Assessing Feasibility for a Binding International Legal Instrument on Cyberweapons

A Maturity Model Approach

Amir Kiyaei

A dissertation presented to the Faculty of Arts in the University of Malta for the degree of Master in Contemporary Diplomacy

December 2018

Declaration

I hereby declare that this dissertation is my own original work.

Amir Kiyaei

31 December 2018

Cape Town

Republic of South Africa

Abstract

Cyberwarfare has emerged from the expeditious expansion of the Internet as a new mode of conflict that can anonymously and remotely disrupt the core functions of a state. An effective arms control regime over cyberweapons however, can facilitate a reduction of threats emanating from that domain and reduce blowback risks and unintended consequences over use of cyberweapons if entered into force. Nevertheless, key impediments towards realising such a regime exist, including insufficient political endorsement and technical challenges related to attribution, compliance and verification. Rooted in contemporary international legal instruments, the paper devised 16 arms control elements applicable to cyberweapons. The feasibility of these were subsequently assessed through a maturity model structure, determined through three rounds of scoring. The results placed a majority of those elements, such as prohibitions on attacks on protected persons, entities and infrastructure, creation of national points of contact, establishment of a secretariat as well as forbidding proliferation of cyberweapons, within the feasible and likely ranges. Recommendations were furnished for those elements that were judged as unlikely, while an additional set of practical actions were proposed to address other impediments, emerging from the research, towards realising a binding international legal instrument on cyberweapons.

Table of Contents

List of Tables

List of Figures

Glossary

AI	Artificial Intelligence
ASEAN	Association of Southeast Asian Nations
ATT	Arms Trade Treaty
BWC	Biological Weapons Convention
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CII	Critical Internet Infrastructure
CVM	Compliance and Verification Mechanisms
CWC	Chemical Weapons Convention
GGE	Group of Government Experts
GVIO	Governing, Verification and Implementation Organisation
EU	European Union
ICRC	International Committee of the Red Cross
ICT	Information and Communication Technology
INSA	Involvement of Non-State Actors
IHL	International Humanitarian Law
JCPOA	Joint Comprehensive Plan of Action
LOAC	Law of Armed Conflict
LAWS	Autonomous Weapons Systems
NATO	North Atlantic Treaty Organisation
NSA	Non-State Actor
OAS	Organization of American States
OSCE	Organization for Security and Co-operation in Europe
PO	Primary Objective
SCO	Shanghai Cooperation Organisation
TLSBR	Type of Limitation on state Behaviour and other Requirements
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNIDIR	United Nations Institute for Disarmament Research
UNSC	United Nations Security Council
VRM	Violation Resolution Mechanisms
WMD	Weapons of Mass Destruction

> “Episodes of cyber warfare between states already exist. What is worse is that there is no regulatory scheme for that type of warfare…the next war will begin with a massive cyber attack to destroy military capacity... and paralyse basic infrastructure such as the electric networks”.
>
> Antonio Guterres, Secretary General of the United Nations
> (Khalip, 2018, p. 1)

1. Introduction

Since time immemorial, humanity, whether for survival, competitive or pleasure purposes, has maintained a role for conflict in its everyday affairs (Diab, 2008). Each epoch presented an opportunity for Homo Sapiens to further their toolkit of means to destroy the other. Parallel to this development has been the formulation of International Humanitarian Law (IHL) and Law of Armed Conflict (LOAC) that sought to develop civil minded rules for conflict situations. As LOAC applies to all methods of warfare, it will in principle be applicable to cyberwarfare as well, thus prohibiting causation of unnecessary suffering and use of indiscriminate weapons or the indiscriminate use of any weapon (Arimatsu, 2012). The application of these principles to clashes scenarios below the threshold of armed conflict however are ambiguous.

The future of warfare is likely to be performed remotely, potentially automatically and autonomously, with an option of being anonymous (Boothby, 2014). Existing body of law, specifically the Additional Protocols to the Geneva Convention, Article 36, requires states to examine the legality of new weapons and ascertain if their use would be prohibited by LOAC (International Committee of the Red Cross, 2010). An article 36 review is the only obligatory mechanism that compels states to assess newly developed weapons and weapons in development against LOAC requirements of military necessity, distinction, proportionality, limitation on usage of certain arms, good faith and humane treatment (Boulanin and

Verbruggen, 2017). Fry (2006), however notes that only ten states have formal weapons review procedures.[1] The low level of universal compliance to Article 36 requirements is one example of many that highlight the norm and legal voids that exists for newly developed means of warfare, including cyberwarfare.

1.1 Cyberwarfare

The notion of cyberwarfare, while having been studied extensively by academics and practitioners alike, has not yet yielded a uniform description of itself, a position that is further exacerbated due to definitional voids in international law.[2] The Law of War Manual of the United States for example fails to mention the term cyberwarfare, instead focusing on the designation cyberspace Operations, which it defines as:

"Cyberspace operations may be understood to be those operations that involve "[t]he employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace." Cyber operations: (1) use cyber capabilities, such as computers, software tools, or networks; and (2) have a primary purpose of achieving objectives or effects in or through cyberspace" (United States of America - Department of Defence, 2015, pg. 995).

The United States has designated cyberspace as an operational domain, on par with land, sea and air. This wide ambit provides for an extensive range of options for their military in cyberspace, including pre-emplacement of operational capability in the form of "cyber access tools or malicious code" (*ibid)*. This, as the dissertation will indicate, is an example where

[1] These countries are: Australia, Belgium, Canada, Denmark, Germany, Netherlands, Norway, Sweden, the United Kingdom and the United States of America. This contrasts with 174 state parties to the Additional Protocol I of the Geneva Conventions.

[2] Note that the term 'cyberwarfare' is used as the research considers both offensive and defensive cyber capabilities versus the term 'cyber attack' that focuses exclusively on offensive operations. This definitional approach is consistent with known military doctrine (Handler, 2012).

international perspectives on what constituents permissible versus non-permissible in cyberspace diverges.

1.2 Arriving at a Pragmatic Definition

In 2013, a Track II approach, guided by the East West Institute, aimed to bridge the terminological gap between the United States and the Russian Federation on cyber related matters. While cyberwarfare was jointly agreed to be "…cyber attacks that are authorized by state actors against cyber infrastructure in conjunction with a government campaign", the key term of cyber attack proved controversial (Godwin III *et al.*, 2014, pg. 43). The bilateral teams could not agree if indistinct attack methods, such as propaganda, could be classified as a form of cyber attack.[3]

Wars, by their nature, are ultimately political and therefore, subservient to political aims and objectives (Waldman, 2010). Cyberspace provides the space for manipulation of public opinion that could drive a nation-state towards a more favoured position towards another. Hirch (2017) provides a case in point of automated opinion engines shifting public discourse in a manipulative manner. When employed by States, cyber based actions on state institutions and manipulation of electoral results could be a form of an attack on a nation through cyberspace and could thus be considered within the ambit of cyberwarfare. Ford (2010) however asserts a delineation between information operations and cyberwarfare. He notes that psychological operations, including propaganda and fake news, do not employ traditional warfare techniques with pure military objectives in mind. The author however concedes that this perspective is U.S. centric while Russian and Chinese military ideologies combine the two.

[3] A cyber attack, according to the Track II process noted, was defined as: "offensive use of a cyber weapon intended to harm a designated target." (Godwin III et al., 2014, pg. 44).

Goel and Hong (2015) argue that the definition of cyberwarfare is contextual and include the following four broad categories:

1. A state seeking to influence the internal politics of another state with the aim of regime change that could take place through social upheaval or via domestic institutional mechanisms;
2. Non-state actors that conduct cyber attacks as well as use cyberspace for communication, propaganda and recruitment purposes;
3. Individual actors that target another country's citizens or institutions due to an existing conflict or for ideological reasons; and
4. Computer based or kinetic means of attack that target critical infrastructure. The authors include industrial espionage in this category.

These categories, while comprehensive, further indicate the complexity in characterising cyberwarfare. For the purposes of the paper however, the following composite description was arrived at:

- Intentional covert and overt applications of cyber capabilities, by state and/or state sanctioned actors, against another state and/or state sanctioned actors, for the realization of strategic and political objectives of a state or a collective of states.

This derived definition considers the following important factors, some of which have been alluded to previously:

- War, conflict, attacks, sanctions and other instruments of statecraft are primarily political in nature and are performed with a political objective in mind;

- Proxy warfare has remerged as a favoured means of conflict in contemporary political savoir-faire for the maintenance of strategic advantage, including use of cyber attacks that are difficult to attribute (Mumford, 2013); and
- Maintains the centrality of the state as a critical actor in international affairs, while noting the role of non-state actors that are, by and large, endorsed by a state through a combination of military, financial, political, infrastructural and/or legislative support (*ibid*).

While recent scholarship, for example Mann (1997) and Salamey (2016), have noted the decline of the state, it remains central in the international system. This is primarily due to the core capabilities and functions that it executes, namely (Ghani, et al., 2005, p. 6):

1. Legitimate monopoly on the means of violence;
2. Administrative control over its territory;
3. Management of public finances;
4. Investment in human capital, including education and skills development;
5. Delineation of citizenship rights and duties towards equality for all;
6. Provision of infrastructure services, including transportation, water and power;
7. Formation and protection of the market;
8. Management of the assets of the state, including environmental, mineral, cultural and other national assets;
9. Authority over international relations, including authority to enter into treaties and borrow from the international market; and
10. Effective rule of law.

The above classification also highlights the vulnerability of a state if it's core functions cannot be executed due to a cyber attack. With increasing dependence on Information and

Communication Technology (ICT) for the execution of state functions, certainty over state behaviour in this arena, for example, arms control in the form of immunity from cyberwarfare over critical infrastructure, becomes increasingly important (Schneier, 2012).

As will be presented in Chapters Two and Three, current state practice and theory surrounding arms control over cyberwarfare is nascent. This is understandable due to the fast pace of weapons research and development juxtaposed with the slow pace of international norms and behaviour maturation as well as theory development in the field of international relations.

Having provided a brief outline of the voids in international law on matters related to cyberwarfare, the next section provides an overview of the dissertation, including its aims and objectives, methodological approach and overall significance of the research.

1.3 Aims and Objectives of Research

The aim of the dissertation is to assess the feasibility for arms control over cyberweapons through a binding international agreement, while acknowledging the norm-defining work currently taking place across a range of intergovernmental initiatives. This will be presented through the prism of a maturity model in order to assess the feasibility of critical elements of the legal text that could form the bedrock of such a convention.[4]

The specific objectives of the study are therefore:

- To determine the landscape of international agreements that partially or completely address matters relating to cyberwarfare, taking into account stages of norm building when applied to emerging technology weapons;

[4] Note that although the word convention is used in this instance and throughout the paper for ease of reference, the envisioned international legal instrument could be in the form of a treaty, or a pact or an agreement, etc. The defining characteristic for a binding treaty is the acceptance of state parties to regulate it through international law (Orellana, 2014).

- To construct a maturity model that takes into consideration the viability of an international legal instrument on cyberweapons through an assessment of its critical components; and
- Taking into consideration the outcomes of the maturity model, develop practical recommendations in bridging negative bargaining zones and expanding zones of possible agreement for an eventual international legal instrument on cyberweapons.

In order to arrive at the objectives, a qualitative approach will be followed, crafting a technique that combines grounded theory and content analysis methodologies. The philosophical paradigm followed fuses critical and critical-realist perspectives with pragmatist and constructivist outlooks. These will be further expanded upon in Chapters Three and Four.

1.4 Significance of Research

Cyberwarfare has become a topic of importance in contemporary diplomacy and has been subject to an increasing level of focus within academic and governmental spheres. However, devoted research on the issue has been sparse. Furthermore, the pace of norm setting on legitimate use of cyberweapons has been glacial, juxtaposed to the breakneck speed at which offensive and defensive cyber capabilities are developing due to competition between states.[5] This dissertation seeks to reduce the knowledge gap that has arisen as a result of expanding cyberwarfare capabilities of states, as well as furthering the international relations discipline that has been lagging behind the significant changes that cyberspace has brought upon the international system.[6]

[5] Although beyond the scope of this paper, the trend towards deeper incorporation of Artificial Intelligence (AI) and robotics into future combat scenarios has a significant cyberwarfare component due to the use of computing hardware and software in the modus operandi of AI and robotic based weapons.

[6] Demchak (2014), takes a deeply critical view of current international relations theory, arguing that scholars are significantly falling behind the rapid evolution of hostilities and combative relations among major actors of a reshaping international system.

1.5 Outline of the Study

Having introduced the research in Chapter One, the paper proceeds to the literature review in Chapter Two. The review of literature will focus on relevant and current works at the nexus of arms control and cyberwarfare as well as core theoretical elements relevant to the paper. Chapter Three will present the conceptual framework for the research, while Chapter Four discusses the methodological approach followed for it. Chapter Five will undertake content analysis of a sample of pertinent arms control agreements, as well as related instruments of IHL, while Chapter Six will deliver the feasibility maturity model for arms control over cyberweapons. Chapter Seven will then discuss the implications of the results towards the realisation of a binding international legal instrument for cyberweapons, after which the study will conclude in Chapter Eight.

> "We are at the end of the frontier period in the evolution of cyberspace during which it spread openly and globally as substrate underpinning most critical processes of modern civil society. Now, we are moving into the transitional conflict era in which the nations struggle over control of the wealth formed in and through the frontier. At the end of this turbulence, as has always happened, the international system will regularize the rights and holdings of winners and losers."
>
> (Demchak, 2014, p. v-vi)

2. Literature Review

The review of literature for the dissertation will begin by presenting the current literature on military capabilities enabled by cyberspace. This will be followed by revealing the increasing military centricity of cyberspace by analysing the assessment of United Nations Institute for Disarmament Research (UNIDIR). The discussion will then be followed by a review of literature focused on arms control in cyberspace, including the rationales for and against. This is then followed by a section dedicated to theories applicable to the study. The chapter will then be concluded with a summary.

2.1 Capabilities Endowed by Cyberweapons

The 2008 Russian - Georgian conflict was the first occurrence of cyber attacks conjoining traditional warfare over air, ground and sea. Handler (2012) categorised Russian use of cyber attacks as either employed in support of conventional forces or to directly achieve objectives without the commensurate physical destruction of targets. Cyberweapons, as the aforementioned scenario presents, occupy a wide spectrum in modern warfare, ranging from "generic but low-potential tools to specific but high-potential weaponry" (Rid and McBurney, 2012). Malware occupy the lower end of the spectrum, while the Stuxnet attack on Iranian centrifuges in 2010 can be classified at the higher end. Unsurprisingly, the latter require extensive research and development, for example, in the development of Stuxnet, the United States National Security Agency, in collaboration with their Israeli counterparts, Unit 8200, developed replicas of Iranian centrifuges in order to test the effectiveness of their cyberweapon (Sanger, 2012).

Literature surveyed indicates broad consensus existing on cyberweapons providing a unique combination of tactical, legal and strategic advantages over conventional weapons. These include (Advisory Council on International Affairs, 2011; Handler, 2012; Iasiello, 2015, Segal, 2016):

- Initial costs for deployment are comparably low vis-a-vis conventional attacks. The costs of a cyberweapon also diminishes over time as programmers become more efficient and build on existing exploits. Note however that in the longer term, the defensive procedures put into place against cyber attacks will likely require more sophisticated attack tools to be developed in response, thus diminishing the aforementioned cost reductions;
- Attacks are difficult to attribute, and in some cases, impossible to trace, allowing for plausible deniability;[7]
- Lowers internal political costs and rarely negatively affects public political support;
- Can be deployed in such a manner to fall below the threshold of an Act of War as defined in LOAC, and may even be utilised outside formal military structures[8]; and

[7] An attack can take place using a chain of hacked computers or devices, or through a botnet of compromised computers, which help mask the origin of the attack.

[8] For example, an alleged hacking group tied to the United States National Security Agency, the Equation Group, has performed at least 500 infections in at least 42 countries, with Iran, Russia and Pakistan as its top targets (Goodin, 2015).

- Provides asymmetric capabilities, especially in contexts where an adversary is highly networked and electronically dependent.

They are however susceptible to the following (Segal, 2016; Smeets, 2016):

- Cyberweapons have a limited shelf-life and are transitory in nature. Once deployed, the weaknesses that they have taken advantage of can be known and corrected rapidly. This correction may take the form of patches that will then increase the defensive capability of the target if it's systems can be updated in an expedited manner;
- The outcomes of an attack are uncertain, making it challenging to determine in advance intentional and collateral damages; and
- The impermanent nature of cyberweapons require ongoing development and therefore alters the cost structure of cyberweapons in political and military decision making on deployment. This therefore negates the asymmetric benefit for weaker actors that may not be able to dedicate sufficient long term commitment towards their cyberweapons programs.[9]

As with any weapon, cyberweapons are therefore bound by design limitations. The nature and extent of threats associated with cyberweapons is however under debate according to literature surveyed. Clark (2009) views the current Internet landscape as one which is under regular, almost constant, cyber attack. Reardon and Choucri (2012) dispute this, citing the lack of specificity in Clark's argument, noting that most of the attacks underlying Clark's position refers to espionage activities, which are "not traditionally considered to be an attack at all, at least not in the context of internationally accepted laws of war" (Reardon and Choucri, 2012, pg. 22). Rid (2012) and Acton (2017) move the debate further, arguing that cyberweapons do

[9] Buchanan (2016) however posits that weaker actors can learn from the exploits of stronger actors and adapt attack methods for their own advantage.

not necessarily provide the requisite offensive capabilities unless used in conjunction with kinetic military activities, with the physical action benefiting from the disruption caused by cyberweapons. Libicki (2013) views the actual risk from a cyberwar to be in an escalation from a virtual war into a real war, contending that the effects of a cyber attack cannot reach the scale officials often warn of, thus arguing that the threat is overhyped. Arquilla (2012) however disputes this notion. Citing the 2007 cyberwar against Estonia, he underscores that the attack was disruptive nature to the small but highly digitised country, resulting in significant financial losses. Although kinetic damages can be limited in a cyber attack scenario, Arquilla's main concern is related to scale, in which an attack against the United States, for example, could result in billions of US dollars of damage given the significantly networked nature of that society.

Iasiello (2015) places cyberweapons as a method of signalling to political opponents, as opposed to means of military conflict, citing the lack of cyber attacks in recent military conflicts due to the absence of strategic advantage being gained by resorting to them.[10] Blank (2017) however contrasts with this position, citing Russian cyber attacks in Ukraine that allowed for the enforcement of Russian interests below the threshold of violence and thus avoiding military escalation. As presented, no consensus has yet to emerge in literature on the actual severity of the risks posed by cyberwarfare. There is however increasing allocation of resources to militarisation of cyberspace. The next section will therefore briefly review the landscape of states dedicating resources in developing cyberwarfare capabilities.

[10] The author cites the 2014 Israel-Hamas conflict, the 2014 Ukraine-Russia crisis, the 2013 Syrian civil war and the 2011 Libyan civil conflict.

2.2 Emerging Military Centricity

Contemporary uses of cyberweapons appear to be in the undefined zone between declared war and peace, where the use of convert means and coercion are the tactics of the day in order to arrive at political objectives and further national interest. Andres (2014) highlights the usefulness of cyberweapons for policy makers in achieving policy objective by relying on plausible deniability advantages afforded through offensive cyber operations, similar to state sponsored piracy and insurgency. The author includes theft of intellectual property, advancing societal disruption and sabotage against critical infrastructure as the three main methods employed by states to achieve their policy objectives through cyber operations.

The increasing use of these tactics, coupled with lack of global agreement on appropriate state behaviour in cyberspace, has led to an increase in the development of offensive and defensive cyber capabilities amongst nations. According to the United Nations Institute for Disarmament Research (UNIDIR, 2013), 68 United Nations (UN) Member States had cybersecurity programmes, of which 32 were classified as having cyberwarfare capabilities in their military organisations in the 2011 assessment. In 2012, UNIDIR repeated the assessment and found that the situation had shifted dramatically. The number of cybersecurity programmes had risen to 114, with the share of military programmes rising to 47. This assessment however is not exact, as upon further examination of UNIDIR's review, as not all of programs are military-offensive centric (UNIDIR, 2013).[11] Table 1 below revises UNIDIR's analysis:

[11] This distinction is important as the mere existence of a cyber unit or capability within the military corps does not imply development of offensive capabilities that is the core focus of this dissertation.

Table 1 - Analysis of UNIDIR's Review of State Cybersecurity Programmes

State	Military-Offensive Centric?	Rationale for Classification (if applicable)
Albania	No	Albania's focus appears to be more on cybersecurity versus developing cyberwarfare capabilities.
Argentina	Yes	A unit within the Argentinian command is tasked with performing 'Cybernetic operations' for the cyberspace battlefield.
Australia	Yes	Australia formally formed an Information Warfare unit in July 2017 to boost its warfare capabilities.[12]
Austria	No	The Austrian capability appears to be centred on cybersecurity best practices and not offensive military capabilities.
Belarus	Yes	Cyberwarfare capabilities are being embedded as part of a new battlefield according to the Belarusian Ministry of Defence.
Brazil	No	Although the Brazilian military oversees cybersecurity for the nation, it appears to be focused solely on securing cyberspace for Brazil and not intended for warfare capabilities.
Canada	Yes	Open source information appears to indicate that Canada is investing heavily on developing cyberweapons.[13]
China	Yes	N/A
Columbia	No	Columbia's efforts are related to cybersecurity as opposed to cyberwarfare.
Croatia	No	The Croatian cyber efforts appear to be in the realm of intelligence gathering and cybersecurity and not cyberwarfare.
Cuba	No	Cuban cyber capabilities, based on UNIDIR and other open sources, appears to be geared for defensive purposes.
North Korea	Yes	N/A
Denmark	Yes	Denmark appears to be on the verge of institutionalising cyberwarfare capabilities.

[12] Note the UNIDIR report was compiled in 2013, while the formation of the Australian Information Warfare unit occurred in 2017, per the Australian Department of Defence (no date).

[13] The UNIDIR data appears to be outdated vis-a-vis open source data appearing in Canadian media (Boutilier, 2017).

State	**Military-Offensive Centric?**	**Rationale for Classification (if applicable)**
Estonia	No	Estonia itself is focused on defensive capabilities, with strong collaboration with the North Atlantic Treaty Organisation (NATO).
Fiji	No	Fijian efforts are focused on cybercrime and related financial offences.
Finland	Yes	The Ministry of Defence of Finland, via its Cyber Defence Unit, provides for mounting of cyber attacks in the event of hostilities.
France	Yes	N/A
Georgia	No	Georgia's efforts appear to be centred on information security and safeguarding critical infrastructure.
Germany	Yes	N/A
Hungry	No	The Hungarian Ministry of Defence is building cybersecurity capabilities in the defensive sphere.
India	Yes	N/A
Indonesia	No	Indonesia's defence ministry's focus in the cyber realm is on defence and protecting information assets.
Iran	Yes	N/A
Israel	Yes	N/A
Italy	Yes	N/A
Japan	Yes	N/A
Kazakhstan	Yes	In 2017, Kazakhstan adopted a new military doctrine that encompasses cyberwarfare capabilities into its operations.[14]
Lithuania	No	The focus of Lithuanian defence officials is on a cyber Defence Plan, slated for completion by 2019.
Malaysia	No	Malaysian efforts are focused on cybersecurity measures and cyber emergency response mechanisms.
Myanmar	Yes	N/A
Netherlands	Yes	N/A
Norway	Yes	N/A

[14] This update relies on open source data (Gussarova, 2017).

State	**Military-Offensive Centric?**	**Rationale for Classification (if applicable)**
Poland	Yes	N/A
South Korea	Yes	N/A
Russia	Yes	N/A
Singapore	No	Singapore has developed advanced defensive capabilities and is setting up additional training centres to further build its cyber expertise.
Slovakia	No	Slovakian authorities have established coordination mechanisms related to cyber defence and participation in NATO cybersecurity exercises.
South Africa	Yes	Cyberwarfare capabilities are in advanced stages for the South African National Defence Force, with the establishment of a cyber Command Centre Headquarters by 2019.[15]
Spain	Yes	N/A
Sri Lanka	No	Sri Lankan efforts are focused on defensive matters as well as coordination on responding to computer emergencies.
Switzerland	No	The Swiss military's focus on cyber matters is defence orientated.
Ukraine	Yes	N/A
United Kingdom	Yes	N/A
United States	Yes	N/A
Vietnam	Yes	N/A

The additional assessment performed in Table 1 above provides a clearer image of cyberwarfare capabilities globally, noting 28 states with active offensive cyberwarfare capabilities. This however cannot be an exact count, bearing in mind that other states may have covert cyberwarfare programs in place. Absent from this list are certain notable exceptions, such as Saudi Arabia. Saudi Arabia is believed to be rapidly increasing its cyberwarfare capabilities

[15] Note that while offensive cyberwarfare capability may not yet be operational, it appears that the key pillars of it are in place (Martin, 2017).

through covert cooperation with Israel (Bocetta, 2017). With this increasing militarisation in mind, the next section will move the discussion in literature onto arms control and its potential applicability to cyberspace.

2.3 Arms Control in Cyberspace

The emerging military centricity of cyberspace, as well as the capabilities endowed through cyberweapons, will make these tactics increasingly attractive, especially to smaller nations (Suciu, 2014). Tangent to this trajectory is the forthcoming revolution in warfare through Artificial Intelligence (AI) based attacks and Lethal Autonomous Weapons Systems (LAWS), which have an inherent design dependence on computers, thus making those weapons vulnerable to being hacked.[16]

Once a weapon system becomes widely available, it can proliferate, be managed through arms control or abolished through disarmament. Given the unique advantages of offensive cyberweapons it is unlikely for it to be abolished, while it is anticipated that the number of countries that have offensive cyberwarfare capabilities will increase. This section will thus explore the position of current literature on arms control in cyberspace, with a view towards determining the contours of viability of such a mechanism in the cyber arena. It will begin with a brief overview of arms control mechanisms, followed by rationales for and against arms control in cyberspace that will be presented in subsequent sections.

2.3.1 Arms Controls Mechanisms

The onset of new forms of mass destruction developed by humanity led to increasing calls to control them, especially as the number of actors possessing them climbed during the 20th century (UNODA, 2017). Arms control over weapons of mass destruction, including Nuclear,

[16] An interesting case in point was the remote hacking and takeover of the RQ-170 US drone by the Iranian military in 2011 (Shane and Sanger, 2011).

Chemical and Biological, has indeed made the interstate conflicts less destructive in terms of indiscriminate lives lost (UNODA, 2017). Tangent to this development has been the growing number of intra-state conflicts as well as military interventions in internal conflicts of other states. This therefore lessens the requirement for use of weapons of mass destruction, although incidents of Chemical weapons use in Syria run counter to this development (UNODA, 2017). Arms control can certainly assist in substantially reducing specific weapon types. The world's stockpile of cluster munition for example has been reduced to only 2% (Landmine and Cluster Munition Monitor, 2017). Countering this however are the inherit limitations of arms control mechanisms that generally suffer from violations and clandestine subversive activities (Strauss, 2015).

Despite these, arms control mechanisms continue to be introduced and maintained. The general motivations for it include (Arimatsu, 2012):

- Reducing military asymmetries between states in order to reduce tensions and instability;
- Forestalling rapid proliferation of new weapons;
- Diverting military spending away from weapons towards economic and social development; and
- Facilitating negotiations between states.

In order to explore this deeper, the next section will seek to ascertain the broad position of cyberspace in existing arms control topologies.

2.3.2 Topologies of Arms Control

While no single framework exists to categorise arms control mechanisms, a number of topologies seek to provide a sense of order. Croft (1996, pg. 202), through an analysis of arms control since ancient times, posits that "conceptually, five types of arms control were identified at being in existence at the beginning of the post-cold war period: arms control at the conclusion of conflicts; arms control to further strategic stability; arms control to create norms of behaviour; arms control to manage proliferation of weapons; and arms control by international organisation". This extensive topology, while useful as a narrative of the past, did not consider the evolving nature of warfare that has shaped conflict in the 21st century. Bailes *et al* (2014, pg. 42), taking into consideration contemporary realities, suggest the following framework:

- Classical Arms Control: Aims to manage military capabilities of parties towards a stable paradigm;
- Non-Proliferation Regimes: Detecting and preventing misuse of dual-use technologies towards hostile ends; and
- Humanitarian Arms Control: Target the extent of suffering during and after conflicts, aiming to restrict and/or prohibit the employment of certain weapons.

The above typology can be extended to offensive cyberweapons in all three cases, although fragile at best when considering classical arms control and non-proliferation regimes due to the inherent nature of cyberweapons discussed previously. From a humanitarian perspective, limitations on targeting civilian and humanitarian objectives could be the basis for arms control on offensive cyberweapons.

The final framework to be presented in this chapter is a recent analysis by Miller (2017) who suggests three broad categories in classifying contemporary arms control mechanisms. These are presented in Table 2 below, augmented with its potential applicability to cyberspace:

Table 2 - Topological Applicability of Arms Control to Cyberspace

Category	Definition	Applicable to Cyberspace?
Limits on forces and force postures	Arms control mechanisms of this type are focused on placing limits on the quantity, characteristics and technological limits of specific weapons. The nuclear treaties between the U.S. and the U.S.S.R. are classic examples of this classification.	Applicable - Limitations on use, such as prohibition on attacks against critical infrastructure, could be apt.
Crisis management measures	This category of arms control develops specialised agencies that focus on crisis management and ensuring the flow of accurate and timeous information in times of extended tension. The creation of the Nuclear Risk Reduction Centers in the U.S. and U.S.S.R significantly reduced the risk of an inadvertent or accidental nuclear confrontation by providing a communication channel between the two countries. These centers therefore aimed to reduce the probability of the occurrence of a misunderstanding or miscalculation between the two nations.	Applicable - Given the anonymous nature of cyber attacks, its critical for lines of communication to remain open in the event of an accidental or automated attack, as in the case of active-defence AI based mechanisms.
Confidence-building measures	Confidence building mechanisms are instrumental in scenarios that exhibit excessive competition and expanded arms races. These measures, including pre-notification of military exercises, missile tests and transparency in weapons information, help prevent misunderstandings and achieve de-escalation.	Not applicable, as confidence building measures require a high degree of verifiability, which is near impossible given the previously mentioned characteristics of cyberweapons.

The categorisation presented by Miller (2017) provided an additional two types of arms control regimes that could apply to cyberspace, namely arms limitation and crisis management measures. As will be discussed in Chapter 6, limitations of use against of certain classes of targets, as well as mechanisms to reduce tensions during crisis, could form the core elements of arms control in cyberspace.

2.3.3 Arms Control in the Middle East - A Possible Illuminator

Before turning to rationale against arms control in cyberspace, the paper will briefly focus on the case of the Middle East and its historical challenges with limitations on weapons, as a possible roadmap of what may lie ahead for arms control in cyberspace. While at the surface the two subjects seem poles apart, certain contextual similarities exist, including (Steinberg, 2005):

- Lack of international consensus on the applicability and degree of arms control;
- Divergent interests amongst key actors;
- Significant asymmetry in defensive and offensive capabilities; and
- Low level of ongoing conflict, with significant reliance on proxies and non-state actors.

In his analysis of arms control in the Middle East, Steinberg (2005) indicates that concluding arms control agreements relied heavily on the "management, amelioration, or resolution of existing conflicts" (Steinberg, 2005, pg. 500). The absence of major cyber conflicts, coupled with the four factors noted above, indicate strongly that achieving an international agreement on arms control in cyberspace is miniscule. This will be further expanded upon in the next section that focuses on challenges facing arms control in cyberspace.

2.4 Challenges Facing Arms Control in Cyberspace

The previous section, while highlighting the potential topological applicability of arms control to cyberspace, concluded with historical realities in other areas of arms control that may similarly hinder its development. This section will bring to light challenges and practical limitations of arms control in cyberspace, beginning with the absence of broad political support.

2.4.1 Insufficient Political Support

Political support is a key driver of initiating and maintaining arms control mechanisms. Apart from a few cases, all arms control regimes have been started by governments who mainly viewed them as continuation of their political means (Trachtenberg, 1991). Therefore, political support of powerful countries for such initiatives will be severely lacking in cases where it is detrimental to their interests (Ford, 2010). This appears to be the case in cyberspace, as the following case will illustrate.

In 1998, the Russian Federation called on fellow members of the United Nations to consider "legal regimes to ban the development, production and use of particularly dangerous information weapons" (United States of America - Department of Defense, 1999). This proposal was however eventually watered down during subsequent negotiations, with the United Nations General Assembly passing resolution 53/70 that:

1. "Calls upon Member States to promote at multilateral levels the consideration of existing and potential threats in the field of information security;
2. Invites all Member States to inform the Secretary-General of their views and assessments on the following questions:
    a. General appreciation of the issues of information security;
    b. Definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources;
    c. Advisability of developing international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality;
3. Requests the Secretary-General to submit a report to the General Assembly at its fifty-fourth session;
4. Decides to include in the provisional agenda of its fifty-fourth session an item entitled "Developments in the field of information and telecommunications in the context of international security" (UNGA, 1998).

The adopted resolution was devoid of Russian concerns around cyberweapons. The United States did not share the urgency of negotiations around cyberwarfare, instead viewing terrorist and criminal threats as more pressing for the international community and the United States (United States of America - Department of Defence, 1999). A secondary reason for the dilution of the Russian proposal, as suggested by Anderson (2016), is the low barrier to entry of cyberweapons, insinuating that states have a reasonable interest in developing and maintaining defensive and offensive cyber capabilities. Despite the lack of political support for comprehensive arms control in cyberspace, there have been several intergovernmental initiatives to develop norms on state behaviour in cyberspace, a trend that will be discussed further in Chapter seven.

2.4.2 Divergent Views on Cyberspace

Arms control mechanisms require a degree of shared understanding over the unit of negotiation. This situation is exacerbated in cyberspace given the vast chasm in perceptions amongst major cyber powers on cyberwarfare and information operations. While Western powers publicly propose a continued free and open Internet, the Russian Federation differs on this issue due to the perceived threat of foreign cultural imperialism and political sedition that could arise from unfettered access to information (Ford, 2010).[17]

This standpoint has been made explicit as a key threat in the Doctrine of Information Security of the Russian Federation (Carman, 2002). The approach of the Peoples Republic of China is almost identical to the Russian position, given the centrality of People’s War in Chinese

[17] Carman (2002) provides additional historical context on this divergence, citing the UNESCO MacBride Commission of 1977, which sought to ascertain a more balanced and open international flow of information. The Western powers were opposed to regulated flow of information while the Soviet Union, its socialist allies and third world countries justified regulations in order to counteract perceived cultural imperialism of the West due to its greater technological capability. The differences were never bridged and the commission was abandoned.

doctrine (Thomas, no date).[18] This divergence in perspectives further complicates arriving at sufficient global political support for arms control mechanisms in cyberspace.

2.4.3 Attribution Challenges

The anonymity provided by cyberspace, as well as the technical sophistication of cyberweapons, will present a significant challenge for any arms control mechanism. Certain attacks are not detected, while those that are, can be made to appear from another territory. While political attribution is possible, finding a technical link is nearly impossible. The cyber attacks on Estonia in 2007 and Georgia in 2008 for example could be politically associated to the Russian Federation, while no actual technical link was ever established (Litwak and King, 2015). This is due to the difficulties around the complexity of the technical forensics required to successfully track a cyber attack to its origin.[19]

At a technical-legal level, four levels of attribution are required in order to confidently assert attribution in cyberspace (Denning, 2005):

- Identification of attacking machines;
- Identification of primary controlling machines;
- Identification of humans responsible for attack; and
- Identification of sponsor organisation.

[18] Additionally, China has developed extensive alternatives to contemporary online services that enable ongoing government over watch while providing the required services to citizens. These include:
- Search engine: Baidu.com
- Streetview software: City8.com
- Online video: Tudou.com & Youku.com
- Twitter equivalent: Fanfou.com
- Photo sharing: Yupoo.com

[19] Note that there have been instances of successful attribution, but more due to careless perpetuators. The attack on Sony Pictures in 2014 was attributed to North Korea only due to mistakes made in incorrectly using proxy servers in attempting to disguise the attack (Litwak and King, 2015).

As shown by Litwak and King (2015), while the identification of attacking machines and primary controlling machines could be partially possible, the remaining vectors are highly challenging to ascertain. Denning (2001) further notes the barrier presented by inadequate legal and regulatory framework of victim or transit countries of cyber attacks, making evidence gathering and prosecution nearly impossible. Brenner (2007) further posits that the difficulties in attributing an attack complicates the responsibility for a response between a civilian or a military one, leading to potential uncertainty in decision making as to the depth and breadth of a response by the victim state.[20]

2.4.4 Verification Mechanism

The third key challenge for arms control in cyberspace is the verification mechanism which may need to accompany it. Monitoring for verification and compliance is near impossible given the ease of concealment of code, as well as ongoing development of tools and techniques of attack (Denning, 2001). This challenge is further exacerbated by the high levels of intrusion that will be required for compliance monitoring, a level that may be too high for state parties to accept.[21]

Comparably, the Biological Weapons Convention (BWC) lacks a verification mechanism given the degree of difficulty in verifying dual-use biological substances, its widespread availability as well as ease of concealment. In a more contemporary context, the Arms Trade Treaty (ATT) which came into force in 2014, similarly lacks a verification mechanism in the text of the legal instrument. Despite these challenges, the BWC and the ATT are heralded as normative successes (Kahn, 2011).

[20] Brenner (2007) further notes the difficulty in boundary setting on these issues, i.e. cybercrime versus cyberterrorism, state-sponsored or not.

[21] For example, a robust verification mechanism would require deep scanning of computers and servers of government agencies and military institutions. This is a near impossibility.

2.4.5 Non-State Actors

Cyberspace has enabled non-state actors to enter the domain of warfare, at or below threshold of war definitions as broadly understood under LOAC (Brenner, 2007). Apart from a direct role, non-state actors have significant proxy fighting value through the use of hacktivists and patriot hackers as detailed by Sigholm (2016). The involvement of non-state actors in cyberspace is a grey area in LOAC as its application requires an armed conflict to exist in the first place. The alternative approach of using existing body of law concerning non-international conflicts suffers from definitional deficiencies in cyberspace that would normally apply to non-state actors, such as ‘level of organisation’, ‘logistical capability’ and ‘control of territory’ (Saxon, 2016). The challenges of verification and attribution discussed above extent to non-state actors, thus enabling the possibility of states agreeing in public on arms control mechanisms in cyberspace, but in secret breaking rank with their commitments through third parties.

The second dimension of challenges borne through non-state actors is the significant ownership of Internet infrastructure by private corporations across multiple political jurisdictions.[22] While a state can introduce regulations to reduce risks emanating from cyberspace, that authority is limited to the network space within its territory, thus reducing its defensive posture given the global flow of information through the Internet (Dittrich and Boening, 2017). Any norm or treaty based approach towards arms control for cyberweapons may have to consider the role of the private sector in setting and enforcing such a regime. Arms control is not a traditional area for state engagement with the private sector, apart from export control mechanisms that entered into force with the BWC and Chemical Weapons Convention (CWC). In the cyber arena, the

[22] By extension, this creates a unique set of legal hurdles - while cyberspace is transnational, the people and infrastructure supporting it are rooted in the physical domain and thus subject to national laws of the jurisdictions they operate from (Nye, 2018).

private sector and states may have to enter into a far more complex arrangement than previously exercised under BWC and CWC (Rathmell, 2003).

The third dimension is linked the conundrum that results from state acceptance of limitations, as that would require a cyber environment where the power of criminals and terrorist is significantly reduced (Rathmell, 2003). A state may therefore argue for the need to maintain an offensive capability in order to combat non-state actors, unless this is addressed through other mechanisms.

2.4.6 Prospects and Possibilities

While some of the challenges presented above are surmountable, others are not, mainly due to the inherent nature of cyberspace and the means of warfare it enables. States have to grapple with the mammoth task of distinguishing between criminal and war acts, near impossibility of attribution and verification mechanisms and thus the exact regulation of this arena of warfare may not be possible, now or in the future. States may simply prefer an evolutionary approach, allowing for normative mechanisms and customary international law to take its course. The next section will thus transition towards rationales for arms control in cyberspace, highlighting the imperatives that may accelerate its birth.

2.5 Rational for Arms Control in Cyberspace

As discussed in chapter 1 and further elaborated on in section 2.4, certain states hold the view that existing bodies of law may be sufficient for the status quo to continue with regards to arms control in cyberspace. The digital arena however, as a domain of crime, espionage, activism and warfare, is dominated by offence rather than defence. The attacking party benefits from anonymity and the element of surprise, while the defending party may not have had key vulnerabilities patched or lack sufficient resources to withstand and subsequently respond to a cyber attack (Advisory Council on International Affairs, 2011). This power imbalance will therefore be a source of tension amongst states given the lack of accepted international norms of behaviour in cyberspace. Anderson (2016) argues that existing body of international law, more specifically the legal weapons review process, will most likely lead to the emergence of shared and agreed upon codes of behaviour. The challenges identified in the previous chapter however indicate otherwise. This section therefore focuses on rationales for arms control in cyberspace as presented in literature, with a particular emphasis on advantages that promote state interest by its implementation, beyond those presented in section 2.3.[23]

2.5.1 Managing Threats

Maurer (2018), citing arms control developments during the Cold War, highlights the strategic benefit it provided to the United States over the Soviet Union. This was achieved by the former competing with “the Soviets in military technologies where the United States was perceived to enjoy significant advantages, while simultaneously entangling the Soviet Union in an arms control regime that would limit areas of Soviet strength” (Maurer, 2018, Para. 1). The author further notes that arms control agreements reduced the pace of competition and military technical developments, enabling the United States to maintain its qualitative military edge.

Cyberweapons, due to the characteristics discussed in section 2.1, provide asymmetric capabilities to less powerful countries (Waddell, 2016). In suggesting means to manage this threat, Arquilla and Ronfeldt (1993) propose a dissuasion model, where procurement of cyberweapons by lesser powered states, including non-Western countries, would be met by strong a response from the United States. This model however has proven to be incapable of addressing the risks presented. Rathmell (2003) indicates that universally accepted arms control and norms governing behaviour over offensive cyberweapons would limit accessibility to and

[23] In line with Rathmell (2003), some of the core arguments in this section are aimed at measures that enhance the national interest of the United States as the likelihood of reaching norms and agreements on limitations to offensive cyberweapons has to appeal to U.S. national interests.

use of cyberweapons by states that do not yet possess cyberweapons capability, thus maintaining hegemony for existing cyber powers. This advantage could be further cemented by adopting a treaty based approach, which allows for inclusion of mechanisms to govern non-compliance, as opposed to a norm based approach which are by nature standards of behaviour and therefore non-binding.

2.5.2 Minimising Blowback Risks and Unintended Consequences

The interdependencies brought about by the Internet creates a blowback conundrum for military planners, with variable degrees of magnitude. Rathmell (2003) highlights the risk of inadvertent spread of the cyberweapon to friendly nations or even the attacker's society due to the dense nature of global interconnections. The United States, as the global cyber power, is further exacerbating the risk of blowbacks by becoming the largest purchaser of spying tools, exploits and zero day vulnerabilities and not disclosing them.[24] This offence minded approach leaves numerous private and public organisations to vulnerabilities that are never patched (Menn, 2013). This position, according to Rathmell (2013), contradicts the interests of the United States in ensuring that the cyberspace is protected given the economic virtues, and therefore national power benefits, that have arisen from it. Hughes (2010) however notes that the United States may not commit to limitations on its behaviour in cyberspace, as a corner stone of American hegemonic power rests in maintaining a maximum array of weapon systems.

2.5.3 Reducing Economic Loss

Classical arms race theories, specifically the repeated prisoner's dilemma and the spiral conceptual models, posit that room for cooperation exists between adversaries. Arms control

[24] Zero day vulnerabilities are computer software weaknesses that are not known or are not yet fixed and can be exploited to compromise information security. Crucially, zero day vulnerabilities have an average life span of 6.9 years, leaving sufficient time for exploitation (Ablon, 2017).

regimes therefore could be beneficial to participating parties (Kydd, 2000).[25] This includes economic benefits in terms of reduced military spending as well as reduced financial loss from zero day vulnerabilities. Nye (2015) argues that the latter could occur if countries, as part of an international agreement, were more forthcoming about secret zero-day vulnerabilities instead of hoarding the knowledge as a deterrent or for potential use in future cyber attacks. The risk arising from such vulnerabilities would then be dramatically reduced, potentially decreasing state and criminal cyber attacks and therefore reducing economic loss. Mueller (2014), arguing for a treaty based approach to control cyberwarfare, puts forward that increased predictability in military uses of cyberspace releases scarce state resources to focus on cross-border cooperation on cybercrime, thus bearing positive economic results.

2.5.4 Upholding Rules Based International Order

The election of Donald John Trump as the 45th President of the United States heralded a seismic shift in the international political system. The unilateral withdrawal of the United States from the Joint Comprehensive Plan of Action (JCPOA), initiation of what is increasingly appearing to be a trade war with China and continual expounding of intolerant and xenophobic perspectives are all indications of a United States that has become a rogue superpower (Kagan, 2018). This presents a significant risk to the international rules based system, especially if other nations start to emulate the behaviour of the United States. Chinese military doctrine for example already views international norms and rules with scepticism, noting that engineering of such constructs tends to benefit United States the most (Rathmell, 2003). This has resulted in China seeking to exploit actions that fall under the threshold of war for its own benefit, including an array of activities in cyberspace (*ibid.)*.

[25] The deterrence model of arms race theory however holds the view that an arms race is a necessary requirement in order to deter enemies, hence arms control is not feasible from this theoretical perspective (Kydd, 2000). Note however that deference theory has low applicability to cyberwarfare as section 2.6 will indicate.

At the same time, China, as an emerging super power, is seeking international consensus for its future vision of cyberspace, representing an opportunity for countries to negotiate towards acceptable military conduct in a domain that is essentially borderless and vital to national interest of all countries (Mai, 2017). Rathmell (2003) adds to this view by noting the potential for increased trust and confidence of the public and private sector through predictable state behaviour in cyberspace (Rathmell, 2003). Nye (2018) furthers this by highlighting the benefit of transitioning normative constraints from a smaller set of nations to encompassing the globe through formal agreements, with the aim of upholding a rule based international order.

2.5.5 Enhancing Existing Protections Afforded by Laws of Armed Conflict

While there is no global disagreement on the application of LOAC to conflict contexts, the sanctuary afforded by the Geneva Conventions will be impossible in the event of a cyberwar due to the interconnectedness between protected and non-protected entities (Rauscher and Korotov, 2011). Hughes (2010) argues that the blurring of civilian and military networks, while it may have been an economic inexorability, complicates the notion of military necessity under LOAC. While arguably not directly relevant, an arms control mechanism, developed through norms or treaty based approach, can advance existing LOAC to resolve the challenge that arises from intertwined civilian and military cyber infrastructure.[26] The United States will therefore be a major beneficiary of such a norm (Rathmell, 2003).

Tangent to enhancing existing protections in LOAC is maintaining, at least a semblance of, civility in international conflicts. Hughes (2010) notes the reduction in humanitarian consciousness of soldiers given the detachment that exists in offensive cyber operations and argues for a treaty based approach to reinforce humanitarian obligations that may arise in this

[26] As Chapter seven will further indicate, a global norm to protect critical infrastructure and the core of the internet is currently developing, which will further the rationale for norm development as noted in this subsection.

context. Arimatsu (2012), noting the limitations in LOAC that require direct damage to come into play, argues that as cyberweapons do not directly inflict damage, reaching an agreement in this arena may be advantageous for the development of international law.

2.5.6 Changes on the Horizon?

The challenges and advantages of arms control in cyberspace, as presented in literature, may appear contradictory. However, even in the absence of an international effort to develop a treaty directing state-level cyber operations, efforts to foster international understanding over cyberweapons will remove legal ambiguities and promote greater consensus about what is acceptable and what constitutes an act of aggression regarding military centric activities in cyberspace. Emerging gaps in LOAC, improving intergovernmental cooperation towards cybercrime as well as increased economic benefits could be significant reasons to forge ahead in developing standards of state conduct.

2.6 Theoretical Perspectives

This chapter seeks to place contemporary theoretical perspectives at the heart of this study, beginning with mainstream theories that seek to explain relations between states. The section then proceeds to introduce norm development theory in international affairs as advanced by Florini (1996). This is then furthered by the notion of life cycles for norm development as posited by Finnemore and Sikkink (1998). The work of Mazanec (2016), which focuses on norm evolution for emerging technology weapons, is then introduced. The chapter is then concluded with a summary of key theoretical concepts relevant to the research.

2.6.1 Relationships Between Nations

Relations between states are characterised by highly complex sets of interplays commonly shaped by national interests of each country. Therefore, a single conceptual framework that can explain state behaviour will not yield the benefits being sought through application of theories in international affairs by relevant stakeholders (Waltz, 2008). This section will therefore present current perspectives on the applicability of the dominant theories of international relations to cyberwarfare, i.e. liberalism, constructivism and realism.

Liberalism posits that "the relationship between states and the surrounding domestic and transnational society in which they are embedded critically shapes state behaviour by influencing the social purposes underlying state preferences" (Moravcsik, 1997). This is based on three assumptions (Moravcsik, 1997; Reardon and Choucri, 2012):

- The key actors in international relations are persons or groups, private or public, who are reckoned to be rational in nature and have an incentive to promote their interests under societal and material limitations;
- States represent a certain degree of domestic society, such as domestic political institutions, media, corporations and prevailing culture, as well as transnational social processes and non-state actors; and
- As each state seeks to achieve its unique objectives, it is influenced by the preferences of other states.

Liberalism, in application to cyberwarfare, has limitations due to the lack of focus on power that is central to discussions related to international peace, war and security. However, liberalism, with its focus on institutionalisation, may be relevant for debates concerning which global institution is most suitable to handle matters arising from cyberwarfare. It may also become more relevant if matters related to cyberwarfare increasingly take on economic dimensions.

Constructivist theories focus on the socially constructed composition of international affairs, applying the lens of historical processes that shape current affairs. The focus, in other words, is on beliefs and ideas and not material resources that determine state behaviour. The other key element of this theoretical paradigm is the centrality of individuals, specifically elites, as the main unit of analysis. The main drawback of constructivist theories in relation to cyberwarfare are twofold, firstly, these theories do well with framing historical contexts, which is not practical towards analysis of emerging technology weapons. Secondly, given the critical role of the state and its military in cyberwarfare, the use of constructivist approaches, that favour the individual, would by extension not be suitable (Walt, 2008).

Realism, which was the eminent theoretical tradition during the Cold War, renders international relations as a competition for power in an anarchic world system that is devoid of a central authority to protect states from one another (Walt, 2008). The end of the Cold War did not see the demise of realism in international relations. On the contrary, large powers have maintained realist principles in their foreign policy (Mastanduno, 1997). The use of cyberspace for increasing power, whether through insertion of backdoors in software by the United States of America or theft of intellectual property by the Peoples Republic of China, validates the core realist philosophy underlying state behaviour (McCarthy, 2015; Goldstein, 2018).

In their review of academic literature at the nexus of international relations and cyberspace, Reardon and Choucri (2012) undertook a detailed analysis of 26 prominent policy and scholarly international relations and political journals[27]. Their work highlighted that constructivist based paradigms appear to prevail in academic literature at the intersection of politics and cyberspace (Reardon and Choucri, 2012). The authors however indicate the prominence of realist perspectives on matters related to cyberwarfare, while liberal perspectives segue towards how

[27] Note that the work of Reardon and Choucri (2012) considered works in the English language and thus may not be representative of global scholarship. Note also the low yield of articles from their research, having identified 49 articles across 26 journals over a 10 year period.

cyberspace can shape state behaviour by expanding the diffusion of political ideas and increasing the capability of civil society organisations.

Cyberwarfare itself fits well within the realist theoretical paradigm due to its military and security dimensions. Realism therefore can suggest how states could use cyberspace to grow their security interests as well as how they may retort to cyberwarfare capabilities of other states. This however is limited in certain instances, for example deterrence theory. This notion relies on the abilities of states to deter an attack by making capabilities known and being able to act on those capabilities. The difficulty in attributing an attack, as discussed in section 2.4, challenges the use of deterrence theory (Grindal & Healey, 2016). Cyberweapons therefore do not fit neatly into static theoretical understandings, many of which were developed during the Cold War. Issues pertaining to emerging weapons are dynamic given their game changing potential (Mazanec, 2016). The next section will therefore switch to the more dynamic theoretical axiom.

2.6.2 Norm Evolution in International Relations

The behaviour of states arising out of non-binding mechanisms, including voluntary self-restraint and acceptance of new standards of conduct, has not been extensively researched. Norms, which regulate and constrain behaviour, have been assumed by certain theories of international relations, notably neoliberalism and neorealism, to be "an unexplained source of exogenously given preferences of actors" (Florini, 1996, pg. 363). However, mankind has witnessed sweeping changes over the past centuries of state behaviour, with some norms eventually being codified into international law. Constructivist, as opposed to liberal and realist scholars, place norms closer to the centre than the periphery. Florini (1996, pg. 366) cites the work of Schelling and Tannenwald who "independently show that a norm prohibiting the use of nuclear weapons has significantly constrained U.S. policy makers".

On issues related to state behaviour in cyberspace, a number of different norms are being suggested by an array of state groupings. These range from bans and limitations on use to no specific international legal regime being acceptable other than the continued applicability of laws of armed conflict to cyberweapons.[28] This suggests that norm development is currently in progress and any possible international agreement on this issue would be borne out of the ongoing norm building process. In order for norms to establish and spread, the following criteria need to be present (Florini, 1996):

1. Prominence: A norm requires an initial foothold in order to maintain a degree of prominence and is likely to gain that support through the efforts of norm entrepreneurs, which could be an individual, organisation or a state that facilitate the development of that norm. Powerful States have an advantage over small States in norm development by having greater number of opportunities to convince other States of their perspectives. Within the arms control context, non-governmental organisations and world leaders have been instrumental in contributing to the success of arms control regimes (Rutherford, 2000).
2. Coherence: As norms do not exist in a vacuum, their development depends on the existence of similarly aligned standards in which the new norm can fit in coherently.[29] The degree of coherence to existing norms therefore dictates the extent of legitimacy that the new norm benefits from at the beginning of its lifecycle.
3. Environment: Norms are by-products of their environment, in which States are the leading influencing factor for them. Florini (1996) posits a neorealist perspective for this criterion, arguing that distribution of power, differences in technological levels and

[28] This has led to an impasse within the international arena in general, and within the United Nations in particular, the latter seeing the work of the Group of Government Experts deadlocked in 2017.

[29] In other words, how logically related is the new norm to existing norms that have successfully resolved past problems that bore similar characteristics.

natural and human resources are significant for norm development. Note however that international norms have emerged that defy the neorealist notions purported by Florini (1996). Ingebritsen (2002) for example, indicates how Scandinavian countries, despite their lower levels of comparative geo-political power and limited natural and human resources, have established key international norms of sustainable development and peaceful resolutions of conflict.

4. Emulation: The reproduction of norms across States primarily occurs when they begin to emulate the new norm between each other. This typically occurs when there are clear failures in current norms or the emergence of new problems in which existing norms do not apply. Emulation, according to Florini (1996), is preferred by states given the large degree of complexity and uncertainty in international affairs.

The theoretical framework discussed above were further advanced by Finnemore and Sikkink (1998), who defined a three-stage lifecycle that can be applied to the phenomena of norm development in international affairs. The first stage, norm emergence, involves the seeding and persuasion of key actors to embrace the norm. The second stage, norm cascade, seeks to socialise the norm as extensively as possible. The final stage, norm internalisation, is when the norm is accepted and implemented. Not all norms complete the three cycles, often failing to reach the tipping of the first or second stage (Finnemore and Sikkink, 1998).

The authors advanced their theory through the development of a practical model outlining the factors that may assist in norm development across the three-stage lifecycle, with each phase characterised by “different actors, motives and means of influence” (Finnemore and Sikkink, 1998, pg. 895). This is summarised as follows (Finnemore and Sikkink, 1998, pg. 898):

Table 3 - Critical Factors Affecting Norm Development across its Life Cycle

Factors per Phase	Norm Emergence	Norm Cascade	Internalisation
Actors	Norm entrepreneurs with organisational platforms.	States, International Organisations, Networks.	Law, Professions, Bureaucracy.
Motives	Altruism, Empathy, Ideational Commitment.	Legitimacy, Reputation, Esteem.	Conformity.
Dominant Mechanisms	Persuasion.	Socialisation, Institutionalisation, Demonstration.	Habit, Institutionalisation.

At the outset, individual norm entrepreneurs, operating within and through an organisation, use persuasion as the key tactic to frame issues of interest and suggest more appropriate standards of conduct to leaders and institutional regimes (Finnemore and Sikkink, 1998). At this first stage, norm entrepreneurs are mainly motivated either by altruism, or empathy and welfare of others or ideational commitment.

While outside the scope of this paper, it is important to highlight other potential motivators for norm entrepreneurs as proposed by sociological and psychological scholars, which include self-interest, public spiritedness and justice (Miller, 1999).[30] The organisation that the norm entrepreneur operates from is equally important given the strong influence it will have on the

[30] Interestingly, Finnemore and Sikkink (1998) do tacitly recognise the motivation of self-interest, and expand it further by suggesting that the norm entrepreneurs redefine notions of self-interest for their targets.

norms being disseminated by one or more of its members, as well as providing information and access to critical audiences and decision makers (Finnemore and Sikkink, 1998).

To reach the second stage of the norm life cycle, norm cascade, requires institutionalisation through codification as “specific sets of international rules and organizations … in international law, in the rules of multilateral organisations, and in bilateral foreign policies” (Finnemore and Sikkink, 1998, pg. 900). Droubi (2017) concurs on the role of institutionalisation as the strongest provider of support for an emerging norm, adding that “institutionalisation clarifies the scope of the norm and of its application; it improves mechanisms of persuasion, as well as enhances the monitoring of levels of compliance with the norm, thereby increasing cultural and social pressure on resilient states” (Droubi, 2017, pg. 258). The other critical factor required to reach norm cascade is active participation of significant States and organisations that have a critical stake in the flowering of the norm (Finnemore and Sikkink, 1998).

Having reached the second stage of the norm life cycle, the emergent norm begins to propagate, in other words, cascade, if socialised sufficiently and furthered through demonstration of benefits arising from adoption of the new standards of behaviour (Finnemore and Sikkink, 1998). Droubi (2017), further characterises this stage by noting the importance leading states place on obtaining compliance from other states, as well as the increasing use of specialised language in communication. The increasing formalisation subsequently tides over the norm into the third stage, internalisation.

This stage is characterised by the complete acceptance of the norm, to the extent that it is taken for granted. The norms, by this stage, have power for they are not readily questioned, and are hard to discern (Finnemore and Sikkink, 1998). Droubi (2017), in contrast with Finnemore and Sikkink (1998) however, views total internalisation as a lesser prerequisite, viewing it as a progressive force that gradually takes hold within a state and as state agents interact amongst each other, the norm is still subject to adjustment. Droubi (2017), highlighting the difficulty in delineating the three stage processes given the fluidity of norm life cycles, suggests a fourth stage, late cascade, where international legal authorities affirm the new norm, potently imply that the norm is customary international law or even begin to utilise it as such.

2.6.3 Norm Evolution in Emerging Technology Weapons

The theory discussed above was furthered by Mazanec (2016) through its application to use and constraints on emerging technology weapons. His work noted the primacy of self-interest in the norm development role of a state, as well as the involvement of vital actors in the norm creation process, which aid in furthering the norm along the lifecycles discussed above.

Alignment between powerful countries plays an additional key role, with Mazanec (2016, pg. 102) noting that "a direct or indirect alignment of national self-interest with a constraining norm leads to norm emergence and the extent to which it is aligned with key or powerful states' perception of self-interest will determine how rapidly and effectively the norm emerges". While logical, and proven through state behaviour according to Mazanec (2016), this perspective fails to take into consideration constructivist rooted emerging norms that are developing in cyberspace (Radunović, 2017) as well as other domains of human activity.[31]

Mazanec (2016), as suggested by realism, places the state at the core of the debate on norms in cyberspace and through analysing the positioning of key cyber powers, concludes that constraining norms in cyberspace are unlikely. In parallel to Mazanec (2016), Finnemore and Hollis (2016) also considered norm construction for cyberspace, although only focusing on the paths the process could take and not the norms itself. Finnemore and Hollis (2016), while acknowledging the importance of the substantive contents of norms, argue that the process

[31] The Paris Climate Change accords and the global movement to ban nuclear weapons are interesting case studies that suggest motivations beyond realism to achieve restraint on state behaviour.

followed to derive them are equally paramount as their eventual acceptance and adherence depends on the means of arriving at the norm as well as the range of actors involved.

2.6.4 Nascent state of Theory

The literature review revealed a lack of scholarly rigour on matters related to key theories of international relations to cyberspace in general, and norm building of arms control mechanisms in cyberspace in particular. This may be in part be due to lack of norm building literature within international relations, and even more so on relevant restraints on state behaviour on matters related to cyberwarfare.

At the same time, it appears that conceptual models and theoretical understandings related to the study are emerging, taking on a blend of constructivist and realist perspectives. While the lack of breadth and depth of theory places limitations on the study, the emergent theories on norm building in international relations is valuable towards developing the conceptual basis, presented in Chapter Three, that underpins this paper.

2.7 Concluding the Literature Review

The review of literature unearthed the existence of a healthy debate surrounding offensive cyberweapons, its use in cyberwarfare and rationales for and against arms control mechanism to control its proliferation, be they treaty or norm’s based. Cyberweapons benefit from unique characteristics of low overall cost, plausible deniability to its wielders and can be operated to fall below thresholds of war as defined by LOAC. They do however have limited shelf lives and may have unintended consequences once employed. Critically, scholars are divided on the actual scale of the threat that offensive cyberweapons pose, although criminal and espionage risks are widely acknowledged. Another point of agreement in literature relates to the expansion of national military programmes in cyberspace, including offensive and defensive capability development, although developments related to LOAC are lagging behind.

Crucially, significant challenges exist to the establishment of formal mechanisms that could constrain the use of cyberweapons by States, including its dual-use capability, near impossibility of attribution of use and verification of compliance, lack of political support and divergence in views of major cyber powers and significant presence in and control of cyberspace by non-state actors operating across multiple political jurisdictions.

In reality however, calls for constraints on state behaviour in cyberspace are beginning to emerge. The literature reviewed for this paper indicated key rationale for forms of arms control over cyberweapons, including managing existing and future threats, reducing risks arising from blowback and unintended consequences, tangible economic benefits, upholding international rules based order and enhancing existing protections afforded under LOAC.

From a topological perspective, arms control literature has not achieved consensus on its categorisation, although several were identified that could be applicable to cyberspace, including non-proliferation regimes, humanitarian arms control, limits on forces and postures and crisis management measures.

Theoretically, few scholars have investigated the positioning of mainstream international relations theory to cyberspace, with most scholarly papers appearing to fall within a constructivist approach. This however contrasts with niche studies that conclude the appropriateness of realism to cyberwarfare, albeit with some deference.

Arms control, which is inherently tied to state behaviour and acceptance of self-restraint, has a normative function that is not well understood theoretically. Recent scholarship has sought to develop conceptual models for norms within the context of international relations, with some consensus at the meta levels of norm lifecycle development, led by Finnemore and Sikkink (1998), Finnemore and Hollis (2016), as well as Florini (1996). However, theoretical literature failed to significantly address emerging norms related to the subject at hand, surfacing a single author that was most closely aligned to the study. Mazanec (2016) taking a realist perspective, concludes that norm emergence is significantly aligned to the self-interest of nations that wield the emerging technology weapon. He furthermore argues that constraining norms are unlikely to emerge in cyberspace given the policy trajectory selected by major cyber powers, although contemporary calls for norms supports the norm building theories advanced by Florni (1996).

The lack of consensus as well as insufficient theoretical material for the paper may be attributed to the nascent nature of this research intersecting norm development in politics and arms control on emergent technologies in general and cyberweapons in particular. The theories gathered however did manage to inform the conceptual framework for this paper, the details of which will be presented in the following chapter.

“Reality is always more complex than any theory can completely capture, and you need to construct a conceptual framework that takes account of this complexity and avoids gross oversimplifications of the things you are studying, as best as you can”.

Joseph Maxwell, cited in Ravitch and Riggan (2017, pg. xii)

3. Conceptual Framework

The conceptual framework for the paper, which are the assumptions, beliefs and concepts underlying the research, are presented in this chapter in order to illustrate the preliminary theoretical understanding of the phenomenon under study (Maxwell, 2013). This is optimally illustrated through triangulating the philosophical and theoretical lattices on which the research is constructed.

3.1 Philosophical Paradigm

The philosophical paradigm, defined as a “set of interrelated assumptions about the social world which provides a philosophical and conceptual framework for the organized study of that world” (Filstead, 1979, pg. 34), positions the context of the study, influencing the ‘how’ and ‘what’ of the study, as well as affecting how results are interpreted. The field of social science is enriched with multitudes of paradigms, including positivism, post positivism, constructivism–interpretivism, critical theory, subjectivism and pragmatism (Kivunja C and Kuyini, 2017; Patel, 2015; Ponterotto, 2015). The distinctions amongst these can be summarised as follows (Patel, 2015, para. 8):

Table 4 - Distinctions Amongst Philosophical Paradigms

Paradigm	Ontology	Epistemology	Theoretical Perspective	Methodology	Methods
Positivism / Realism	There is a single reality or truth (more realist).	Reality can be measured and hence the focus is on reliable and valid tools to obtain that.	Positivism Post-positivism	Experimental research Survey research	Usually quantitative, could include: Sampling Measurement and scaling Statistical analysis Questionnaire Focus group Interview
Constructivist / Interpretive	There is no single reality or truth. Reality is created by individuals in groups (less realist).	Reality needs to be interpreted. It is used to discover the underlying meaning of events and activities.	Interpretivism (reality needs to be interpreted): Phenomenology Symbolic interactionism Hermeneutics Critical Inquiry Feminism	Ethnography Grounded Theory Phenomenological research Heuristic inquiry Action research Discourse analysis Feminist standpoint research	Usually qualitative, could include: Qualitative interview Observation Participant Non participant Case study Life history Narrative Theme identification
Pragmatism	Reality is constantly renegotiated, debated, interpreted in light of its usefulness in new unpredictable situations.	The best method is one that solves problems. Finding out is the means, change is the underlying aim.	Deweyan pragmatism Research through design	Mixed methods Design based research Action research	Combination of any of the above and more, such as data mining, expert review, usability testing, physical prototype
Subjectivism	Reality is what we perceive to be real.	All knowledge is purely a matter of perspective.	Postmodernism Structuralism Post-structuralism	Discourse theory Archaeology Genealogy Deconstruction	Autoethnography Semiotics Literary analysis Pastiche Intertextuality
Critical	Realities are socially constructed entities that are under constant internal influence.	Reality and knowledge is both socially constructed and influenced by power relations from within society.	Marxism Queer theory Feminism	Critical discourse analysis Critical ethnography Action research Ideology critique	Ideological review Civil actions Open-ended interviews Focus groups Open-ended questionnaires Open-ended observations

As Guba and Lincoln (1994) note, paradigms are ultimately human creations and thus none are irrefutably correct in an absolute sense. As conceptual frameworks, underpinned by philosophical paradigms, are constructions of the researcher, the paradigm selected by the researcher can be composed of more than one, even those which are seemingly contradictory (Maxwell, 2013). In order to further understand the unique perspective of the researcher, Maxwell (2013) further suggests, ascertaining the experiential knowledge of the researcher and as well as the prior theory and research of others to hone the conceptual framework of the study.

3.2 Experiential Knowledge

The philosophical paradigm of the researcher, in the context of this research, is closely aligned towards critical realism. This, ontologically, stems from a belief that the world exists separately from beliefs, theories and assumptions of the researcher. Epistemologically however, our apprehension, assumptions and intuitions about the world are created subjectively, power has a core role in determining that subjective reality which the researcher then bases their opinion on and lastly, no absolute truth exists, leaving room for doubt as to the complete utility and appropriateness of conclusions arrived at.

3.3 Research and Theory of Others

The research of others presented in Chapter Two in general, and the theories explored in Chapter 2.6 in particular, were published under a multitude of philosophical paradigms. In most cases the authors did not overtly state under which paradigm their work was produced on. It will therefore be essential to ascertain the research paradigm of the authors that are at the core of this paper. These, arranged in alphabetical order, are:

1. Droubi (2017);
2. Finnemore and Sikkink (1998);
3. Finnemore and Hollis (2016);
4. Florini (1996);
5. Goel and Hong (2015) in Jajodia *et al* [Eds.]
6. Ingebritsen (2002);
7. Mazanec (2016);
8. Miller (1999);

9. Nye (2015);

10. Nye (2018);

11. Radunović (2017);

12. Rathmell (2003);

13. Rauscher and Korotkov (2011); and

14. Steinberg (2005).

The work of each author was analysed in order to determine its philosophical paradigm, together with a summary of their theoretical perspective. These are presented in Table 5 below:

Table 5 - Classification of Philosophical Paradigms of Scholars Central to the Research

Author	Philosophical Paradigm of the Work	Summary of Theory and Rationale for Classification
Droubi (2017)	Constructivist	The author's paper analyses how norms have a higher probability of becoming customary international law if adopted by the United Nations, therefore taking a constructivist approach.
Finnemore and Sikkink (1998)	Critical - Realist	The authors acknowledge the constructive elements that drive norms in their paper. This however is contrasted with their critical perspective vis-a-vis rationale choice theory and the role of persuasion and power in norm formation, thus leaning towards realist paradigms. The work is therefore classified as critical-realist.
Finnemore and Hollis (2016)	Critical-Pragmatic	The main focus of this work is on the processes of norm development at the nexus of cyberspace and International affairs, with strong emphasis on its dynamic construction and power influences. Furthermore, the study provided solutions towards enhancing the norm development process. The work is therefore classified as critical-pragmatic.

Author	Philosophical Paradigm of the Work	Summary of Theory and Rationale for Classification
Florini (1996)	Critical-Constructivist	The author, in discussing norm development in international affairs, explicitly underlines the constructivist nature of their work, while at the same time, maintaining a critical philosophical stance, thus being classified as Critical-Constructivist for the purposes of this research.
Goel and Hong (2015) in Jajodia *et al* [Eds.]	Positivist	The paper, which focused on the employment of cyberweapons as a strategic weapon, was based on game theory models, which are quantitative and positivist in nature.
Ingebritsen (2002)	Subjectivist	This paper, in highlighting its liberal paradigm towards international affairs, sought to develop an alternative basis for power relations, nominally entitled 'social power'. This approach, which needs further empirically analysis, is deeply subjective, hence the subjectivism classification of the author and their paper.
Mazanec (2016)	Critical	Mazanec's conclusion, which predicts that national self-interest and constraints on cyberweapons are incompatible, is inherently taking on a critical philosophical paradigm due to the central placement of international power dynamics and coercively constructed institutional structures in developing his arguments.
Miller (1999)	Critical	Central to Miller's paper on the norm of self-interest is the role that the theory of self-interest plays in development of institutions that are created based on that notion, which in turn becomes reality, thus emphasising the socially constructed nature of self-interest, and by implication, national interest.
Nye (2015)	Pragmatic	This specific work of Nye can be classified as pragmatic given its focus on suggesting solutions for reaching international agreement on arms control in cyberspace, despite ideological differences amongst major powers.
Nye (2018)	Constructivist	In contrast to the 2015 paper, the 2018 work of Nye has a strong constructivist basis, advocating strongly for normative frameworks for cyberspace, thus being classified as constructivist for the purposes of this paper.

Author	Philosophical Paradigm of the Work	Summary of Theory and Rationale for Classification
Radunović (2017)	Pragmatic	The work of Radunović, which provides an overview of various diplomatic instruments focusing on state behaviour in cyberspace, seeks to transition the debate towards achieving agreements in the cyber arena, hence its pragmatic classification.
Rathmell (2003)	Critical - Realist	The worldview presented in this paper is closely aligned with realism, although the author allows manoeuvring space for possible future alternatives, hence its conjoined paradigm of critical-realist.
Rauscher and Korotkov (2011)	Pragmatic	The authors of this paper detail five proposals for governing cyber conflicts, with a strong solution focus in order to determine potential rules of the road in the event of a full blown cyber war as well as irregular cyber activities that fall below the threshold of armed conflict.
Steinberg (2005)	Critical - Realist	The work of Steinberg, while acknowledging the socially constructed basis of foreign policy of nations in the Middle East, takes on a realist current in developing its key argument, concluding that arms control will not be possible in the Middle East unless a range of issues resolutely resolved.

Briefly summarising the above results indicate a strong leaning towards critical and critical-realist philosophies, while at the same time supported by pragmatist and constructivists perspectives. This result corresponds with both the author’s own philosophical stance as well as the overall pragmatic aim of the research.

3.4 Theoretical Implications

The specific implications on the preliminary theoretical understandings for the paper are fivefold:

1. While no international treaty exists for arms control in cyberspace, norms are beginning to emerge to constrain state behaviour in this arena;

2. Norms have life cycles and exhibit specific characteristics for each phase, with some eventually becoming international law;
3. Power and persuasion play a significant role in the development and acceptance of a norm, and its subsequent transmutation into international law, only in certain circumstances, with big power cooperation and compromise required in other cases;
4. Prioritisation of the national interest, hand in hand with realist perspectives, pervade in matters related to international security in general, and with cyberwarfare in particular; and
5. Arms control in cyberspace, similar to arms control in a physical context, will not be possible unless a confluence of factors is present, including international consensus towards it, convergent interests amongst key actors to realise it, similarities in capabilities amongst critical participants is present, non-state actors and the private sector are included in developing it and, ironically, existence of significant regular and irregular cyber conflicts.

These key theoretical implications and the aforementioned philosophical paradigms strongly influence the chosen methodology for the research, the details of which will be presented in the next chapter.

4. Methodology

Guided by the conceptual framework arrived at in the previous section, this chapter seeks to outline the methodology and the rationale thereof for the research. As Chapters Two and Three indicated, the area of study under consideration, being interdisciplinary in nature, suffers from research challenges related to "lack of theory, conceptual definition, interdisciplinary approach, qualitative research and longitudinal research" (Gomez, 2013, pg. 2). The paper aims to contribute towards addressing the aforementioned concerns through the development of a maturity model that assesses the feasibility for a binding international legal instrument on cyberwarfare, taking into consideration the objectives of the paper as presented in the First Chapter.

Due to the embryonic nature of the study, the research will be exploratory in nature. A qualitative approach will be taken in order to have a more open and emerging research as opposed to "cause-and-effect type of thinking…associated with quantitative research" (Creswell, 2009, pg. 130). In addition, qualitative approaches are more suitable in research contexts that are chiefly characterised by insufficient scholarly work. The time frame of the research is cross-sectional, although a follow-up longitudinal study may be helpful in ascertaining adjustments to overall maturity score based on external changes.

4.1 Data Collection and Analysis Methods

Data collection method for the paper will be guided by Grounded Theory, treating document artefacts and literature as forms of data. This method was selected due to its alignment with the conceptual framework of the paper, as well as its inherent flexibility and responsiveness to the research situation (Bryant and Charmaz, 2010). Note that a more emergent method of Grounded Theory as espoused by Glaser (1992) will be followed in order to allow for as much emerging information as possible. The process for data collection will therefore be as follows (Bryant & Charmaz, 2010 and Glaser, 1992):

- Identify key elements of existing arms control treaties and extract generic elements;
- Identify patterns in the elements and compare results with literature on generic elements of arms control treaties;
- Identify core categories emerging from data and distil arms control treaty elements pertinent to cyberspace; and
- Validate categories and arms control treaty elements identified through a Delphi study.

The data and subsequent core categories will be analysed through content analysis techniques, primarily based on the structured content analysis method developed by Mayring (2008). The general procedure for the analysis is illustrated as follows:

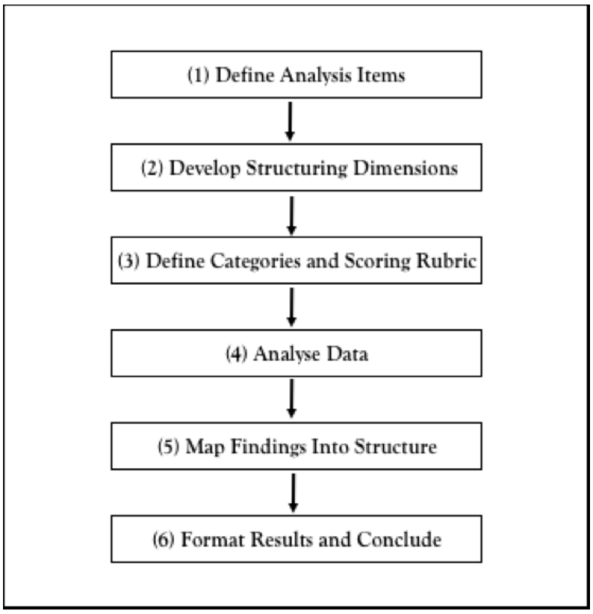
(1) Define Analysis Items
(2) Develop Structuring Dimensions
(3) Define Categories and Scoring Rubric
(4) Analyse Data
(5) Map Findings Into Structure
(6) Format Results and Conclude

Figure 1 - Structured Content Analysis - A General Procedure

The process begins with defining the units of analysis of the emergent categories and arms control treaty elements, and will subsequently, focus on developing feasible structuring dimensions for a maturity model through analysis of key structuring questions and sub questions. The categories will then be further defined, leading to the development of scoring rubrics that will be used to determine the maturity values for the model. The data will then be analysed according to the derived structure and mapped accordingly. The process followed and outcomes will be presented in Chapter Five. Chapter Six will concentrate on developing the maturity model and will be guided by the works of Kohlegger *et al.* (2009), Liang *et al.* (2016) and Wendler (2012). This will entail the following:

- Construction of a four-stage maturity model, with the generic arms control elements as derived at in Chapter Five forming the vertical axis. The horizontal axis will indicate the level of maturity, with higher scores for higher levels of maturity;
- Initial scoring of the rubric based on existing international legal texts that relate directly or indirectly to cyber Operations, cyberwarfare and cyberweapons;
- Second round of scoring, taking into consideration emerging norms; and
- Third round of scoring, taking into consideration the national security interests, as a well as state Practice, of a core group of countries.[32]

4.2 Research Limitations

Several significant limitations exist given the methodological approach chosen for the research. Firstly, content analysis techniques, by implication, exclude knowledge and wisdom that may be present in individuals involved with the field. This impacts the breadth of potential outcomes, although the aforementioned Delphi study is intended to reduce this. The second limitation relates to the validity of the derived categories. The research seeks to minimise this

[32] The countries selected will be a subset of the states discussed in section 2.2.

limitation through fine tuning of the rubric during its development, as well as the maturity model score itself through three rounds of modification. Thirdly, the research was conducted primarily in the English language, thus limiting incorporation of material in other languages to translations where available. While these limitations affect the extent of the work, the core model that it envisions to develop should be sufficiently accurate to serve as a reasonable foundation for other scholars.

5. Data Collection and Content Analysis

As outlined in the methodology section, this chapter will develop and present the results of the structured content analysis. The chapter will therefore begin with defining the analysis items, after which it will develop the structuring dimensions. The categories and scoring rubric are then detailed, while the fourth step will present the results of the data analysis. This are then further refined towards creating the elements of analysis for the maturity model.

5.1 Define Analysis Items

The unit of analysis for this paper are generic elements of arms control regimes as derived from contemporary arms control treaties and instruments of international humanitarian law, as well as UN resolutions, that fall within suitable topologies for a cyberweapons convention as specified in section 2.3.[33] The total population of applicable treaties and UN resolutions identified were 36, of which 12 were judgmentally chosen for analysis. The aforementioned were obtained from an index compiled by the United Nations Office for Disarmament Affairs[34] as well as list of Treaties, state Parties and Commentaries as published by the International Committee of the Red Cross.[35] This resulted in the following UN Security Council and General

[33] For ease of reference, these are:
- Classical Arms Control Mechanisms;
- Non-Proliferation Regimes;
- Humanitarian Arms Control Regimes;
- Limitation on Forces Regimes; and
- Crisis Management Mechanisms

[34] http://disarmament.un.org/treaties/

[35] https://ihl-databases.icrc.org/ihl

Assembly Resolutions, as well as arms control treaties and multilateral legal texts, being selected for analysis:

1. UN Security Council Resolution (UNSC) 1540 (UNSC, 2004);
2. Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (International Committee of the Red Cross, 2005);
3. Geneva Conventions and Associated Protocols (International Committee of the Red Cross, 2010 and International Committee of the Red Cross, 2016);
4. Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict and its Two (1954 and 1999) Protocols (UNESCO, 2010).
5. International Convention for the Suppression of Acts of Nuclear Terrorism (UN, 2005);
6. The Arms Trade Treaty (Arms Trade Treaty, no date);
7. The Biological and Toxin Weapons Convention (UNOG, no date);
8. The Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (Organisation for the Prohibition of Chemical Weapons, 2005);
9. The Treaty on the Non-Proliferation of Nuclear Weapons (UNODA, no date);
10. Treaty on the Prohibition of Nuclear Weapons (International Committee of the Red Cross, no date);
11. Treaty on the Prohibition of the Emplacement of Nuclear Weapons and Other Weapons of Mass Destruction on the Sea-Bed and the Ocean Floor and in the Subsoil Thereof (UN, 1974); and
12. Treaty on the Southeast Asia Nuclear Weapon-Free Zone (Association of Southeast Asian Nations, 2012).

5.2 Develop Structuring Dimensions

Structuring dimensions were derived by exploring the analysis question “What generic arms control elements can be discerned by reviewing arms control regimes and instruments of international humanitarian law?”. This main question comprised of the following sub-questions:

- What are the key generic mechanisms utilised in the arms control regimes and instruments of international humanitarian law? Arms control regimes typically have one or more key functions, for example limitation of type and use, prohibition on proliferation, complete disarmament and so forth. This sub-question therefore aims to extract the generic mandates and limitation on state behaviour for further analysis;
- What are the general verification mechanisms? Depending on the nature of arms control regime that will be suitable for cyberspace, the means of verifying compliance will be equally important given the nature of cyberweapons. The aim of this sub-question is therefore to ascertain the means of verification utilised for subsequent classification into detailed categories;
- How are violations determined and managed generically? Given the anonymous nature of cyberspace, attributing violations and managing them successfully will be critical for the success of an arms control regime in cyberspace. The aim of this sub-question is to ascertain methods agreed upon in contemporary arms control legal instruments to adequately identify and manage violations;
- To what extent are governing, implementing and verification organisations utilised? Some treaties have an administrative organisation that manages the arms control work of the treaty. The aim of this sub-question is to ascertain the generic elements of those as a cyberweapons convention may require a central organisation to facilitate its work, especially given the multiplicity of actors involved in cyberspace; and

- To what extent are non-state actors involved in the arms control regime and what are their roles if applicable? Given the nature of cyberspace, non-state actors, including private corporations, may have a significant role in achieving the objectives of arms control in cyberspace. The aim of this sub-question is therefore to identify the generic roles that non-state actors may have been assigned to in previous arms control regimes.

Note that due to the research limitations identified in Chapter Four, no specific coding scheme and category definitions were identified beforehand. This therefore required a more inductive approach to be followed in order to arrive at the categories and scoring rubrics. These are presented in the next section.

5.3 Define Categories and Scoring Rubric

The categories, which will represent the generic elements for the maturity model to assess feasibility for a cyberweapons Convention, are as follows:

1. Primary Objectives (PO);
2. Type of Limitation on state Behaviour and other Requirements (TLSBR);
3. Compliance and Verification Mechanisms (CVM);
4. Violation Resolution Mechanisms (VRM);
5. Governing, Verification and Implementation Organisation (GVIO); and
6. Involvement of Non-state Actors (INSA).

Each category will be composed of sub-elements that will be arrived at in Section 5.4 below. The maturity indicators for the maturity model will be comprised of the following four levels:

1. Unfeasible: The sub-element is not feasible for a cyberweapons convention;
2. Unlikely: The sub-element is unlikely to be suitable for a cyberweapons convention, it may however become suitable should exogenous factors change;

3. Likely: The sub-element is likely to be feasible for a cyberweapons convention, which could be characterised by its acceptance by some state and non-state actors; and
4. Feasible: The sub-element is feasible for a cyberweapons convention.

Each sub-element will be judgementally assessed and scored during each round of tallying as follows:

1. Unfeasible: score of 0;
2. Unlikely: score of 1;
3. Likely: score of 2; and
4. Feasible: score of 3.

The overall maturity score for each sub-element will be arrived through division of the mean average score of each sub-element over the frequency of its occurrence for each round of scoring. This method was selected as most sub-elements could not be scored during the first round due to lack of broad based international agreements on rules pertaining to cyberwarfare. This technique therefore revises the maturity score higher for each sub-element that may already exists in LOAC and IHL.

5.4 Analyse Data

The data analysis began with ascertaining the PO of each unit of analysis, after which they were reviewed and classified according to the aforementioned structuring dimension. The PO of each unit of analysis was obtained from sources indicated in the list under Section 5.1 above and were determined as follows:

Table 6 - Primary Objective of the Units of Analysis

Unit of Analysis	Unit Code	PO
UN Security Council Resolution 1540	A	Prohibition on state support to non-state actors that seek to utilise nuclear, biological and chemical weapons as well as their delivery systems.
Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects	B	Seeks to prohibit certain weapons, while restricting others. Also reinforces the distinction principle in LOAC. Extends the Convention and associated protocols to non-international armed conflicts.
Geneva Conventions and Associated Protocols	C	Primary instrument of IHL. Prohibits cruel and degrading activities by participants engaged in conflict, and affords protection for wounded military personnel, medical professionals, civilians, prisoners of war, as well as civilian and cultural objects. It also sets minimum standards of behaviour and responsibility on all parties involved or neutral in a conflict.
Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict and its Two (1954 and 1999) Protocols	D	Focuses on the protection of cultural property and associated infrastructure during an arms conflict.
International Convention for the Suppression of Acts of Nuclear Terrorism	E	Renders nuclear terrorism, including attacks on nuclear facilities, as a criminal act and promotes judicial and law enforcement cooperation to impede, investigate and prosecute criminal acts.
The Arms Trade Treaty	F	Seeks to regulate international trade in arms, limited to conventional weapons, through establishment of national control systems to regulate export of armaments as well as provide arms trade information to the secretariat of the Treaty.

Unit of Analysis	Unit Code	PO
The Biological and Toxin Weapons Convention	G	Prohibits non-peaceful development, production and use of biological agents. It furthermore requires complete destruction, or transformation to peaceful purposes, of existing biological weapons.
The Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction	H	Prohibits development, production and use of chemical weapons. It also requires complete destruction of chemical weapons, which needs to take place under the verification of its Secretariat.
The Treaty on the Non-Proliferation of Nuclear Weapons	I	Restricts the number of nuclear weapon States, requiring those States to not transfer nuclear weapons, as well as technical know-how, to other States. Encourages pursuit of peaceful nuclear development. Mandates striving towards eventual disarmament of nuclear weapons by nations possessing them.
Treaty on the Prohibition of Nuclear Weapons	J	Prohibits development of nuclear weapons as well as their placement, on territory controlled by the state Party. Requires state Parties that possess nuclear weapons to begin process of disarming and destroying those weapons.
Treaty on the Prohibition of the Emplacement of Nuclear Weapons and Other Weapons of Mass Destruction on the Sea-Bed and the Ocean Floor and in the Subsoil Thereof	K	Prohibits placement of weapons of mass destruction on the sea-bed and subsoil, beyond a 12 mile territorial zone. The prohibition includes structures for storing, testing and using such weapons.
Treaty on the Southeast Asia Nuclear Weapon-Free Zone	L	Prohibits the acquiring, development, manufacturing, testing, transporting and employment of nuclear weapons inside or outside the geographical zone agreed to by the state Parties.

Table 7 below presents the results of the data analysis, grouped by categories as defined in Section 5.3:[36]

Table 7 - Data Analysis Results

Arms Control Element	A	B	C	D	E	F	G	H	I	J	K	L
Type of Limitation on State Behaviour and other Requirements												
Prohibit state support to NSA regarding WMD's.	X											
States required to introduce domestic legislation in line with PO	X	X	X	X	X	X	X	X		X		
Forbids transfer of weapons to prohibited entities	X	X				X	X					
Distinction must be made between civilians and combatants		X	X									
Prohibit weapons that inflict excessive injury or suffering on combatants or render their death inevitable		X										
Only permits weapons that self-destruct, self-neutralise or self-deactivate after a period of time		X										
All feasible precautions need to be taken to protect civilians from the effects of weapons concerned		X										
Full disclosure of equipment, material, scientific and technological information of the weapon if required for clearance purposes.		X										
Prohibit use or targeting of cultural artefacts and associated infrastructure, with additional protection afforded to 'Cultural Property Under Enhanced Protection'				X								
Mandates cooperation between States through exchange of information and judicial coordination					X	X		X				
Places record keeping requirements on armament transfers						X						
Requires the establishment of a national point of contact						X						
Prohibits development, production, stockpile and retention of biological agents that have no peaceful purposes, as well as weapon delivery systems							X					

[36] Note that only characteristics that were judged to be directly relevant to the scope of this paper are presented in Table 7

Arms Control Element	A	B	C	D	E	F	G	H	I	J	K	L
Requires destruction or diversion to peaceful purposes of existing biological weapons							X					
Prohibits development, production, stockpile and retention of chemical agents that have no peaceful purposes, as well as weapon delivery systems								X				
Requires destruction or diversion to peaceful purposes of existing chemical weapons								X				
Prohibits transfer of nuclear weapons, as well as related technical know-how to non-nuclear weapon States									X			X
Prohibits development, production, stockpiling and retention of nuclear weapons										X		X
Prohibits placement of nuclear weapons on territory controlled by the state Party										X		X
Requires destruction or diversion to peaceful purposes of existing nuclear weapons										X		
Prohibits emplacement of WMD's, as well as supporting infrastructure, on the sea-bed and its subsoil, beyond a 12-mile territorial limit											X	
Compliance and Verification Mechanisms												
Self-reporting mechanisms	X	X				X		X	X	X		X
Dependent on International Organisations for compliance and verification purposes			X	X								X
Provides for a Fact Finding Commission for States that have accepted its jurisdiction			X									X
Requires state intervention on violations committed in its territory					X	X						
Secretariat has power to verify compliance to treaty through regular, random and challenge inspections								X	X			
Verification through observation by state Parties, with additional procedures agreed upon between parties if required											X	
Violation Resolution Mechanisms												
Consultation through the UN or other international procedures to resolve disputes. May include UNSC Chapter VII referral.	X	X							X		X	

Arms Control Element	A	B	C	D	E	F	G	H	I	J	K	L
Violations can be resolved by an international court or through United Nations mechanism, such as International Tribunals			X	X								
Violations are treated as war crimes, which permit the possibility of individuals being investigated and prosecuted.			X									
Bi-lateral dispute mechanism, with option for international arbitration or referral to the International Court of Justice					X	X				X		X
state party is required to lodge a complaint with the UNSC if it finds another state party to be in violation of the Convention. Violations to be investigated by the UNSC.							X					
Organisational dispute mechanism, with option to refer to International Court of Justice, suspend membership, enact sanctions and/or refer matter UNGA and UNSC.								X				X
Governing, Verification and Implementation Organisation												
Adhoc Committee of the UNSC	X											
Full time Secretariat, under auspices of the UN - Office for Disarmament Affairs		X										
Full time Secretariat, under auspices of the UN - UNESCO				X								
Full time Secretariat, under auspices of the ICRC			X									
Full time Inter Governmental Secretariat						X		X	X			X
Full time Implementation Support Unit under auspices of the UN - Office for Disarmament Affairs							X					
Involvement of Non-State Actors												
Incorporation of significant mechanisms to protect confidentiality of information arising from the private sector.								X				
Involvement of the private sector in the negotiations								X				

Table 7 highlights the similarities, as well as divergences, across the units of analysis. Given their heterogeneous nature and extent of scope, the diverse outcome is to be expected. While some legal texts focused on elimination and non-proliferation, others limited the types of permissible targets. The majority of arms control treaties analysed required state Parties to enact domestic legislation supporting the objectives of the treaty. Furthermore, self-reporting mechanisms were greatly favoured, although some verification mechanisms were agreed upon between state Parties, particularly those related to WMDs. Dispute resolution mechanisms also varied according to the extent of agreements. Some treaties benefited from organisational structures, while others were not required to create one due to being pure instruments of public international law. Only one treaty appeared to have significant non-state actor involvement from a negotiation perspective. For the purposes of the paper, the results obtained in Table 7 were narrowed towards those generic arms control elements that could be applicable to arms control for cyberweapons, irrespective of their degree of feasibility.

5.5 Map Findings Into Structure

Maintaining the grouping structure from the previous section, the potential elements for a cyberweapons convention, as derived from the results of the data analysis, are as follows:

- Type of Limitation on state Behaviour and other Requirements
    - Prohibits proliferation of cyberweapons, as well as related technical knowhow, to state and Non-state entities
    - Prohibition on employment of cyberweapons outside specific geographic zones
    - Prohibition on placing, transferring and using cyberweapons on specific layers as well as zones of the Internet
    - Prohibition on attacks against personnel, physical and information infrastructures of Computer Emergency Response Teams (CERT) of state Parties
    - Prohibition on attacks against Critical Infrastructure (CI) and Critical Internet Infrastructure (CII)
    - Criminalisation of prohibited activities in domestic laws and penal codes

    - Mandates the creation of national points of contact and agreement to establish direct communication channels during times of tension and conflict
    - Permits cyberweapons that self-neutralise after a period of time
    - Protection of civilian population from effects of cyberweapons remains paramount
    - Requires full disclosure of cyberweapons, means of reversal and other technical information, if cyberweapons was used erroneously or in contravention of the Convention or International Humanitarian Law
    - States Parties are obliged to provide mitigation and judicial assistance, on request, to other state Parties, in the event of a cyber attack
    - Requires eventual disarmament of cyberweapons by state Parties
- Compliance and Verification Mechanisms
    - The Secretariat has the power to verify compliance to the Treaty through challenge inspections, where cases of non-compliance are brought to its attention by state Parties
- Violation Resolution Mechanisms
    - Multilateral dispute resolution mechanism, with option to refer case to International Court of Justice, the UNGA or the UNSC
- Governing, Verification and Implementation Organisation
    - Full time Secretariat, under auspices of the UN - Office for Disarmament Affairs
- Involvement of Non-State Actors
    - Participation of the private sector in negotiations for the Treaty, as well as including responsibility for security strengthening of their products and services

The aforementioned elements will be scored in the next chapter in order to ascertain feasibility for a binding international agreement on cyberweapons through a maturity model structure.

“If you do something for long enough, the world will accept it. The whole of international law is now based on the notion that an act that is forbidden today becomes permissible if executed by enough countries… After we bombed the reactor in Iraq, the Security Council condemned Israel and claimed the attack was a violation of international law… Today everyone says it was preventive self-defense. International law progresses through violations”.

Colonel (res.) Daniel Reisner, Former Head of International Law Division, Military Advocate’s General Office, Israeli Defence Force
(Feldman & Blau, 2009)

6. Arms Control over Cyberweapons - The Feasibility Maturity Model

Kohlegger *et al.* (2009, pg. 59), in their analysis of 16 maturity models, advanced the following definition for maturity models: “A maturity model conceptually represents phases of increasing quantitative or qualitative capability changes of a maturing element in order to assess its advances with respect to defined focus areas”. The intention of applying maturity models to assess feasibility of a cyberweapons convention is precisely to assess progress towards those elements that it could be composed of. As discussed in the methodology chapter, the maturity model was scored thrice, with the first round taking into consideration existing LOAC, public international law and international disarmament frameworks. The second round considered emerging norms and other diplomatic instruments. During the final round, scores were allocated based on national security considerations, as well as emerging state practice, of States judged critical to the cyberweapons convention. The results of the scoring are as follows:

Table 8 - Maturity Model with Scored Rubric

	Round 1				Round 2				Round 3			
Arms Control Element	**Unfeasible**	**Unlikely**	**Likely**	**Feasible**	**Unfeasible**	**Unlikely**	**Likely**	**Feasible**	**Unfeasible**	**Unlikely**	**Likely**	**Feasible**
TLSBR												
Prohibits proliferation of cyberweapons, as well as related technical knowhow, to state and Non-state entities							2		0			
Prohibition on employment of cyberweapons outside specific geographic zones						1			0			
Prohibition on placing, transferring and using cyberweapons on specific layers as well as zones of the Internet								3		1		
Prohibition on attacks against personnel, physical and information infrastructures of Computer Emergency Response Teams (CERT) of state Parties								3			2	
Prohibition on attacks against Critical Infrastructure (CI) and Critical Internet Infrastructure (CII)								3		2		
Criminalisation of prohibited activities in domestic laws and penal codes								3				3
Mandates the creation of national points of contact and agreement to establish direct communication channels during times of tension and conflict								3				3
Permits cyberweapons that self-neutralise after a period of time						1				1		
Protection of civilian population from effects of cyberweapons remains paramount				3				3				3
Requires full disclosure of cyberweapons, means of reversal and other technical information, if the cyberweapon was used erroneously or in violation of the Convention or International Humanitarian Law							2				2	
States Parties are obliged to provide mitigation and judicial assistance, on request, to other state Parties, in the event of a cyber attack								3				3
Requires eventual disarmament of cyberweapons by state Parties						1			0			
CVM												
The Secretariat has the power to verify compliance to the Treaty through challenge inspections, where cases of non-compliance are brought to its attention by state Parties							2			1		
VRM												
Multilateral dispute resolution mechanism, with option to refer case to International Court of Justice, the UNGA or the UNSC							2				2	
GVIO												
Full time Secretariat, under auspices of the UN - Office for Disarmament Affairs								3				3
INSA												
Participation of the private sector in negotiations for the Treaty, as well as including responsibility for security strengthening of their products and services								3			2	

The results obtained in Table 8 provide an early indication of the level of feasibility for the elements of a cyberweapons convention. Table 9 below presents the elements according to the overall score derived according to the formula presented in Section 5.3:

Table 9 - Maturity Levels Indicating the Feasibility of the Core Elements for a Cyberweapons Convention, Ranked by Level of Feasibility

Arms Control Element	Score	Feasibility Level
Criminalisation of prohibited activities in domestic laws and penal codes	3	Feasible
Mandates the creation of national points of contact and agreement to establish direct communication channels during times of tension	3	Feasible
Protection of civilian population from effects of cyberweapons remains paramount	3	Feasible
States Parties are obliged to provide mitigation and judicial assistance, on request, to other state Parties, in the event of a cyber attack	3	Feasible
Full time Secretariat, under auspices of the UN - Office for Disarmament Affairs	3	Feasible
Prohibition on attacks against personnel, physical and information infrastructures of Computer Emergency Response Teams of state Parties	2.5	Possibly Feasible
Prohibition on attacks against Critical Infrastructure and Critical Internet Infrastructure	2.5	Possibly Feasible
Prohibition on placing, transferring and using cyberweapons on specific layers as well as zones of the Internet	2	Likely
Requires full disclosure of cyberweapons, means of reversal and other technical information, if the cyberweapon was used erroneously or in contravention of the Convention or International Humanitarian Law	2	Likely
Multilateral dispute resolution mechanism, with option to refer case to International Court of Justice, the UNGA or the UNSC	2	Likely
Participation of the private sector in negotiations for the Treaty, as well as including responsibility for security strengthening of their products and services	2	Likely
The Secretariat has the power to verify compliance to the Treaty through challenge inspections, where cases of non-compliance are brought to its attention by state Parties	1.5	Possibly Unlikely
Prohibits proliferation of cyberweapons, as well as related technical knowhow, to state and Non-state entities	1	Unlikely

Arms Control Element	Score	Feasibility Level
Permits cyberweapons that self-neutralise after a period of time	1	Unlikely
Prohibition on employment of cyberweapons outside specific geographic zones	0.5	Highly Unlikely
Requires eventual disarmament of cyberweapons by state Parties	0.5	Highly Unlikely

Figure 2 below indicates the feasibility distribution of the 16 elements derived for the research:

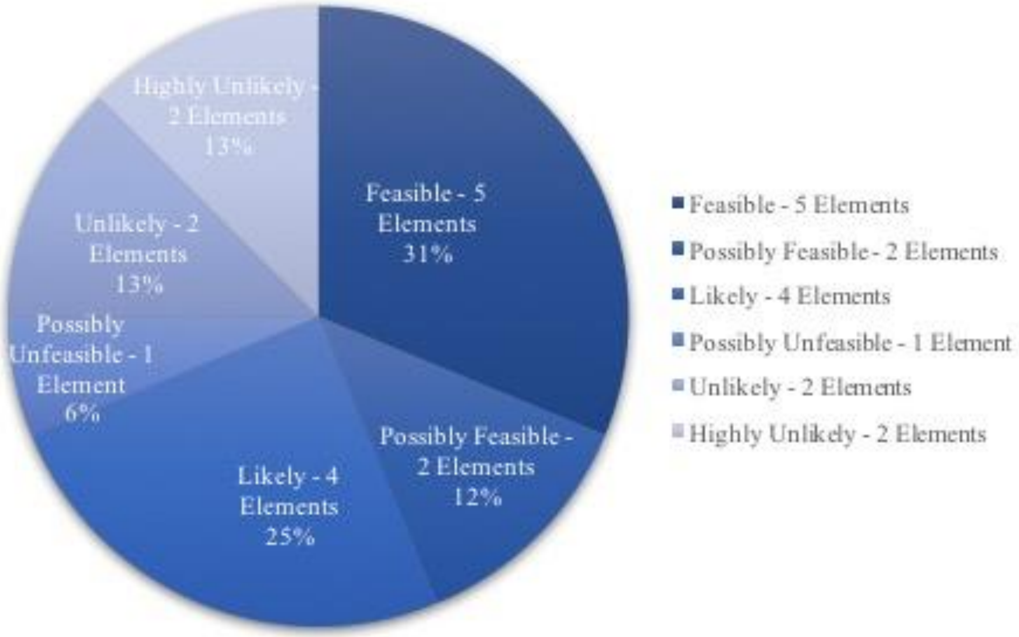

Figure 2 - Feasibility Distribution of Core Elements of a Cyberweapons Convention

This outcome, taking into consideration the three objectives of the study, firstly indicate that while matters related to cyberwarfare have not yet fallen under the purview of an international agreement, generic core mechanisms of such a treaty can be grafted from other arms control regimes.

Tackling the second objective, the maturity model added the feasibility dimension to those generic core elements through its assessment. Given that the majority of the elements reviewed fell under TLSBR, the greatest divergence of results was naturally found in that grouping.

While the GVIO grouping appears to be feasible, elements found within VRM and INSA are noted as likely. The CVM grouping was scored as unlikely. Crucially, no grouping and element were found to be unfeasible.

The implications of these results, together with the third objective of the study, that of development of practical recommendations towards realisation of the cyberwarfare convention, will be discussed in the next Chapter.

“The place where I think it will be most helpful to senior policymakers is what I call in ‘the space between’. What is the space between? … You have diplomacy, economic sanctions…and then you have military action. In between there’s this space, right? In cyber, there are a lot of things that you can do in that space between that can help us accomplish the national interest.”

Eric Rosenbach, United States Assistant Secretary of Defence
(Cited in Maurer, 2014)

7. Discussion

As detailed in the previous chapter, a significant portion of the generic core elements of a cyberweapons convention, which emerged from the data analysis, fell into feasible and likely levels. A minority however were classified into the unlikely grouping. This chapter aims to interpret those results, as well as general implications drawn from the research, towards the potential realisation of such a convention. The chapter will begin by highlighting the pertinent outcomes from the paper, which will be followed by practical recommendations towards addressing the key challenges that emerged from the findings. The chapter will then conclude by shedding light on areas for further research that emanated from this study.

7.1 Implications

The first key implication of the study was the high number of feasible and likely elements that emerged in favour of a cyberweapons convention, a result that was further amplified through increasing harmony between various norm creating institutions on their proposals for appropriate state behaviour. The Global Commission on the Stability of cyberspace for example, in November 2018, launched the following six norms (GCSC, 2018):

- “Norm to Avoid Tampering;

- Norm Against Commandeering of ICT Devices into Botnets;
- Norm for States to Create a Vulnerability Equities Process;
- Norm to Reduce and Mitigate Significant Vulnerabilities;
- Norm on Basic Cyber Hygiene as Foundational Defense; and
- Norm Against Offensive Cyber Operations by Non-state Actors".

Another norm actor, the ICT4Peace Foundation, proposed a mechanism for addressing the attribution challenge in cyberspace in December 2018 (ICT4Peace Foundation, 2018). At a more regional level, the Association of Southeast Asian Nations (ASEAN), European Union (EU), Organization of American States (OAS), Organization for Security and Co-operation in Europe (OSCE), Shanghai Cooperation Organisation (SCO) and other regional organisations have developed and are socialising their own sets of standards of responsible state behaviour in cyberspace (Radunović, 2017). While some of the norms converge, others do not, leading to what Meyer (2018, pg. 3) has termed "something of a proliferation of recommended sets of norms which may make it more difficult to gain support from states for implementing any of them". Additionally, while this trend may satisfy the formative elements of responsible state behaviour in cyberspace, the norms espoused in contemporary times lack the technical details that go hand in hand with the complex nature of cyberspace. Furthermore, taking into consideration the norm lifecycle model of Finnemore and Sikkink (1998), it appears likely that the debate is currently in the norm emergence phase. The results of this paper could therefore be utilised as a basis in bringing together competing interests and norms, thus transitioning the norm development process from a profusion of ideas towards international institutionalisation.

The second important implication of the research relates to the sharp asymmetry between the extent of norms that were revealed versus the universality of the norm processes for the subject under study. It appears that state practice on norm creation, socialisation and institutionalisation is more focused on specific calls for norms, often appearing as a collective call of norms echoed by like-minded nations. The pervasive nature of cyberspace requires traditional adversaries to arrive at common positions and thus a supporting mechanism that works to nurture an inclusive and internationally representative norm creating process appears to be lacking, with the possible exception of the UN Groups of Government Experts (GGE) process. This issue is further exacerbated by lack of domestic and transnational pressure from civil society organisations.

Connected with the second implication, the third critical ramification of the paper is the lack of international consensus on responsible state behaviour in cyberspace. Furthermore, no clear alignment of interests, and willingness, amongst nations with offensive cyber capabilities exists to curtail the proliferation of cyberweapons. The UN GGE, as the only international fora that is mandated to pursue this issue, has mutated into hitherto uncharted territory. In the latest session of the First Committee of the UN, two GGE's emerged, one led by Russian Federation and the other by the United States, with the UN acknowledging that both will seek to further the work of previous GGE's on developing "Rules for States on Responsible cyberspace Conduct" (UN, 2018).

The creation of a dual GGE process indicates a bifurcation of what those standards could be. Mechanisms that help bind competing interests, and converge those towards an agreement, are more urgently required, especially given the unravelling of a number of international treaties and agreements since the ascension of the Trump administration in the United States of America. The practical recommendations in the next section seek to equip the work of diplomatic officials, as well as non-governmental and private sector practitioners, to redress the situation towards reducing negative bargaining zones and increasing zones of possible agreement.

7.2 Practical Recommendations

The research revealed five generic elements of a cyberwarfare convention that were categorised outside of the likely and feasible range. Table 10 below seeks to provide practical recommendations for each one in order to increase its level of maturity:

Table 10 - Practical Recommendations for Cyberwarfare Convention Elements that Require Further Maturity

Element	Scoring and Classification	Practical Recommendation
The Secretariat has the power to verify compliance to the Treaty through challenge inspections, where cases of non-compliance are brought to its attention by state Parties	1.5 Possibly Unlikely	The challenging aspect of this element relates to the ability to perform inspections on cyberwarfare facilities of a state party, given that these can be hidden from sight. Faced with a similar challenge in other arms control mechanisms, negotiations sought to mandate the marking of weapons, indicating country of manufacture and serial number to enable identification. A similar approach can be suggested for cyberweapons, whereby origin information is embedded into the code of the weapon. This may also facilitate clearer attribution if used. An employed cyberweapon that is found to contravene such a provision will be submitted for international investigation by a Treaty body in order to assign attribution and direct the subsequent violation resolution mechanisms.

Element	Scoring and Classification	Practical Recommendation
Prohibits proliferation of cyberweapons, as well as related technical knowhow, to state and Non-state entities	1 Unlikely	Although it is in the interest of States to limit proliferation to Non-state entities, especially due to the risk of terrorism, dissemination of cyberweapons to other States will be difficult to get agreement on due to existing military collaborations for offensive and defensive cyberweapons. The Treaty may therefore be drawn up to delineate defensive and offensive cyberweapons, and to subsequently permit cooperation on the former, while prohibiting the latter.
Permits cyberweapons that self-neutralise after a period of time	1 Unlikely	While achieving this element at a technical level is possible, the political will to agree to specific time periods is lacking. A possible option, akin to the other arms control agreements, is to sub-classify cyberweapons, for example based on a specific layer of Internet at which it is deployed, and require those to self-neutralise after a period of time. This can both reduce inadvertent cyber attacks, as well as act as a confidence building measure.
Prohibition on employment of cyberweapons outside specific geographic zones	0.5 Highly Unlikely	While this element was rated as highly unlikely, it may prove opportune for regions that are witnessing sustained periods of peace to enshrine additional prohibitions on weapons employment.
Requires eventual disarmament of cyberweapons by state Parties	0.5 Highly Unlikely	Although this element may be agreed by state parties for inclusion in an international arms control agreement, its probability of success is very slim. Similarly, the Treaty on the Non-Proliferation of Nuclear Weapons includes an article that calls for eventual disarmament, a mandate that has had very little traction towards its fulfilment.

Apart from the aforementioned recommendations, which are aimed towards an international arms control agreement, the following practical actions address other pertinent challenges that were revealed through the research:

- Extending current arms control regimes to prohibit employment of cyberweapons at targets and facilities that fall under the purview of those international legal instrument. The Treaty on the Non-Proliferation of Nuclear Weapons for example can be amended to prohibit cyber attacks against declared Nuclear facilities;
- Laying the groundwork for the GGE process to increase its formality and reach, as the negotiation capacity of the GGE is limited due to their status as advisors to the UN Secretary General (Nye, 2018). A natural transition for example may be to introduce disarmament negotiations for cyberspace as part of the work program of the Conference on Disarmament; and
- Formalising common practices amongst states, at the very least on a technical level, in order to expand collaboration across both likeminded and adversarial nations on issues related to cyberspace. While the commercial world already enjoys integrated practices across borders, academia and non-governmental organisations should also increase their cooperation, in order to broaden the possibilities of an international agreement.

7.3 Areas of Further Research

Cyberspace, with a cornucopia of applications, is a broad area of study. During the research phase of this paper, as well the research limitations that subsequently emerged, additional avenues of further research were revealed. These include:

- Utilising the regional organisations as the unit of analysis, seeking to incorporate the official and future positions of those institutions in ascertaining both arms control elements for cyberspace as well as potential feasibility of each;

- Comparative case-study approach that takes into consideration the positioning of certain countries on the topic, including traditional adversaries;
- Incorporating into the generic element lists contemporary norms called for by multilateral organisations, countries, civil society and the private sector; and
- Adopting an Action Research approach, possibly within the UN GGE process or through a regional organisation.

With these areas of further investigation in mind, the next Chapter will formally conclude the paper, by providing a summary of the pertinent points arrived at during the research.

“State and non-state actors increasingly exploit the Internet to achieve strategic objectives, while many governments—shaken by the role the Internet has played in political instability and regime change—seek to increase their control over content in cyberspace. The growing use of cyber capabilities to achieve strategic goals is also outpacing the development of a shared understanding of norms of behaviour, increasing the chances for miscalculations and misunderstandings that could lead to unintended escalation.”

James Clapper, Former United States Director of National Intelligence (Office of the Director of National Intelligence, 2013)

8. Conclusion

Cyberweapons enjoy relatively low costs, benefit from a high degree of plausible deniability, have reduced domestic political costs, can be successfully used at a level below threshold of war and provide asymmetric capabilities to its operator. The primary disadvantages of cyberweapons however are their limited shelf lives, uncertain attack outcomes and potential risk of blow back. The impact of the latter being commensurate with the level of network infrastructure and social dependency on stable functioning of the Internet based systems. As a consequence of these factors, the emerging modus operandi of States has been to expand offensive and defensive cyber capabilities, with proliferation occurring at a rapid pace.

In response, this dissertation aimed to serve as a bridge between the disciplines of cyberwarfare and arms control, espoused through the following research objectives:

- To determine the landscape of international agreements that partially or completely address matters relating to cyberwarfare, taking into account stages of norm building when applied to emerging technology weapons;

- To construct a maturity model that takes into consideration the viability of an international legal instrument on cyberweapons through an assessment of its critical components; and
- Taking into consideration the outcomes of the maturity model, develop practical recommendations in bridging negative bargaining zones and expanding zones of possible agreement for an eventual international legal instrument on cyberweapons.

With regards to the first objective, the research revealed that while LOAC and IHL apply, in principle, to conflicts in cyberspace, no international legal instrument explicitly states this. This gap in international law appears, for now, to be useful for states with significant military capability in cyberspace, which goes hand in hand with the ambiguous capabilities of cyberweapons. This equation changes slightly when taking into consideration the increasing number of norm statements and other non-binding calls for responsible state behaviour in cyberspace. While this increasing diversity may hamper reaching an international agreement on the matter, the existence of such debate indicates that the issue is in the midst of the first of three phases of norm development in international affairs.

Turning to the second objective, the paper devised a four-stage maturity model, which measured the feasibility of an international agreement for arms control over cyberweapons through three rounds of scoring. The generic elements for the maturity model were based on an analysis of twelve contemporary arms control agreements. The results suggested a substantial number of those elements which are feasible and likely for an international legal instrument over cyberweapons. A summary of the most pertinent are:

- Prohibition on attacks against personnel, physical and information infrastructures of Computer Emergency Response Teams;

- Prohibition on placement, transfer and use of cyberweapons on specific layers as well as zones of the Internet;
- Requires full disclosure of cyberweapons, means of reversal and other technical information, if the cyberweapon was used erroneously or in contravention of the Convention or International Humanitarian Law;
- Creation of national points of contact and agreement to establish direct communication channels during times of tension; and
- Creation of a full-time secretariat under the auspices of the UN.

The third objective advanced the results of the maturity model into practical recommendations for the majority of elements that were not scored as feasible nor as likely, such as:

- Recommending a mechanism to embed origin information into code of cyberweapons, analogous to certain contemporary arms control mechanisms to assist inspections and facilitate resolution of attribution;
- Reducing proliferation of offensive cyberweapons through permitting cooperation on defensive tools, while prohibiting offensive ones; and
- Enhancing confidence between states, as well as reducing risk of unintended deployment of cyberweapons, through permitting cyberweapons that self-neutralise after a period of time, a model that has been successfully agreed to by States on certain mine based weapons.

These practical recommendations were largely based on existing arms control regimes in order to equip negotiators towards arriving at an agreement. As the research limitations section in Chapter 4 eluded to however, the 16 elements derived and analysed in this paper are not a complete representation of potential constituent parts of an arms control agreement, thus requiring further research.

Barriers to arms control in cyberspace certainly exist, given the dual-use capabilities of cyber tools, technical difficulties in arriving at accurate attribution and verification mechanisms and lack of international consensus and political willingness to mandate arms control in cyberspace. On the other hand, a binding agreement between states can reduce risks of unintended consequences, clarify state responsibilities and obligation and facilitate communication between adversaries in times of crisis. Additional economic benefits, as well as greater judicial cooperation, may also arise. The conceptual framework around this research, which took on a blend of critical-realism, pragmatism and constructivism, as well as the latest trends related to normative infrastructure on the topic at hand, indicate that norms are still in the emergent phase. This implies that institutionalisation of these norms, and their potential subsequent transformation into international law, is distant.

Norm development in this arena also requires the involvement of the private sector, given that sector's ownership and operating control over pertinent internet infrastructure. The aforementioned multiplicity of actors therefore requires a stronger degree of cooperation amongst all, while reducing use of coercive means towards inducing collaboration. Extending contemporary arms control regimes to limit the use of cyberweapons at targets and facilities that fall under its scope, transitioning the work of the UN GGE towards the purview of the Conference on Disarmament and expanding technical collaboration between adversarial nations can accelerate the momentum on arms control in cyberspace towards institutionalisation.

International collaboration in this arena, with strong presence of global and regional leaders, can reinforce cooperation and right relations in cyberspace between states. The pages of history vividly illustrate the progression of human kind, with headway in weaponry being followed by advances in arms control. It is hoped that humanity, in this instance, does not await a major outbreak of cyberwarfare in order to subsequently agree on limitations of its use.

9. References

1. Ablon L (2017) RAND Study Examines 200 Real-World ‘Zero-Day’ Software Vulnerabilities. *RAND Corporation.* Available at: https://www.rand.org/news/press/2017/03/09.html [Accessed: 10 June 2018].
2. Acton J (2017) cyber Weapons and Precision-Guided Munitions. In Perkovich G and Levite A [Eds.] *Understanding cyber Conflict: 14 Analogies*. Washington D.C. : Georgetown University Press
3. Advisory Council on International Affairs (2011) *cyber Warfare*. Available at: https://aiv-advice.nl/6ct/publications/advisory-reports/cyber-warfare [Accessed: 20 February 2018].
4. Anderson K (2016) Why the Hurry to Regulate Autonomous Weapon Systems - But Not cyber-Weapons. *Temple International and Comparative Law Journal*, (30), pp. 17-41.
5. Andres R (2014) Inverted-Militarized-Diplomacy: How States Bargain with cyber Weapons. *Georgetown Journal of International Affairs, International Engagement on cyber IV*, pp. 119-129.
6. Arimatsu L (2012) *A treaty for governing cyber-weapons: Potential benefits and practical limitations*. Proceedings of the 2012 International Conference on cyber Conflict, North Atlantic Treaty Organisation Cooperative cyber Defence Centre of Excellence, 5-8 June 2012. Tallinn: North Atlantic Treaty Organisation Cooperative cyber Defence Centre of Excellence.
7. Arms Trade Treaty (no date) *Treaty Text*. Available at: https://thearmstradetreaty.org/treaty-text.html [Accessed: 10 October 2018].
8. Arquilla J and Ronfeldt D (1993) Cyberwar is Coming!. *Comparative Strategy*, 12(2), pp. 141-165.
9. Arquilla J (2012) Cyberwar is Already Upon Us. *Rational Security* Blog, 27 February 2012. Available at: http://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/ [Accessed: 25 April 2018].
10. Association of Southeast Asian Nations (2012) *Treaty on the Southeast Asia Nuclear Weapon-Free Zone*. Available at: https://asean.org/?static_post=treaty-on-the-southeast-asia-nuclear-weapon-free-zone [Accessed: 10 October 2018].
11. Association of Southeast Asian Nations (2014) *ASEAN’s cyber Confidence Building Measures.* Available at: http://www.unidir.ch/files/conferences/pdfs/the-asean-s-cyber-confidence-building-measures-en-1-958.pdf [Accessed: 25 April 2018].
12. Australian Department of Defence (no date) *Information Warfare Division.* Available at: http://www.defence.gov.au/jcg/iwd.asp [Accessed: 25 April 2018].
13. Bailes A *et al* (2014) *The Future of Arms Control*. Berlin: Heinrich Böll Foundation.

14. Blank S (2017) cyber War and Information War à la Russe. In Perkovich G and Levite A [Eds.] *Understanding cyber Conflict: 14 Analogies*. Washington D.C. : Georgetown University Press
15. Bocetta S (2017) Old Enemies, New Customers: Saudi, Israel, and the Strange World of cyber Warfare. *Gun News Daily.* Available at: https://gunnewsdaily.com/old-enemies-new-customers-saudi-israel-strange-world-cyber-warfare/ [Accessed: 27 April 2018].
16. Boothby W (2014) The Legal Challenges of New Technologies: An Overview. In Nasu H and McLaughlin R [eds] *New Technologies and the Law of Armed Conflict*. The Hague: T.M.C. Asser Press, pp. 21-28.
17. Boulanin V and Verbruggen M (2017) *Article 36 reviews: Dealing with the challenges posed by emerging technologies* Stockholm: Stockholm International Peace Research Institute. Available at: https://www.sipri.org/publications/2017/other-publications/article-36-reviews-dealing-challenges-posed-emerging-technologies [Accessed: 15 April 2018].
18. Boutilier A (2017) Canada Developing Arsenal of cyber-weapons. *The Star.* Available at: https://www.thestar.com/news/canada/2017/03/16/canada-developing-arsenal-of-cyber-weapons.html [Accessed: 27 April 2018].
19. Brenner S (2007) At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare. *Journal of Criminal Law and Criminology*, 97(2), pp. 379-475.
20. Bryant, A. & Charmaz, K. (2010). *The SAGE Handbook of Grounded Theory: Paperback Edition.* London: Sage Publishing
21. Buchanan B (2016) The Dangerous Diffusion of cyber Operations. *War on the Rocks* Blog, 29 February 2016. Available at: https://warontherocks.com/2016/02/the-dangerous-diffusion-of-cyber-operations/ [Accessed: 25 April 2018].
22. Carman D (2002) Translation and Analysis of the Doctrine of Information Security of the Russian Federation: Mass Media and the Politics of Identity. *Pacific Rim Law Policy Journal*, 11(2), pp. 339-370.
23. Clark R (2009) War from cyberspace. *The National Interest*, 104, pp. 31-36.
24. Creswell J (2009) *Research Design: Qualitative, Quantitative and Mixed Methods Approaches* – Third edition. London: Sage Publishing
25. Croft S (1996) *Strategies of Arms Control: A History and Typology*. Manchester: Manchester University Press.
26. Demchak C (2014) Forward. In Kremer J and Müller B [Eds.] cyberspace and International Relations. Berlin: Springer.
27. Denning E (2001) Obstacles and Options for cyber Arms Control. *Arms Control in cyberspace* Conference Proceedings, Heinrich Boll Foundation. Available at: http://faculty.nps.edu/dedennin/publications/Berlin.pdf [Accessed: 10 April 2018].
28. Denning E (2005) cyber Attack Attribution: Issues and Challenges. *cyber Conflict Studies Association Presentation.* Available at: http://www.cyberconflict.org/attributionworkshop.asp [Accessed: 20 May 2018].

29. Diab K (2008) *Natural Born Killers* The Guardian. Available at: https://www.theguardian.com/commentisfree/2008/nov/22/genetics-evolution [Accessed: 15 April 2018].
30. Dittrich P and Boening B (2017) More Security in cyber Space: The Case for Arms Control. *Security Policy Working Paper*, No. 9/2017. Available at: https://www.baks.bund.de/sites/baks010/files/working_paper_2017_09.pdf [Accessed: 15 June 2018].
31. Droubi S (2017) Institutionalisation of Emerging Norms of Customary International Law through Resolutions and Operational Activities of the Political and Subsidiary Organs of the United Nations. *International Organizations Law Review*, 14(2), pp. 254-290.
32. Feldman Y and Blau U (2009) Consent and Advise. *Haaretz*. Available at: https://www.haaretz.com/1.5069101 [Accessed: 18 October 2018].
33. Filstead W (1979) Qualitative Methods: A Needed Perspective in Evaluation Research. In T. D. Cook & C. S. Reichardt (eds.), *Qualitative and quantitative methods in evaluation research*. Beverly Hills, CA: Sage, pp. 38-48.
34. Finnemore M and Sikkink K (1998) International Norm Dynamics and Political Change. *International Organization*, 52(4), pp. 887-917.
35. Finnemore M and Hollis D (2016) Constructing Norms for Global cybersecurity . *The American Journal of International Law*, 110(3), pp. 425-479.
36. Florini A (1996) The Evolution of International Norms. *International Studies Quarterly*, 40(3), pp. 363-389.
37. Ford C (2010) The Trouble with cyber Arms Control. *The New Atlantis*, 29, pp. 52-67.
38. Fry J (2006) Contextualized legal reviews for the methods and means of warfare: Cave Combat and International Humanitarian Law. *Columbia Journal of Transnational Law*, 44(2), pp. 453-519.
39. Ghani A *et al* (2005) Closing the Sovereignty Gap: An Approach to state-Building (Working Paper 253). London: Overseas Development Institute
40. Glaser B (1992) *Basics of Grounded Theory Analysis: Emergence vs Forcing.* Mill Valley, Ca.: Sociology Press
41. Global Commission on the Stability of cyberspace [GCSC] (2018) *Global Commission Introduces Six Critical Norms Towards cyber Stability*. Available at: https://cyberstability.org/news/global-commission-introduces-six-critical-norms-towards-cyber-stability/ [Accessed: 1 December 2018].
42. Godwin III J *et al* (Eds) (2014) *Critical Terminology Foundations 2.* Available at https://www.eastwest.ngo/idea/critical-terminology-foundations-2 [Accessed :20 April 2018].
43. Goel S and Hong Y (2015) CyberWar Games: Strategic Jostling Among Traditional Adversaries. In Jajodia S *et al* [Eds.] *cyber Warfare: Building the Scientific Foundation*. New York: Springer.
44. Goldstein P (2018) Intellectual Property and China: Is China Stealing American IP? *Legal Aggregate* blog, 10 April 2018. Available at: https://law.stanford.edu/2018/04/10/intellectual-property-china-china-stealing-american-ip/ [Accessed: 25 April 2018].

45. Gomez R (2013) The Changing Field of ICTD: Growth and Maturation of the Field, 2000-2010. *The Electronic Journal on Information Systems in Developing Countries*, 58 (1), pp. 1-21.
46. Goodin D (2015) How "Omnipotent" Hackers Tied to NSA Hid for 14 Years - and Were Found at Last. *Ars Technica.* Available at: https://arstechnica.com/information-technology/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/ [Accessed: 25 April 2018].
47. Grindal K and Healey J (2016) *cyber Conflict state of the Field Workshop Report.* Available at: http://www.cyberconflict.org/storage/SOTF_Review_Copy.pdf [Accessed: 25 May 2018].
48. Guba E and Lincoln Y (1994) Competing Paradigms in Qualitative Research. In Denzin N and Lincoln Y [Eds.] *Handbook of Qualitative Research*. Thousand Oaks, CA: Sage.
49. Gussarova A (2017) Kazakhstan Adopts New Military Doctrine. *Eurasia Daily Monitor*. Available at: https://jamestown.org/program/kazakhstan-adopts-new-military-doctrine/ [Accessed: 27 April 2018].
50. Handler S (2012) The New cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare. *Stanford Journal of International Law*, 48(1), pp. 209-237.
51. Hirch P (2017) Windmills in cyberspace. *Journal of Business Strategy*, 38(3), pp. 48-51.
52. Landmine and Cluster Munition Monitor (2017). *Press Release*. Available at: http://the-monitor.org/media/2582211/CMM2017_PressRelease_final.pdf [Accessed: 28 April 2018].
53. Lasiello E (2015) Are cyber Weapons Effective Military Tools?. *Military and Strategic Affairs*, 7(1), pp. 23-40.
54. Liang C *et al.* (2016) Development of a Multifunctional BIM Maturity Model. *Journal of Construction Engineering and Management*, 142(11).
55. ICT4Peace Foundation (2018) Trust and Attribution in cyberspace: A Proposal for an Independent Network of Organisations Engaging in Attribution Peer Review. Available at: https://ict4peace.org/wp-content/uploads/2018/12/Attribution-Peer-Review-Network-final-2018.pdf [Accessed: 7 December 2018].
56. Ingebritsen C (2002) Norm Entrepreneurs - Scandinavia's Role in World Politics, *Journal of the Nordic International Studies Association,* 37(1), pp. 11-23.
57. International Committee of the Red Cross (2005) *Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects and Additional Protocols*. Available at: https://www.icrc.org/eng/assets/files/other/icrc_002_0811.pdf [Accessed: 10 September 2018].
58. International Committee of the Red Cross (2010) *Protocols Additional to the Geneva Convention of 12 August 1949*. Available at: https://www.icrc.org/eng/assets/files/other/icrc_002_0321.pdf [Accessed: 10 April 2018].

59. International Committee of the Red Cross (2016) *The Geneva Conventions of 12 August 1949.* Available at: https://shop.icrc.org/icrc/pdf/view/id/17 [Accessed: 10 October 2018].

60. International Committee of the Red Cross (no date) Treaty on the Prohibition of Nuclear Weapons. Available at: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/432A1729D8F44DA9C125825D0046F9E9/FULLTEXT/TPNW-EN.pdf [Accessed: 10 October 2018].

61. International Security Advisory Board (2014) *Report on A Framework for International cyber Stability*. Available at: https://www.state.gov/documents/organization/229235.pdf [Accessed: 25 April 2018].

62. Jajodia S *et al* (Eds.) (2015) *cyber Warfare: Building the Scientific Foundation.* New York: Springer.

63. Kagan R (2018) Trump' America Does Not Care. *Order from Chaos* Blog, 17 June 2018. Available at: https://www.brookings.edu/blog/order-from-chaos/2018/06/17/trumps-america-does-not-care/ [Accessed: 10 July 2018].

64. Khalip A (2018) *U.N. chief urges global rules for cyber warfare* Reuters. Available at: https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4 [Accessed: 20 April 2018].

65. Khan L (2011) The Biological Weapons Convention: Proceeding Without a Verification Protocol. *Bulletin of the Atomic Scientists.* Available at: https://thebulletin.org/2011/05/the-biological-weapons-convention-proceeding-without-a-verification-protocol/ [Accessed 25 May 2018].

66. Kivunja C and Kuyini A (2017) Understanding and Applying Research Paradigms in Educational Contexts. *International Journal of Higher Education*, 6(5), pp. 26-41.

67. Kohlegger M *et al.* (2009) *Understanding Maturity Models Results of a Structured Content Analysis*. Proceedings of the 9th I-KNOW and I-SEMANTICS Conference, Graz, 2-4 September. Innsbruck: University of Innsbruck.

68. Kydd A (2000) Arms Races and Arms Control: Modeling the Hawk Perspective. *American Journal of Political Science*, 44(2), pp. 228-244.

69. Libicki M (2013) Don't Buy the Cyberhype. *Foreign Affairs*. Available at: https://www.foreignaffairs.com/articles/united-states/2013-08-14/dont-buy-cyberhype [Accessed: 20 May 2018].

70. Litwak R and King M (2015) Arms Control in cyberspace?. *Wilson Briefs.* Available at: https://www.wilsoncenter.org/sites/default/files/arms_control_in_cyberspace.pdf [Accessed: 23 May 2018].

71. Mai J (2017) *Xi Jinping Renews 'cyber Sovereignty' Call at China's Top Meeting of Internet Minds* South China Morning Post. Available at: https://www.scmp.com/news/china/policies-politics/article/2122683/xi-jinping-renews-cyber-sovereignty-call-chinas-top [Accessed: 20 July 2018].

72. Mann M (1997) Has Globalization Ended the Rise and Rise of the Nation-state?. *Review of International Political Economy*, 4(3), pp. 472-496.

73. Martin G (2017) Department of Defence Aims to Beef Up cyber Security. *Defence Web*. Available at:

http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=49368:department-of-defence-aims-to-beef-up-cyber-security&catid=111:sa-defence&Itemid=242 [Accessed: 27 April 2018].

74. Mastanduno M (1997) Preserving the unipolar moment: realist theories and US grand strategy after the Cold War. *International Security*, 21(4), pp. 49-88.
75. Maurer J (2018) The Forgotten Side of Arms Control: Enhancing U.S. Competitive Advantage, Offsetting Enemy Strengths. *War on the Rocks* Blog, 27 June 2018. Available at: https://warontherocks.com/2018/06/the-forgotten-side-of-arms-control-enhancing-u-s-competitive-advantage-offsetting-enemy-strengths/ [Accessed: 10 June 2018].
76. Maurer T (2014) The Future of War: cyber is Expanding the Clausewitzian Spectrum of Conflict. *Best Defence* Blog. Available at: http://foreignpolicy.com/2014/11/13/the-future-of-war-cyber-is-expanding-the-clausewitzian-spectrum-of-conflict/ [Accessed 27 April 2018].
77. Maxwell J (2013) *Qualitative Research Design: An Interactive Approach.* Washington D.C.: Sage Publications Inc.
78. Mayring P (2008). *Qualitative content analysis. Basics and techniques.* Weinheim: Beltz.
79. Mazanec B (2016) Constraining Norms for cyber Warfare are Unlikely. *Georgetown Journal of International Affairs*, 17(3), pp. 100-109.
80. McCarthy T (2015) NSA director defends plan to maintain 'backdoors' into technology companies. *The Guardian*. Available at: https://www.theguardian.com/us-news/2015/feb/23/nsa-director-defends-backdoors-into-technology-companies [Accessed: 20 April 2018].
81. Menn J (2013) Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback. *Reuters*. Available at: https://www.reuters.com/article/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510 [Accessed: 10 July 2018].
82. Meyer P (2018) Global cyber Security Norms: A Proliferation Problem?. *ICT4Peace Foundation*. Available at: https://ict4peace.org/wp-content/uploads/2018/12/cyber-SecNormsProlifICT4PNov2018.pdf [Accessed: 7 December 2018].
83. Miller D (1999) The Norm of Self-Interest. *American Psychologist*, 54(12), pp. 1053-1060.
84. Miller S (2017) cyber Threats, Nuclear Analogies?. In Perkovich G and Levite A [Eds.] *Understanding cyber Conflict: 14 Analogies*. Washington D.C.: Georgetown University Press
85. Moravcsik A (1997) Taking preferences seriously: a liberal theory of international politics. *International Organization*, 51(4), pp. 514–553.
86. Mueller B (2014) Why We Need a Cyberwar Treaty. *The Guardian.* Available at: https://www.theguardian.com/commentisfree/2014/jun/02/we-need-cyberwar-treaty [Accessed: 10 September 2018].
87. Mumford A (2013) Proxy warfare and the future of conflict. *The RUSI Journal*, 158(2), pp. 40-46.
88. Nye J (2015) *The World Needs an Arms-control Treaty for cybersecurity* Harvard: Belfer Center for Science and International Affairs. Available at:

https://www.belfercenter.org/publication/world-needs-arms-control-treaty-cybersecurity [Accessed: 10 June 2018].

89. Nye J (2018) *Normative Restraints on cyber Conflict* Harvard: Belfer Center for Science and International Affairs. Available at: https://www.belfercenter.org/publication/normative-restraints-cyber-conflict [Accessed: 10 June 2018].

90. O'Connell M and Arimatsu L (2012) *cyber Security and International Law* London: Chatham House. Available at: https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/290512summary.pdf [Accessed: 10 April 2018].

91. Office of the Director of National Intelligence (2013) *Worldwide Threat Assessment of the US Intelligence Community*. Available at: https://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf [Accessed: 25 May 2018].

92. Orellana M (2014) Typology of Instrument of Public Environmental International Law. *Environment and Development Series*, No. 158. Santiago: United Nations.

93. Organization for Security and Co-operation in Europe (OSCE) (2013) *Decision No. 1106 Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies.* Available at: https://www.osce.org/pc/109168?download=true [Accessed: 25 April 2018].

94. Organisation for the Prohibition of Chemical Weapons (2005) *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction*. Available at: https://www.opcw.org/sites/default/files/documents/CWC/CWC_en.pdf [Accessed: 10 October 2018].

95. Patel S (2015) *The Research Paradigm – Methodology, Epistemology and Ontology – Explained in Simple Language*. Available at: http://salmapatel.co.uk/academia/the-research-paradigm-methodology-epistemology-and-ontology-explained-in-simple-language [Accessed: 10 September 2018].

96. Ponterotto J (2005) Qualitative Research in Counseling Psychology: A Primer on Research Paradigms and Philosophy of Science. *Journal of Counseling Psychology*, 52(2), pg. 126-136.

97. Radunović V (2017) *Towards a Secure cyberspace via Regional Co-operation*. Geneva: DiploFoundation. Available at: https://www.diplomacy.edu//sites/default/files/Diplo-Towards_a_secure_cyberspace-GGE.pdf [Accessed: 10 September 2018].

98. Rathmell A (2003) Controlling Computer Network Operations. *Studies in Conflict and Terrorism*, 26(3), pp. 215-232.

99. Rauscher K and Korotkov A (2011) *Working Towards Rules for Governing cyber Conflict* New York: The EastWest Institute. Available at: https://www.eastwest.ngo/sites/default/files/ideas-files/US-Russia.pdf [Accessed: 10 September 2018].

100. Ravitch S and Riggan M (2017) *Reason and Rigour: How Conceptual Frameworks Guide Research.* Thousand Oaks, California: Sage Publications Inc.

101. Reardon R and Choucri N (2012) *The Role of cyberspace in International Relations: A View of the Literature*. Paper presented at the 2012 ISA Annual Convention, San Diego, CA, United States of America, April 1, 2012. Available at: http://ecir.mit.edu/images/stories/Reardon%20and%20Choucri_ISA_2012.pdf [Accessed: 20 April 2018].

102. Rid T and McBurney P (2012) cyber-Weapons. *Rusi Journal*, 157(1), pp. 6-13.

103. Rose G (1998) Neoclassical Realism and Theories of Foreign Policy. *World Politics* 51(1), pp. 144-172.

104. Russian Federation (2000) *Information Security Doctrine of the Russian Federation.* Available at: https://info.publicintelligence.net/RU-InformationSecurity-2000.pdf [Accessed: 25 May 2018].

105. Russian Federation (2016) *Doctrine of Information Security of the Russian Federation.* Available at: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163 [Accessed: 25 May 2018].

106. Rutherford K (2000) The Evolving Arms Control Agenda: Implications of the Role of NGOs in Banning Antipersonnel Landmines, *World Politics*, 53(1), pp. 74-114.

107. Salamey I (2016) *The Decline of Nation-States After the Arab Spring: The Rise of Communitocracy*. New York: Taylor & Francis.

108. Sanger D (2012) *Confront and Conceal: Obama's Secret Wars and Surprising use of American Power.* New York: Crown Publishing.

109. Saxon D (2016) Violations of International Humanitarian Law by Non-state Actors during cyberwarfare: Challenges for Investigations and Prosecutions. *Journal of Conflict and Security Law*, 21(3), pp. 555-574.

110. Schneier B (2012) *An International Cyberwar Treaty Is the Only Way to Stem the Threat*. U.S. News. Available at: https://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/an-international-cyberwar-treaty-is-the-only-way-to-stem-the-threat [Accessed: 10 April 2018].

111. Segal A (2016) How Much Does a cyber Weapon Cost? Nobody Knows. *Council on Foreign Relations.* Available at: https://www.cfr.org/blog/how-much-does-cyber-weapon-cost-nobody-knows [Accessed: 25 April 2018].

112. Shane S, Sanger D (2011) *Drone Crash in Iran Reveals Secret U.S. Surveillance Effort.* The New York Times. Available at: https://www.nytimes.com/2011/12/08/world/middleeast/drone-crash-in-iran-reveals-secret-us-surveillance-bid.html [Accessed 27 April 2018].

113. Sigholm J (2016) Non-state Actors in cyberspace Operations. *Journal of Military Studies*, 4(1), pp. 1-37.

114. Sofaer A and Goodman S (2000) *A Proposal for an International Convention on cyber Crime and Terrorism* Stanford: The Center for International Security and Cooperation. Available at: http://cisac.fsi.stanford.edu/sites/default/files/sofaergoodman.pdf [Accessed: 10 April 2018].

115. Suciu P (2014) Why cyber Warfare is so Attractive to Small Nations. *Fortune*. Available at: http://fortune.com/2014/12/21/why-cyber-warfare-is-so-attractive-to-small-nations/ [Accessed: 27 April 2018].

116. Steinberg G (2005) Realism, Politics and Culture in Middle East Arms Control Negotiations. *International Negotiation* 10(3), pp. 487-512.

117. Strauss B (2015) Lessons of Past Arms Control Agreements for the Proposed Iran Deal. *Strategica*, (26), pp. 9-10.

118. Thomas T (2009) *Decoding the Virtual Dragon.* Available at: http://www.ists.dartmouth.edu/docs/ThomasSlides.pdf [Accessed: 25 May 2018].

119. Thomas T (no date) *Like Adding Wings to the Tiger: Chinese Information War Theory and Practice.* Available at: http://www.au.af.mil/au/awc/awcgate/fmso/chinaiw.htm [Accessed: 25 May 2018].

120. Trachtenberg M (1991) The Past and Future of Arms Control. *Daedalus*, 120(1), pp. 203-216.

121. Waldman T (2010) Politics and war: Clausewitz's paradoxical equation. *Parameters*, 40(3), pp. 1-13.

122. Walt S (1998) International Relations: One World, Many Theories. *Foreign Policy*, (110), pp. 29-46.

123. Wendler R (2012) The Maturity of Maturity Model Research: A Systematic Mapping Study. *Information and Software Technology*, 54(12), pp. 1317-1339.

124. United Nations [UN] (1974) *Treaty on the Prohibition of the Emplacement of Nuclear Weapons and Other Weapons of Mass Destruction on the Sea-Bed and the Ocean Floor and in the Subsoil Thereof*. Available at: https://treaties.un.org/doc/Publication/UNTS/Volume%20955/volume-955-I-13678-English.pdf [Accessed: 10 October 2018].

125. UN (2005) *International Convention for the Suppression of Acts of Nuclear Terrorism*. Available at: https://treaties.un.org/doc/db/terrorism/english-18-15.pdf [Accessed: 10 October 2018].

126. UN (2018) *First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible cyberspace Conduct*. Available at: https://www.un.org/press/en/2018/gadis3619.doc.htm [Accessed: 1 December 2018].

127. United Nations Educational, Scientific and Cultural Organization [UNESCO] (2010) *The 1954 Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict and its two (1954 and 1999) Protocols.* Available at: http://unesdoc.unesco.org/images/0018/001875/187580e.pdf [Accessed: 10 October 2018].

128. United Nations General Assembly [UNGA] (1998) Resolution 53/70. *Developments in the Field of Information and Telecommunications in the Context of International Security* (A/RES/53/70).

129. United Nations Institute for Disarmament Research [UNIDIR] (2013) *The cyber Index: International Security Trends and Realities*. Available at: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf [Accessed: 27 April 2018].

130. United Nations Institute for Disarmament Research [UNIDIR] (2017) *The United Nations, cyberspace and International Peace and Security Responding to Complexity in the 21st Century*. Available at: http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf [Accessed: 11 February 2018].
131. United Nations Office for Disarmament Affairs [UNODA] (2017) *Disarmament A Basic Guide*. New York: United Nations Publication.
132. UNODA (no date) *The Treaty on the Non-Proliferation of Nuclear Weapons*. Available at: https://www.un.org/disarmament/wmd/nuclear/npt/text [Accessed: 10 October 2018].
133. United Nations Office in Geneva [UNOG] (no date) *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction.* Available at: https://www.unog.ch/80256EDD006B8954/(httpAssets)/C4048678A93B6934C1257188004848D0/$file/BWC-text-English.pdf [Accessed: 10 October 2018].
134. United Nations Security Council [UNSC] (2004) Resolution 1540 (S/RES/1540).
135. United States of America - Department of Defense (1999) *An Assessment of International Legal Issues in Information Operations*. Available at: http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf [Accessed 30 May 2018].
136. United States of America - Department of Defense (2015) *Law of War Manual.* Available at: https://www.defense.gov/Portals/1/Documents/law_war_manual15.pdf [Accessed:15 April 2018].
137. Waddell K (2016) The Rise of Asymmetric cyberwarfare. *The Atlantic.* Available at: https://www.theatlantic.com/technology/archive/2016/03/the-troubling-rise-of-asymmetric-cyberwarfare/474972/ [Accessed: 10 June 2018].
138. Wendler R (2012) The Maturity of Maturity Model Research: A Systematic Mapping Study. *Information and Software Technology*, 54(12), pp. 1317-1339.
139. White House (2013) *Fact Sheet: U.S. - Russian Cooperation on Information and Communications Technology Security.* Available at: https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol [Accessed: 25 April 2018].