).

cyberwarfare. The goal of the strategy was to execute the OODA loop process more quickly than an opponent in order to infiltrate and disrupt the enemy´s decision cycle (R. Clarke & Knake, 2019).

All states are vulnerable to such activities; a 2015 report to the Norwegian defense ministry concluded on the significance of the threat that hybrid warfare poses.

> Open and trust orientated western societies are vulnerable and poorly equipped to face this type of unconventional or hybrid wars. Countermeasures demand high input, good quality intelligence, high reactionary capabilities, and substantial coordinated efforts across all governmental sectors (Moen, 2016, p. 20).

To lay the foundation for sustainable development practices, the integrity of the state and the state-apparatus are seen as necessary precursors. The state's role as the primary actor for service delivery can easily be compromised due to its reliance on ICT's. Hence any lack in sufficient management of the risks associated with this increased reliance on ICT's can represent a ´point of failure,` threatening to undo development progress. Mainly as economic, institutional, and societal development, are increasingly more reliant on digital technologies (Pawlak, 2014; 2017).

ICTs are now an integral component in several national security strategies (Macron, 2017; Trump, 2017; Utenriksdepartementet, 2017). There are no speculations on whether this will come to fruition or not; this is now a part of the reality of the increasingly complex security environment. There are also clear trends in how different approaches deal with malicious cyber activity in cyberspace are being formulated. It would be a watershed moment if, or when, we were to see armed kinetic responses to digital attacks. This is, however, something that is clearly formulated in today's security strategies, and should therefore not be dismissed (Brent, 2019; ISC, 2017, pp. 35-36; Macron, 2017, p. 30; Trump, 2018, p. 21). Also, current security strategies dictate that pre-emption is a part of the said strategy (ibid). Classic pre-emption matters just as much in cyberspace as it does elsewhere. Cyber-capabilities will be used to deter and pre-empt attacks that can be disruptive or harmful to the recipient target.[21] Including the authorized use of pre-emptive, or first-strike options (Sanger, 2018, p. xv; Trump, 2017; 2018, p. 21).

In terms of deterrence and pre-emption strategies, NATO has made clear that a digital attack on one of its members can constitute an invocation of Article 5 – collective self-defense. This means an attack against one NATO member is equivalent to an attack on any or all members with the implication that the alliance as a whole has the right to strike back in self-defense (Brent, 2019; NATO, 2019a). One of the best possible outcomes in Russia's grand strategy and its information

[21] For a state that does not have strong institutions to oversee that such powerful tools are not being misused, cyber capabilities can provide a powerful toolkit for political social control (Sanger, 2018, p. xv).

warfare campaign is to undermine Western alliances and partnerships. If this could be achieved to the point where NATO would not put up a united front, effectively undermining confidence in, for example, the invocation of Article 5, is one main objective in the Russian information warfare campaign. One primary goal in Russian military doctrine is to destabilize the US and EU politically; such tactics carry the overall aim of ultimately weakening its opposition, i.e., the West/NATO (Giles, 2016).[22]

The potential for a military crisis developing due to a cyber incident should be a cause for concern. Even if the cyber incidents in themselves would not be considered jus ad bellum, a cyber incident may develop the escalatory dynamics required to facilitate such a trajectory (Singh, 2019). Nevertheless, there is a significant distance between escalations and the outbreak of military conflict. Historical analogies like that of the assassination of Archduke Franz Ferdinand are hyperbolic, but they do serve some purpose. In terms of recent military tensions in the Persian Gulf, the author does not believe such escalations are a prelude to war. Rather that there will be a continuum of low-key attacks that will exist on a spectrum of conflict that can still fluctuate without a full escalation to interstate war.

In the case of the Russian interference in the US 2016 presidential election, this shows a level of reciprocity from Russia. If the Department of Justice´s indictments is deconstructed, it becomes clear that the US had pre-positioned cyber implants within Russian military networks, which are easy to distinguish as acts of aggression. This potentially, or hypothetically provides a legal cover to the Russian act of interference in US domestic politics. ´It was a mode of retaliation to defend Russian sovereignty, guaranteed by the law of armed conflict` (Singh, 2019). When Russia uses cyber operations to attack and disrupt Norwegian infrastructure, it regards this as self-defense measures. By responding to NATOs training exercise Trident Juncture, Russia is operationalizing its capabilities vis-à-vis NATO (NIS, 2019, p. 9).

It is critical to get to terms with how to deal with these new challenges relating to cyber. Furthermore, the corresponding notion and realization of why getting it right matter. Risks exist not just at the extremity of a scale, in this sense, typically labeled war. Conflict in cyberspace also

[22] To former Assistant Secretary of State for Political-Military Affairs Mark Kimmitt, Russia´s role, though important, is not significant in this respect. China is to be regarded as the main adversary in both political and military terms. It is the US-Sino relation that is, and will continue to be, the predominant factor in the years to come. He regarded Russia as "playing its cards well", but that in the end of the day, these are not backed up by anything substantial enough to carry the weight required fundamentally alter the current status quo. Which is not the case with China. As such, this will shape the coming years in geopolitical terms.

includes the destabilization of countries' political spheres using ICT´s, i.e., a continuous ongoing process (Giles, 2016).

These complexities, including how deeply they are integrated into contemporary society and provide the necessity to address such issues across government and private sectors. Not just within a specific field of study. In this sense, risk management, security, and planning processes are needed and addressed across sectors, from planning processes to tactical and operational points of contact. By highlighting how we use and share information is not straightforward. While ICTs and CCB are facilitating for conflict in cyberspace, which directly threatens human security, there is no divergence from the fact that CCB is an integral part of contemporary developmental processes. The internet is now a fundamental component of human society globally. What is then needed is a global effort to establish the norms and laws that govern it. In order to maintain first principles, we should all agree upon, namely, the attempt to promote human security.

Technology does not have inherent traits; it is created to serve specific purposes. From a historical perspective, historians would warn that technology permeates war, ´but does not govern it.` It is how technology is utilized and organized, broadly speaking, that is important (Arquilla & Ronfeldt, 1997, p. 25). Cyber is just another domain in which to operate in, just as land, sea, air, and space. Both the DOD and NATO use this terminology, addressing cyber as a sphere of knowledge, influence, or activity (Crowther, 2017, p. 63). Cyber is then just a natural progression on a historic evolutionary narrative. This is not an attempt at an alarmist view on the implementation of technology in general.

Nevertheless, an emphasis on the dominant role cyber will have in shaping limited, irregular, and threshold warfare is significant in both today´s and tomorrow´s world. Digital capabilities can also work in conjunction with military operations in terms of enhancing relations between the military and the civilian populace. This was done successfully with the NATO missions in the Balkans. However, there have been proven difficulties in recent wars such as Iraq and Afghanistan to transmute military victories into political ones. Digital capabilities can, if used right, facilitate this process since successes in irregular conflicts require an ´understanding of the physical, cultural, and social environments in which they take place (Egel et al., 2019).

Understanding such terrains are critical in Russian security strategies, which echoes a long line of authoritative political rule. The contemporary Russian strong autorotative state is not something new. The Romanov dynasty lasted for three centuries, only to be succeeded by the repressions of

the Communist Party of the Soviet Union, which was but a change, and not for the force of emancipation or liberation as promised by the Bolsheviks. This is referenced by highlighting that a wish for fundamental political change in Russia could lead to precarious alternatives. This includes how change in Russia, is not always change. Also, when change does materialize, it is not always for the better (Giles, 2019). Today, Putin, a former KGB agent and director of the FSB (Waage, 2012, p. 494)[23] is a true a man of the Soviet Union, and who no stranger to Stalinist approaches in his methods to government. (Hedenskog, Konnander, Nygren, Oldberg, & Pursiainen, 2013; Brian D Taylor, 2011; Walther, 2014). Moreover, Putin can be described as a practitioner of the Cold War, where Russia´s external geopolitical relations continue to this day to be dealt with through the prism of hard power through great-power politics (ibid).

Russia today, comparatively speaking, is at a rather liberal country with liberal practices (Giles, 2019), looked at from a Russia focused historical perspective. That being said, there is no question that there is no such thing as a free press or freedom of speech and expression. The Russian Federation strictly links its national security to the *nature of information*, both as a potential for opportunities and as a threat. This stems from the continuity of leadership, with ´alumni´s of the former KGB running the country` (Giles, 2016, p. 36; Walther, 2014). The Russian Federations approach to information security is thus severely tight and regards the circulation of information as a ´threat to its security and stability` (ibid). The keyword being stability. And it is stability, in a hierarchical structured international system, which is what is at the center of the Russian vision. ´The small gaps of information that existed immediately after the fall of Communist Russia have slowly been sealed tight by Putin` (T. Snyder, 2018; Waage, 2012, pp. 494-500). It is an authoritarian state, that deals with what it deems threatening in the harshest manners. Examples of their unforgiving nature include the execution and imprisonment of undesirables.

Russia does not define statehood and sovereignty like the West. The West's notion of these concepts is firmly rooted within the premises of a Westphalian definition of statehood. Russia regards sovereignty as a capacity. A capacity that is used to promote Russian national interests. For Putin, and in effect, Russia, the only way to regard international politics is through zero-sum, realist, great-power politics (Giles, 2016).

The international system repositioned itself after the end of the Cold War. In the post-Cold War setting, Washington emerged as the one sole superpower, reflecting Fukuyama's famous

[23] FSB are the Federal Security Service of the Russian Federation and the successor agency to the KGB.

aphorism, ´end of history` (Fukuyama, 1989). It is this political landscape that is under stress. Revisionists and dominant regional powers, like Russia and China, are today reasserting themselves in this system by challenging established power structures, often through forceful means. Such reorientations have occurred frequently in the past. The repositioning of empires is, in large part, what makes history, including what we witness today. Though it might not be an existential threat to the current interstate system, it is worrisome to see the alternatives, such as if a new international order, would come to fruition, with its main seat in Beijing. Based on the premise that contemporary China would reflect policies that it would project on a global scale. Also, the relationship between Russia and China is a partnership the West is ignoring at its peril. This is based on western principles, such as a deep-rooted belief in liberal policies, the individual, the rule of law, and democracy.

That the Chinese would abandon their set of Confucian values are not, and should not, be expected. It is, however, with deep concern, we are witnessing domestic Chinese policies of social control. A good example is Chinas social credit system (Liang, Das, Kostyuk, & Hussain, 2018), and not least the crackdown on ethnic minorities. The treatment of the Uighur population by the Chinese authorities is tremendously concerning and has been highly criticized with a focus on detention centers and internment camps (Allen-Ebrahimian, 2019; Ramzy & Buckley, 2019). For these people suffering from the sharp end of the CCPs stick, Orwell's dystopic world is very much a reality. In the UN HRC, a group of signatories, representing 22 states, have asked China to ´uphold the highest standards in the promotion and protection of human rights and fully cooperate with the council.` Including to ´uphold its national laws and international obligations, keeping with international humanitarian law, respecting human rights and fundamental freedoms` (Co-Signatories, 2019).[24] All that being said, China has benefitted immensely under the current geopolitical leadership. That China would seek alternative models to restructure the international system might, in such terms, could seem counterintuitive. This would, however, be out of the scope of this thesis to address.

To predict what current experiences will mean in a future setting is impossible to determine with accuracy and are thus not a fruitful exercise. In terms of how a parallel to the liberal rules-based order, which would be based in either Moscow or Beijing, are, therefore, only speculations. Such states do regard themselves to a certain extent as in opposition to the current established order, which they see as western made, primarily to serve western interests. We see several severe and

[24] Such countries include the UK, France, Germany, Japan, Norway, Canada ...

profound challenges that stem from this with states such as China and Russia's blatant disregard for IHL, the far-reaching implications for human, national, and international security should not be underestimated.

Still, it seems like history is being echoed in conjunction with the contemporary foreign policy environment, stepping back into a post-WWII world seems to mirror such topics.

> At the present moment in world history, every nation must choose between alternative ways of life. The choice is too often not a free one. One way of life is based upon the will of the majority, and is distinguished by free institutions, representative government, free elections, guarantees of individual liberty, freedom of speech and religion, and freedom from political oppression. The second way of life is based upon the will of a minority forcibly imposed upon the majority. It relies upon terror and oppression, a controlled press and radio, fixed elections, and the suppression of personal freedoms. I believe that it must be the policy of the United States to support the free peoples who are resisting attempted subjugation by armed minorities or by outside pressures … the free peoples of the world look to us for support in maintaining their freedoms (Truman, 1947).

This speech addressed Congress by President Truman initiated the Truman Doctrine and was delivered more than 70 years ago. It could still just as quickly be stated today, exemplifying current Russian and Chinese state behavior. Also, in such a context, the Truman doctrine ought to be regarded as a globalized, scaled-up version of the Monroe Doctrine, which can again be considered in more critical terms as strict colonial practices (Bulmer-Thomas, 2018, p. 148). For Fanon (1963), this lies in the dichotomy where specific political structures would proclaim abstract principles. Such as the right for self-determinization, and the affirmation of the principle *one man-one vote*. However, the ´realities only refrain from issuing them in real definite commands,` with the idea that it is easy to promulgate grand ideas, yet another to have said ideas implemented in real constructive terms. Since the words of Fanon and Truman, genuine attempts have been made to implement action into deeds - this will be touched upon briefly at a later stage concerning interventions and the responsibility to protect.

The search, and declaration for human rights, is not strange to the development or the security discourse by referring to the previous point of the US policy of Soviet containment, how many development projects were affected by these geopolitical attributes between 1947 and 1991, mainly sourced in the superpowers quest for dominating spheres of influences (Giles, 2016). If

not by one of the most significant development schemes of all – the resurrection of Western Europe post-WWII, better known as the Marshall Plan (Bulmer-Thomas, 2018, p. 149).

This is also how Russia views the West, who they are confident are on a constant mission to undermine and destroy Russia´s sense of self, position in the international system and is a direct existential threat to Russian sovereignty. New allegations include the building of a "trojan horse" strategy by the West to implement against Russia. By mixing "color revolutions" with conventional, high-precision weapons and military capabilities. Its essence is to destabilize a situation and simultaneous striking key-targets (McDermott, 2019). In this case. Russia has accused the West of being at fault in terms of the Ukraine crisis. Where Russia had to respond to Western encroachment. Tensions between Russia and NATO continued to rise with NATOs enlargement policy. For Russia, NATOs eastward expansion had to be countered and to make sure that Ukraine would never become a part of NATO (Wolff, 2015).

The current crisis in Ukraine is then a critical area between Russia and Western foreign policy. Post-soviet Russia has been attempting at keeping and maintaining influence and control in its "near abroad." From the Western perspective, a stable Ukraine is of strategic importance, not just for Ukraine, but for Europe and the cross-Atlantic partnership. The situation in the Donbas region, as well as on the Crimean Peninsula, is still critical in terms of shaping foreign policy initiatives. One element is how Russia has "returned" the naval fleet base at Sevastopol back to the Russian Federation. This carries significant strategic value as it provides the Russian fleet with warm water port access through the Black sea.[25] Crimea is also a critical component in Russian foreign policy and grand strategy. Overall the war in Ukraine, and Syria, has served as a testbed or laboratory for the Russian armed forces to apply its capabilities in both conventional and unconventional spaces (RUSI, 2019, p. 57). In the case of Russia´s annexation of Crimea and Eastern Ukraine, the lack of a coherent response from the West is regrettable (Polyakova, 2019). Yet the Russian invasion of Ukraine was not that straightforward. Because of Russian fears of the possible Western responses, it employed hybrid warfare techniques that would provide some levels of plausible deniability. The use of troops referred to as "little green men" were (Russian) soldiers who did not bear any identification marks (Abrams, 2016; Schnaufer, 2017).

Furthermore, Russia encouraged the formation of local militias as proxies and enabled the support of Russian volunteers and mercenaries (Lawson, 2019, p. 9). The archetype usage of

[25] A warm water port is a port that does not freeze during winter and are thus not limited in seasonal terms.

cyber as a critical category in this conflict has concerned the incident was Malaysian Airline MH17 was shot down, followed by massive Russian efforts to distance themselves by trying to undermine, cast doubts on, and seeking the de-legitimize proof of Russian involvement in this instance (ibid). And was successful to a certain extent. That is to seed sufficient doubt to the process, as to assigning responsibility becomes a challenge (Gibney, 2015). Continuous efforts have come to fruition in the case of the MA MH17 incident. Through a JIT investigation. Three Russian nationals with ties to the Russian intelligence services GRU and FSB, along with a Ukrainian militia leader, have been formally charged with the incident (BBC, 2019a; en Veiligheid, 2020; Troianovski, 2019).

In other terms of Russian external force projection by unconventional military means. The conflict in Ukraine and the use of cyber in this conflict makes it clear how Russia regards the cyber operations as a part of a broader domain of information warfare (Geers, 2015; Giles, 2016). On the 23rd of December 2015, power grids in eastern Ukraine were shut down due to cyberattacks resulting in approximately 225 000 people losing power. The attack was attributed to Russian security services (Lee, Assante, & Conway, 2016). This was, however, *not concluded*, further establishing the notion of the difficulties that are involved with attribution in cyberspace. Though that day was not unusually cold, that changed rapidly, to several degrees below zero (TD, 2019). This resulted in the death of 11 people (Harding & McLaughlin, 2009). The cyberattacks in 2015, only shut down this particular set of critical infrastructures for three hours. It is showcasing its damage potential, as this is situational dependent on the duration of the attack. Also, recently there have been attribution to Russian intrusion into western (US and European) networks and critical infrastructure, including nuclear powerplant, water, and electrical systems – with the power to sabotage said systems (Perlroth & Sanger, 2018). Also, Russia uses private enterprises such as Gazprom to effectively enforce hybrid warfare tactics. By taking advantage of how Gazprom is a prime deliverer of natural gas to many countries in Europe, the Russian state uses this leverage for political influence. Though this in itself is not controversial, how this is used as a foreign policy tool sometimes is. When Russia cut Ukraine´s gas supply in the winter of 2006 and in 2009 as a method to coerce Ukraine to comply to Russian monetary demands (Chivvis, 2017). To further emphasize this point. Energy security and national security are a precarious topic for Ukraine. As it is a strategic liability for Ukraine to be energy-dependent on Russia. This is an element which is taken advantage of in Russian hybrid warfare tactics. In particular to destabilize Ukraine politically (Ruehle & Grubliauskas, 2015).

This is not just limited malicious state behavior. There are many types of actors committing clandestine operations in cyberspace. ´Global ransomware incidents such as WannaCry and NotPetya affected nearly all sectors in 150 and 65 countries respectively`. NotPetya was a Russian broadside cyber-attack on Ukraine, launched on Ukrainian constitution day. With the indiscriminate computer code that was used, the malicious attack was not confided to Ukraine and quickly spread globally. Several big corporations like MAERSK and FedEx reported significant financial losses with this attack. NotPetya is the costliest cyberattack to date, with over 10 billion USD in damages (Buchanan, 2020). Liberia was taken offline entirely due to cyberattacks (Morgus, 2018b, p. 7). This was done through a DDoS attack, that crippled the entirety of Liberia's digital infrastructure, effectively disconnected the entire country for a week (Woolf, 2016). Nigeria has suffered from cybercrime in general, as illicit cyber activities are receiving conservable attention from Nigerian authorities. Where internet penetration went from 5% in 2003 to 40% in 2015. The digital transformation in Nigeria has been a critical driver in the country's economic development. Moreover, FDIs have increasingly been reduced in the country as a consequence of malicious cyber practices (NCC, pp. 7-8). Moreover, extensive amounts of hard currency are stolen daily (ITU, 2019b). This includes, identity thefts, massive theft of personal information, such as passwords, social security, and health data, amounting to an estimated 2 trillion USD at the end of 2019 (ibid).[26] Though cybercrime has not a theme in this thesis, it provides a significant challenge to digital, open societies. Contemporary development underpinned by ICT´s is unsustainable *if* the security aspect is not thoroughly acknowledged (OLA, 2010). Without cybersecurity, ICT´s have the potential of disrupting developmental processes. Including contributing to a proliferation of conflict – which ripple effects will have more extensive and more dire implications (Pawlak, 2014).

The US, UK, and Israel created Stuxnet and other cyber weapons to work in junction with more comprehensive operations. Operation Nitro Zeus was a plan to shut down the entirety of the country effectively. By shutting Iranian ICT systems, it would effectively cripple the country. Such as shutting down Iran´s A2AD capabilities. Providing amble opportunities to conduct air raids without a threat to Israeli forces (Buchanan, 2016; Sanger, 2018). In the case of Stuxnet to specifically target Iran´s nuclear facility in Natanz. A plan conducted with pressure from Israel concerning Iran´s ongoing nuclear uranium enrichment programs (Sanger, 2018, p. 39). Iran has responded with the use of cyberoperations as a valuable foreign policy tool. These attacks have

[26] The theft of intellectual property is a serious security issue (Halbert, 2016). The topic of intellectual property will, however, not be addressed in this thesis.

been relatively disorganized but have still caused significant damage. In 2012, operation Ababil targeted the US banking system with DDoS attacks. The Shamoon malware caused hundreds of millions of USD in damage to Saudi Arabia´s national oil company Aramco (RUSI, 2019).

Bangladesh has suffered from North Korea's quest for hard currencies. In 2016, a series of cyberattacks on banks in Bangladesh and Southeast Asia resulted in the theft of approximately 81 million USD`. Mere coincidences halted the total theft of 1 billion USD. In this specific case, some investigators believe that the North Korean attack was aided by Chinese intermediaries (Chanlett-Avery, Rosen, Rollins, & Theohary, 2017, p. 6; Zetter, 2016). These examples are made to illustrate the digital transformation we are experiencing, also known as the fourth industrial revolution (Schwab, 2017). Though this holds great promise in terms of development potential, and untold possibilities to transform our societies going into the future, the backside of this medal also consist of the cyber risks involved as threats to ´erase progress, or even worsen the human condition` (Morgus, 2018b, p. 7).

Keeping this in mind, the body of literature within development studies have had a significant increase over the last couple of decades (Joost, Gilles, Aude, & Leo, 2017). This does not however sufficiently address the risk elements that are tackled through security studies. As previously mentioned, (in essence) all contemporary systems are grounded on ICTs. Due to the exponential growth of ICTs and internet-related mobile technologies (Pawlak, 2014). Development processes underpinned by this infrastructure is then unsustainable if the security aspect is not acknowledged, and how to properly manage the risk that follows a greater reliance on ICTs. Without the security element, there is a real risk of undermining the main aim and scopes of development processes (Morgus, 2018b, p. 5).

The term development can, in itself, have the ability for confusion. To clarify, development is understood as; one, a vision or measure of the desired state of being for society; two, a historical process of social change in which societies are transformed over a long period of time, and three, deliberate efforts aimed at improvement on the part of various agencies (Hewitt, 2000, p. 289). Coupled with the term *sustainability*, which was introduced by the Brundtland report in 1987. Which defined the key concept of planning in sustainable terms as to not compromise future gains (UN, 1987). On the international arena, "sustainable development" is the formed consensus and implemented as overarching goals for the EU, WTO, and the UN. However, despite considerable support, there are still differences in how the term is interpreted (Langhelle, 2002, p. 225).

When discussing development, it is essential to acknowledge that all conceptions of the idea carry with it particular sets of ´social and political values`(Baylis et al., 2017, p. 473). It is then vital when discussing development that it is understood within the ideological framework from which it is presented. This means that the platform from which development is discussed shapes the direction and orientation of the suggested developmental approaches.

3.5 How to think about security

International security is a contentious, precarious, evocative, and highly charged subject (Baylis et al., 2017, pp. 228-230; Browning, 2013; P. Williams, 2008). Mainstream conceptions of security often fall on notions such as state security, conflict, the UNSC, blue-helmet operations, nuclear proliferation, interventions, usually portrayed through a zero-sum game, played on the international arena in quests for power and influence (Browning, 2013, p. 1). Though to several extents this is true, security is also a more complex, dynamic, and nuanced topic. By expanding the understanding of security beyond these stereotypical and narrow conceptions, we can acknowledge that security is more about the ´complex dynamics and multiple factors that are frequently underlying narrower concerns with war and peace` (ibid). There is then significant potential to further our understanding of what constitutes and how to think about security issues. Since there are and will continue to be different interpretations on how to view and think about security – there should not be and adherence to any single one understanding of the term (P. Williams, 2008, p. 2). This is why it is the author´s view that; security is not just the absence of conflict but the creation of an environment from where sustainable political, social, economic, and cultural development processes can take place. Conflict, in this case, is understood as unwanted or imposed hindrances that limits the potential for achieving specific goals on both individual and state levels, either in terms of crime, environmental, social, economic, or political.

Because there are many ways to think about security, specific underlying questions should always accompany any discussion of any particular topic, such as; who´s security? Security provided by whom, and security of what, and for what purpose? Because of this multi-dimensional nature of the term, the concept will need to be addressed shortly, beyond a consensus-oriented definition.

As mentioned in the introduction to this thesis, the Norwegian defense sectors working definition of the term security are; state security, societal security, and individual security

(Forsvarsdepartementet, 2015, p. 17). This is the basis on which Norwegian security policies are made (ibid).

In this operational definition, many elements can be unpacked. Nevertheless, it needs to be stated clearly that this reflects the political reality of the international environment in which we are operating (Norheim-Martinsen et al., 2019, p. 41). This operational definition fits well in established discussions on how to focus on security inquiries either on the individual, national, or international level (Baylis et al., 2017).

Security after the attacks of September 11, 2001, has taken on a substantial new role. Security, in this case, became the forefront in protecting society from the existential threat of Terrorism. This threat then constituted the incorporation of serious security measures that deeply cut through privacy issues and democratic principles. It was still popularly accepted as the existential threat that was depicted outweighed the ideas of personal privacy. Moreover, from the post-9/11 world, an entire security apparatus and industry were born. This industry has actively pushed on the security policy side with a heavy focus on the global war on terror.

> State-regulated security sectors, both private and public, are being reinforced in terms of budgets, media coverage, powers and influence overall domains of governance, including the management of welfare systems, refugees, migration, money transfers, internet use and so forth (Buur, Jensen, & Stepputat, 2007, p. 9).

Within this framework, development has inexorably merged with security concerns (Duffield in Buur, et al., 2007, p. 9). The periphery to the West have in general, been described in chaotic means and that it is only through core capabilities (western technology, human capital, security institution, organizations) that a good order can be established (Bachmann, 2014). The security doctrines in the West have asserted that the global south ´needs assistance,` legitimized through descriptions such as state fragility, radicalization, internal power-struggles, and humanitarian disasters. Such disasters are the driving force in creating conflict, particularly, in cases where states themselves do not have the capabilities to deal with such problems by themselves and are thus pushed into ´persistent conflict` (ibid, p. 119). This has also emancipated the US liberal "crusading" state regarding the GWOT, which has expanded into a ´globe-spanning security assemblage defending the liberal order through the ´War on Terror` (Bachmann in Rampton & Nadarajah, 2017, p. 459).

Consensus has been formed around the security-development nexus in the interrelationship between security, development, and democracy (Hendricks, 2006). The security-development

nexus is for external actors meant to have a new comprehensive approach, as to their ´mutually supportive coexistence` (Schnabel in Jesperson, 2016, p. 30). With the development sector taking on more responsibilities with regards to economic development, infrastructure, education, health, sanitation, etc. This has also converged with enhancing security and ´non-violent forms of behavior` in all aspects of a stratified society. The securitization of development has had severe implications as international development has been linked to interventions (Williams, 2013, p. 1213). Within created existing created structures, some actors are not acting in accord with currently established norms. The establishment has then labeled this as actors who act with indifference to international laws and norms (Kirchner & Sperling, 2007, p. 3), which then legitimizes the external interference to balance the status quo.

This, then is linked to how themes are presented. Knowledge, including those who produce and reproduce it, are thus consequential perceptions—labeling an increasing number of actors (both state and non-state) as security threats for not abiding the regulated norms in the system. The major actors in the system have inclined towards the usage of both *hard* and *soft* power to resolve these security challenges (Nye in Kirchner & Sperling, 2007, p. 3).

Security, as a topic of academic inquiry, is mostly an Anglo-American invention. It is also typically regarded as a subfield to IR and became prominent after WWII (P. Williams, 2008). It then follows that this academic exercise follows from its conception with a particular political and historical evolutionary narrative.

In the development discourse, an essential element is to criticize established principles. One major component in critical theory in the development discourse is Ethnocentrism (Eriksen & Eraker, 2010, p. 18). Ethnocentrism is a common baseline to assess all societies from single arbitrary principles as a core principle to mitigate in the development discourse (ibid), so are the case with security issues. The idea of how security has been thought of has been widely criticized for being ethnocentric (culturally biased) and too narrowly defined (Baylis et al., 2017). Expanded orientations of security have evolved from a primarily parochial state-based view, expanding mainly through critical theory, into incorporating security issues into the political, economic, societal, environmental, as well as military aspects (Buzan, 1983).

International development has been a project of the restructuring of states, where this has been pushed through by strong transnational forces (D. Williams, 2013). This has also brought with it a strong connection of certain practices; one among them is interventions (ibid). The security-development nexus has been a rising trend that has received significant attention relating to post-

conflict reconstruction (Jesperson, 2016, p. 1). With several decades of official development policies, and a focus on economic growth, the discrepancies between the global north/south are growing (Baylis et al., 2017, p. 470). This has often been represented as liberal north and illiberal south. The global north/south divide is not a clear geographical line. The general relation of inequalities is not confined to the south. These inequalities have arisen both between as well as within states (ibid). With the incorporation of neoliberal economic policies, often referred to as the Washington Consensus,[27] Eastern Europe was incorporated into the global south or what has also been called the ´third world.` These policies have also actively pushed millions of people around the world, typically in former colonies, into poverty with the direct transitions to market economies (ibid).

Though thinking critically about security, and thus to diverge from centrist perspectives carries significant importance, this does not negate the security dilemma as a concept. To do so is to dismiss the security dilemma as a concept is to dismiss several theoretical approaches to international relations, such as realism, liberalism, or constructivism (Baylis et al., 2017; Dunne et al., 2016).

3.6 Human security

The dramatic rise of China as a global economic and political power and as an incipient ideological and strategic hegemon, especially in the global South, represents a political challenge to the tenets of the "Washington Conesus" on development` (Rodrik; Stiglitz; Williamson in Pike et al., 2017, p. 8; Rigg, 2007, p. 11; Winkel & Aase, 2008, p. 222). Whether or not this is a force for good or not is speculative. Nevertheless, the highly authoritative nature of countries such as China and Russia are problematic on several ethical, normative, and legal grounds. In terms of the SDGs, there are fundamental differences between those states who carry political objectives that divert from the SDGs premises but still claim to adhere to them. This is also complicated in terms of having a coherent strategy, especially in terms of the SDGs. Hence, in several aspects, core attributions of several significant actors in the international geo-political arena are in direct contradiction to the concept of human security.

[27] Which have been referred to in this thesis through the Bretton Woods institutions that created them.

When discussing security, the notions of war, conflict, interventions, UN peacekeepers (blue helmet operations)[28], zero-sum security dilemmas, geopolitical rivalries, and struggles for resources, political power, and influence are predominant. However, it is imperative to understand how this is just part what the idea of what security entails. As already mentioned, security is a broad concept, and other issues are imperative to it besides state rivalries and the use of military force – which are integral in state practice (Mearsheimer, 1990). Including topics are refugee camps, piracy, famine, migration, climate change, national liberation struggles, and personal freedoms.

In terms of China´s social credit system many analogies has been drawn to Orwell's depiction of a dystopian world. In China, characterized by its panopticon surveillance system that is coercing social control, and are a legitimate cause for concern (Co-Signatories, 2019; Kendall-Taylor, Frantz, & Wright, 2020). China´s massive facial recognition programs are created in conjunction with its more comprehensive social credit program. Which are on a systemic level incorporated into Chinese society without triggering the proper responses it merits. While Silicon Valley can oppose ´big brother` at home, by refusing to cooperate with US intelligence agencies on the collection of big data (Sanger, 2018), it still sells facial recognition technology to China´s societal panopticon industry. This technology is then used in the Chinese´s repressive social credit program that coerces social conformity—creating incentives and punishments for all who do not adhere to strict social policies. This program is implemented for the essential purpose of direct social control (Condliffe, 2018; Ma, 2018; Marr, 2019). The infamous STASI employed a significant amount of resources, employing almost 100 000 individuals, to achieve security through controlling information flows. Attempting to permeate East-German society. Through the transformation of ICTs, governments today who employ similar methods are able to do so, through the usage of digital surveillance systems. Though China, is not the German Democratic Republic. Systems of surveillance used by digital autocracies, spearheaded by China, to monitor and control information flows as substantial (Kendall-Taylor et al., 2020). China´s social credit system, characterized by its ultimate efforts of creating a more secure society based on surveillance, represents the more muddy and complex notion of the security realm. Deploying the latest technology to collect big data which is compiled in its social credit score program. Which are setting the parameters for acceptable behavior for Chines citizens (ibid) Moreover, it is

[28] In terms of UN peace-keeping activities, China are a significant contributor. It is the second-largest financial contributor, and have currently over 2000 troops in eight different UN missions (Hirono & Lanteigne, 2011; SIPRI, 2009; UN, 2020b). China also chairs four out of 15 organizations in the UN system. Which can be viewed as an indication of a transition of global leadership roles.

indicative of the vital component that security serves when talking about a broad range of issues (Browning, 2013, p. 1).

> In the final analyses, human security is a child who did not die, a disease that did not spread, a job that was not cut, and ethnic tension that did not explode into violence, a dissident who was not silenced. Human security is not a concern with weapons – it is a concern with human life and dignity (UNDP, 1994, p. 22).

Measuring all the acts that did not happen is, of course, impossible. However, the UNDP was able to shortly and consistently, to emphasize what security is. Human security can rightfully be regarded from many different perspectives. Since the word security is vague, we have to ask questions like ´the security of what? ´Security by whom, and for whom? What are we securing, and what are the underlying interests and premises? When the UNDP talks about human security, it is not just security in terms of the broader conflict in question but creating secure environments for people to have the ability to express themselves in an environment with the absence of fear.[29] A ´dissident not silenced` is very much one key issue. "Cruelty and injustice, intolerance, and oppression. Moreover, where once you had the freedom to object, to think and speak as you saw fit. You now have censors and systems of surveillance, coercing your conformity and soliciting your submission".[30] Like China´s treatment of its minorities, along with the already referenced social credit scheme - like Orwell´s depiction of a dystopian future with traits such as *hate week* and *big brother is watching you* (Co-Signatories, 2019; Orwell, 2008). The control of information is integral to the political discourse, and it is because of this a critical component in information warfare or hybrid warfare (Giles, 2016; NATO-lib, 2019).

Because of this, different conceptions of the term security needs to be addressed. P. Williams (2008, pp. 230-231) describes these as; one, is the natural rights/the rule of law conception of human security. Firmly rooted in the liberal foundation of human beings have the fundamental rights to ´life, liberty, and the pursuit of happiness,` and the international community must commit to these rights. Second, is the idea of human security being humanitarian. This has its backing in the international efforts to strengthen international laws and norms, including how to deal with instances where these are not followed and backed up with credible response options when this happens. Such responses are principally through sanctions and at the far end of the

[29] The UN Charter Article 2 section 2.4 and 2.7 are explicitly stating the rules of non-intervention. Article 2 are however superseded by Chapter 7, article 51, and the inherent right for self-defense.

[30] Quote from the movie V for Vendetta (19:54) – a pop cultural refurbished version of Orwell´s 1984.

scale (humanitarian) interventions. Interventions are structured mainly around the terminology of R2P (Annan & Mousavizadeh, 2012; Curran, 2017, pp. 75-76; Dunne et al., 2016, p. 98; Masters, 2015).[31] It effectively states that if a sovereign is not able to deliver on its obligation to the civilian population, external actors might have the duty to assist, or intervene, to protect said population (Morris, 2013). Typical normative arguments against R2P would be based on how R2P in itself is an infringement of Westphalian rights because a sovereign nation will not willingly relinquish its sovereign rights, in terms of domestic control, unless it is highly dependent on outside support. This vesicates the consent from the sovereign from outside intervention.[32] Other normative arguments may reside in which actors have the capacity and capability to dictate how, when, and where interventions are needed, including for whom. This then boils down to how important language is. How it is used, what it justifies, and the forces that pushes a language that supports a certain narrative. In terms of a geopolitical reference point, when the language used encompass threats against international peace and security. This is very much code for possible interventions.

In such terms, even the anti-slavery crusade at the end of the 19th century was fraught in imperial terms. Drawing attention to the slave trade and raids in Eastern Africa and the Arab slave traders. Initiatives resulted in the Brussel Anti-slavery conference of 1889-1890, which contain the legal provision for the suppression of the slave trade (Laqua, 2011). Several anti-slavery associations came to be, such as the British and Foreign Anti-Slavery Society and the Aborigines´ Protection Society. Such transnational activism marked a new period of internationalism and in the shared language used. However, though the anti-slavery movement certainly was a humanitarian effort, it is still necessary to scrutinize it for its colonial setting in which it operated. The shared language that was used still encapsulated within a conceptual framework still rooted in ´new imperialism` characterized by the period in question. The anti-slavery discourse was, in itself, a component of the civilizing mission, which legitimized Western expansion. Raising significant questions ´between humanitarian activism and European expansion in Africa` (Laqua, 2011, p. 706).

The author would be remised, however, not to mention the strong presence of a multitude of actors on a global scale contributing to both humanitarian interventions and peace operations.[33]

---

[31] R2P was the galvanizing norm that played a key role in the UNSC conclusion on intervening in Libya with the use of NATO forces. This was to protect a group of people who was described by, and was said to be dealt with, by Gadhafi in a similar language that was used prior to the genocides of Rwanda in 1994 (Morris, 2013).

[32] There is a myriad of strong normative arguments against interventions. It would be out of the scope of this thesis to address them all.

[33] Meaning peacebuilding, peacemaking and peace-enforcement

For example, Rwanda has built up a strong reputation as a strong contributor of troops for peacekeeping missions. Notably, since 2004, it has participated vigorously in AMIS, and UNAMID, situated in a framework of ´African solutions to African problems.` Yet, like China, Rwanda has received praise for its altruistic contributions to the international community through peacekeeping missions. However, there are also other factors involved. Rwandan security forces can be used in terms of ensuring domestic stability within Rwanda (Beswick, 2010; Kendall-Taylor et al., 2020). It can also be used in the pursuit of ´destabilizing foreign policy objectives.` Such as training rebel groups who operate in the DRC (Beswick, 2010). This is meant to showcase difficulties associated with terminologies like sovereignty, security, and the politics that evolve on local, regional, and global narratives.

4. Cyber Capacity Building

The previous chapter laid out the theoretical foundation for this thesis. This chapter will look at some of the multilateral efforts that have been made in order to mitigate malicious cyber activity. It will focus on two specific efforts, namely the Tallinn manual, which is an attempt to apply international law to cyber. Also, it will focus on the UN GGE process, which is the main body within the UN system that works at addressing this issue. Including to highlight how digital security issues are vital in terms of development and planning processes. It will also highlight the different dimensions that cyber capacity comprises of.

4.1 Development and ICT´s

Already in 2001, the HDR was strongly advocating the potential that ICTs possessed for human development and poverty reduction. Labeling ICTs as not just a reward of successful development, but as a critical tool for achieving it (UNDP, 2001, p. iii). The emphasis was on the focus on technology as the ´heart of economic and societal transformation` to all countries (UNGA, 2013). Few technologies have had such an impact as ICTs in reshaping economies, societies, and international relations. Along with the benefits, there was a quick realization and accentuation of how the misuse of ICTs carried with it significant risk elements and an ensuing threat to international peace and security (UNODA, 2019). With the risks assessment that followed the emergence of digital technologies, CCB was considered the tool to promote a ´minimum level of cybersecurity globally` (Pawlak & Barmpaliou, 2017, p. 124).

The rationale behind CCB is a focus on the broader societal implications that stems from the current technological shifts, *not* just with a sole focus on national security, though the themes converge on numerous terms (Pawlak, 2014, p. 5, 2017; Schia & Gjesvik, 2018, pp. 6-9).

With the exponential advancements of ICTs, this continues to integrate more deeply into society, ranging from government structures to infrastructure. In this technological advancement, there still exists a very distinct uneven distribution of the state of society's technological incorporation, creating different or unequal challenges.

The ´readiness of societies to address the security challenges associated with this uneven distribute process` caused the international community to rethink how regulated and unregulated

physical spaces addressed cyber in itself, including this unregulated digital domain (Burgess, 2018; Sanger, 2018). CCB emerged from the international cybersecurity community to address these challenges (Pawlak & Barmpaliou, 2017). It must be stressed that the uneven readiness of societies to address security challenges, does not mean that challenges exist only for some but not for others. Challenges presented in this thesis are facing all state and non-state actors across the inter-state system. Though different actors will have various issues concerning how illicit cyber activities are affecting the specific state/actor in question. CCB aims to inject a more ´strategic reflection` on the processes involved in CCB, such as showcasing and mitigating dilemmas and politics, which are associated with it (Pawlak & Barmpaliou, 2017, p. 124).

As an illustration of what technological maturity means in terms of challenges posed, a good example was the Russian cyberattacks on Estonia in 2007 and Georgia in 2008 - Estonia is a vastly more technologically integrated country than Georgia (Deibert et al., 2012, p. 4). When the Estonian government in 2007 decided to move a WWII memorial, commemorating the Soviet liberation of the country from the city square, it triggered riots amongst the native Russian population. This was followed by cyberattacks on Estonia's critical economic and political infrastructure by Russia.[34] In parallel with western countries, Estonia is deeply reliant on its ICT networks. The ICT systems are integral to Estonia's government functions, water supply, electric power grids, and banking services (Connell & Vogler, 2017, p. 13; Herzog, 2011). The attacks caused severe disruptions to Estonia, impeding the country's ability to communicate or share information efficiently, essentially shutting the country down for much of the duration of the attack (Connell & Vogler, 2017, p. 13; Schmitt, 2017, p. 28).

In the case of Georgia, cyber operations worked in conjunction with conventional kinetic ones. The Russo-Georgian conflict of 2008 that escalated, due to Georgian pro-western foreign policy of then-President Saakashvili, and the relationship between Georgia and the separatist republics of South Ossetia and Abkhazia. Since the end of the Cold War and the dissolution of the USSR, the Russian Federation and Georgia have had territorial disputes regarding these provinces

---

[34] ´The European Commission and NATO technical experts were unable to find credible evidence of Kremlin participation in the DDoS strikes` (Herzog, 2011, p. 51). This does not per definition absolve any Russian involvement, it highlights important traits about the ubiquitous yet anonymous character of digital attacks, mainly the problem of attribution.

´Given Russia's advanced cyber-war capabilities and the gravity of the attacks on Estonia, it is a legitimate question to ask if the attacks were truly executed by autonomous networks of Russian-speaking hackers or if they were committed or sponsored by the Kremlin`(Herzog, 2011, p. 53). ... While we may never know the true extent of Kremlin involvement in the cyber-attacks on Estonia, it is clear that Russian officials encouraged the hackers by accusing Tallinn of altering history, perpetrating human rights violations, and encouraging fascism (ibid).

(Connell & Vogler, 2017, p. 17; Deibert et al., 2012, p. 7). Though the conflict was short-lived, cyber operations played a crucial role in the engagement. Not just as a yet another tool used in armed conflict – but also as an ´object of contestation and as a vector for generating strategic effects, and ´controlling outcomes` (Deibert et al., 2012, p. 4; Giles, 2016, p. 35). The possibility to narrate the intent and the desired outcome of the conflict proved to be of great importance in the broader strategic setting (ibid). Russia saw the armed conflict with Georgia as an opportunity to overhaul and transform its information war efforts, alongside the Russian armed services. This meant that the Russian Federation significantly increased its exploitative capabilities towards cyberspace (ibid).

Controlling and shaping information are integral components in the Russian grand strategy of which its information warfare campaign is a part of (Geers, 2015, pp. 29-30; Giles, 2016, p. 35). Though cyber was a handy tool in Russia's information war, Georgia's low level of dependence on ICTs made it more resilient to the attacks, as they did not cause the same levels of disruption as they did in Estonia in 2007. In this case, Georgia's unsophisticated critical infrastructure worked as an advantage, strictly from a digital perspective in the Russo-Georgian conflict. The focus on the digital elements in the conflict became more about who was controlling the narrative associated with the Russo-Georgian war. This happened on both sides. In the Russian case, primarily through actors or ´information troops` like; hackers, journalists, and specialists in strategic communication and psychological operations (Connell & Vogler, 2017, pp. 17-18; Giles, 2016, pp. 35-36). As previously mentioned, what we are witnessing now in Ukraine is not just a continuum of Russian capabilities in contested spaces. It is a testing ground for grey-zone, or threshold warfare, that is proving challenging to respond too. The further implications of these capabilities are to be implemented by Russia in its information warfare campaign. Specifically to interfere in Western political election processes (Polyakova, 2019; RUSI, 2019, pp. 56-57).

NIS's latest report highlights that the current and most pressing security challenges to Norway and Norwegian interests are the intelligence threat from other states – with particular reference to China and Russia (NIS, 2019, p. 8). Because of the accessibility and practicalities that cyberoperations provides, it is also frequently be used. It is much cheaper than conventional weaponry, there are issues of attribution, and normative responses has not been developed yet (McKenzie, 2017, p. ix; Sanger, 2018). These qualities to the fifth domain make CO grow in traction and applied to both states, as well as non-state actors' practices (ISC, 2017, p. 31).

Capacity building is not the sole overall solution, through which the cyber community is addressing the challenges imposed by an increasing dependency upon ICTs with the following

security risks. It has to come with joint agreements from the wider international community on legal parameters on responsible behavior in cyberspace. Though the threat represented is real, there has been no agreement on how the digital domain ought to be regulated to address them. The creation of norms, a regulatory framework, or binding treaties does not today look like something that will come to fruition in the foreseeable future. As of this, today, there exists no binding global charter.

In terms of how different perceptions ranges between different actors in the international community is a significant component, where the different conceptualizations of what the digital domain entails is a predominant element. There is no one single point of entry to how the definitional aspect ought to be regarded. The Western perspective is firmly rooted in information sharing, education, and the potential for economic growth. Other actors such as China and Russia consider the free flow of information as a direct threat to regime stability, in the sense that the political establishment cannot control information flow. It is such "irreconcilable´s" that is proving difficult in coming to terms in processes on ratifying universally agreed-upon treaties that can be incorporated into the UN Charter.[35]

4.2 Applying international law to cyberspace

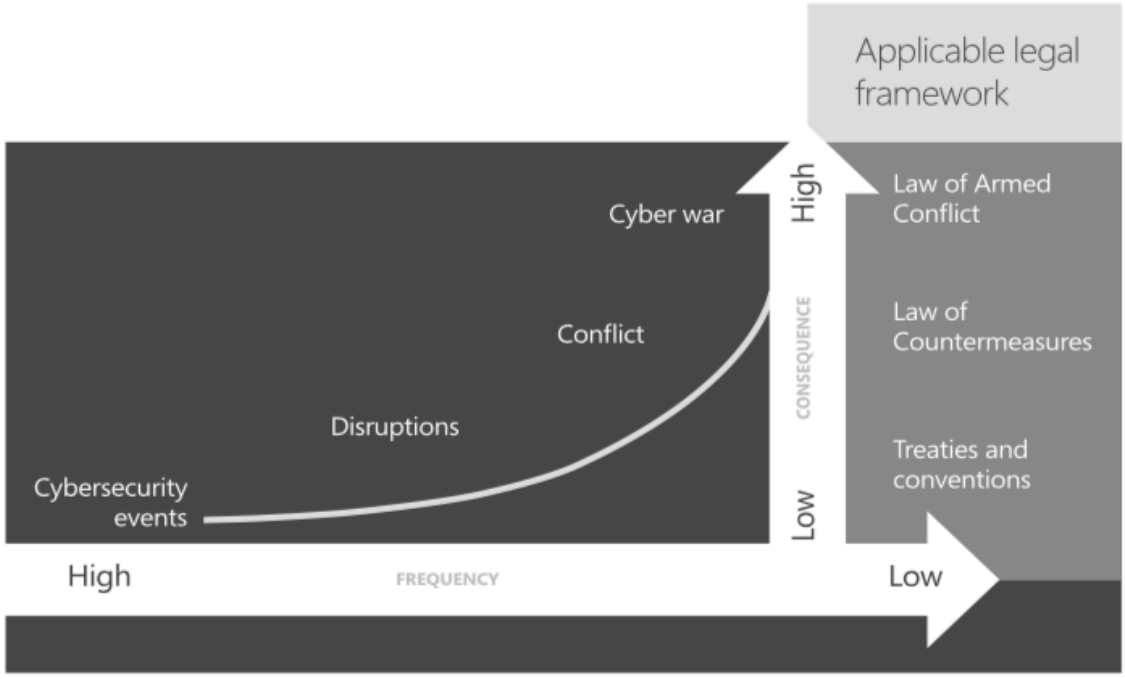
In 2009, NATO CCD COE put together a group of (western) experts that created the Tallinn Manual, that came to be due to the attacks on Estonia in 2007 (Henriksen, 2019, p. 3). This document address how international law applies to cyberspace and is regarded as an initial set of guidelines regarding responsible state behavior in cyberspace (Henriksen, 2019; Schmitt, 2013, 2017). Resolutions have been adopted in the UNGA on ´the right to privacy in the digital age,` and that the rights offline must also be protected online. The UN GGE have also pointed out that states have jurisdiction on servers located on their territory and must observe the principles of sovereignty, and the non-intervention in the internal affairs of other states. including that obligations under international law are applicable for states usage of ICTs. Still, there has been no ultimate success in drafting a census report, wherein 2017, Russia, China, and Cuba did not accept the final UN GGE draft. The UN GGE has to date, thus been unable to bring clarity to how international law applies to cyberspace (Henriksen, 2019, p. 3).

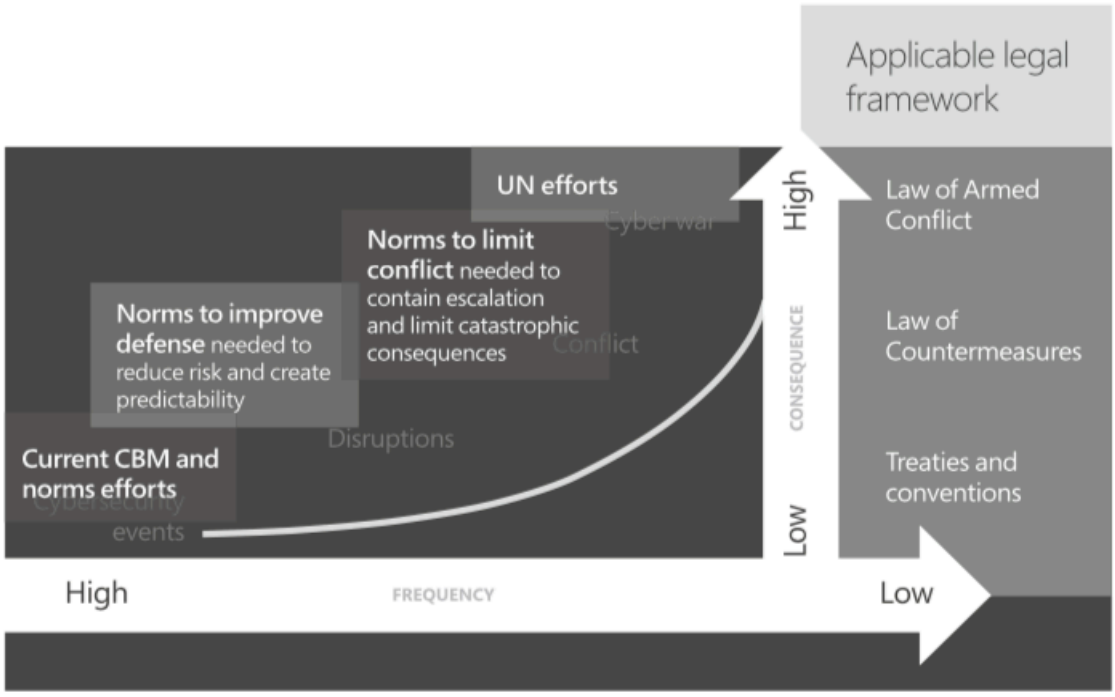
[35] Lawson in comments for this thesis.

The issue of how security and ICT are linked has been on the UN agenda since 1998 when the Russian Federation introduced a draft resolution in the UNGA. The UN GGE process has been the primary body to address how cyberspace should be regulated in accordance with international law. This is, however, extremely difficult, and progress has been slow. The UN GGE 2017 report, along with the Tallinn manual, exists as the best effort to accomplish this today.

The work by the UN GGE focuses on:

- Existing and emerging threats
- How international law applies in the use of ICTs
- Norms, rules, and principles of responsible behavior of States
- Confidence-building measures
- Capacity building
  (UNODA, 2019)





(Osula & Rõigas, 2016, pp. 244-245).

Capacity building is not only something that is directed at developing countries. As building and strengthening existing capacities are crucial to any state today (Forsvarsdepartementet, 2015). Capacity, in terms of security, has been focused on how the digital elements are facilitating development processes, yet simultaneously undermines national security efforts. The exertion to bridge these gaps is therefore vital. The digital security dilemma, therefore, works as a great entry analysis into the process on how to deal with the challenges facing the modern global society. Thus the debate about how international law applies to cyberspace is not merely an academic exercise in legal interpretation, but also – if not fundamentally – about trying to reconcile colliding strategic interests and clashing ideological worldviews (Henriksen, 2019, p. 4).

A focus then should be on how closing the digital divide can work as a conduit between the security and development communities – recognizing how it will mutually serve both interests. To which neither side would consider outcomes sub-optimal (Pawlak & Barmpaliou, 2017), and to further strengthen the analogous foundations to create robust regulatory frameworks.

Current cyber strategies do have CCB in focus, highlighting the importance of multilateral treaties, cooperation, and policy to sufficiently address and respond to contemporary threat levels. The support and promotion of CCB, particularly in developing countries, are seen as crucial issues in longer-term strategies. In such a context, CCB includes, but is not limited to, institution building (e.g., national telecommunication and CERTs), capacities to investigate

cybercrime, e-government, e-health, and educational assistance, digital infrastructure and the development of early warning systems (Utenriksdepartementet, 2017, p. 11).

The UN GGE process focused on norms, principles, and confidence-building measures. Such as increasing cooperation and transparency, primarily as processes that would reduce the risk of conflicts. Through regular dialogue with ´broad participation under the auspices of the UN and bilateral, regional, and multilateral forums`(UNGGE, 2015).

Furthermore, by emphasizing how ICTs are placed under IL, and applies to how states should conduct themselves in the international community. This includes how states ought to cooperate in order to prevent harmful use of ICT practices. Specifically, by not knowingly allowing their territory to be used for international wrongdoings in relation to malicious CO. One measure were to stress how cooperation and mutual benefits exists within an increased information-sharing environment. Which produced results in terms of prosecuting the illegal usage of ICT´s. While simultaneously providing a guarantee that states fully respect human rights, focusing on privacy and freedom of expression. Highlighting the importance that states should not either conduct or knowingly facilitate activities that intentionally damages the use and operation of critical infrastructure, CERT efforts, or use these efforts in malicious international activities (ibid).

While CCB has different interpretations in different strategies, the US National Cyber Strategy regards capacity building as a tool to strengthen partners. By equipping partners correctly, they can protect themselves and ´assist the US` in addressing threats that target ´mutual interests` (Trump, 2018, p. 26) - highlighting important, yet precarious elements associated to how security elements are applied in shaping policy.

The exponential growth of internet users and systems connected all across the world have brought into focus the need to address and leverage this in development circles. Cyberspace, as of today, is a very non-governmental structure, yet it will require broad national and international cooperation for the best possible outcomes. It is through state action presented through such national and international programs and international multilateral bodies through which real strategies will have the best chance for success (Utenriksdepartementet, 2017).

Nevertheless, it will require serious efforts from multilateral bodies to aid in this process. To accomplish the work to implement the digital into development practice successfully dictates that security-issues will go hand-in-hand with the development of digital capabilities. If not, then the exercise, however, "will be futile if it is not accompanied by a serious discussion about the need to address risks posed by the proliferation of ICT infrastructure and internet applications for

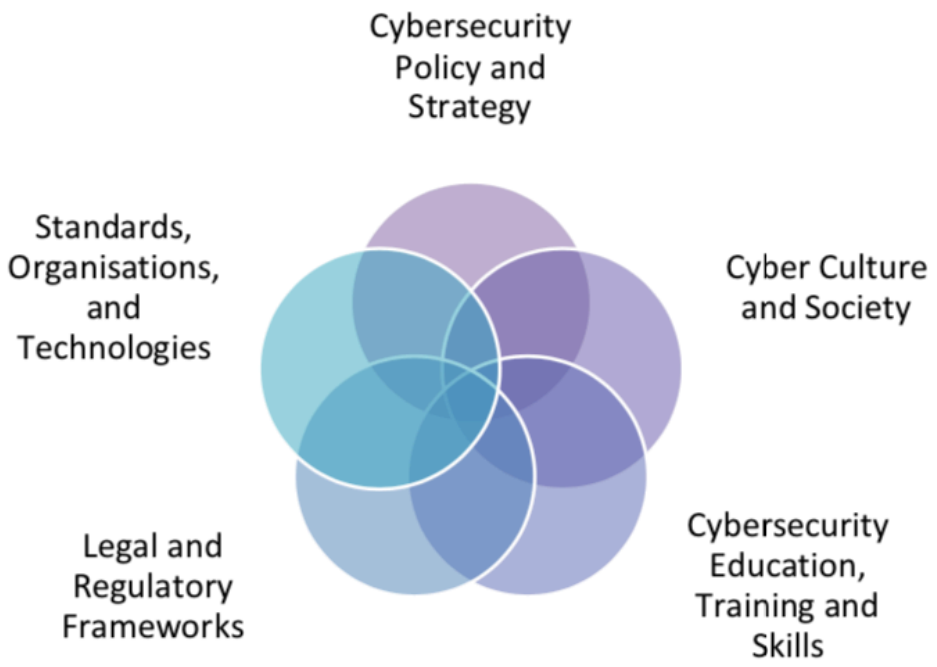
sustainable development" (Pawlak, 2014).[36] This is a core area that requires constant diligence in order to make the real progress needed to face current and future challenges of cyberspace as a domain that facilitates a conflagration of conflict.

Today, the digital domain is mostly characterized by ´complex, transnational interconnections and functional interdependence of actors and components on a global level.` On the national level, a state's "well-being" is dependent on its security and resilience in general. One component more specifically relates to that of its digital networks and systems. Also, it depends not just on domestic security, but also the security of networks located outside of its national borders and jurisdiction (Bellasio et al., 2018, p. 1). What "well-being" in this case constitutes, is the state's ability to provide services, without being limited by disruptions on its digital infrastructure, its domestic political space, and its citizens. Also, the transnational element of this comprehensive digital system cannot be in any comprehensible sense, secured independently, by anyone actor, be it state or non-state. For this reason, international cooperation and diplomatic efforts are vital in building shared frameworks on issues relating to cyber (ibid).

Cybersecurity capacity is comprised of five dimensions.

- Devising cybersecurity policy and strategy
- Encouraging responsible cybersecurity culture within society
- Developing cybersecurity knowledge
- Creating effective legal and regulatory frameworks; and
- Controlling risks through standards, organizations, and technologies
  (GCSCC, 2016, p. 5)

[36] Sustainable development is understood as defined in the Brundtland report. Sustainable development is ´development that meets the needs of the present without compromising the needs of the future` (UN, 1987).



(GCSCC, 2016, p. 5).

Digital Dividends, a World Bank development report of 2016, explicitly addressed the importance of cybersecurity coupled in developmental processes. With the spread of ICTs due to globalization, The report noted that ´some of the perceived benefits of technologies are offset by emerging risks` (WorldBank, 2016, p. 3). However, the integration of security elements into developmental processes has been slow. This is a time where it should be a focus on incorporating security concerns into existing developmental practices (Morgus, 2018a).

CCB then is established as the mechanisms that will aid in bridging gaps between problems related to poor governance, a well-established concept in the development discourse, and the state's ability to effectively provide acceptable levels of state service delivery of core functions (Hameiri, 2009; Pouligny, 2005; Wilén, 2009).

Capacity building is, in this sense, understood as the development and maintenance of institutions that are ´capable of learning and bringing about transformation,` to be better suited to play a more robust role in sustaining national development processes (Pawlak & Barmpaliou, 2017, p. 124). SDG target 17.9 of Agenda 2030, is dedicated to capacity building, with the overall aim to

> "Enhance international support for implementing effective and targeted capacity-building in developing countries to support national plans to implement all the sustainable development goals, including through North-South, South-South, and triangular cooperation" (UN, 2019b).

By highlighting the extensive connected issues of the security/development nexus and the role that large multilateral institutions such as the UN, AU, NATO, and the EU can provide. Contributions to economic and social development can take place while being agile defenders of the international rules-based order, which lays a foundation for the concept of human security (Browning, 2013, pp. 62-76; Pawlak, 2014, p. 5; P. Williams, 2008, pp. 230-231). In such processes, large multilateral organizations are key actors. In this context, the EU has proven committed to ´building resilient capabilities to mitigate digital security risks around the world` (Pawlak, 2014, p. 5).

Sub-Saharan Africa is heavily represented in the literature as a region where cyber-related illicit activities are pervasive (Kritzinger & Von Solms, 2012). A substantial body of literature in the humanistic and social study of technology, argues that technology is not to be viewed merely as independent material, but that it is political to its core (Nissenbaum, 2005, pp. 61-62). With several issues that mature technological states are dealing with, there must be a focus on the effects the implementation of digital infrastructure carries. Further issues involved, such as the properties of ICTs, is explicitly making the world ever more interdependent. This has to be interpreted into local processes that are being analyzed. Including how the potential for global impact works from local, regional, and international perspectives.

Different actors conduct conflict in cyberspace. These range from state to non-state actors. These non-state actors, typically described as "script kiddies," who`s technological savviness is advanced but still ranges as non-professional in comparison to state-actors. Also, such actors include groups like Anonymous, who have gotten media attention amongst others through the case of WikiLeaks. Other actors include criminal groups, which impose legal severe, economic, and political challenges. The economic impact of cybercrime is immense (ITU, 2016, 2019b; Kaldor, 2013). All states are affected by cybercrime. Providing real potential space as a conduit for further diplomatic engagement and cooperation on the regulatory frameworks on cyberspace governance (ibid).

Conducting actions in cyberspace that fall under categories of conflict in cyberspace provides an opportunity for obfuscation. This further solidifies the strong links between cyber as a new

domain where conflicts exist, in addition to the traditional land, sea, air and space, and its central role in hybrid warfare campaigns. Specifically, due to its traits to provide levels of anonymity (RUSI, 2019), which brings up several questions relating to attribution and standards of proof, these concepts are essential elements in cybersecurity. One of these issues is with the anonymity that comes with the digital domain. In a court of law, the practice is to "prove beyond a reasonable doubt." A strategic tactic in grey zone conflict is to use western legal premises in terms of attribution, as a weapon in its own right (RUSI, 2019). In this sense, there has become a notion that if there is not a hundred percent proof of a cyber operation, then it is not conclusive, therefor the accused actor per definition cannot be rightfully indicted. This is to hinder in terms of due process, capabilities, and resource management, concerning conflict in cyberspace (Rid, 2012, pp. 15-16). This is, however, out of the scope of this thesis to adequately address.

Capacity building is a contentious issue in its own right. Like that of security, arguing for both development and security processes, questions of who's security, security from what, and what are we securing are real legitimate questions. In terms of capacity building, this is a well-established concept (Browning, 2013). So, in terms of building cyber capacity, whose capacity is built? Who is doing the capacity building? Furthermore, for what reason or outcome are specific actions implemented? Also, is capacity building something that should be applied unilaterally across the globe?

As mentioned briefly earlier, the West carries a significant amount of baggage concerning its colonial history (Laqua, 2011). Exemplified through key seminal works such as Heart of Darkness, Wretched of the Earth, and Orientalism (Conrad, 1996; Fanon & Sartre, 1963; Said, 2014). Europe´s historical global ventures are fraught with precarious testimony. Encapsulated by Conrad, who phrased it as it was not so much the Europeans who were civilizing Africa, as it was Africa who turned the Europeans into savages. For Said (1979), the boundaries between the production of knowledge and material power could not diverge (Said, 1979, p. 1). History is, after all, primarily written by the victors.

Nevertheless, the sins of our fathers do not doom history to indefinitely repeat itself. Though this thesis will not address Foucault´s power dynamics, the production and reproduction of systems of power[37] would provide for an interesting analysis of some of the critical components of this

[37] Power and knowledge. The idea of de-colonizing academia are to incorporate a broader and encompassing literature to academia. The reflection are that academia are dominated through the colonial systems from which they were established. And are because of a narrow western prism, not reflected accurately in terms of a global production of knowledge. In this debate, deep philosophical

thesis. The point of shortly addressing the violent and capricious historical narrative of colonialism is to give accurate testimony too and to discuss elements of the vicious past that followed European global expansion. This also carries significant implications embedded in terminology, like that of sovereignty and interventions. Despite this colonial baggage, there has been a recent background of promoting democracy, IHL, and human rights globally from Europe, which includes a strong commitment to the rule of law, and a focus on more comprehensive economic development.

What then happens when an authoritative state like China is setting up its alternative and very successful development model (Fidler, 2018; Segal, 2017)? The belt and road initiative is one of Beijing´s most ambitious foreign and economic policy (Cai, 2017). While most often described in positive-sum terms – as opportunities to create trust, economic cooperation, and mutually beneficial ties. The One Belt One Road initiative could also be regarded as strengthening Chinese ´political influence and security situation along its strategically important periphery`, by undermining existing ones (Swaine, 2015). Chinas current model of ensuring that its resource demand are met has also been described as exploitive neo-colonial practices (CSIS, 2018). This is often described in the context of a rising China, reasserting itself on the world stage. The Belt and Road Initiative is a way for China to fulfill its domestic resource demands. To fuel China´s economic and hence political stability in conjunction with its sense of self. That is to fund its external political ventures. Which is also shaped by how China regards itself and the position it holds in the world. In this discussion, a rising China will have ´significant effects on the global balance of power` (Mearsheimer, 2010). The US pivot to Asia, stem chiefly for such reasons. And this debate will continue to dominate the foreseeable future.

Furthermore, some of China's capabilities manifest themselves in a domestic setting where a focus on strict social cohesion is vital, provided through well-institutionalized security apparatuses. By not placing such capabilities under sufficient restrictive measures, this carries significant negative consequences for the parts of China's population. This will be addressed at a later stage.

FreedomHouse (2018) has reported that for 12 consecutive years, there has been a slide on civic and political freedoms, not just in China, but across the globe. There is currently a growing body of literature detailing an extensive abuse of nation-state surveillance by authoritative states to

discussion on ontology and epistemology in relations to the historical narrative that shape peoples sense of self are key (Hall & Tandon, 2017; McDowell & Hernández, 2010; Swadener, 2004).

target and silence/disrupt the opposition, political threats, and critiques (Brechenmacher, 2017; Kendall-Taylor et al., 2020; Marczak, Alexander, McKune, Scott-Railton, & Deibert, 2017; Rutzen, 2015). We see this in China, Russia (CSIS, 2018), and other counters such as Saudi Arabia, following the War on Terror (Hegghammer, 2010). Deterrence, through the application of cyber travels from macro to micro levels, in its application. In terms of rapid development processes and unintended consequences. The international pressure applied to Saudi Arabia in the wake of 9/11[38] caused a massive surge in the Saudi security apparatus. Though the Saudi regime did not react initially to the pressure after 2001, it did become concerned with QAP, after the East Riyadh bombings in 2003. From then on, the Saudi regime entirely devoted its resources to combating Islamist militants - which included state-of-the-art surveillance systems — assisted by the US and the UK governments (Hegghammer, 2010, p. 217). The new approaches to CT practice in Saudi Arabia proved most efficient, and the advances that came with the latest security apparatus gave the police de facto complete hegemony over the internet, telephone, and road networks. This has been described as the most ´spectacular capability increase` in modern history (ibid). This new apparatus proved invaluable to the Saudi regime in exercising social and political control and deterring any political dissidents or other divergent actors of Saudi policies. Particularly useful under the Arab uprisings that swept the region in 2011. The regime's effective internal ´cyberwar` explicitly benefitted the political leadership (Al-Rasheed, 2013, p. 28; Kendall-Taylor et al., 2020) and are actively working on silencing criticisms towards the Saudi regime. The recent murder of the Washington Post columnist Khashoggi is a good example where the state needs to control the flow of information and the consequences that this brings forth within a framework that regards the free flow of information as a security threat.

This is not just limited to authoritarian styled governed countries. Democratic countries also use social media as propaganda in terms of distorting the truth to change or manipulate public opinion (Bradshaw & Howard, 2019). The created narrative is that malevolent external forces are subverting virtuous and innocent democracies. Which in itself is a distraction from how susceptible democratic institutions are to disinformation (Gunitsky, 2020). This is, however, not synonymous with democracies and authoritarian governments being indistinguishable. The extent of repression, censorship, and consequences of civil dissent and protest are far more significant in authoritarian states than democratic ones (Gunitsky, 2020; Kendall-Taylor et al., 2020).

[38] The majority of the hijackers aboard the airplanes on September 11 was Saudi nationals.

The ICNL has provided data showing that between 2004 and 2010, over fifty countries have imposed policies or other measures that have been restricting civil society. These actions are given legitimacy through being described as protecting state sovereignty and pursuing national security and often grounded in issues such as terrorism and the external interference in domestic affairs (Rutzen, 2015, pp. 30-31). FreedomHouse (2019) reported that since June 2018, ´33 of the 65 countries assessed in Freedom on the Net, experienced a deterioration in internet freedom`. Such processes are global in scale and are a cause for concern. Internet freedom in the US is in decline as US law enforcement, and immigration agencies are increasingly ´monitoring social media and conduct warrantless searches of traveler´s electronic devices.` CCB is essential to incorporate in systemic terms to safeguard the integrity of a state and its citizens. Both in top-down and bottom-up terms such perspectives are well studied in development programs (FreedomHouse, 2019; Muller, 2015, p. 5). While focusing on constructing productive top-down and bottom-up solutions are essential. This needs to be done while simultaneously addressing the foreign policy environment. For as this environment is complicating how we look at modes of warfare, conflict, and security both in domestic and international terms. There is not a single dimension that supersedes the process and thus requires the utmost attention. Instead, Lieberman (1993) argues that ICT's both have explicit and implicit "Orwellian dimensions," which not just carries the potential to, but facilitates repression in important ways (Liberman, 1993, p. 148). So, adhering to principles of human security while simultaneously have the national interest in mind is another point where security and development studies converge.

5. Digital superstructures, security, and development

As the previous chapter highlighted, there are serious efforts made at regulating technologies to dampen different dimensions concerning security competition. This chapter will combine theory and practice to showcase how security competition continues to evolve with the emergence of new technologies, including how security competition is opening both old vulnerabilities and creating new ones—emphasizing how this highlights the necessities for stronger international cooperation and more robust regulatory frameworks.

5.1 Digital infrastructures and vulnerabilities

All national cyber strategies make it clear that protecting critical infrastructure is of fundamental importance (Franke & Brynielsson, 2014; Luiijf, Besseling, & De Graaf, 2013; Nissenbaum, 2005; Trump, 2018; Utenriksdepartementet, 2017). Therefore, it has in recent years been diverted significant attention towards the domain of cyber and its utilities. As long as nations rely on computer networks to operate their infrastructure, power, water, military, economy, national security issues to any country in question are at risk (McKenzie, 2017, p. ix; Stickings, 2019). This includes how cyber has become operationalized in military terms. These strategies also mention one of the critical components to address these issues, namely that of multilateral partnerships (ibid). As highlighted earlier, the issues relating to a lack of international law, norms, and codes of conduct of actions in cyberspace are very much contentious, political issues. Though accepted that international law applies to cyberspace, it has not yet ratified in any treaty (ISC, 2017). And we have not, however, seen any real consequences of digital breaches of sovereignty. It is emphasizing the need to further build widespread cooperation on the subject matter. And how this will be crucial to tackle the security issues presented by this new domain (Schmitt, 2013, 2017). This is challenging in terms of cyber because of the opaque nature of the digital realm.

Other than calling out actors, by highlighting when cyber operations do take place, making them public and effectively shaming the guilty party in question, there is little real effect. Pluss that such activities can be challenging in their own right. Because of this intertwined, opaque, and omnipresent nature of cyberspace – the severe problem of attribution continues to haunt the regulatory process (ibid).

Also, though intelligence agencies are good at attributing such attacks, by breaching the OODA loop, decision-making processes can still be severely compromised. When Russia is aiming to ensure that its actions do not cross any perceived thresholds, the use of ´obfuscation and disinformation and planting doubts in the minds of key decision-makers is key.` Russia continues to employ what we call *active measures,* along with conventional and diplomatic efforts. These active measures include measures already mentioned like the control of traditional media, blackmail, and increasingly social media to achieve these aims (Giles, 2016; Lawson, 2019, p. 9; RUSI, 2019).

The critical importance of robust international cooperation on building such understandings is thus key. These issues have also become a significantly pressing issue in recent years (Bellasio et al., 2018, p. 1). Despite substantial amounts of attention; and significant progress, it is discouraging that international agreements have not yet come to fruition. Though through repeated attempts, such as the UN GGE, the Tallinn manual, or the Wassenaar Arrangement – which in 2013 proposed arms controls treaties on cyberweapons – there is yet to reach a consensus on how to regulate cyber (Henriksen, 2019; Singh, 2019). Though the Tallinn manual, along with the UN GGE, are the most robust effort of creating an overall view on the application of international law in cyberspace (ibid). The Tallinn manual ´reflects a western view on cyber warfare, as covered by existing international law,` and will most likely continue to be offset by Eastern powers (Lawson in Venkataramakrishnan, 2019).

Constructing a robust digital infrastructure is instrumental, not just in terms of international peace and security, but also in sustainable development practices. This includes the implementations of the regulatory systems that are needed to govern it. By 2025 the economic benefits of internet-related economic activities are expected to reach somewhere between 14 trillion and 33 trillion USD annually (Manyika et al., 2013). The ability to reap the economic benefits of the impact of the technological shift is significant for human development, but are conditioned on a safe and secure digital environment (Healy & Hughes, 2015, p. 2) Furthermore, as an instrumental tool within development processes the Norwegian cyber strategy states that

> ´Cyberspace provides a foundation for national and global innovation, growth, and development. With stable, robust digital infrastructure in place, there are almost no limits to what the internet can facilitate. Over the past 20 years, the internet has impacted most spheres of society`. The internet is now a superstructure from which all other infrastructures depend (Utenriksdepartementet, 2017, p. 5).

Following this, the digital flow of all communication is ´intrinsic to the development of any country` (Muller, 2015, p. 3). It should be stressed that it is not the view of the author that security policies are to dictate development policies or vice versa. However, a central element defining any cyber defense strategy, that the security/development nexus carries critical importance. Also, as developmental processes are built on ICT´s, *not* taking the necessary precautions needed to manage risks associated with ICT´s are, by definition, unsustainable (Morgus, 2018b). More so, this is actively pursued in Norwegian foreign policy. To the question of "what principles are applied when the strategic leadership of the Ministry (Norwegian ministry of foreign affairs) reviews new foreign policy initiatives or contemplate how to respond to new developments?" The reply was that; if they conclude that "Norway could make a difference," the next step would be to determine what "is in Norwegian interests to do." Such a response is textbook definitions in the application of FPA (Fermann, 2019, p. 83), and codifies the security dilemma.

Current Norwegian foreign policy on cyber is based on several threat assessments. DSB is the Norwegian directorate responsible for providing a comprehensible national threat assessment. This is an overview of risks and vulnerabilities in the Norwegian society and are subject to the Ministry of Justice and Public Security. They have been providing risk assessment reports since 2011; these risk assessments related to both natural and human-made crises that are both national and international. DSB threat assessment is one out of four threats, and risks assessments published each year. The other threat-assessment reports are delivered by PST, NSM, and NIS (DSB, 2019a). These assessments are technical and security-focused. Nevertheless, it would benefit from constructive input from the development community. Concerning a comprehensive understanding of who the external actors are on an intersubjective level. Specifically, towards understanding the operating environment and the actors in it. Which is a significant part of creating the assessments in the first place. Understanding the culture will thus be crucial. Culture is directly linked to understanding that this operating environment, which is not just digital, have real-world consequences, and are grounded in something tangible somewhere. This also means that as hybrid threats are going to characterize the future. Grey zone conflict will be the dominant form of ´persistent engagement` (Edelston, 2014), and current strategies need reappraisal to match and counter such realities as different national security strategies are based on different contexts. When strategies discuss the influences of external actors, often in terms of potential existential crises, and how to counter such, from many different audiences. You will not be able to base extensively sufficient analytical output, referring to those audiences, without a knowledge base that is set on from where those actors came.

The security-development nexus was further exacerbated in 2010, in the US national security strategy. That stated that cybersecurity threats represent one of the most critical national security, public safety, and economic challenges facing the US, highlighting that the very technology that empowers the US, also enable the ones who seek to disrupt them (Obama, 2010, p. 27). It also brings with it challenges of malicious behavior in the same digital domain. In 2016, estimates put the financial costs to the US, due to illicit or malicious cyber activity, at between 57 and 109 billion USD (CEA, 2018, p. 1). The global average of data breaches went up 6,4 percent in 2018, and recent numbers project a total cost of cybercrime at the end of 2019, to be an estimated 2 trillion USD (ITU, 2019b, p. 6). However, even though some countries will have supportive and enabling infrastructure that is required in place, including competency levels, theft, disruption, and espionage will still pose significant threats. However, despite these threats, there will be substantial economic benefits from these technologies (Pawlak & Barmpaliou, 2017, p. 123).

5.2 The Space Race – A source for conflict and cooperation

The space race was a characteristic defining feature of the Cold War. Exemplifying yet again that the link between development, and thinking about state security, is not something new. The Soviet Union was the first to reach space with the launch of the Sputnik One satellite in 1957. The US quickly followed suit. Initially shocked, US President Eisenhower and his successor, John F. Kennedy, responded swiftly and successfully in its aim of overall predominance vis-à-vis the USSR in space– under its overall foreign policy objective of soviet containment. Establishing the National Aeronautics and Space Administration (NASA) in 1958 (NASA, 2007). It quickly caught up with and accelerated past the USSR, which has never been able to catch up with US technological prowess.

Like Britain exerted its imperial dominance on the high seas, the US went on establishing its dominance in space. The US sought to create a principal, and thus an unchallenged role in space, securing military and commercial interests, with its right to govern space. It now operates nearly half of all satellites in space, both military, and civilian (Bulmer-Thomas, 2018, pp. 225-226). In 2010, the US further cemented its position in space with articulating clear strategic goals for its civilian/military critical infrastructure in space. The national space policy of the US government stated that;

> The United States is committed to encouraging and facilitating the growth of a US commercial space sector that supports US needs, is globally competitive, and advances US leadership in the generation of new markets and innovation-driven entrepreneurship … The United States will employ a variety of measures to help assure the use of space for all responsible parties, and, consistent with the inherent right of self-defense, deter other from interference and attack, defend our space systems and contribute to the defense of allied space systems, and, if deterrence fails, defeat efforts to attack them (ibid).

This perfectly illustrates the status-quo nature of the national interest, coupled with the concept of security competition. The space race is another example of how technological prowess fuels the security dilemma, as technology has done throughout time. Space has been increasingly militarized since the Sputnik One launch in 1957 (Stickings, 2019, p. 49). According to the former commander of the PLA Air Force Quiliang, ´If you control space, then you also control land and the sea` (Qiliang in Dowd, 2012). Whether through accurate artillery or the successful incorporation pf airplanes in combat or the nuclear bomb emerging technologies have always dominated the battlespace, this perhaps most apparent in space (Stickings, 2019). Also, we now see how cyber capabilities are deployed into a more extensive array of conflicting narratives. Controlling information, including the ability to dictate the narrative, is deeply rooted in core functions of the digital domain. Along with other offensive capabilities, deterrence has entered space as well as cyberspace (Buchanan, 2016, p. 64; Schmitt, 2013, 2017).

Yet, since the security dilemma is not deterministic, the space race is a good analogy to use in the search for common causes. The space race, for its quest for technological prowess, did not exclude cooperation. During the Cold War, the USSR and the US recognized the potential for space to be used for destructive purposes. The 1967 Outer Space Treaty banned the stationing of weapons of mass destruction in outer space (ACA, 2017). Article I states that space exploration should benefit and be in the interest of all countries (UNOOSA, 1966).[39] Also, the two states collaborated on their respective space programs (Buchanan, 2016). The symbolic value of this ought to be looked back to today in searching for common grounds in creating frameworks for the digital domain today. Creating parallel efforts in cybersecurity, as with the respective space programs, is possible. Not just between the US and Russia, but all actors in the interstate system.

[39] Yet compliance to this treaty are somewhat in the grey area. As satellites supports "all" military communications, intelligence, surveillance, recognizance and weather satellites proves crucial operation information. It is also worth noting that the Outer Space Treaty does not have enforcement mechanisms (Stickings, 2019).

Strong states have here a strong potential for cooperation to strengthen cybersecurity measures. It would require severe levels of trust-building, which are hard, but achievable (Buchanan, 2016, pp. 168-169; RUSI, 2019, pp. 52-53).

With the significant potential that the digital domain holds for creating conflict in cyberspace, which we have witnessed earlier, there is a significant escalatory dynamic as an inherent part of the properties of cyber. Concerning the applications of digital capabilities in the pursuit of domestic and foreign policies, this is particularly the case on the international level in terms of state-on-state interactions. As such, thinking about the development of digital networks and our dependency on ICTs, deterrence has entered cyberspace.

Up until this moment, the only invocation of NATO, Article 5, was following the attack on the US on September 11, 2001 (Gordon, 2007). Article 5 is the principle of collective self-defense and is the core of NATOs' founding treaty (NATO, 2019a). Though it is doubtful that such reactions will happen as reprisals from a cyberattack. Appropriate responses are currently being worked on (Schmitt, 2013, p. 42, 2017). NATO is presently pursuing such strategies, where the Secretary-General has publicly stated that armed responses could be initiated against a severe cyber-attack. The 2014 Wales summit declaration stated that there are currently real threats towards democracies and the purposes and principles to the UN Charter on a global scale. Also, it is now required extensive investments to uphold the political will that is necessary to safeguard the principles of liberty, human rights, democracy, and the rule of law (NATO, 2014). This involves a whole new set of legal, normative, and ethical dilemmas that are out of the scope of this thesis to address. By this, in short, the author is referring to how coordinated responses, which are in keeping with the rule of law and fundamental human rights, ought to look. Calling for measured responses to prevent, discourage and deterring malicious activity in cyberspace are key priorities – further showcasing the theorization on classic deterrence theory by retaliation in contemporary settings, and supplementary, how the establishment of security competition in cyberspace.

Other contemporary important issues on cyber and how to appropriately respond are

- How will democracies defend themselves against cyberattacks without triggering escalations?
- Foreign interventions in political processes.
- Digital attacks on critical infrastructure.
- Controlling narratives - The future of public discourse and political outcomes.

- The Huawei question, and the global development of the 5G network coupled with national security interests.
- The question of privacy online
- The 2017 attack on Aramco, and what this means for the global petroleum sector.[40]

Sustainability is the central influence in contemporary developmental processes. Challenges to development (local, regional, international) are faced universally for different actors. The transformation of economic, social, political, and environmental potentials is centrally integrated into the historical evolutionary narrative that is the continuum in which we operate. The forces of globalization are the driving force of current narratives – and this highly uneven process, which has, and will continue to distribute dividends disproportionately (Baylis et al., 2017, p. 470).

Highly developed digital infrastructure incorporated into authoritarian security regimes is neither security nor development, at least in sustainable terms (Deibert et al., 2012, p. 17).

5.3 Cyber as acts of development, conflict, or something in between.

´Cyberwar will not take place` (Rid, 2012, p. 6) versus ´cyberwar will take place` (Stone, 2013). A to be, or not to be question of our time. The debate on what conflict in the digital domain will look like, its implications, how to define it, and what it means in terms of future norms building, are serious questions concerning how we think about planning for tomorrow. This includes how to deal with escalations of cyber events and the applicable legal frameworks. There exists a significant space for creating cybersecurity norms. Particularly with the evolving and more conflict-oriented characteristics of the foreign policy environment (NIS, 2019, p. 6). Threshold warfare, and jus ad bellum, incorporated in domestic and foreign policy implications, are central contemporary political issues (Arquilla & Ronfeldt, 1997; Kiggins, 2013; Kretzmer, 2013; Rid, 2012; Sanger, 2018; Stone, 2013).

Rid (2012), argues against what was perceived as a coming new and fundamentally altering change to modes of conflict, namely that of cyberwarfare (Stone, 2013). Both contests to argue from a Clausewitzian standpoint. Rid (2012) argues that cyber war will not happen. This is because the tenants of how Clausewitz defined war are not met in the realms of cyber. Clausewitz defined war as; *War is an act of force to compel our enemy to do our will* (Clausewitz, 1832 Book one,

[40] NUPI have addressed implications for cyber-attacks against the Norwegian petroleum sector (DISP).

Chapter one) Rid (2012) argues that cyber-attacks are in themselves not violent, and since they are not, they do not constitute acts of war (Rid, 2012, p. 9).

The argument put forth by Rid (2012) came as a counter-argument against the hypothesis put forward by Arquilla and Ronfeldt (1997), that cyber war *will* take place. The notion was that the information revolution would cause shifts in both ´how societies may enter a conflict, but also how they will wage war.` In Clausewitz's terms, it is framed through victory on the battlefield is not just material, but who has the best information about the battlefield, creating *knowledge into capability* (Arquilla & Ronfeldt, 1997, p. 32). Furthermore, they argued that cyber will now dictate future conflict – this has yet to happen. However, US policymakers have determined that the same justifications for war in the domains of land, sea, air, and space, also applies to cyberspace – and thus reserve itself the same right to utilize force in response to a cyber-attacks (Kiggins, 2013).

To Clausewitz, war is a continuation of politics by other means - exemplified when Russia attacked Estonia in 2007, Georgia, in 2008 or Ukraine in 2014. Here the point of what the digital domain means in terms of state reliance's on ICTs came to bear. As coordinated attacks hit Estonia, the international community came to be attentive to the severe risks posed to advanced states by their technological reliance, for both the state and its populace (Schmitt, 2017, p. xxiii). Though the attack in 2007 was considered relatively mild, it was the first time we could apply Clausewitz's aphorism in principle in conjunction with cyber (ibid). It has been a failure in western policies to respond to Russian aggression in Ukraine adequately.

The EU failed to create coherent responses, vis-à-vis the Russian annexation of Crimea and Eastern Ukraine. The EU has still responded to challenges in other regions that it deems vital for security purposes. Vigorous policies in terms of the security/development nexus have been created since 2003 when the EU produced its first ESS. The ESS is now a deeply integrated concept to EU strategies, both in local, regional, and global settings. The Sahel region is one of these integral parts of European security doctrine. The EU sees development in this region as symbiotically to that of its own. The EU is, therefore, actively invested in numerous countries in the Sahel region. Though this is not cyber-related, it focuses intensely on what the holistic take of this thesis— namely that of the security/development nexus. The EU prioritizes a specific region that it sees as instrumental to its security. The EU runs significant investments into capacity building and general developmental projects across the region to promote sustainable development, security and stability - in conjunction with other multilateral bodies and operations,

such as MINSUMA, EUTM, EUCAP MALI and EUCAP Niger (ACSS, 2019b; EU, 2018b, 2019).

Cyber also plays a fundamental key role in the joint effort of combat terrorism, specifically violent Islamic jihadism and right-wing terrorism. As ICTs greatly facilitates the ability to radicalize remotely, as well as fund and facilitate in terrorist operations. (ACSS, 2019a; EU, 2018a, 2018b). The EU saw numerous violent jihadist attacks on the continent between 2014 and 2017. Primarily due to the ISIS campaign on establishing an Islamic State in the Levant, and the subsequent link to the ongoing fight against ISIS in Iraq and Syria. The high influx of foreign fighters further complicated this particular threat environment. Here there was a significant proportion of European foreign fighters. The digital networks involved in communicating, recruiting, funding, and disseminating propaganda are some of the dangerous elements of what ICTs can facilitate. ICTs are deeply involved and embedded in such terrorists´ networks. The ability to accurately deliver hyper-specific propaganda through social media signatures to vulnerable individuals is one specific risk element. The critical work of western intelligence agencies is a crucial factor in hindering continued attacks in Europe, with substantial success rates (Egel et al., 2019; Kilcullen, 2016).

5.4 A legal framework for norms building in cyberspace

So, how to counter the digital security dilemma, and thus mitigate the proliferation of conflict in cyberspace?

"Cybersecurity norms that limit potential conflict in cyberspace are likely to bring predictability, stability, and security to the international environment – far more than any set of confidence-building measures" (Osula & Rõigas, 2016, p. 243). Though cyberspace today is considered in real practical terms, an unregulated system (Henriksen, 2019; Kiggins, 2013), there have been made significant strides to apply international law to cyberspace. Political priorities still, however, takes precedence, impeding to date the considerable progress that has already been made into real tangible law-binding documents (Schmitt & Vihul, 2019). To date. ´efforts to delineate how states understand IL application in cyberspace have had limited success` (D. Hollis, 2020). This is in large part due to the obfuscation of cyber, and how it is interpreted. Particularly in areas of self-defense, IHL, countermeasures, due diligence, and sovereignty (ibid).

So even if it is recognized that international law applies to cyberspace, though this is not yet ratified to an international treaty. As it stands today, it serves more as guidelines rather than a universal codified charter (ISC, 2017; NATO, 2014; Schmitt, 2017, p. xxiii). There is a sense that states seems reluctant in large parts to codify cyberoperations within a legal framework. This includes a reluctance to invoke the language of IL into accusations against other states cyber operations (D. Hollis, 2020)

In an ever-increasing, complex, and volatile security environment, the (digital) security dilemma plays a significant role in shaping foreign policies – that serve both domestic national and international agendas. This is, in large part, on the failures on the ability to agree on what constitutes legitimate threats to national security doctrines, which are interpreted intersubjectively. As an example, The Tallinn Manual is the best document to date that sets up guidelines for responsible state behavior in cyberspace. This is in accordance with IHL and its application to cyberspace. However, this is perceived by the Russians and the Chinese as a conduit of western premises in shaping the legalities that will govern the legal interpretation of cyberspace (Venkataramakrishnan, 2019). — representing severe challenges regarding the creation of codified norms. As witnessed before, arms treaties are possible, but then again, so are the possibility of walking away from such established treaties and agreements. The recent termination of the INF and the JCPOA is examples showing how potentially vulnerable overarching premises are to local, regional, and global developmental processes. The regulation on the conduct of cyberwar, or responsible state behavior, has several significant obstacles that prevent its practical sufficiency – namely, a lack of definitional clarity and problems of attribution, rendering it unable to enforce consequences for transgression. It thus recommends an International Cyberwar Convention (ICWC), which would serve several vital institutional functions: rule clarification, a collective attribution mechanism, incentives for compliance, and authorization for countermeasures against transgressors (Eilstrup-Sangiovanni, 2018).

The UN established in 2004, the UN GGE. An UN-mandated group tasked with working on the field of information security. In terms of achievements, the UN GGE is credited for outlining the global security agenda and introducing the principle that IL applies to cyberspace, which was further established by the NATO CCD CE (GIP, 2019; Schmitt, 2013, 2017). Though progress has been slow, real progress on the development of state-behavior in cyberspace has been established. The UN GGE failure to ratify the final draft due to Russia, China, and Cuba's denial to be participatory to it should not be regarded as a failure of the UN GGE per se. The items on which Russia, China, and Cuba could not agree with the rest of the UN GGE was under

consensus in 2015. This leaves just the option that the lack of consensus in 2017 is strictly a political move, and not how international law in principle applies to cyberspace. The conservative approach adopted by these states in 2017 can, in some part, be viewed as an overall strategic aim of an international outlook shrouded in zero-sum tactics (Eilstrup-Sangiovanni, 2018; Henriksen, 2019; Singh, 2019). The Tallinn Manual is the most robust documents in terms of guidelines to how IL applies to cyberspace. For Eastern states such as Russia and China, the manual reflects a western view of cyber warfare, as covered by existing IL. And are thus not incumbent to adhere to the specifics of the document. This then suits western countries like the UK and the US, who have particularly effective digital espionage capabilities (Lawson in Venkataramakrishnan, 2019). Russia sees cyber operations as something radically different than their western counterparts. Cyber is instead another element in a broader information war (Giles, 2016; RUSI, 2019; Lawson in Venkataramakrishnan, 2019).

The Tallinn Manual, and the subsequent Tallinn Manual 2.0, are now considered the operational guideline on the application of international law to cyber operations (Schmitt, 2013, 2017). Also, domestic governments have invested considerable efforts to establish regulatory frameworks for cyber-capabilities. This includes the establishment of just not legal principles but norms, and perhaps of equally importance, transparency (D. Hollis, 2020). Other non-state actors have also sought to fill this information gap. The most prominent being the ICRC who have been significant in its attempt to apply IHL to cyberspace (ibid).

The US created its cyber command 2009, Russia passed three critical-data-infrastructure laws in 2017, and China recognized as early as 1999 that internet warfare was of ´equal significance` to kinetic war. Nevertheless, the Tallinn manual is the most ´comprehensive analysis of international law applicable to cyberoperations` - States have also recognized that international law applies to cyberspace. Also, IHL, which is a balancing act between military necessities and humanitarian concerns, is supplemented with overlapping bodies of that law that has emerged to protect civilians in conflicts, IHL being the most prominent one.

International law applies to how a state acts in cyberspace in the same way as anywhere else. This is now generally accepted, including at the UN level. Although the principle is not laid down in any binding international instrument. The practice and precedents of how cyber activity should be classified under existing international legal principles and concepts [are] underdeveloped. As a result, the application and analysis of existing legal norms to the analysis of cyber activity can vary considerably (ISC, 2017).

To adequately respond to these challenges, there is a real need for robust and multifaceted approaches. Both on the strategic level, to make shifts in the development community, as well as operation integrity in developmental processes. According to Morgus (2018b, p. 6), this can be done by;

- **"Reframe cybersecurity in the context of development** by shifting discourse to "security for" instead of "security from"; reframing cybersecurity around risk management, resilience, sustainability, and trust; and creating more opportunities to communicate and collaborate.

- **Build a library of credible and politically useful information to present to key development decision-makers**, like deep statistical studies on the impact of cybersecurity on development and a library of case studies and examples of the positive and negative impacts of cybersecurity on key development outcomes.

- **Demystify cybersecurity for aid recipients** by identifying good practices in cybersecurity capacity building that are backed by rigorous empirics and developing a toolkit to enable bottom-up agenda-setting.

- **Bring more expertise into cybersecurity donor institutions** by exploring short- term solutions like fellowships and secondments and leveraging funding mechanisms to create long-term cybersecurity portfolios in development donor institutions.

- **Create and implement digital risk impact assessments for development projects and programs**, following a model similar to that of human rights or environmental impact assessments"

Thus far, this thesis has covered how the digital space is incorporated into another domain in which national interest drives different agendas. As these agendas often reflect mutually excluding interests, they serve as sources for conflict, which continues to prove as significant challenges.

Best practices thus far have stemmed from robust multilateral cooperation. Yet, the operating environment seems to reflect an increased divergence of interest, rather than a focal point for cooperation. It is within this space that the author argues that both the security and the development community would benefit from a closer collaboration to meet future challenges.

6. Summary

For the author, the main challenge is how intersubjective interpretations drives different national interests. Including how several narratives can exists simultaneously, and that it is these narratives that drives said national interests. How to address and explained such issues are done from different theoretical fields and backgrounds. And it would not serve a purpose to critique such positions here. Rather, the critique could be specifically allocated towards the thesis premises and underlying assumptions. That is security competition in cyberspace will continue to serve as a source for future conflict. Also, that security competition will continue to exist not just in, but also outside of cyberspace. Including how ICT´s will function as an element in a broader hybrid warfare endeavor. And finally, that the development community should encompass security elements if it is to succeed in planning processes for sustainable development processes in the 21st century.

The following section will point to the politics and policy implementation in conflict zones and how the theoretical groundwork that has been the bases of this thesis ought to be viewed in practice. It will be a summary of the central premises that will be used in order to discuss several serious challenges faced today. It will describe the security dilemmas foundational role in terms of thinking about politics on local, regional, and international scales, including the intrinsic value to this concept as an analytical tool.

6.1 The security dilemma has lost its relevance

Interstate wars on a grand narrative have lost much of its immediate sense of imminence. From this, there have been arguments made that the security dilemma has lost much of its value. Instead, new dilemmas are emerging; these are principally concerned with values, or insecurity dilemmas. These dilemmas are intersubjective creations, identities, and interests that are ´constituted by collective meanings and are always in process` (Sørensen, 2007; Wendt, 1992, p. 407). In terms of values, this is what was promulgated by the West since the end of the Cold War. What has been dominant since the ´end of history` is a battle for values, and the export of democracy through the barrel of a gun has also proved faithful for the liberal project (ibid).

This is, however, not the case. Though it can be argued whether or not the security dilemma still constitutes as a priority - epistemological discussions on the value of any concept are always fruitful. However, *"competitive systems of interaction are prone to security "dilemmas," in which the efforts of actors to enhance their security unilaterally threaten the security of the others, perpetuating distrust and alienation"* (Wendt, 1992, p. 407). The nature of the concept has, thus consequently not, lost its inherent value as a system of analysis. Therefore, the security dilemma and subsequent security competition still provide a useful analytical tool in examining contemporary geopolitical state interaction.

With the new wars´ thesis and the following notion of the changing features of state-on-state and intrastate wars, some classic characteristics might be looked at as remnants of the past, rather than fruitful components of contemporary geopolitical discussions. However, as has been described throughout this thesis, classic perceptions still carry significant weight in shaping present policies. The changing dynamics and the ´myriad of transnational connections that blurs the distinction between internal and external, between aggression (attacks from abroad) and repression (attacks from inside the country), or even between local and global,` are not necessarily new. Rather the Cold War overshadowed such elements (Kaldor, 2013). The New Wars thesis encapsulates how a category of new wars have emerged around the mid-1980s. Now globalization acted as a catalyzer where a ´contradictory process involving both integration and fragmentation, homogenization and diversification, globalization and localization` (Kaldor, 2013, p. 4). Within such a framework, conflict is based around the disintegration of states with the following pursuit of violence. In this pursuit, the struggle for control of the state by different, and opposing actors, who are fighting for control of the state while simultaneously imposing their own definition of a specific national identity (Baylis et al., 2017, p. 222).

Clausewitz still offers the most concise concept of war. ´War is an act of force to compel the enemy to do our will` (Clausewitz, 1832, p. 11). The politics of tomorrow will continue to be shaped liked the politics of today. That is concerning the intersubjective components that make up the system. And thus, conflict will continue to permutate as conflicts of interests will continue to exist.

The security dilemma through security competition encapsulates such dynamics as well. Arguing that intrastate and interstate war of the past is not something entirely different from contemporary intrastate/interstate wars. The potential for spillover effects carries influential factors in shaping other state actor's national strategies. For example, the creation of ISIS had destructive security implications in the Levant. Isis was off course not confined to the Middle

East or the greater MENA region. The security implications that stemmed from the creation of ISIS was global in scale, reaching from the Philippines to the EU and the US (Kilcullen, 2016).

Since ISIS was not restricted to the Middle East, there were several direct security threats that rose from this from an EU perspective. Some of these security implications were; foreign fighters leaving Europe for Syria to join ISIS, and the threat that this posed of these (and other) fighters returning with a mission to conduct terrorist operations on the European continent.[41] Europe experienced several significant terror operations in conjunction with the war on ISIS, which led Europe to adopt security strategies that made inwards migration a severe issue.[42] The political climate got skewed further right, legitimizing far-right discourse as normative in the public political sphere. Far-right reactions in terms of terrorist actions have also come as a response to what is in far-right milieus labeled as a "Muslim" threat to Christian Europe (Kilcullen, 2016; Nesser, 2015).

Afghanistan from 2001 and Iraq from 2003 are obvious cases where we can reference both state and non-state actors. Where the national interests of the US, in the case of Iraq, drove the world community into the GWOT – the war in Afghanistan came as the response to the attack of September 11, followed by the invocation of Article 5 from NATO. In terms of Afghanistan, the intervention was justified in accordance with international law (Baylis et al., 2017, p. 323; Tuschhoff, 2005).[43]

The 2003 Iraq war is, however, a different case altogether. The invasion of Iraq can be described as the most significant foreign policy blunder of the 21st century. With a profound lack of understanding of the people, culture, economic, social and political setting in Iraq, the US sledgehammer approach led to the disintegration of the Iraqi state, unequipped to provide

---

41 Some of the security implications in relation to European foreign fighters was the fact that these held European passports. In terms of the European idea, this provided the opportunities to travel freely on the European continents. Providing additional mobility in terms of planning terror attacks.

42 Migration is a contentious and precarious political subject. In terms of securitization theory, including the war on terror, migration and its political implications is a frequent subject to be addressed (Romaniuk & Webb, 2015; Stritzel, 2007). Also, ´The spread of ideas, cultures, and information … both among like-minded peoples and between different cultural groups – reinforcing simultaneous tendencies towards both an expanded sense of global solidarity among the like-minded and difference, if not outright hostility, between different culture, nations, and ethnic groupings` (Baylis et al., 2017, p. 17).

43 Afghanistan have been continuously in war since 1978. State capacity in Afghanistan are seriously diminished. Such capacities refers to the Afghan states ability to create an administration capable of effectively tax its population, creating robust coercive agencies (police, military), and forging strong national identities and social cohesion (Brian D. Taylor & Botea, 2008).

essential basic services to its populace. Consequently, the US failed to convert its military victories into political ones. The implosion of Iraq after the removal of Saddam and virtually every state structure in the country ultimately left a power vacuum where al Qaida in the Levant eventually seized the opportunity and consequentially morphed into the much more sinister group, Daesh (Holbrook, 2015). Gaining traction after the US de-prioritized Iraq from 2011 onwards, which ultimately left a significant gap for the ISIS campaign to gain significant traction, the US had to renew its military commitments to Iraq in 2014 as a result of the resurgence in violence. Daesh or ISIS posed a severe threat to domestic local groups in both Iraq and Syria. The Yazidis are a particular group of people who particularly suffered under the atrocities of Daesh. As well as posing significant threats to the broader region, as well as for international peace and stability. Daesh posed significant dangers on both local, regional, and global levels (Abuza & Clarke, 2019; Kilcullen, 2016; Nesser, 2015).

The civil war in Syria, though being intrastate in nature, has had great significance in its application in geopolitical affairs. This applies to both different state and non-state actors, both on and off the ground. Acting out of national interest, such actors include Syria, Russia, Iran, Turkey, the US, UK, France, and Israel (CFR, 2019a; Stent, 2016). Though Daesh is mostly defeated in territorial terms, ideas are not geographically fixed. ISIS is still active in Africa, the Middle East, South, and South-East Asia (Coats, 2019). The effort to suppress a further resurgence of a significant terrorist threat, not just in Iraq and Syria, but also concerning Libya and Afghanistan should be warranted. In short, this is a threat that will require constant diligence to suppress in the foreseeable future, not just in the Levant, but on a global level as threat levels concerning terrorism and terror operations are high (Coats, 2019; MI5, 2020; NSM, 2019).

In the case of Libya, we can identify precise junctures both in terms of development processes and the implications that the geopolitical environment exerts on these processes. In terms of thinking about economic development relating to the petroleum sector, Gadhafi was revolutionary in many terms. Specifically, in regard to economic development, in the 1970s, Gadhafi claimed full sovereignty on Libyan oil, causing that all negotiations for Libyan oil export had to be renegotiated. For the first time in history, an Arab oil-producing nation would sit with the majority of the income created by petroleum exports (Rogan, 2011, p. 417). With the growing dynamics of the Arab spring in 2011, Ghaddafi made diligent efforts to suppress the revolts. Some of these efforts resided in threatening to *exterminate* the civilian population in Tripoli. The world community, particularly after cases of non-intervention in the ´90s, with a particular

reference to Bosnia and the genocide in Rwanda,[44] needed to respond to the actual, and threatening atrocities that were happening on the ground in Libya (Morris, 2013, p. 1265). To avoid what was perceived as an immediate humanitarian catastrophe a resolution 2009 was drafted by the UNSC, to invoke R2P on behalf of the civilian population in Libya. In this sense, sovereignty was effectively breached in Libya because the sovereign, in this case, Ghaddafi, was not meeting its obligation to its people. Due to the severe nature of this transgression, external actors, primarily NATO through the UNSC, had the right and the responsibility to intervene to remedy the situation (Morris, 2013; UNSC, 2011). The mission was to protect the civilian population on the ground from the threats and actions taken against them by Libyan forces. In more specific terms, "R2P" was set in effect and executed by NATO, with the implementation of operation Unified Protector (NATO, 2012). NATO´s Unified Protector supported the rebel movements with aerial mission sorties of targeted airstrikes against the Ghaddafi regime. This was sanctioned under the mandate to protect the civilian population from government forces by the UNSC (Curran, 2017; Hehir, 2013; NATO, 2012; UNSC, 2011).

Like Iraq in 2003, the potential consequences for what would happen in Libya after the removal of such a state institution as Ghaddafi were not adequately addressed before the intervention. However, the possibilities of the genocide that Ghaddafi threatened justified the response (Morris, 2013). With the start of the Arab spring, people optimistically hoped that a wave of democracy would spread across the region (Wolfsfeld, Segev, & Sheafer, 2013). Instead, the story of Libya took a more sinister route. It morphed into a civil war that continues to this day. And are now described as the ´drone strike capital of the world` (Lacher, 2020). Where all facets of hybrid warfare elements are frequently used. The usage of drones provides plausible deniability. Giving actors involved more leeway in terms of operational rules of engagement. The usage of actors on the ground. Libya´s warring factions are supported by different external state-actors, contributing to the ongoing civil war. External actors involved ranges from Russia, the US, France, UAE, Saudi Arabia and more. The use and spread of disinformation are rampant in Libya. If successful, it can sow confusion in the populace, and legitimize war crimes, or blame

44 ´Following catastrophic experiments with peace enforcement in Somalia in the early 90s, the inability of UN missions in Bosnia and Rwanda to protect civilians from egregious abuses led to the Brahimi report of 2000. Institutionalizing a relational for subsequent missions whereby the 'minimum use of force´ principle was reinterpreted to include the application of force in defense of the mandate as well as themselves` (Hunt, 2017, p. 110).

said crimes on the enemy. In blaming opposing actors, the possibility to create and invent narratives and mobilize larger publics becomes increasingly useful (Lacher, 2020).

The political landscape is fractured with disputing components in its political and military systems, including the economic setup of the country. With regard to the political system, this is currently split between several institutions that claim legitimacy in different regions of the country. The GNA is the internationally recognized government body in Libya, though it only holds low levels of legitimacy in the country. It stands in opposition to the self-proclaimed field marshal Khalifa Haftar who is linked to the parliament in Tobruk, and are the leader of the LNA (Trauthig, 2019).

In terms of Cyber, Libya offers a particularly fertile environment for the use of digital propaganda and information operations. Directing disinformation campaigns towards a country that provides little history of independent, professional journalism is "productive." Particularly if a specific country carries a legacy of mass indoctrination by governments attempting at shielding society from global information flows, which are again the case of Libya. Such conditions make perfect for the spread of conspiracy theories. By "weaponizing" media news outlets, the promotion of hate speech and lies, also give grounds for atrocities that are happening on the ground. There is always an opponent to blame. It is not just confined to local actors, as such operations carry significant international elements (Lacher, 2020).[45] The net result is a Libyan public sphere that contains a ´toxic mix` of disinformation, where ´nothing is immune to manipulation`(ibid).

The Libyan case has also proved precarious for Europe due to several other issues. The humanitarian element has been immensely coupled with the security risks that the civil war in Libya has provided. Libya. As the country served as a critical route of human trafficking, weapon, drug, and oil smuggling, including the function as an essential migrant route between MENA and Europe (Eaton, 2019; SIPRI, 2019b; UN, 2017).

With respect to Iran, the US´s withdrawal from the established JCPOA, tensions have continued to rise in the Persian Gulf - with recent attacks on oil tankers and facilities, including cyber operations (CFR, 2019b; S. Gross, Maloney, Riedel, & Byman, 2019). The US diverged from international norms in significant ways with the assassination of General Soleimani, the

[45] Facebook and Twitter has taken down hundreds of pages of "created" content that has been produced in order to distort the realities on the ground in Libya. Actors involved in these disinformation campaigns include Saudi Arabia, Egypt, UAE, who ´coordinated inauthentic behavior` against Libya (Facebook, 2019; Twitter, 2019).

commander of Iran´s Islamic Revolutionary Guard Corps´ Quds Force – in Baghdad on the 3 of January 2020. Further escalating tensions between Iran and the US to new heights, risking sparking direct conflict between the two states. This *is* a watershed moment. The US has now taken it upon itself to expand its AUF to target not only non-state actors but also state-actors. In the GWoT, drone strikes have been a frequently used tool in US strategies based on forward presence. The use of targeted killing operations directed against terrorists and terrorist affiliates have only increased in size (Romaniuk & Webb, 2015). The use of drones and targeted killing operations should not be considered problematic as they are just another tool used in warfare. However, the use of drones or military means outside of formally recognized warzones are problematic. Including when control of such weapons of war is provided to intelligence organizations to operate, such as the CIA.

It is not new that there have been divergences in terms of normative, ethical, and legal dimensions and principles in the GWoT. The classic case of a successful securitization attempt described by securitization theory is the GWoT. With the acceptance that the GWoT was battling an existential threat,[46] the extreme measures taken as consequential actions were legitimately justified; from the removal of civil liberties, acceptance of extensive collateral damages, torture, drone assassination programs and the invasion of Iraq (Romaniuk & Webb, 2015, p. 223). In regard to the attack on General Soleimani, the US has now effectively sanctioned assassination programs on state officials. The POTUS disregard for the rules of international engagement will have significant effects across the region. Consequences will carry both short-term and long-term implications. Iran has already taken some of the short-term actions and responded with cautionary measures. With Iran signaling strength vis-à-vis the US, with recent attacks on US military bases in Iraq. Though Iran simultaneously warning the US prior to the incoming attacks, ensuring not to directly kill US forces, which would have furthered the escalatory dynamic of the situation. Some of the long-term consequences will be further strained relations on the US and its allies. Both in Europe and in the Middle East. This also includes a broader resurgence of a terrorist threat. Mainly as it creates a window for terrorist organizations in the region to respond to already strained coalition alliances, including the potential fallout it will have for the wider region, both in MENA and South-Asia (Karim, 2020; Vakil, Mansour, & Khatib, 2020; White, 2020).

[46] The existential threat in this case is terrorism. Specifically, violent jihadi extremism.

Other recent developments include the Turkish invasion into Syria. This invasion was in large part due to what Turkey saw as a direct national security issue, namely the Kurdish issue (Guzel & El Deeb, 2019). Kurdistan is a large and contested area that reaches into Iran, Iraq, Syria, and Turkey. Concerning statehood, or the lack thereof, the Kurds are the largest nation in the world without a recognized independent state. In Northern Iraq, the KRI have achieved a recognized semi-autonomous region, after the end of the first Gulf War of 1991. The Kurdish issue has continued to grow to one of the central issues in the Middle East (Gunter, 2004, p. 197; Pike et al., 2017, p. 301). Kurdistan is hard to define in precise terms. After WWI and the dismantlement of the Ottoman Empire, Kurdistan was approximately divided between 6 states. Turkey has the largest share (43 percent), Iran (31 percent), Iraq, (percent), Syria (6 percent), Azerbaijan, and Armenia (2 percent) (Gunter, 2004).

Pike et al. (2017, p. 301) address the KRI as situated between rentier states,[47] economies markets that carry both internal and external geopolitical instabilities. It suggests that this disfranchised group ´have endured a century of statelessness.` With the experience of recurrent periods of ´destabilization, crises, including destabilization over decades.` This has had profound effects on local and regional development in recent history being suppressed under British colonial rule, implemented in 1918 and then subsequent marginalization and oppression under Iraqi nationalist rule, by the Ba´ath regime.

Though this is not wrong per se, it implies that contemporary western colonialism is solely responsible for this precarious subject, which is too simplistic, in the sense that it is neglecting four centuries of Ottoman rule to that specific region. That being said, WWI was tremendously influential in the making of the modern Middle East. The Middle East transitioned from an Ottoman-ruled "monolithic empire," to the Arabs being divided into several newly created states under British and French colonial rule. Some Arab States achieved independence – Turkey, Iran, and Saudi Arabia; others, such as the Kurds[48], did not. These state lines and systems of governance were discussed throughout the lengths of the war and, in retrospect, only makes sense within its wartime context. From the Sykes-Picot Agreement to the Balfour Declaration, these outlandish agreements were made to advance European imperial expansion (Rogan, 2011).

[47] Rentier state, or rentierism, is typically explained as the financial autonomy of oil states grants them immunity from social pressures.

[48] The Kurds was never attributed a state in the European partition of the Middle East, following the victory of the allies in WWI. Though ambitions for self-determination existed at that time. The Kurdish issue was “solved” from a European imperial perspective in the Sykes-Picot Agreement.

In the effect of balancing power dynamics in a colonial setting, the security dilemma proved as a catalyst to such processes. However, neglecting prolonged Ottoman rule is not something that should be done frivolously in such a historical context.

Addressing the Kurdish issue is integral to overall stability in this regional context. As mentioned, Kurdistan encompasses four states, all of whom hold more extensive interests in the region, both foreign and domestic. Turkey has recently invaded Syria, as US troops are being pulled out of north-eastern Syria (a small US force continues to be active in Syria). The US foreign policy objectives in Syria were to align themselves with partners in the fight against Daesh. The primary partner who provided functional combat forces were the YPG. Thus, the US engaged in an unholy alliance that proved tactically sound—but doomed in a strategic sense. The YPG, with support from the US, proved capable of fighting Daesh. Nevertheless, recent policy developments from the current Trump administration has been to cut ties with the YPG, leaving them in a highly precarious situation (Feaver & Inboden, 2019). However, this was inevitable as the US has failed on many terms to come up with any viable enduring strategies in this region. A major concern is the fact that Kurdish independence is a direct threat to the political and territorial integrity of all of the KRGs neighbors. Thus, failing to see the wide-ranging implications of what Kurdish autonomy would look like in the region and to the specific countries in question. Neither Turkey, Iraq, Syria, or Iran would see its borders formally changed to make way for an independent Kurdistan. Furthermore, the relationship between the YPG and the PKK would make any long-term partnership with the US unsustainable. The US, EU, and NATO define the PKK as a terrorist organization. Turkey is a NATO ally. Any alliance with the PKK, or PKK affiliates such as the YPG, would be opposed internally in the alliance - as well as externally. The moment that the US allied itself with the YPG in the fight against Daesh, it put itself on a collision course with Turkey (Taleblu & Tahiroglu, 2017; Zalewski, 2014).

With the US effectively having greenlit a Turkey invasion of northern Syria, Turkey is on its way to create what has been designated a safe zone in northern Syria. This buffer zone on the border between Syria and Turkey have been created for several reasons. The recent Turkish invasion has been masked as a humanitarian intervention to bring stability to the region, which is an essential language for diplomatic purposes to legitimize actions to the world community. The raison d´état of Turkish operations in Syria are far less altruistic. Turkey seeks to hamper or kill any initiative of Kurdish independence and sees any struggle for Kurdish independence as interlinked with the PKK mission to partition Turkey to create a Kurdish state (Kaufman, 2019; Todman, 2019). It has also speculated on the forceful relocation of millions of Syrian refugees who are currently in

Turkey due to the Syrian civil war. If Turkey is to resettle a significant amount of refugees on the border, this will have the potential to change the ethnic makeup of this specific region dramatically, fueling further instability (BBC, 2019b; Belkaïd, 2019; Todman, 2019). With the exfiltration of US troops, the YPG turned to the Syrian army to halt the Turkish invasion. The Syrian army, led by President Bashar al-Assad, was then deployed to counter Turkish-led forces. Russia, Presidents Assad´s staunch ally and security guarantor, have, in conjunction with the US negotiated the Sochi agreement. It was signed with Turkey on the 22 October 2019, which in essence re-configures the Kurdish autonomous zone. Kurdish forces through this ceasefire agreement are required to pull back from the border. Alternatively, leave Turkeys buffer zone.

As was mentioned in the methodology, the limiting scope of this essay acknowledges that it cannot correctly address all topics that have been brought forward. Such a volume would have to come, either as an extension of this thesis or as a response to critique. There has not been made attempts to adequately address such specific topics and consequences of the Russian annexation of Donbas and Crimea. Other topics include the security competition of Russian and Chinese military posturing and security competition vis-à-vis the West. This includes several situations that are currently existing on the African continent. Specifically located in areas ranging from the Maghreb and across the Sahel region, and in the greater MENA region, which includes seven blue helmet operations such as MINSUMA, and UNAMID (Koops & Tercovich, 2016; UN, 2020a).[49] The overall point that would be in the latter instance is the massive implications the last 20 years have posed on the civilian population in the greater MENA area and the significant effects this has had on development projects in the area.

The security dilemma is still an axiom in international relations and carries real-world implications. Which can result in severe outcomes in terms of human security. It is because of these implications that there needs to be a stronger bond between the development and security communities to thoroughly create capabilities to address situations where people will be at their most vulnerable. This weigh more cumbersome on the development community as critical theory is already playing a significant role in shaping security studies (Barkawi & Laffey, 2006; Hopf, 1998; Wendt, 1992). Wars and conflicts are carried out through and among people.

[49] UN peacekeeping operations in Africa are currently located in the Sudan, South Sudan, Central African Republic, Democratic Republic of the Congo, Mali and Western Sahara.

Moreover, the interaction between troops, enemy, and friendly combatants, as well as civilians on the ground, requires a deep anthropological understanding of the geographical area[50] where the specific conflict is taking place. In convergence with essential surroundings, the information war is the control of information and the battle between the narratives. In a security setting, this is significant as lessons learned, or at least lessons identified, is that there are no ´good crusades` and the battle of the narrative will be crucial in terms of security being first and foremost political.

> There is no need to give a lengthy description of all the misery inherent in war—you know that already. No one is forced to war unwittingly, and no one is deterred from war if they think they will gain from it. So what happens is that one side sees the advantages as outweighing the dangers, and the other is prepared to face the risks rather than suffer an immediate loss (Thucydides, 2009, Book four).

6.2 A Eurocentric perspective.

The thesis carries a pro-western centric point of view, not addressing or reflecting, an accurate picture of the threat landscape, but cherry-picking selected and "created" hypothetical entities. Also, it does not discuss the West's role in creating conflict, not solving it.

The UN was originally a western build organization, meant to serve western interests. That does not mean that this is now the overall focus of this multi-lateral body. The world order that we currently live in was established post-WWII. This is not something that one can change, but it can be pointed out, and that has been the case in this thesis. The Russians and the Chinese have been much of the focus point (with emphasis) on Russia. Primarily because of the international state system built by the US post-WWII. The American "empire" never included those key countries. The US was thus never a truly a global hegemon. Instead, it is best described as a semi-global empire because its global reach never included Russia or China. These have rather existed outside of the West. It is now this polarization which is dominating the geopolitical arena.

The UN has established a set of principles codified in the UN Charter to maintain international peace and security.

[50] This could be described from a military perspective as the battlefield. Or it can be defined from the NGO sector as the humanitarian field.

> and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace (UN, 2019c, pp. Chapter one, Article 1.1).

There are reasons for concern within the language used by the UNSC. From a post-colonial perspective, the UNSC would serve particular interests in international politics. Not just interests, international politics in itself would be regarded as a western exercise. This exercise has been essentially through a Eurocentric focus within world politics and security studies itself. Which produced and reproduced already established international systems of governance (Barkawi & Laffey, 2006). Last and not least, the very language of the UNSC should be viewed with cautious means. When the language of ´threats against international peace and security` is used, this can be seen as a prelude to interventions sanctioned by the UNSC.

However, not all contemporary western practices need to be observed through a prism where the reproduction of systems is facilitates western oppression of the designated third world. They are not all excluding, with the sole aim of forwarding western interests. The UN, as an institution, can be critiqued in legitimate terms. However, it would be disingenuous to dismiss the entirety of its mission. As a vehicle to promote dialogue on an international level, this serves as a critical function of the UN. Seeking developmental processes based on justice and IHL rather than exclusion and oppression (Benjaminsen & Svarstad, 2009).

The authoritative states of China and Russia regard such principles as western made and not to be taken seriously. It is therefore correct to a certain extent that there is a western bias in this thesis, as this lies in a direct opposition to authoritative state repressive practices through all modes of governance. Free societies ought to be valued, in order to safeguard citizens across nations. Where the rule of law and constitutional restraints on the political leaderships are not comparable to deep state or authoritarian regimes, preventing such constraints should be enforced in certain specific domestic policies. Like that of Chinese practices in relation to its Uighur population. However, in the US, there still exist issues that seem to be counteractively intuitive of this, examples including the Guantanamo facility in Cuba and the current ICE facilities. Such policies are contradictions in light of the political message it sends of perceived democracy and human rights—highlighting yet again the precarious nature of how the state views security and takes what it deems necessary the necessary precautions deal with a securitized topic.

Also, the UK and the US are primary state actors with offensive cyber-capabilities. It should, however, be clear lines between the offensive coercive measures taken of authoritarian versus open, democratic nations. Though much of the information in this domain would be classified top secret, democratic countries do limit all-encompassing centralized state authority as one key element in terms of state-structures.

Democracy is the mitigation of arbitrary and authoritative power. This does not mean that democracies are untarnished or are not using surveillance in lieu of national interests. When US intelligence agencies wiretapped Chancellors Merkel's phone (Landau, 2016), this is not just disconcerting, but a severe breach of trust among allies, threatening to undermine existing partnerships between the two nations respectively. Placed on a level of how coercive this particular instance is, by putting in context with what western adversaries are doing, the case of Merkel is not as grave. Though this should not be seen as an argument of trying to legitimize the extents to which spying on allies are legitimized. The GWoT has also initiated several severe surveillance programs, which does not distinguish in friends or foes. The collection of bulk meta-data is intrusive but for security purposes are (perceived) as legitimized. The reason why this is different in terms of other surveillance-oriented programs can be displayed through the EU's work on GDPR. Where again, the protection of the individual by law, reflects a mode of governance that distinguish it from other more repressive methods of governance.

In this respect, there is a need to refer to the case to the democratic peace debate - another axiom of international relations. Democratic, or liberal peace theory, simply states that democracies do not go to war with one another (Dunne, et al., 2016, p. 75). However, that they are more peaceful in general terms is controversial (ibid). This brings forth important questions in how democracy, liberalism, and force ´contribute to a peaceful world.` With particular references to how liberalism has been spearheaded by looking at democracies and war in terms of historical processes of global societal change (Barkawi & Laffey, 1999). Doyle (1983) argued that even if liberalism has had striking success in the creation of a ´zone of peace.` Primarily through cooperation between states similar in character, it has equally been a failure. This failure is directed at liberal states using liberalism in spearheading their foreign policy outside the liberal world (Doyle, 1983, p. 323).

> our soldiers overseas, rejecting the universalism of the mother country, apply the ´numerus clausus´ to the human race: since none may enslave, or kill his fellow man without committing a crime, they lay down the principle that the native is not one of our fellow-men (Sartre in Fanon & Sartre, 1963, p. 13).

There have been made several examples of critiques against Western policies in this thesis. Particularly that of the US in terms of adding to the current evolving threat landscape. Including European and US colonialism.[51] Such as the withdrawal from the JCPOA or the US policy on Israel. There is a clear argument of what can be labeled as the inconsistencies in US foreign policy and security strategies. For example, western democracy promotion is the source of conflict, not the solution to it (Durac & Cavatorta, 2009, pp. 3-4). It would, however, be academically idle to single handily use a post-colonial perspective in addressing several issues the current international global order is facing. This is why, yet again the importance of not sticking to a single dogma will be vital in addressing critical issues going forward. This will require substantial institutional foundations in IHL. And not by repressive approaches loosely legitimized in foreign threats.

Though several complexities are addressing such issues, some are founded; others are not. Russia and the West have very different approaches on how to handle information, as they have in terms of the application of IL and IHL. Furthermore, the issues of foreign, or existential threats, are problematic, as mentioned introductory in this thesis. This is why it is crucial to dissect presented security issues to discover what they entail explicitly. Who are actors involved, what is being threatened, or in need of additional security? What is the object being secured against, etc.?

Securitization theory is an excellent example of the application of critical theory on security studies. Most commonly referred to as the "Copenhagen school" (Romaniuk & Webb, 2015, p. 224). Securitization is defined as

> Successful speech act ´through which an intersubjective understanding is constructed within a political community to treat something as an existential threat to a valued referent object, and to enable a call for urgent and exceptional measures to deal with the threat (Buzan and Wæver in Stritzel, 2007, p. 358).

In other words, there is an existential threat to a valued referent object, accepted by a target audience that will allow steps taken of extraordinary measures. This then makes it a socially constructed issue. What this in effect does, is explaining how a particular issue becomes securitized. Furthermore, how such issues are consequently dealt with through extraordinary measures. These measures are allowed to exist outside the realms of normal politics (ibid). Using

[51] It should be mentioned that US colonial practices are characterized as more indirect, rather than direct. In comparison to former French or British colonial practices.

such analytical tools will be fruitful in de-securitize several matters which are falsely portrayed as existential crises. Both to western and non-western audiences. Securitization theory then is a handy element to incorporate in the analysis of threat assessments and strategies. Securitization theory then provides a valuable asset, not only to the field of security studies but also to critical theory and development studies. The sophisticated, pragmatic, and innovative analytical framework provided is of high usage dissecting policies that have left the public domain. This sophisticated and straightforward nexus provides a taxonomy in which securitization theory addresses particular issues. And are able to dissect key elements like actors, messages, audiences, and measures applied to solve specific challenges. All of this as being within a framework of normal politics, or if it has been securitized. And by which one sanction extraordinary means to deal with particular political issues. The ability to separate concerns and then to elaborate on them provides means of adequately explaining, critically, when policies are taken out of, or back into the realms of ordinary politics.

The importance of the public to be critical of policy implementation done by its government are as crucial as ever before. With disinformation existing all around us, useful tools to analyze former and current policies are essential. The continuation of critical theory is pivotal in achieving this. To achieve lessons learned (or lessons identified) comes through the critique and analysis of how to better existing structures, such as legal, economic, or political.

It can be that when the Western hegemon position disappears, it will be a joyful experience of the international peace and security, and not least prosperity and a focus on SDGs that have not yet come to pass. The author believes that that is not the case.

Epilogue

This interdisciplinary project has addressed some of the challenges that modern societies are facing as a consequence of globalization. These societies are built upon the superstructure which is our digital infrastructure. Meaning that ICTs functions as a supra-infrastructure that serves as a foundation for all other infrastructure projects. This thesis highlighted int the introduction how Britain is both more secure and more vulnerable than in the majority of her long history. It is this ambiguity that has to be balanced, not just for Britain, but for all societies.

The flow of information are highly susceptible to manipulation and therefore will prove to be a significant task as to not only mitigate such actions, but to create the conditions where sound political decision-making processes can take place. Decision-making which is not caused as a conclusion of a successful CO, which have manipulated, altered, or otherwise changed one outcome, due to altering an agenda, changed a narrative, seeded additional distrust or polarized a society. Also, by creating awareness of how such systems can facilitate repressive state actors and undermine democratic ones.

As previously mentioned, STASI had an entire army, whose sole focus was to keep tabs on people living and operating in East-Germany. The daunting scale of such an operation to control information testifies to the centrality of how important information is, and how it is regarded as a security matter. This includes governments attempts to control information flows. Contemporary ICTs can facilitate such processes, in which the immense size of the STASI bureaucracy is no longer needed. In addition, computing power has replaced manpower, which has contributed to both increased scale and intensity of which governments can spy and keep track of its citizens.

Though there has been a strict focus on some of the implications relating to security issues that modern societies are facing, this thesis has been about the significant opportunities that exists for cooperation. Not just between the security and development community, but between states. The role of moderator which the UN plays is significant in this task. Furthermore, how the development community´s fundamental principle of understanding people on their own criteria´s can play a significant role in terms of national security. To understanding the operating environment the actors who occupy this space has to be considered. This means that when a

Norwegian grand strategy vis-à-vis Russia would be formulated, Russia would need to be understood on Russian terms, with everything that this entails.

Limitations

The scope of this thesis has produced some limitations. There have been some occasions where specific topics that are interrelated ought to have been expanded upon. However, due to the scope of the thesis, they have not been addressed. Some of these are; different theories and following critiques within the development, IR and IS studies, the topic of interventions, and subsequent legal, normative, and ethical dilemmas. The Chinese practices in terms of its social credit program, and the Chinese domestic policy on the treatment of the Uighur minorities. Also, Chinese activities in the South China Sea and the military installations on man-made islands such as Scarborough, Senkaku/Diaoyu, Paracel, and Spratly islands are concepts that were not discussed further.

Moreover, this work is predominantly grounded in theories relating to security studies. This leads to the potential of writing a mirror image thesis based on a development studies approach to security in terms of hybrid warfare. Second, this thesis is written for through the department of global development and planning. Because of this, there was a need to base a significant proportion of the thesis precisely on the security dilemma and underlying theory to be able to defend statements made in the overall argument adequately. As this theory is primarily linked to IS and IR studies, it was needed to convey the fundamentals and base these fundamental issues on the thesis premises. Such as security competition, the operating environment, and state-actors who are seeking divergent national interests.

It has, however, been a constant effort to try and balance the theme of the thesis between matters of security and development. It could be argued that it lacks specific depths for either trajectory. This is undoubtedly the case when a strict focus on either side would provide a more in-depth and thorough analysis through that particular prism. That would, however, defeat the very purpose of this thesis. The author would instead argue that this literary study has had the opportunity to address both broader trends (adding breadth), while simultaneously addressing more narrowly defined cases (adding depth). And has done so with sufficient quality.

Though development and security are intimately interlinked, they have different approaches. They are typically represented through actor-structure/structure-actor perspectives. While there

has been a constant focus on balancing the topics, the center of gravity of this thesis lies with the security perspective, directed at the development community. Its core function has been a critique of development studies failures to incorporate security matters into its body of literature.

Afterthoughts

Democracy is not flawless in its execution. However, it is the best political system to date, specifically in legal terms, with a focus on protecting the individual - Democracy is the mitigating force against arbitrary authoritarian power. A functioning bureaucracy, with its role as prime service deliverer, is then needed in a democratic society to manage best the state's role in governing a larger population. Emphasizing how it, too, is subjugated to a political system where the populace has a real say in the political development of the nation-state. Being a contemporary open society, the people that make up these societies are susceptible to external influence in real-time. The Dewey-Lippman debate on democracy might prove as tenable as ever going forward in shaping the political future for contemporary democracies in the 21st century.

On such a historical evolutionary narrative, it is tough to go back and start over, which means that there needs to be determined efforts in the attempt to make the best possible decisions today. Hence planning processes will need to consider several different perspectives as it is planning for a sustainable tomorrow. It is vital to ensure that the new digital infrastructure and other necessary elements that are a part of overarching strategies are incorporated into planning processes. At least to the point to create awareness of the implications of decisions made today and the consequences they carry with them. If planning processes would facilitate repressive activities or objectives, or be susceptible to foreign interference, this would, or *should,* be considered a problem. It is not possible to be immune to such external influence in a globalized society, but how to address and manage these external pressures are. The gap between the macro and micro levels is relatively small. Which has been the continuous thread that brings about the conclusion of this thesis. This conclusion is that the development and security communities will need to emphasize the strategic partnership they could share. Primarily as to adequality address contemporary challenges continuing into the 21st century.

This then poses a whole array of different questions, which will be vital to our time. Questions that are out of the scope of this thesis to address but require further studies. Like how democracies will defend themselves against cyberattacks without triggering escalations? As more and more states are acquiring higher levels of digital capabilities, including military ones, it is most

likely that the trends we are currently witnessing with higher and higher frequencies in attacks will not slow down, but rather accelerate. The debate on how to mitigate this to tolerable levels will be central in the foreseeable future.

Such themes and questions that have been addressed in this thesis will continue to be in focus on debates about national security. As we continue to evolve our understanding of how the cyber domain functions, how it will affect modern societies, and how this digital space ought to be regulated. It should be incorporated into the development community too, as planning processes need robust inputs of associated threats as well as opportunities. It is now firmly established that cyber acts as a vehicle to promote development and provide a new domain for warfare and conflict. NUPI is currently working on global data flows and their impact on national autonomy and sovereignty, mapping this increasingly fragmented and elaborate picture that is presently unfolding in cyberspace, affecting authentic outcomes to international relations, national security, development processes, and international peace and security.

Conclusion

The security dilemma has traversed into cyberspace. A concept that is most commonly known for explaining how states fall into security competitions has expanded into the digital domain. A domain that has been added to the classic domains of war, namely that of land, air, sea, and space.

Revisionist states such as Russia and China are currently testing the limits of what has been considered acceptable state behavior, whose norms primarily stems from the international order established in the aftermath of World War II. This happens both in and outside of cyberspace, with the overall objective of inserting their respective political footprint in what has been dubbed a return to great-power competition. This also includes a significant element, which is to control spheres of influence on a global level. Unlike the escalations that threatened military conflict during the Cold War, this is now done with the primary premise to prevent Western kinetic responses, which is regarded as superior in military terms.

While this is happening, the security dilemma in cyberspace also seems painfully hard to mitigate, at least in real constructive terms. This is in great respect due to the complicated nature of cyber attribution, detection, terms of deniability, and appropriate responses, including that the creation of normative responses is still very much in the making. These factors are also elements in a broader hybrid, grey zone, or threshold conflict/warfare arena, where states use political

influence, economic coercion, use of cyber, and information operations, including military posture, to assert influence on the international stage. Though this carries sizeable military dimensions, it also has significant broader civilian implications. These include spillover effects from military doctrines, which include large political and economic destabilizing operations, with a grand strategy of divide and conquers tactics, seeking to destabilize established political systems. Though ¨conquer¨ is not necessarily meant in its literal sense, in which a state conquers the physical territory of another state, this does happen. In the case of this thesis, there have been references made to the Russian annexation of Crimea and Eastern Ukraine.

In terms of cyber, it provides tools that are recognized with the possibility for asymmetrical responses from states that do not want to engage dominant actors conventionally, such as the US and EU, through NATO. From the Russian perspective, the main objectives are to undermine confidence in such Western state institutions, alliances, and partnerships of states in terms of information/hybrid warfare campaigns. By manipulating information, it can create effects in the West of a diminishing political cohesion and a greater polarization. This includes elements of manipulating information in order to coarsen public discourse and exacerbates its divisions, effectively undermining the democratic political project. This is not limited to single operations, but a part of a broader information warfare campaign. Its longevity is a concern in strategic political and economic perspectives, which again has impacts on planning and development processes, particularly in open democratic societies.

Though in this sense, the configuration of different political conceptual schemes and competing for its respective national interests, this is also what has led us to the most promising efforts to mitigate cyber threats today, namely the 2017 UN GGE. Also, the Tallinn Manual is a crucial step in the direction of applying IL to cyberspace. However, challenges in this polarized political area, between West and East, are also making it a normative issue, more than a strictly legal one. Problems of clarifications and definitional differences will impact how states react to processes codifying IL to cyberspace.

Priorities driven by national interests and the competition between such interests will continue to be the foreseeable trend in the international arena. This is most likely not going to facilitate constructive progress in terms of future cooperative measures. Though this is also the space in which cooperation can take place, it will require considerable effort to do so. Current trends do not provide confidence for significant progress to make on the multilateral level in terms of international peace and security in general terms.

One crucial element that would provide a valuable addition to strategy formulation, and thus inserting more confidence in this respect, is the incorporation of components from the development community in the creation of said security strategies. The development communities focus on historical, cultural, and social aspects of different groups of people ranging from local, regional to national; it can provide significant, profound elements in terms of understanding actors in the inter-state system. One of which is understanding interests, drives, and political motivations. A reprisal of security strategies to better incorporate such elements is a critical issue in addressing the future conflict environment. This will then include creating strategies that convey a significant understanding of the "other", that might help in the process of cooperation, by the simple reason of understanding the opposition's point of view, while formulating said strategies.

While doing so, there is still a reality that describes a continuous increase in tensions in the foreign policy environment. This is important to acknowledge, as it will be directly irresponsible to base national security on the goodwill of other nations. If you want peace, prepare for war. Though such hyperbolic sentiments carry significant constructive underlying assumptions, such as the state´s ability to defend itself. It is simultaneously essential to keep in mind Clausewitz´s notion that war is just politics by other means. In the case of this thesis, there are no signs that any agreements will be made in the foreseeable future to ratify any legal principles on cyber into the UN Charter. However, global ICT challenges can only be addressed in a real sense by strengthened international cooperation. So, reaching a consensus on responsible state behavior will continue on the basis that there is no other choice. No one is better served with a fragmentation of the international community, which is already profoundly interconnected in cultural, historical, political, and economic terms.

Cybersecurity is integral to sustainable development processes going forward. Laws, norms, and regulations on ICTs are essential to democratic oversight. By highlighting the responsibility of the state for its integrity, which are a liberal rules-based order to primarily to safeguard its citizens—requiring real efforts from the international community to strengthen international cooperation and to reach multilateral agreements on responsible state conduct that can be codified into the UN Charter. Cybersecurity is, therefore, synonymous with human security by protecting people. This is then a concept that needs to be addressed in the broader security setting, but not least is discussed further within the development community.

What is clear is that the complexity of social and economic structures, if this is taken to be a characteristic of development, can only be delivered by the state. Alternatively, formal complexity requires the state. These can only be delivered under circumstances of security. The relationship between security and development is, therefore, in principle, straightforward. Security creates the preconditions for development. Without security, there can be no development.

Security, like development, is first and foremost political. Security is not just the absence of conflict. It is to create the environment from which real political action can be taken for the betterment of the populace. This applies just as much to the digital domain as the physical one.

There needs to be a refocus on the strategic level, including the need for new approaches. This will have to consist of a reappraisal of current narratives and methods concerning the effects of the digital elements on planning sustainable development processes. There is also a need to improve engagement, not just in the literature on security and development topics, but how these are affecting contemporary political realities.

This is not a call to militarize or securitize development, planning, or society in general. However, it does recognize that everyone in a democratic society has a role to play. To increase societal awareness of challenges that we are facing and moving beyond the topic existing on a solely state-on-state level.

Current assessments that are the baselines for creating policy to mitigate malicious activities in cyberspace effectively are extremely security-focused. These interactions are fundamentally intersubjective. To understand the operating environment, comprehending culture is key. As the future of the conflict environment will continue to be characterized by threshold warfare, there will be a need to focus on persistent engagement properly. This will mean basing analytical output on trying to understand the foreign policy environment by its constituents while simultaneously have the capabilities to respond in real-time to information operations. Emphasizing a focus on the actors involved, where they come from, and the specific goals that are being articulated will be critical when addressing contemporary security and development challenges.

This highlights how a core issue for conflict is definitional. That is, the intersubjective interpretation of definitions provides grounds for conflict. As different narratives are set up for collision courses, this thesis has emphasized from a security perspective, the role that the development community can play in shaping future security strategies. There is a sincere

acknowledgment in the security discourse of how an understanding of the environment and those who occupy it is vital in future conflict scenarios.

The goal of this thesis is a call to bridge the security and development community to better address future (digital) challenges in accordance with the principles of sustainable development. There is a need then to create a more forceful to achieve this by highlighting how the two communities have overall shared interests in mind. That security is first and foremost political. Thus, peace (security) is not just the absence of conflict, but about creating an environment where sustainable political solutions can flourish.

Tactics without strategy are the noise before defeat

Sun Tzu

Bibliography

Abrams, S. (2016). Beyond Propaganda: Soviet Active Measures in Putin's Russia. *Connections, 15*(1), 5-31.

Abuza, Z., & Clarke, C. (2019). The Islamic State Meets Southeast Asia - ISIS Seeks New Outposts Across the Indian Ocean. Retrieved from https://www.foreignaffairs.com/articles/southeast-asia/2019-09-16/islamic-state-meets-southeast-asia

ACA. (2017). The Outer Space Treaty at a Glance. Retrieved from https://www.armscontrol.org/factsheets/outerspace. from Arms Control Association https://www.armscontrol.org/factsheets/outerspace

ACA. (2019a). New START at a Glance. Retrieved from https://www.armscontrol.org/factsheets/NewSTART

ACA. (2019b). Nuclear Weapons: Who Has What at a Glance. Retrieved from https://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat. from Arms Control Association https://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat

ACA. (2019c). Timeline of Nuclear Diplomacy With Iran. Retrieved from https://www.armscontrol.org/factsheet/Timeline-of-Nuclear-Diplomacy-With-Iran. from Arms Control Association https://www.armscontrol.org/factsheet/Timeline-of-Nuclear-Diplomacy-With-Iran

ACSS. (2019a). The Complex and Growing Threat of Militant Islamist Groups in the Sahel. Retrieved from https://africacenter.org/spotlight/the-complex-and-growing-threat-of-militant-islamist-groups-in-the-sahel/

ACSS. (2019b). A Review of Major Regional Security Efforts in the Sahel. Retrieved from https://africacenter.org/spotlight/review-regional-security-efforts-sahel/

Al-Rasheed, M. (2013). Saudi Arabia: local and regional challenges. *Contemporary Arab Affairs, 6(1)*, 28-40.

Allen, T., & Thomas, A. (2000). *Poverty and development into the 21st century* (Rev. ed. ed.). Oxford: Oxford University Press.

Allen-Ebrahimian, B. (2019). CHINA CABLES - Exposed: China's Operating Manuals For Mass Internment And Arrest By Algorithm. *International Consortium of Investigative Journalists*. Retrieved from https://www.icij.org/investigations/china-cables/exposed-chinas-operating-manuals-for-mass-internment-and-arrest-by-algorithm/

Allison, G. T. (2017). *Destined for war : can America and China escape Thucydides's trap?*

Anderson, J. (2018). Applying Speech Act Theory to Regional Integration. *DISCUSSION PAPERS*.

Annan, K. A., & Mousavizadeh, N. (2012). *Interventions: A life in war and peace*: Penguin.

Arquilla, J., & Ronfeldt, D. (1997). Cyberwar is comming! In *In Athena´s Camp: Preparing for Conflict in the Information Age* (pp. 23). Santa Monica, CA; Washington, D.C.: Santa Monica, CA; Washington, D.C.: RAND Corporation.

Arquilla, J., & Ronfeldt, D. (2001). *Networks and netwars: The future of terror, crime, and militancy*: Rand Corporation.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks, 54*(15), 2787-2805.

Bachmann, J. (2014). Policing Africa: The US military and visions of crafting 'good order'. *Security Dialogue, 45*(2), 119-136.

Barkawi, T., & Laffey, M. (1999). The imperial peace: Democracy, force and globalization. *European Journal of International Relations, 5*(4), 403-434.

Barkawi, T., & Laffey, M. (2006). The postcolonial moment in security studies. *Review of International Studies, 32*(2), 329-352.
Barnett, M., & Duvall, R. (2005). Power in International Politics. *Intl. Org., 59*(1), 39-75. doi:10.1017/S0020818305050010
Baylis, J., Smith, S., & Owens, P. (2017). *The globalization of world politics : an introduction to international relations* (4th ed. ed.). Oxford: Oxford University Press.
BBC. (2019a). MH17: Four charged with shooting down plane over Ukraine. *BBC*. Retrieved from https://www.bbc.co.uk/news/world-europe-48691488
BBC. (2019b). Turkey v Syria's Kurds: The short, medium and long story. *BBC*. Retrieved from https://www.bbc.com/news/world-middle-east-49963649
Beall, J., Goodfellow, T., & Putzel, J. (2006). Introductory article: on the discourse of terrorism, security and development. *Journal of International Development: The Journal of the Development Studies Association, 18*(1), 51-67.
Belkaïd, A. (2019). Ankara's military offensive against the Kurds - Turkey and Russia redraw the map in northeast Syria. *Le Monde diplomatique*. Retrieved from https://mondediplo.com/2019/11/02turkey
Bellasio, J., Flint, R., Ryan, N., Sondergaard, S., Monsalve, C., Meranto, A., & Knack, A. (2018). *Developing Cybersecurity Capacity - A proof-of-concept implementation guide*. Retrieved from https://www.rand.org/pubs/research_reports/RR2072.html
Benjaminsen, T. A., & Svarstad, H. (2009). *Samfunnsperspektiver på miljø og utvikling [Societal perspectives on environment and development]* (2 ed.): Universitetsforl.
Beswick, D. (2010). Peacekeeping, regime security and 'African solutions to African problems': exploring motivations for Rwanda's involvement in Darfur. *Third World Quarterly, 31*(5), 739-754.
Biddle, T. (2020). Coercion Theory: A Basic Introduction for Practitioners. *Military Strategy, 3*(2). Retrieved from https://tnsr.org/2020/02/coercion-theory-a-basic-introduction-for-practitioners/?fbclid=IwAR2VrYTOC5UFQ77VfBl62b83fyOA1cVBJ5TjtWpX8jpgBzLRt2IKAt2Khj8
Biersteker, T. J. (2002). State, sovereignty and territory. *Handbook of international relations*, 157-176.
Biscop, S., Francioni, F., Graham, K., & Ortega, M. (2005). The European Union and the United Nations: partners in effective multilateralism.
Booth, K., & Wheeler, N. (2007). The security dilemma: Fear, cooperation, and trust in world politics. *Springer Nature*.
Bradshaw, S., & Howard, P. N. (2019). *The global disinformation order: 2019 global inventory of organised social media manipulation*: Project on Computational Propaganda.
Brantly, A., & Collins, L. (2018). A Bear of a Problem: Russian Tactical Cyber Operations. *ARMY Magazine*. Retrieved from https://www.ausa.org/articles/bear-problem-russian-special-forces-perfecting-their-cyber-capabilities
Brechenmacher, S. (2017). *Civil society under assault: Repression and responses in Russia, Egypt, and Ethiopia*: Carnegie Endowment for International Peace.
Bredesen, M., & Reichborn-Kjennerud, E. (2016). Hybrid krigføring – hva er det? [Hybrid warfare - what is it?]. Retrieved from https://www.nupi.no/Skole/HHD-Artikler/2016/Hybrid-krigfoering-hva-er-det
Brent, L. (2019). NATO's role in cyberspace. Retrieved from https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm. from NATO https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm
Brom, S. (2005). Is the Begin Doctrine Still a Viable Option for Israel? *Getting Ready for A Nuclear Iran, Strategic Studies Institute*.
Brown, C., Cerny, P., Grieco, J., Groom, A., Smith, S., Higgott, R., . . . Lamy, S. (1996). *State sovereignty as social construct* (Vol. 46): Cambridge University Press.

Brown, D. (2011). *Palmerston: A Biography*: Yale University Press.
Browning, C. (2013). *International Security: A Very Short Introduction*: Oxford University Press.
Brundtland, G. H., Khalid, M., Agnelli, S., Al-Athel, S., & Chidzero, B. (1987). Our common future. *New York*.
Bryman, A. (2012). *Social research methods* (4th ed. ed.). Oxford: Oxford University Press.
Buchanan, B. (2016). *The Cybersecurity Dilemma - Hacking, Trust, and Fear Between Nations*. New York: Oxford University Press.
Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*: Harvard University Press.
Bulmer-Thomas, V. (2018). *Empire in Retreat: The Past, Present, and Future of the United States*: Yale University Press.
Burgess, M. (2018). We need a global cyberwar treaty, says the former head of GCHQ. *Wired*. Retrieved from https://www.wired.co.uk/article/gchq-uk-robert-hannigan-cyberwar-definition
Buur, L., Jensen, S., & Stepputat, F. (2007). *The security-development nexus: Expressions of sovereignty and securitization in Southern Africa*: Nordiska Afrikainstitutet; HSRC Press.
Buzan, B. (1983). *People, States, and Fear - The National Security Problem in International Relations*: Wheatsheaf Books.
Cai, P. (2017). Understanding China's belt and road initiative.
Cameron, D. (2010). A Strong Britain in an Age of Uncertainty: The National Security Strategy. *London, England*.
Carin, B., & Mehlenbacher, A. (2010). Constituting global leadership: which countries need to be around the summit table for climate change and energy security? *Global Governance, 16*(1), 21-37.
Carnoy, M., & Castells, M. (2001). Globalization, the knowledge society, and the Network State: Poulantzas at the millennium. *Global Networks, 1*(1), 1-18. doi:10.1111/1471-0374.00002
Carter, D. B., & Goemans, H. (2011). The making of the territorial order: New borders and the emergence of interstate conflict. *International organization, 65*(2), 275-309.
Cartledge, P. (2016). *Democracy: A life*: Oxford University Press.
Cartwright, J., & James, W. (2010). Joint terminology for cyberspace operations. *Joint Chiefs of Staff (JCS) Memorandum, Nov*.
Castells, M. (2000). Toward a Sociology of the Network Society. *Contemporary Sociology, 29*(5), 693-699. doi:10.2307/2655234
Cavelty, M. D. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and engineering ethics, 20*(3), 701-715.
CEA. (2018). *The Cost of Malicious Cyber Activity to the U.S. Economy*. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf
Cerny, P. (2000). The New Security Dilemma: divisibility, defection and disorder in the global era. *Rev. Int. Stud., 26*(4), 623-646. doi:10.1017/S0260210500006239
Cerny, P., & Prichard, A. (2017). The new anarchy: Globalisation and fragmentation in world politics. *Journal of International Political Theory, 13*(3), 378-394. doi:10.1177/1755088217713765
CFR. (2019a). Global Conflict Tracker - Civil War in Syria. Retrieved from https://www.cfr.org/interactive/global-conflict-tracker/conflict/civil-war-syria
CFR. (2019b). Global Conflict Tracker - Confrontation Between the United States and Iran. Retrieved from https://www.cfr.org/interactive/global-conflict-tracker/conflict/confrontation-between-united-states-and-iran
Chandler, D. (2001). International Justice. *New Left Review, 6*, 55-66.
Chandler, D. (2007). The security–development nexus and the rise of 'anti-foreign policy'. *Journal of International relations and Development, 10*(4), 362-386.
Chanlett-Avery, E., Rosen, L., Rollins, J., & Theohary, C. (2017). *North Korean Cyber Capabilities: In Brief*. Retrieved from Washington D.C:

Chivvis, C. S. (2017). Understanding Russian hybrid warfare. *Rand Corporation*.
Clark, I. (1989). *The hierarchy of states: Reform and resistance in the international order*: Cambridge University Press.
Clarke, R., & Knake, R. (2019). *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*: Penguin Press.
Clarke, R. A., & Knake, R. K. (2014). *Cyber war*: Tantor Media, Incorporated.
Clausewitz, C. (1832). *On war* (J. Graham, Trans.): Princeton University Press.
Co-Signatories. (2019). *Co-signatories in response to misuse of state powers targeting Uighures minorities in Xinjiang, China*. UN HRC Retrieved from https://www.hrw.org/sites/default/files/supporting_resources/190708_joint_statement_xinjiang.pdf
Coats, D. (2019). *Worldwide threat assessment of the US intelligence community*. Retrieved from https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf
Condliffe, J. (2018). Big Investors Are Placing Bets on China's Facial Recognition Start-Ups. Retrieved from https://www.nytimes.com/2018/07/24/business/dealbook/china-facial-recognition.html
Conley, H., Ruy, D., Stefanov, R., & Vladimirov, M. (2019). *The Kremlin Playbook 2 - The Enablers*. Retrieved from Washington DC:
Connell, M., & Vogler, S. (2017). *Russia's Approach to Cyber Warfare (1Rev)*. Retrieved from
Conrad, J. (1996). Heart of darkness. In *Heart of Darkness* (pp. 17-95): Springer.
Cormac, R., & Aldrich, R. J. (2018). Grey is the new black: covert action and implausible deniability. *International Affairs, 94*(3), 477-494.
Coultrup, A. (2019). GPS Jamming in the Arctic Circle. Retrieved from https://aerospace.csis.org/data/gps-jamming-in-the-arctic-circle/?fbclid=IwAR2s8YnRg2FqDETbS4RR0-0cYyNnolOQVp5CZgOcozZkPPwKKGsBw_Tb4pg
Covington, S. R. (2015). Putin's choice for Russia. *Cambridge, MA, EUA: Belfer Center for Science and International Affairs, Harvard Kennedy School*.
Cox, R. W. (1981). Social forces, states and world orders: beyond international relations theory. *Millennium, 10*(2), 126-155.
Crowther, G. (2017). *The Cyber Domain* Retrieved from
Croxton, D. (1999). The Peace of Westphalia of 1648 and the Origins of Sovereignty. *The International History Review, 21*(3), 569-591. doi:10.1080/07075332.1999.9640869
CSIS. (2018). *Canadian Security Intelligence Service: China and the Age of Strategic Rivalry*. Retrieved from https://www.canada.ca/content/dam/csis-scrs/documents/publications/CSIS-Academic-Outreach-China-report-May-2018-en.pdf:
CSIS. (2020). *Significant Cyber Incidents*. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/200108_Significant_Cyber_Events_List.pdf?aj4_VlDq2hSan2U8O5mS29Iurq3G1QKa
CUP. (Ed.) (2019) Cambridge University Press. Cambridge University Press.
Curran, D. (2017). Muddling on through? Cosmopolitan peacekeeping and the protection of civilians. *International Peacekeeping, 24*(1), 63-85.
Davenport, K. (2019). EU Trade Tool Seeks to Save Iran Nuclear Deal. Retrieved from https://www.armscontrol.org/act/2019-03/news/eu-trade-tool-seeks-save-iran-nuclear-deal
Deibert, R., & OpennetInitiative. (2010). *Access controlled: the shaping of power, rights, and rule in cyberspace*: Cambridge, Mass.: MIT Press.
Deibert, R., Rohozinski, R., & Crete-Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. *Security Dialogue, 43*(1), 3-24.
Dempsey, J. (2018). Can the Iran Nuclear Deal Be Rescued? Retrieved from https://carnegieeurope.eu/strategiceurope/77672
DOD, U. (2019). *DOD: Dictionary of Military and Associated Terms*. Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf
Donais, T. (2009). Inclusion or exclusion? Local ownership and security sector reform. *Studies in social justice, 3*(1), 117-131.

Dowd, A. (2012). Defending the High Ground. Retrieved from https://ascfusa.org/defending-the-high-ground/
Doyle, M. W. (1983). Kant, liberal legacies, and foreign affairs, part 2. *Philosophy & Public Affairs*, 323-353.
DSB. (2019a). Direktoratet for samfunnssikkerhet og beredskap. Retrieved from https://www.dsb.no/
DSB. (2019b). *DIrektoratet for samfunnssikkerhet og beredskap [The Norwegian Directorate for Civil Protection] - Analyser av krisescenarioer 2019* Retrieved from
Dunne, T., Kurki, M., & Smith, S. (2016). *International relations theories* (4th ed. ed.): Oxford University Press.
Durac, V., & Cavatorta, F. (2009). Strengthening authoritarian rule through democracy promotion? Examining the paradox of the US and EU security strategies: the case of Bin Ali's Tunisia. *British journal of Middle Eastern studies, 36*(1), 3-19.
Easterly, W. (2003). IMF and World Bank structural adjustment programs and poverty. In *Managing currency crises in emerging markets* (pp. 361-392): University of Chicago Press.
Eaton, T. (2019). Libya - Rich in Oil, Leaking Fuel. Retrieved from https://chathamhouse.shorthandstories.com/libya-rich-in-oil-leaking-fuel/index.html?utm_source=Chatham%20House&utm_medium=email&utm_campaign=10863731_%5Bupdated%5D%20MENA%20September%20Newsletter%20&dm_i=1S3M,6GUIB,T99X2J,PZLWT,1
Edelston, R. (2014). *Persistent Engagement in the Era of Minimal Footprint*. Retrieved from
Egel, D., Robinson, E., Cleveland, C. L. G. R., & Oates, C. (2019). AI and Irregular Warfare: An Evolution, not a Revolution. Retrieved from https://warontherocks.com/2019/10/ai-and-irregular-warfare-an-evolution-not-a-revolution/
Eilstrup-Sangiovanni, M. (2018). Why the world needs an international cyberwar convention. *Philosophy & Technology, 31*(3), 379-407.
en Veiligheid, M. v. J. (2020). Opening Statement public prosecutor (9-3-2020)-MH17 plane crash-Public Prosecution Service.
Eriksen, T. H., & Eraker, R. (2010). *Små steder - store spørsmål : innføring i sosialantropologi [Small places - big questions: an introduction to social anthropology]* (3. utg. ed.). Oslo: Universitetsforl.
Escobar, A. (1995). Encountering development: the making and unmaking of the third world. *Princeton Studies in Culture/Power/History. Princeton University Press. Princeton. New Jersey*.
EU. (2018a). *The EU´s Partnership with the Sahel*. European Commission Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/g5_sahel_factsheet_final.pdf
EU. (2018b). *Implementing the EU Global Strategy (Year 2) - From Shared Vision to Common Action: A Global Strategy for the European Union's Foreign and Security Policy*. European Union Retrieved from https://eeas.europa.eu/sites/eeas/files/eugs_annual_report_year_2.pdf
EU. (2019). "The Sahel is a strategic priority for the EU and its member states": Council adopts conclusions. Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2019/05/13/the-sahel-is-a-strategic-priority-for-the-eu-and-its-member-states-council-adopts-conclusions/
Facebook. (2019). Removing Coordinated Inauthentic Behavior in UAE, Egypt and Saudi Arabia. Retrieved from https://about.fb.com/news/2019/08/cib-uae-egypt-saudi-arabia/amp/?__twitter_impression=true
Fanon, F., & Sartre, J.-P. (1963). *The wretched of the earth* (C. Farrington, Trans. Vol. 36): Grove Press New York.
Farago, N. (2016). Washington's failure to resolve the North Korean nuclear conundrum: examining two decades of US policy. *International Affairs, 92*(5), 1127-1145.
Feaver, P., & Inboden, W. (2019). Elephants in the Room: The Realists Are Wrong About Syria. *Foreign Policy*. Retrieved from https://foreignpolicy.com/2019/11/04/the-realists-are-wrong-about-syria/

Ferguson, N. (2011). *Civilization: The Six Killer Apps of Western Power*. London: Penguin Group.
Fermann, G. (2019). *Coping with Caveats in Coalition Warfare - An Empirical Research Program*: Palgrave Macmillan.
Fidler, M. (2018). African Union Bugged by China: Cyber Espionage as Evidence of Strategic Shifts. Retrieved from https://www.cfr.org/blog/african-union-bugged-china-cyber-espionage-evidence-strategic-shifts
Fitzpatrick, M. (2017). Assessing the JCPOA. *Adelphi Series, 57*(466-467), 19-60. doi:10.1080/19445571.2017.1555914
Follath, E., & Stark, H. (2009). How Israel Destroyed Syria's Al Kibar Nuclear Reactor. *Spiegel Online, 11*, 22-26.
Forman, S., & Segaar, D. (2006). New coalitions for global governance: the changing dynamics of multilateralism. *Global Governance, 12*, 205.
Forsvarsdepartementet. (2015). *Forsvarsdepartementet [Ministry of Defence] - Kampkraft og bærekraft Langtidsplan for forsvarssektoren*. (Prop. 151 S (2015–2016)). Retrieved from https://www.regjeringen.no/no/dokumenter/prop.-151-s-20152016/id2504884/
Forsvarsdepartementet. (2017). *Forsvarsdepartementet [Ministry of Defence] - Vi trenger et digitalt grenseforsvar*. Retrieved from https://www.regjeringen.no/no/aktuelt/vi-trenger-et-digitalt-grenseforsvar/id2573968/
Franke, U., & Brynielsson, J. (2014). Cyber situational awareness – A systematic review of the literature. *Computers & Security, 46*(C), 18-31. doi:10.1016/j.cose.2014.06.008
Frazier, D., & Stewart-Ingersoll, R. (2010). Regional powers and security: A framework for understanding order within regional security complexes. *European Journal of International Relations, 16*(4), 731-753.
Freedman, L. (1998). Britain and the revolution in military affairs. *Defense Analysis, 14*(1), 55-66.
FreedomHouse. (2018). *Freedom in the wolrd 2018: Democracy in Crisis*. Retrieved from https://freedomhouse.org/report/freedom-world/freedom-world-2018:
FreedomHouse. (2019). *Social media are a growing conduit for electoral manipulation and mass surveillance*. Retrieved from Washington D.C: https://freedomhouse.org/article/social-media-are-growing-conduit-electoral-manipulation-and-mass-surveillance
Fukuyama, F. (1989). The end of history? *The national interest*(16), 3-18.
GCSCC. (2016). *Cybersecurity Capacity Maturity Model for Nations (CMM) Revised Edition*. Retrieved from Oxford: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf
Geers, K. (2015). *Cyber war in perspective: Russian aggression against Ukraine*: CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence.
Gerring, J. (2017). *Case Study Research*: United Kingdom: Cambridge University Press - M.U.A.
Gibney, M. (2015). The downing of MH17: Russian responsibility? *Human Rights Law Review, 15*(1), 169-178.
Giles, K. (2016). *Handbook of Russian information warfare*: NATO Defence College Research Division.
Giles, K. (2019). *Moscow rules: What drives Russia to confront the West*: Brookings Institution Press.
GIP. (2019). The UN GGE - United Nations Group of Governmental Experts on Developments. Retrieved from https://dig.watch/processes/ungge
Gordon, P. H. (2007). NATO after 11 September. *Survival, 43(4)*, 89-106.
Gray, C. S. (1999). *Modern strategy* (Vol. 42): Oxford University Press Oxford.
Grimen, H. (2004). *Samfunnsvitenskapelige tenkemåter [*(3. utg. ed.). Oslo: Universitetsforl.
Gross, L. (1948). The Peace of Westphalia, 1648-1948. *The American Journal of International Law, 42*(1), 20-41. doi:10.2307/2193560
Gross, S., Maloney, S., Riedel, B., & Byman, D. (2019). Around the halls: Brookings experts react to the attack on Saudi oil facilities. Retrieved from https://www.brookings.edu/blog/order-from-chaos/2019/09/17/around-the-halls-brookings-experts-react-to-the-attack-on-saudi-oil-facilities/

Gunitsky, S. (2020). THE GREAT ONLINE CONVERGENCE: DIGITAL AUTHORITARIANISM COMES TO DEMOCRACIES. Retrieved from https://warontherocks.com/2020/02/the-great-online-convergence-digital-authoritarianism-comes-to-democracies/
Gunter, M. M. (2004). The Kurdish question in perspective. *World Affairs, 166*(4), 197-205.
Guzel, M., & El Deeb, S. (2019). https://www.apnews.com/2beb641ae63a4a4fb07e77cfa962d68f?fbclid=IwAR3zYq8f7p46KRzlmtDtEq6_wwafpT62vNvwuUYr_7a-G4Xgn1hhZOWENAo. *AP News*. Retrieved from https://www.apnews.com/2beb641ae63a4a4fb07e77cfa962d68f?fbclid=IwAR3zYq8f7p46KRzlmtDtEq6_wwafpT62vNvwuUYr_7a-G4Xgn1hhZOWENAo
Halbert, D. (2016). Intellectual property theft and national security: Agendas and assumptions. *The Information Society, 32*(4), 256-268.
Hall, B. L., & Tandon, R. (2017). Decolonization of knowledge, epistemicide, participatory research and higher education. *Research for All, 1*(1), 6-19.
Halperin, S. (2004). *War and social change in modern Europe: the great transformation revisited*: Cambridge University Press.
Hameiri, S. (2009). Capacity and its fallacies: International state building as state transformation. *Millennium, 38(1)*, 55-81.
Harding, L., & McLaughlin. (2009). Deal to resume Russian gas eludes EU as 11 people die in big freeze-up. *The Guardian*. Retrieved from https://www.theguardian.com/world/2009/jan/11/russia-ukraine-gas-supplies-dispute
Healy, J., & Hughes, B. (2015). *Risk nexus. Overcome by cyber risks? Economic benefits and costs of alternate cyber futures*. Retrieved from https://www.atlanticcouncil.org/images/publications/risk-nexus-september-2015-overcome-by-cyber-risks.pdf
Hedenskog, J., Konnander, V., Nygren, B., Oldberg, I., & Pursiainen, C. (2013). *Russia as a great power: dimensions of security under Putin*: Routledge.
Hegghammer, T. (2010). *Jihad in Saudi Arabia : Violence and Pan-Islamism since 1979* (Vol. 33). New York: Cambridge University Press.
Hehir, A. (2013). The permanence of inconsistency: Libya, the Security Council, and the Responsibility to Protect. *International Security, 38*(1), 137-159.
Heickerö, R. (2010). *Emerging cyber threats and Russian views on Information warfare and Information operations*: Defence Analysis, Swedish Defence Research Agency (FOI).
Heller, T., & Sofaer, A. (2001). Sovereignty: The practitioners´ Perspective. In S. Krasner (Ed.), *Problematic Sovereignty Contested Rules and Political Possibilities*. S.l.]: S.l. : Columbia University Press.
Hendricks, C. (2006). From state security to human security in Southern Africa: policy research and capacity building challenges. *Institute for Security Studies Monographs, 2006*(122), 97.
Henriksen, A. (2019). The end of the road for the UN GGE process: The future regulation of cyberspace. In.
Herrera, G. (2010). *International Relations and Security in the Digital Age* (Vol. 27). Malden, USA: Routledge.
Herz, J. H. (1950). Idealist Internationalism and the Security Dilemma. *World Politics, 2*(2), 157-180. doi:10.2307/2009187
Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security, 4*(2), 49-60.
Hewitt, T. (2000). Half a century of development. In T. Allen & A. Thomas (Eds.), *Poverty and development into the 21st century* (Rev. ed. ed.). Oxford: Oxford University Press.
Higgins, A. (2019). Apple, Bowing to Russian Pressure, Recognizes Crimea Annexation on Map. *The New York Times*. Retrieved from https://www.nytimes.com/2019/11/28/world/europe/crimea-apple-maps-russia.html
Hirono, M., & Lanteigne, M. (2011). Introduction: China and UN peacekeeping. *International Peacekeeping, 18*(3), 243-256.

Hobbes, T. (1996). *Leviathan* (J. Gaskin Ed.). Oxford: OUP Oxford.
Hobolt, S. B. (2016). The Brexit vote: a divided nation, a divided continent. *Journal of European Public Policy, 23*(9), 1259-1277.
Hoffman, F. (2007). *Conflict in the 21st century: The rise of hybrid wars*: Potomac Institute for Policy Studies Arlington.
Hoffman, F. (2009). Hybrid warfare and challenges. *JFQ, 52, 1*.
Holbrook, D. (2015). Al-Qaeda and the Rise of ISIS. *Survival, 57*(2), 93-104.
Hollis, D. (2020). *96th REGULAR SESSION - IMPROVING TRANSPARENCY: INTERNATIONAL LAW AND STATE CYBER OPERATIONS - FOURTH REPORT.* Paper presented at the OEA/Ser.Q, Rio de Janeiro, Brazil.
Hollis, M., & Smith, S. (1990). Explaining and understanding international relations.
Holmes, A., & Rofe, S. (2016). *Global Diplomacy: Theories, types, and models*: Boulder: Westview Press.
Hopf, T. (1998). The promise of constructivism in international relations theory. *International Security, 23*(1), 171-200.
Hunt, C. T. (2017). All necessary means to what ends? the unintended consequences of the 'robust turn'in UN peace operations. *International Peacekeeping, 24*(1), 108-131.
IISD. (2019). Sustainable Development. Retrieved from https://www.iisd.org/topic/sustainable-development
ISC. (2017). *Intelligence and Security Committee of Parliament - Annual Report 2016–2017*. Retrieved from https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/2016-2017_ISC_AR.pdf?attachauth=ANoY7cobrrbiYY2AnFsOVmC2CP4Q8cLWlVLltq8azC1VjtrKHzDgAxHG-Uxh6zAW1by_LKB8eGVBGIt1NBZUl0jAto62DK7yYx7kFOx8fMdPlrUfbi7nw7VHQb0BxIKUibkr20P-6sofWuR97W1nrK8pz50GaRYuIwLmfCKpiPYadhY_2mhpEGciMZUKXgNA1nCLQFcP_XIU-MtXewdrjum_nbOE0cjwJEwidsLZRdtIaiUYAxvJQMc%3D&attredirects=0
ITU. (2016). Facts and Figures 2016. In: ITU.
ITU. (2019a). Definition of cybersecurity. Retrieved from https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx
ITU. (2019b). *Global Cybersecurity Index (GCI) 2018*. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf
Jackson, R. (2013). International Relations as a Craft Discipline. In C. Navari (Ed.), *Internasjonal politikk* (pp. 284-287): Palgrave, macmillan.
Jervis, R. (1978). Cooperation Under the Security Dilemma. *World Politics, 30*(2), 167-214.
Jervis, R. (1989). *The meaning of the nuclear revolution: Statecraft and the prospect of Armageddon*: Cornell University Press.
Jesperson, S. (2016). *Rethinking the Security-Development Nexus: Organised crime in post-conflict states*: Routledge.
Jonas, A. E. G., McCann, E., & Thomas, M. (2015). *Urban geography : a critical introduction (Critical introductions to geography) / Andrew E.G. Jonas, Eugene McCann, and Mary Thomas*. Chichester: Chichester: Wiley-Blackwell.
Joost, M., Gilles, C., Aude, M., & Leo, De h. (2017). Towards a Renewed Vision of Development Studies. *Revue Internationale de Politique de Développement, 8*(1). doi:10.4000/poldev.2393
Kaldor, M. (2013). *New and old wars: Organised violence in a global era*: John Wiley & Sons.
Karim, U. (2020). Death of Qassem Soleimani: What to Expect in Afghanistan and Pakistan. Retrieved from https://rusi.org/commentary/death-qassem-soleimani-what-expect-afghanistan-and-pakistan
Kassab, H. S. (2014). *In search of cyber stability : international relations, mutually assured destruction and the age of cyber warfare*: Springer.

Kaufman, A. (2019). Israel's Occupation of Lebanon Failed. Turkey's Invasion of Syria Probably Will, Too. *Foreign Policy*. Retrieved from https://foreignpolicy.com/2019/11/07/israels-occupation-of-lebanon-failed-turkeys-invasion-of-syria-probably-will-too/

Kendall-Taylor, A., Frantz, E., & Wright, J. (2020). The Digital Dictators: How Technology Strengthens Autocracy. *Foreign Aff., 99*, 103.

Kennan, G. (1946). *The long telegram*. Retrieved from https://memoriapoliticademexico.org/memoria/Textos/6Revolucion/IM/1946-feb-22-the_kennan_telegram.pdf

Keukeleire, S., & Raube, K. (2013). The security–development nexus and securitization in the EU's policies towards developing countries. *Cambridge Review of International Affairs*(26(3)), 556-572.

Kiggins, R. (2013). US leadership in cyberspace : transnational cyber security and global governance. In J. F. Kremer & B. Müller (Eds.), *Cyberspace and international relations: Theory, prospects and challenges.* (pp. 161): Springer Science & Business Media.

Kilcullen, D. (2016). *Blood Year: Islamic State and the failures of the War on Terror*. London: Hurst & Company.

Kirchner, E. J., & Sperling, J. (2007). *Global security governance: Competing perceptions of security in the twenty-first century*: Routledge.

Konadu-Agyemang, K. (2000). The best of times and the worst of times: structural adjustment programs and uneven development in Africa: the case of Ghana. *The Professional Geographer, 52*(3), 469-483.

Koops, J. A., & Tercovich, G. (2016). A European return to United Nations peacekeeping? Opportunities, challenges and ways ahead. In: Taylor & Francis.

Kramer, A. (2019). Russia Pulls Out of I.N.F. Treaty in 'Symmetrical' Response to U.S. Move. *The New York Times*. Retrieved from https://www.nytimes.com/2019/02/02/world/europe/russia-inf-treaty.html

Krasner, S. D. (2001). Sovereignty. *Foreign Policy*, 20-29.

Krasner, S. D. (2004). Sharing sovereignty: New institutions for collapsed and failing states. *International Security, 29*(2), 85-120.

Krauthammer, C. (1990). The unipolar moment. *Foreign Aff., 70*, 23.

Kretzmer, D. (2013). The inherent right to self-defence and proportionality in Jus Ad Bellum. *European journal of international law = Journal europeen de droit international, 24*(1), 235-282. doi:10.1093/ejil/chs087

Kritzinger, E., & Von Solms, S. H. (2012). A framework for cyber security in Africa. *Journal of Information Assurance & Cybersecurity,, 1*.

Kurowska, X., & Pawlak, P. (2009). Introduction: The Politics of European Security Policies. *Perspectives on European Politics and Society, 10*(4), 474-485.

Lacher, W. (2020). DRONES, DENIABILITY, AND DISINFORMATION: WARFARE IN LIBYA AND THE NEW INTERNATIONAL DISORDER. Retrieved from https://warontherocks.com/2020/03/drones-deniability-and-disinformation-warfare-in-libya-and-the-new-international-disorder/?fbclid=IwAR0DGwD8T8I8oh0oee6WJ-8gPMyvhxuCUb8vzSuh47rN8cYrEEuk6XX-eaA

Landau, S. (2016). Is It Legal? Is It Right? The Can and Should of Use. *IEEE Security & Privacy, 14*(5), 3-5.

Langhelle, O. (2002). Bærekraftig Utvikling [Sustainable development]. In T. A. Benjaminsen & H. Svarstad (Eds.), *Samfunnsperspektiver på miljø og utvikling* (2. utg. ed.). Oslo: Universitetsforl.

Laqua, D. (2011). The tensions of internationalism: transnational anti-slavery in the 1880s and 1890s. *The International History Review, 33*(4), 705-726.

Lawson, E. (2019). Back to the Future? Thresholds, Hybridity and Tolerance Warfare in Russia's Concept of Limited War. In P. Roberts (Ed.), *The Future Conflict Operating Environment Out to 2030* London: Royal United Services Institute for Defence and Security Studies.

Lee, R., Assante, M., & Conway, T. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*. Retrieved from E-ISAC:
Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure. *Policy & Internet, 10*(4), 415-453.
Liberman, P. (1993). The Spoils of Conquest. *International Security, 18*(2), 125-153. doi:10.2307/2539099
Lonsdale, D. J. (2016). Britain's Emerging Cyber-Strategy. *The RUSI Journal, 161*(4), 52-62.
Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cyber security strategies. *Int. J. of Critical Infrastructures, 9*(1/2). doi:10.1504/IJCIS.2013.051608
Ma, A. (2018). China has started ranking citizens with a creepy 'social credit' system — here's what you can do wrong, and the embarrassing, demeaning ways they can punish you. Retrieved from https://www.businessinsider.de/china-social-credit-system-punishments-and-rewards-explained-2018-4?r=US&IR=T
Machiavelli, N. (2013). *Discorsi ; Om fyrster* (J. Bingen, Trans.): Vidarforl.
Macionis, J., & Plummer, K. (2008). *Sociology : a global introduction* (4th ed. ed.). Harlow: Pearson.
Macron, E. (2017). *Defence and National Security Strategic Review 2017*. Department of Defence Retrieved from https://www.defense.gouv.fr/layout/set/popup/content/download/520198/8733095/version/2/file/DEFENCE+AND+NATIONAL+SECURITY+STRATEGIC+REVIEW+2017.pdf
Manson, K. (2018). What the US withdrawal from the Iran nuclear deal means. *the Financial Times*. Retrieved from https://www.ft.com/content/e7e53c72-538c-11e8-b3ee-41e0209208ec
Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P., & Marrs, A. (2013). *Disruptive technologies: Advances that will transform life, business, and the global economy*. Retrieved from San Francisco: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies
Marczak, B., Alexander, G., McKune, S., Scott-Railton, J., & Deibert, R. (2017). *Champing at the cyberbit: Ethiopian dissidents targeted with new commercial spyware.* . Retrieved from Toronto: http://welkait.com/wp-content/uploads/2017/12/Ethiopian-government-Targeted-Dissidents-with-Cyberbit-dec-5-2017.pdf
Marr, B. (2019). Chinese Social Credit Score: Utopian Big Data Bliss Or Black Mirror On Steroids? Retrieved from https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/#5faa294948b8
Masters, J. (2015). What are economic sanctions? *Council for Foreign Relations*.
Mattis, J. (2018). *National Defense Strategy*. Retrieved from Washington:
Maurer, T. (2018). *Cyber Mercenaries: The State, Hackers, and Power*: Cambridge University Press.
McDermott, R. (2019). Gerasimov Unveils Russia's 'Strategy of Limited Actions'. Retrieved from https://jamestown.org/program/gerasimov-unveils-russias-strategy-of-limited-actions/
McDowell, T., & Hernández, P. (2010). Decolonizing academia: Intersectionality, participation, and accountability in family therapy and counseling. *Journal of Feminist Family Therapy, 22*(2), 93-111.
McGaughey, E. (2018). Could Brexit be Void? *King's Law Journal, 29*(3), 331-343.
McKenzie, T. (2017). Is Cyber Deterrence Possible? *Air University Press*.
Mearsheimer, J. (1990). Back to the Future: Instability in Europe after the Cold War. *International Security, 15*(1), 5-56. doi:10.2307/2538981
Mearsheimer, J. (1994). The False Promise of International Institutions. *International Security, 19*(3), 5-49. doi:10.2307/2539078
Mearsheimer, J. (2001). *The tragedy of great power politics*: WW Norton & Company.
Mearsheimer, J. (2010). The gathering storm: China's challenge to US power in Asia. *The Chinese Journal of International Politics, 3*(4), 381-396.
Mearsheimer, J. (2016). Structural realism. In S. Smith, M. Dunne, & M. Kurki (Eds.), *International Relations Theories: discipline and diversity*. Oxford: Oxford University Press.

Merriam-Webster. (2019). Definition: arms race Retrieved from https://www.merriam-webster.com/dictionary/arms%20race
MI5. (2020). THREAT LEVELS. Retrieved from https://www.mi5.gov.uk/threat-levels. from MI5 Security Service https://www.mi5.gov.uk/threat-levels
Miyoshi, M. (2012). China's "U-Shaped Line" Claim in the South China Sea: Any Validity Under International Law? *Ocean Development & International Law, 43*(1), 1-17.
Moen, T. L. (2016). Russisk hybridkrig - et strategisk overfall på Norge. *Norsk tidsskrift for sjøvesen, 131*(2), 20-32.
Morgus, R. (2018a). Getting the International Development Community to Care About Cybersecurity. Retrieved from https://www.cfr.org/blog/getting-international-development-community-care-about-cybersecurity?fbclid=IwAR11s-XQpzcPnNrYxjjl6RCVJggnUZqh1QthNv9dOEMuVzxWOivIlAn_FnQ
Morgus, R. (2018b). Securing Digital Dividends - Mainstreaming Cybersecurity in International Development. Retrieved from https://www.newamerica.org/cybersecurity-initiative/reports/securing-digital-dividends/executive-summary/?fbclid=IwAR2q6xOJTp7NfebzOKw6H8velO3pqS90jTtBNxDZmrcLc5qfHJkKkc4vQpM
Morris, J. (2013). Libya and Syria: R2P and the spectre of the swinging pendulum. *International Affairs, 89*(5), 1265-1283. doi:10.1111/1468-2346.12071
MSC. (2015). *Munich Security Report 2015*. Retrieved from https://securityconference.org/assets/02_Dokumente/01_Publikationen/MunichSecurityReport_2015.pdf
Mueller, K. P., Castillo, J. J., Morgan, F. E., Pegahi, N., & Rosen, B. (2006). *Striking first: preemptive and preventive attack in US national security policy*: Rand Corporation.
Mueller, R. (2019). Report on the investigation into Russian interference in the 2016 presidential election. *US Dept. of Justice. Washington, DC*.
Muller, L. P. (2015). Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities. In: Norwegian Institute of Foreign Affairs.
NASA. (2007). NASA History. Retrieved from https://history.nasa.gov/sputnik/
NASA. (2017). Global Positioning System History. Retrieved from https://www.nasa.gov/directorates/heo/scan/communications/policy/GPS_History.html
NATO. (2012). NATO and Libya - Operation Unified Protector. Retrieved from https://www.nato.int/cps/en/natolive/71679.htm. https://www.nato.int/cps/en/natolive/71679.htm
NATO. (2014). Wales Summit Declaration. Retrieved from https://www.nato.int/cps/ic/natohq/official_texts_112964.htm
NATO. (2019a). Collective defence - Article 5. Retrieved from https://www.nato.int/cps/en/natohq/topics_110496.htm
NATO. (2019b). Cyber defence. Retrieved from https://www.nato.int/cps/en/natohq/topics_78170.htm
NATO. (2019c). NATO's response to hybrid threats. Retrieved from https://www.nato.int/cps/en/natohq/topics_156338.htm
NATO. (2019d). WHAT IS NATO? Retrieved from https://www.nato.int/nato-welcome/index.html
NATO. (2019e). *AAP-06: NATO Glossary of Terms and Definitions*.
NATO-lib. (2019). Hybrid Warfare. Retrieved from http://www.natolibguides.info/hybridwarfare
NCC. *Nigerian Communications Commission - Effects of Cybercrime on Foreign Direct Investment and National Development*. Retrieved from https://www.ncc.gov.ng/documents/735-nmis-effects-cybercrime-foreign-direct-investment/file
Nesser, P. (2015). *Islamist terrorism in Europe*: Hurst & Company.
NIS. (2019). *Focus 2019 - The Norwegian Intelligence Service´s assessment of current security challenges*. Retrieved from

NIS. (2020). *Focus 2020 - The Norwegian Intelligence Service´s assessment of current security challenges*. Retrieved from
Nissenbaum, H. (2005). Where Computer Security Meets National Security 1. *Ethics and Information Technology, 7*(2), 61-73. doi:10.1007/s10676-005-4582-3
Norheim-Martinsen, P., Bjerga, K., Endregard, M., Håkenstad, M., Johansen, S., Listou, T., . . . Thomstad, A. (2019). *Det nye totalforsvaret*: Gyldendal.
NSM. (2019). *RISIKO 2019 - Krafttak for et sikrere Norge*. Retrieved from https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2019_final_enkeltside.pdf
Obama, B. (2010). *National Security Strategy*. Washington D.C: White House
OLA, U. (2010). United Nations Office of Legal Affairs (OLA). Retrieved from http://legal.un.org/ola/
OPIL. (2019). Sovereignty. In: Oxford Public International Law.
Orwell, G. (2008). *1984*: Penguin Books.
Osula, A. M., & Rõigas, H. (2016). *International Cyber Norms Legal, Policy & Industry Perspectives*: NATO CCD COE Publications.
Pawlak. (2014). *Riding the digital wave : the impact of cyber capacity building on human development*. Paris]: Paris : ISS.
Pawlak, & Barmpaliou, P. (2017). Politics of cybersecurity capacity building: conundrum and opportunity. *Journal of Cyber Policy, 2(1)*, 123-144.
The Permanent Court of Arbitration - Island of Palmas arbitral award: Island of Palmas (Neth. v. US) 2 RIAA 829 (Perm. Ct.Arb. 1928). (1928).
Perlroth, N., & Sanger, D. (2018). Cyberattacks Put Russian Fingers on the Switch at Power Plants. *The New York Times*. Retrieved from https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html
Petraeus, D. H. (1986). Lessons of history and lessons of Vietnam. *Parameters, 16*(3), 43.
Pike, A., Rodríguez-Pose, A., & Tomaney, J. (2017). *Local and Regional Development* (Second edition. ed.): Routledge Ltd.
Polyakova, A. (2019). Five years after the Revolution of Dignity: Ukraine's progress and Russia's malign activities. Retrieved from https://www.brookings.edu/testimonies/five-years-after-the-revolution-of-dignity-ukraines-progress-russias-malign-activities/
Pomerantsev, P. (2019). *This is NOT propaganda: Adventures in the war against reality*: Hachette UK.
Posen, B. (1993). The security dilemma and ethnic conflict. *Survival, 35(1)*, 27-47.
Pouligny, B. (2005). Civil society and post-conflict peacebuilding: Ambiguities of international programmes aimed at building 'new'societies`. *Security Dialogue, 36(4)*, 495-510.
Rampton, D., & Nadarajah, S. (2017). A long view of liberal peace and its crisis. *European Journal of International Relations, 23*(2), 441-465.
Ramzy, A., & Buckley, C. (2019). Absolutely No Mercy': Leaked Files Expose How China Organized Mass Detentions of Muslims. *New York Times*. Retrieved from https://www.nytimes.com/interactive/2019/11/16/world/asia/china-xinjiang-documents.html?action=click&module=Top%20Stories&pgtype=Homepage
Regjeringen. (2018). *Eksport til Iran – gjeninnføring av amerikanske sanksjoner og EUs blokkeringsforordning*. Retrieved from https://www.regjeringen.no/no/tema/utenrikssaker/Eksportkontroll/sanksjoner-og-tiltak1/eksport-til-iran--innforing-av-amerikanske-sanksjoner-og-eus-blokkeringsforordning/id2607722/
Rid, T. (2012). Cyber war will not take place. *Journal of strategic studies, 35*(1), 5-32.
Rigg, J. (2007). *An everyday geography of the global south*. London: Routledge.
Rodrik, D. (1990). How should structural adjustment programs be designed? *World development, 18*(7), 933-947.
Rogan, E. (2011). *Araberne : historien om det arabiske folk* (G. Nyquist, Trans.). Oslo: Gyldendal.
Romaniuk, S. N., & Webb, S. T. (2015). Extraordinary Measures: Drone Warfare, Securitization, and the "War on Terror". *Slovak Journal of Political Sciences, 15*(3), 221-245.

Rose, F. (2019). The end of an era? The INF Treaty, New START, and the future of strategic stability. Retrieved from https://www.brookings.edu/blog/order-from-chaos/2019/02/12/the-end-of-an-era-the-inf-treaty-new-start-and-the-future-of-strategic-stability/
Ruehle, M., & Grubliauskas, J. (2015). *Energy as a tool of hybrid warfare*: NATO Defense College, Research Division.
RUSI. (2019). *The Future Conflict Operating Environment Out to 2030* Retrieved from London: https://rusi.org/sites/default/files/201906_op_future_operating_enviroment_web.pdf
Rutzen, D. (2015). Civil society under assault. *Journal of Democracy, 26*(4), 28-39. doi:10.1353/jod.2015.0071
Said, E. (2014). Orientalism. In *Geopolitics* (pp. 75-79): Routledge.
Sanger, D. (2018). *The Perfect Weapon*. London: Scribe.
Schia, N., & Gjesvik, L. (2018). Managing a Digital Revolution - Cyber Security Capacity Building in Myanmar ; Managing a Digital Revolution - Cyber Security Capacity Building in Myanmar. In: NUPI.
Schmitt, M. (2013). *Tallinn manual - On the international law applicable to cyber warfare*: Cambridge University Press.
Schmitt, M. (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* (M. Schmitt Ed.): Cambridge University Press.
Schmitt, M., & Vihul, L. (2019). International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms. Retrieved from https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/
Schnaufer, T. A. (2017). Redefining hybrid warfare: Russia's non-linear war against the West. *Journal of Strategic Security, 10*(1), 17-31.
Schwab, K. (2017). *The fourth industrial revolution*: Currency.
Schwartau, W. (1995). *Information warfare: Chaos on the electronic superhighway*: Avalon Publishing Group.
Schwartau, W. (2000). *Cybershock: Surviving hackers, phreakers, identity thieves, internet terrorists, and weapons of mass disruption*: Avalon Publishing Group.
SCI. (2019). *Report of the Select Committee on Intelligence*

United States Senate on Russian active measures capaigns and interference in the 2016 U.S. election. . Washongton D.C: United States Senate Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf
Segal, A. (2017). Chinese Cyber Diplomacy in a New Era of Uncertainty. *Hoover Institution, 2*.
Shannon, R. (2009). Playing with principles in an era of securitized aid: negotiating humanitarian space in post-9/11 Afghanistan. *Progress in Development Studies, 9*(1), 15-36.
Simmons, B. A. (2019). Border Rules. *International Studies Review, 21*(2), 256-283.
Singh, P. (2019). A death knell for the International norms of Cyber Conflict. Retrieved from https://mwi.usma.edu/death-knell-international-norms-cyber-conflict/?fbclid=IwAR18Ak99hxXHlnI_eA2vskaH3waE_RBNprP9VmWmLTAD-o7MQZnoTPGpGW8
SIPRI. (2009). China's expanding peacekeeping role: its significance and the policy implications.
SIPRI. (2019a). *SIPRI Yearbook 2019: Armaments, Disarmament, and International Security*: Oxford University Press, USA.
SIPRI. (2019b). UN Arms embargo on Libya. Retrieved from https://www.sipri.org/databases/embargoes/un_arms_embargoes/libya/libya_2011
Snyder, G. (1984). The Security Dilemma in Alliance Politics. *World Politics, 36*(4), 461-495. doi:10.2307/2010183
Snyder, T. (2018). *The Road to Unfreedom: Russia, Europe, America*: Tim Duggan Books.
Stavridis, J. (2017). The United States Is Not Ready for a Cyber-Pearl Harbor. *Foreign Policy*. Retrieved from https://foreignpolicy.com/2017/05/15/the-united-states-is-not-ready-for-cyber-pearl-harbor-ransomware-hackers-wannacry/

Stent, A. (2016). Putin's Power Play in Syria: How to Respond to Russia's Intervention. *Foreign Aff., 95*, 106.
Stern, M., & Öjendal, J. (2010). Mapping the security—development nexus: conflict, complexity, cacophony, convergence? *Security Dialogue, 41*(1), 5-29.
Stickings, A. (2019). *Space, Strategic Advantage and Control of the Military High Ground*. Retrieved from London:
Stone, J. (2013). Cyber War Will Take Place! *Journal of strategic studies, 36*(1), 101-108. doi:10.1080/01402390.2012.730485
Strang, D. (1990). From dependency to sovereignty: an event history analysis of decolonization 1870-1987. *American Sociological Review, 55*(6), 846. doi:10.2307/2095750
Stritzel, H. (2007). Towards a Theory of Securitization: Copenhagen and Beyond. *European Journal of International Relations, 13*(3), 357-383. doi:10.1177/1354066107080128
SunTzu. (2005). *The Illustrated Art of War.* (S. Griffith, Trans.): Oxford University Press.
Swadener, K. M. B. B. (2004). *Decolonizing research in cross-cultural contexts: Critical personal narratives*: SUNY press.
Swaine, M. D. (2015). Chinese views and commentary on the 'One Belt, One Road'initiative. *China Leadership Monitor, 47*(2), 3.
Sørensen, G. (2007). After the Security Dilemma: The Challenges of Insecurity in Weak States and the Dilemma of Liberal Values. *Security Dialogue, 38*(3), 357-378. doi:10.1177/0967010607081516
Taleblu, B., & Tahiroglu, M. (2017). Kurd Your Enthusiasm: The U.S. Needs to Talk About Its Favorite Allies. *Foreign Affairs*. Retrieved from https://www.foreignaffairs.com/articles/syria/2017-11-08/kurd-your-enthusiasm
Taylor, B. D. (2011). *State building in Putin's Russia: Policing and coercion after communism*: Cambridge University Press.
Taylor, B. D., & Botea, R. (2008). Tilly Tally: War-Making and State-Making in the Contemporary Third World. *International Studies Review, 10*(1), 27-56. doi:10.1111/j.1468-2486.2008.00746.x
TD. (2019). Past Weather in Kharkiv, Ukraine — December 2015. Retrieved from https://www.timeanddate.com/weather/ukraine/kharkiv/historic?month=12&year=2015
Thagaard, T. (2013). *Systematikk og innlevelse : en innføring i kvalitativ metode* (4. utg. ed.). Bergen: Fagbokforl.
Thucydides. (2009). *The Peloponnesian War* (M. Hammond & P. J. Rhodes, Trans.): United Kingdom: Oxford University Press.
Tilly, C. (1990). *Coercion, capital, and European states, AD 990*: Cambridge: Basil Blackwell.
Tobey, W. (2012). Nuclear scientists as assassination targets. *Bulletin of the Atomic Scientists, 68*(1), 61-69.
Todman, W. (2019). The Implications of a Turkish Intervention in Northeastern Syria. Retrieved from https://www.csis.org/analysis/implications-turkish-intervention-northeastern-syria?amp&__twitter_impression=true&fbclid=IwAR3vAyE3b-Py_4btuzShVLifQeH4t9Jv1ieYFTv7Kl8hF7hyMfG61gM1KO0
Trauthig, I. (2019). *Assessing the Islamic State in Libya - The current situation in Libya and its implications for the terrorism threat in Europe*. Retrieved from file:///Users/magnusstavenes/Downloads/inga_trauthig_islamic_state_libya.pdf
Troianovski, A. (2019). Investigation into downing of Flight MH17 charge four suspects with ties to Russian intelligence, pro moscow militia. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/europe/investigation-into-downing-of-flight-mh-17-over-ukraine-names-four-russian-ukrainian-suspects/2019/06/19/02d52e42-9280-11e9-aadb-74e6b2b46f6a_story.html
Truman, H. (1947). *The Truman Doctrine - President Harry S. Truman's Address before a Joint Session of Congress, March 12, 1947*. Retrieved from http://courses.kvasaheim.com/common/docs/truman.pdf

Trump, D. (2017). *National security strategy of the United States of America*. Washington DC: Executive Office of The President
Trump, D. (2018). *National Cyber Strategy of the United States of America*. Washington: Executive Office of The President
Tuschhoff, C. (2005). NATO cohesion from Afghanistan to Iraq. In *European Security and Transatlantic Relations after 9/11 and the Iraq War* (pp. 149-164): Springer.
Twitter. (2019). New disclosures to our archive of state-backed information operations. Retrieved from https://blog.twitter.com/en_us/topics/company/2019/new-disclosures-to-our-archive-of-state-backed-information-operations.html
Tödtling, F. (2011). Endogenous approaches to local and regional development policy. In A. Pike, Rodriguez-Pose, A. & Tomaney, J (Ed.), *Handbook of Local and Regional Development* (pp. 333-343). Routledge.
UN. (1987). Report of the World Commission on Environment and Development: Our Common Future. *Strategic Imperatives, 10*. Retrieved from http://www.ask-force.org/web/Sustainability/Brundtland-Our-Common-Future-1987-2008.pdf
UN. (2017). Security Council condemns reported slave trade of migrants in Libya. Retrieved from https://refugeesmigrants.un.org/fr/node/100045760
UN. (2019a). Decisions by Topic: Capacity-building. Retrieved from https://sustainabledevelopment.un.org/index.php?menu=1243
UN. (2019b). Goal 17 - Capacity-building. Retrieved from https://sustainabledevelopment.un.org/topics/capacity-building
UN. (2019c). *United Nations: Charter of the United Nations*: United Nations.
UN. (2020a). CURRENT PEACEKEEPING OPERATIONS. Retrieved from https://peacekeeping.un.org/en/current-peacekeeping-operations. from United Nations Peacekeeping https://peacekeeping.un.org/en/current-peacekeeping-operations
UN. (2020b). UN Peace Keeping - China. Retrieved from https://peacekeeping.un.org/en/china. from UN https://peacekeeping.un.org/en/china
UNDP. (1994). *Human Development Report*. Retrieved from
UNDP. (2001). *Human Development Report: Making new technologies work for human development*. Retrieved from United Nations Development Programme: http://hdr.undp.org/sites/default/files/reports/262/hdr_2001_en.pdf
UNGA. (2013). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* Retrieved from United Nations General Assembly: http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf
UNGGE. (2015). *Seventieth session: Item 93 of the provisional agenda* - Developments in the field of information and telecommunications in the context of international security - Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved from
UNODA. (2019). Developments in the field of information and telecommunications in the context of international security. Retrieved from https://www.un.org/disarmament/ict-security/
UNOOSA. (1966). 2222 (XXI) - Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies. Retrieved from https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html. from United Nations Office for Outer Space Affairs https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html
UNSC. (2011). Resolution 2009 (2011) - Adopted by the Security Council at its 6620th meeting, on 16 September 2011 Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2011_09/20110927_110916-UNSCR-2009.pdf. from United Nations Security Council

https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2011_09/20110927_110916-UNSCR-2009.pdf
UNSC. (2020). Purposes and Principles of the United Nations. Retrieved from https://www.un.org/securitycouncil/content/purposes-and-principles-un-chapter-i-un-charter. from UNITED NATIONS SECURITY COUNCIL https://www.un.org/securitycouncil/content/purposes-and-principles-un-chapter-i-un-charter
Utenriksdepartementet. (2017). *International cyber strategy for Norway*. https://www.regjeringen.no/globalassets/departementene/ud/dokumenter/sikpol/cyberstrategy_2017.pdf: Norwegian Ministry of Foreign Affairs
Vakil, S., Mansour, R., & Khatib, L. (2020). How the Soleimani Assassination Will Reverberate Throughout the Middle East. Retrieved from https://www.chathamhouse.org/expert/comment/how-soleimani-assassination-will-reverberate-throughout-middle-east
van Bergeijk, P. (2015). Sanctions against Iran-A preliminary economic assessment.
Venkataramakrishnan, S. (2019). Experts struggle to set red lines for cyber warfare. *Financial Times*. Retrieved from https://amp.ft.com/content/fcf2a06c-c8ae-11e9-af46-b09e8bfe60c0?__twitter_impression=true&fbclid=IwAR1q6YRmn-QRsdXfNbi8YOdqOmTm8VjUhLpzeeAGzk2ZBhjy_Nzehw8hLcc
Voss, K. (2016). Plausibly deniable: mercenaries in US covert interventions during the Cold War, 1964–1987. *Cold war history, 16*(1), 37-60.
Walt, S. M. (1998). International Relations: One World, Many Theories. *Foreign Policy*(110), 29-46. doi:10.2307/1149275
Walther, U. (2014). Russia's Failed Transformation: The Power of the KGB/FSB from Gorbachev to Putin. *International Journal of Intelligence and CounterIntelligence, 27*(4), 666-686.
Waltz, K. N. (2000). Structural realism after the Cold War. *International Security, 25*(1), 5-41.
Weldes, J. (1996). Constructing national interests. *European Journal of International Relations, 2*(3), 275-318.
Wendt, A. (1992). Anarchy is what states make of it: the social construction of power politics. *International organization, 46*(2), 391-425.
White, J. (2020). Soleimani's Killing: The Regional Ripple Effects are Yet to Come. Retrieved from https://rusi.org/commentary/soleimanis-killing-regional-ripple-effects-are-yet-come
Wilén, N. (2009). Capacity-building or capacity-taking? Legitimizing concepts in peace and development operations. *International Peacekeeping, 16(3)*, 337-351.
Williams, D. (2013). Development, intervention, and international order. *Review of International Studies, 39*(5), 1213-1231.
Williams, P. (2008). *Security Studies: an introduction*: Routledge, Tylor & Francis Group.
Winkel, K., & Aase, A. (2008). *Hvorfor er det så mange fattige i Afrika?* Kristiansand: Portal.
Wolff, A. T. (2015). The future of NATO enlargement after the Ukraine crisis. *International Affairs, 91*(5), 1103-1121.
Wolfsfeld, G., Segev, E., & Sheafer, T. (2013). Social media and the Arab Spring: Politics comes first. *The International Journal of Press/Politics, 18*(2), 115-137.
Woolf, N. (2016). Massive cyber-attack grinds Liberia's internet to a halt. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2016/nov/03/cyberattack-internet-liberia-ddos-hack-botnet
WorldBank. (2016). *Digital dividends*(Vol. 2016).
Waage, P. N. (2012). *Russland er sitt eget sted : streker til et lands biografi*. Oslo: Arneberg.
Zalewski, P. (2014). Contentious Kurds: Is Turkey Right to Fear the PKK in Kobani? *Foreign Affairs*. Retrieved from https://www.foreignaffairs.com/articles/turkey/2014-11-02/contentious-kurds
Zetter, K. (2016). That insane, $81M Bangladesh bank heist. *Wired*. Retrieved from https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/

Zuppo, C. M. (2012). Defining ICT in a boundaryless world: The development of a working hierarchy. . *International journal of managing information technology, , 4(3)*, 13-22.

Aarsæther, N., Falleth, E., Nyseth, T., & Kristiansen, R. (2015). *Utfordringer for norsk planlegging : kunnskap, bærekraft, demokrati*. Kristiansand: Cappelen Damm Høyskoleforl.

Appendix

Security and development perspectives to Winkel & Aase (2008).

Winkel and Aase (2008) address the proliferation of new states in a post-colonial Africa as the case where now Benin formally had the same vote in the UN as that of the US, at least in the UNGA (Winkel & Aase, 2008, p. 216) This analysis can be described as naïve at best, destructive at its worst. Benin's standing in the world and the influence it wields in the international community does not equate to the premise to that of the US, formally or otherwise. One need only look to the P5s of the UNSC to see that this is factually incorrect. In the UNSC, the veto that the US has is by definition a vote that counts more than that of Benin or any other member state who are not on the UNSC (Bulmer-Thomas, 2018; Dunne et al., 2016, p. 119). Though they reference Benin´s and the US standing in the UNGA, this is circumnavigating the UNSC. Or is a shallow description by knowingly disregarding the UNSC altogether. It should not be eluded to as it is, even in a formal setting, that there is symmetry between Benin and the US. It points to the two votes between the US and Benin in the UN weights the same in the UNGA. As have been discussed earlier, it was only when the US could no longer dictate the UN member list where the US lost its safe majority in the UNGA. At this point the US had to start exercising its veto in the UNSC. Furthermore, separating the UNSC and the UNGA in reference of voting in the UN makes a precarious case for Benin and the US, including the position of the P5 and the veto in the UN system. Moreover, the influence of the US to use soft and hard power, that is to suave or coerce other countries to follow its lead as it is pursuing US interests has to be factored into the equation. The leverage that the US holds as a military, economic, and political super-power in comparison to Benin is not equal in any terms. And should not in any case be presented as such.

Also, it reflects on contemporary Africa as being better served with a redrawing of the borders of post-colonial states (on the premise that this could be done peacefully) (Winkel & Aase, 2008, p. 212). This is a complete disregard of the structure of the inter-state system, international law, and challenges the concept of sovereignty at its core- ´international borders are one of the central institutions defining states and organizing international politics`(Carter & Goemans, 2011; Heller & Sofaer, 2001; Krasner, 2001; OPIL, 2019; Simmons, 2019). Also, it seems to display a narrow understanding of state behavior with the suggestion that you would redraw in essence almost

every state on earth – and that this can be done peacefully. Any border dispute is precarious. Though it only references the continent of Africa, at its core, the suggestion is to redraw the borderlines to every country that was ever colonized. According to (Fanon & Sartre, 1963), ´decolonization is always violent.` Its focus on internal conflicts in several African nation-states with a disregard to the debate on ´African solutions to African problems` (Beswick, 2010), and are generally limiting in scope. To meaningfully address conflicts on the African continent, it necessitates highlighting changing narratives on Africa's role in international security (ibid). This includes incorporating security studies into the development discourse.

Last but not least, (Winkel & Aase, 2008, pp. 213-214) also brushes over the severe implications that the Cold War had on the African continent. Primarily by not referencing one of the main catalysts of the Cold War, the focus on controlling spheres of influence (Bulmer-Thomas, 2018). It does depict some of the most devastating conflicts as being fueled by outside support. Highlighting South Africa (during apartheid), Cuba, USSR, and the US, meddling in civil wars such as took place in Mozambique and Angola (Winkel & Aase, 2008, p. 182). However, it does so without addressing underlying causes. The Cold War was cold in name only. Which means that several of the warm wars on the African continent should be regarded as facilitated through the national interests located in Moscow and Washington. Who played on opportunities that had been shaped by former colonial practices and thus exacerbating conflict. Also, it dismisses what this period meant in shaping current African and global politics (Winkel & Aase, 2008).

It then goes on to suggest that during the Cold War, Africa (along with other developing countries) played a neutral role between the West and the East (Winkel & Aase, 2008, p. 216). This is *not* the case! Exemplified by referencing to all the wars and conflicts that took place, not just on the African continent, but in the global south throughout the duration of the Cold War (Voss, 2016; Winkel & Aase, 2008). Not least one of the pinnacle moments of the Cold War, the Cuban missile crises. Only by removing all agency from Cuba (and other nations), could you argue that the global south played a neutral role during the Cold War (Barkawi & Laffey, 2006). Instead, it is because of Cuba, that this pivotal moment took place. ´Castro, realistically fearful of another invasion after the Bay of Pigs, turned to the USSR for help in defending Cuban sovereignty and the Cuban revolution.` Without these motivations, it would be unlikely that the October crises would have taken place (Barkawi & Laffey, 2006)

Informants:

Informants were used in the preliminary research phase to map key areas of interest. These conversations were considered useful in terms of getting outside perspectives by practitioners. The range between these informants was considered necessary, in order to address some of the broad issues tackled in this thesis. Ranging from micro- to macro levels. Thus, the main focus was a conversation on the general topics of the thesis.

- Helge Høynes
  Senior engineer. Responsible for CERT and the datacenter at the University of Agder
- Geir Myrdahl Køien
  Then Professor at the University of Agder – Department for Information and Communication technologies
- Hans Kjetil Lysgård
  Vice-Rector at the University of Agder – and former program coordinator for the department of global development and planning´ master´s program
- Jan Ledang
  Director of Kuben, Arendal. Former General Consul of Norway to South Sudan.
- Per Martin Norheim-Martinsen
  Associated Professor – the Norwegian Defense University College
- Ewan Lawson
  Senior research fellow at the Royal United Service Institute
- Mark Kimmitt
  Former Assistant Secretary of State for Political-Military Affairs

Informants who for different reasons were not able to attend an interview:

- National Security Authority (Nasjonal sikkerhetsmyndighet)

  NSM responded that they did not have the capacity to sufficiently devout resources for an interview. They did reply by email and provided ample material in the forms of reports and documents on current engagements. Specifically orientated towards the digital threat environment that the Norwegian state is currently engaged.

- Norwegian Police Security Service (Politiets Sikkerhetstjeneste)

  PST offered a similar response as NSM.

What this then means is explicitly the following;

- *Høynes* is the Senior engineer and responsible for CERT and the data center at the University of Agder. His role was to provide technical insight on digital capabilities in terms of servicing a university. Dealing with cybersecurity on a local level (UiA). The conversation was centered around his role in implementing cybersecurity measures at the University of Agder.

- *Køien* was the former program coordinator for UiA master´s program on cybersecurity. He also holds a position as principal scientist at the Norwegian Defense Research Institute (FFI). Køien was able to provide a comprehensive link between in terms of dealing with cyber issues daily in a growing complex security environment also, how development processes from local, regional, and global development processes are shaping cyber. Both in terms of its purpose and its application. The pernicious use of digital capabilities from state-actors dominated the conversation.

- *Lysgård* is the Vice-rector at UiA. He was the program coordinator for the master´s program in global development and planning when this thesis was initiated. Lysgård was essential in addressing a vital issue. The author states that there is a severe lack of security focus in both development and planning processes. Lysgård did not agree with this statement, with the response that security questions are implicit in the literature. It is the author´s perspective that this is not the case. Not from the bachelor´s program in development studies, nor the master´s program in development and planning.

- *Ledang* is the director of Kuben, Arendal, and former General Consul of Norway to South Sudan. His role was not to provide insight into matters of cybersecurity. Ledang´s role to this thesis was to provide a comprehensive background in how Norwegian foreign policy is executed in practice—based on his experience as General Consul in South Sudan — also benefitting from his experience as the director of Norwegian people´s aid, and several of his international stations. Such as his involvement as a peace broker and head of SLMM in Trincomalee (peace process in Sri Lanka), as a UN observer in the Balkans, and his role as an army officer stationed in Lebanon.

- *Norheim-Martinsen´s* role from the Norwegian Defense College was a valuable contribution. The conversation focused on the digital security dilemma, along with topics of trans-Atlantic partnerships, EU security and defense policies, and NATO. *Norheim-Martinsen´s* role provided both academic, as well as practical insight into how states, alliances, and global shifts in the international system are affecting foreign policy analysis. The link to a digital security dilemma was then established as an important one, mainly as this will be a large piece of the continued trend of threshold warfare.

  Lawson is a senior research fellow at the Royal United Service Institute, and professor of international security at SOAS, University of London. As a former serving officer in the Royal Air Force, Lawson has a highly varied experience in policing and security. With a practical interest in peacekeeping operations, mainly on the African continent, and most recently in South Sudan. Lawson has been in contact by mail. He has commented on the topic of cyber, the digital security dilemma, and the attempts at creating robust regulations of responsible state behavior in cyberspace.

- *Kimmitt* is the former Assistant Secretary of State for Political-Military Affairs, serving in the Bush administration from 2008 to 2009. As a retired brigadier general, and previous Deputy Assistant Secretary of Defense for the Middle East, Kimmitt was able to provide critical insight in the application of US foreign policy. With a background that encompasses roles at CENTCOM, spokesman for the Coalition forces in Iraq, and serving at NATO SHAPE. Kimmitt challenged the notion of Russian and Chinese foreign policy initiatives being equal, in the sense that the Russian perspective lacks substantial, long term threat potential, compared to China. With his overall conclusion that Russia is skillfully maneuvering itself in the foreign policy environment, it lacks the extensive depth required to back up its ambitions on the international arena. In terms of great power politics, the US-Sino relations will dominate in the foreseeable future.

Definitions

Capacity building

Capacity building, in general, is viewed as a mechanism to ´bridge the gap between the problems of poor governance and what is considered an acceptable level of state capacity to deliver its core functions. Defined by the UN as a mean to help recipient countries to bring about a continuous transformation in order to better play a ´dynamic role to sustainable development processes (Pawlak & Barmpaliou, 2017, p. 124)

Cybersecurity is defined using the ITU´s definition of cybersecurity:

> "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user´s assets. Organization and user´s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user´s assets against relevant security risks in the cyber environment" (ITU, 2019a).

Cyberspace

The US DOD defines cyberspace as ´a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computers systems, and embedded processors and controllers`

(DOD, 2019)

Cyber Capacity Building

´Capacity building (including public awareness campaigns, frameworks for certification and accreditation of cybersecurity professionals, professional training courses in cybersecurity, educational programs or academic curricula, etc.) is intrinsic to other institutional pillars, such as legal measures (meaning legislation and regulation, with appropriate response mechanisms). Technical, as the primary frontier in defending systems against cyberthreats. Cybersecurity is most often tackled from a technological perspective, even though there are numerous socio-economic and political implications. Human and institutional capacity building is essential to raise awareness, knowledge, and the know-how across sectors, for systematic and appropriate solutions, and to promote the development of qualified professionals. Capacity building is evaluated based on the number of research and development, education and training programs, and certified professionals and public sector agencies` (ITU, 2019b, p. 9).

Cyber Operations / Computer Network Attack

The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid (Cartwright & James, 2010, p. 8).

Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the network itself. Note: A computer network attack is a type of cyber-attack (NATO, 2019e, p. 30).

Globalization

Globalization can be a notorious hard concept to define and is widely misused in both academic and political discourse (Pike et al., 2017, p. 3). In this thesis, globalization, in its simplest form, is seen as the ´increasing connectedness of societies` (Macionis & Plummer, 2008, p. 42). However, a more comprehensive definition is needed. Carnoy and Castells (2001) provides an adequate and satisfying definition that states that globalization is

"The economy whose core, strategic activities have the technological, organizational, and institutional capacity to work as a unit in real-time, or in chosen time, on a planetary scale.

> Empirically documented by Held, McGrew, Goldblatt, and Perraton (1999), a global economy is a new reality, different from processes of internationalization in previous times, for one simple reason: only at this point in history was a technological infrastructure available to make it possible. This infrastructure includes networked computer systems, advanced telecommunications, information-based technology, fast transportation systems for people, goods and services, with a planetary reach, and the information processing capacity to manage the complexity of the whole system" (Carnoy & Castells, 2001, p. 3).

ICTs

ICTs can potentially be a complex issue to define. This becomes apparent as the term ICT is being used frequently and diverse, while simultaneously existing in many different contexts. Though the concept and definition can vary widely within the different sectors from which it is applied. However, the primary foundation is unison in that ICTs revolve around the ´devices and infrastructure that facilitates the transfer of information through digital means` (Zuppo, 2012, p. 13). What this means in effect is that different types of understandings of the concept can be found for different frameworks, or researchers can find a particular understanding relevant to their specific framework (ibid).

Security

Security to the author is not just the absence of conflict. It is just as much about creating the environment from where sustainable political, social, economic, and cultural development processes can take place. However, a more formal definition is required. This is difficult because security can mean very distinctly different things to different people. It can thus be a very subjective and elastic term (P. Williams, 2008, p. 1). For this reason, as a definition, there cannot be a consensus to its distinct meaning (Baylis et al., 2017; Browning, 2013; P. Williams, 2008)

At an abstract level, the most common working definition of security is the; ´alleviation of threats to cherished values` (Baylis et al., 2017, pp. 228-230; P. Williams, 2008, p. 1). Because there are implications to such a working definition. The concept and definition of security will be addressed briefly at a later state in this thesis.

The basis on which Norwegian security policies are made is articulated in the Norwegian defense department's government white paper ´kampkraft og bærekraft.` This states that

> The purpose of security policy is to safeguard state security, which means to safeguard the state´s sovereignty and integrity, as well as to ensure political freedom of action … The Norwegian authorities also have a responsibility to safeguard societal security, where the security of the civilian population, central social functions, and infrastructure can be challenged, but without the state's existence being threatened. Threats to individuals and the wider society, for example, in the form of terrorism and cyberattacks, can ultimately develop to threaten state security. This underlines the need for close security and emergency preparedness cooperation across sectors. The overall defense concept includes mutual civil-military support throughout the crisis spectrum. Mutual support and cooperation between the Armed Forces and civil society shall contribute to the prevention, contingency planning, and crisis and consequence management.
>
> (Forsvarsdepartementet, 2015, p. 17).

Sovereignty

In an increasingly interconnected globalized world, information flow due to ICTs makes traditional understood concepts such as borders into a more fluid concept. It is, therefore, paramount to have a clear working definition of sovereignty. A well-accepted definition was set forth in the Island of Palmas arbitral award of 1928. It states that: 'Sovereignty in the relations between States signifies independence. Independence, in regard to a portion of the globe, is the right to exercise therein, to the exclusion of any other State, the functions of a State (PCA, 1928).

Sustainable development

Sustainable development is understood as defined by the Brundtland report *our common future.* ´Sustainable development is the development that meets the needs of the present without compromising the ability of future generations to meet their own needs` (Brundtland, Khalid, Agnelli, Al-Athel, & Chidzero, 1987; IISD, 2019)