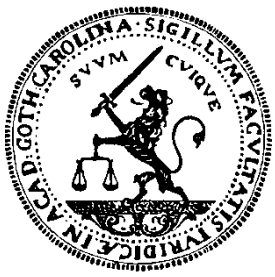

FACULTY OF LAW
Lund University

Antonia Ball

Self-defence and the notion of Armed Attack in the context of Hybrid Warfare:
Accumulation of events; a hybrid solution to a hybrid problem.

JAMM07 Master Thesis

International Human Rights Law
30 higher education credits

Supervisor: Letizia Lo Giacco

Term: Spring 2020

Table of Contents

Abstract

This thesis explores the link between hybrid warfare and the notion of armed attack in that it asks the question of whether the notion of armed attack is competent to encompass hybrid warfare.

The thesis is approached in two parts. In the first part, Chapter two describes the legal framework surrounding the notion of armed attack as a threshold in triggering the use of force in self defence. The third chapter moves on to explore the phenomenon of hybrid warfare, its origins and activities and to examine claims that utilising hybrid warfare exploits ambiguities in the armed attack framework.

Part two then proceeds to analyse these claims by applying the law to hybrid warfare through two perspectives. Firstly, in chapter four, through an individual activities lens. And secondly, in chapter five, by taking all the activities together as a composite whole.

Consequently, the thesis argues that the notion of armed attack is effective in encompassing hybrid warfare but only under a limited set of circumstances. Specifically, under the proviso that the international community recognise a ‘overall campaign’ approach to the doctrine of accumulation of events.

Acknowledgements

This thesis is dedicated to Mogens. Thank you for always believing in me and for your unwavering love, support and advice.

Many thanks to my wonderful supervisor Letizia Lo Giacco for all the insights and support without which this thesis would not exist.

Abbreviations

CoE - Council of Europe
CHW - Countering Hybrid Warfare
ARIWA - Draft Article on the Responsibility of States for Internationally Wrongful Acts
DDoS - Distributed Denial of Service
DRC - Democratic Republic of Congo
ECS - East China Sea
EEAS - Europes External Action Service
EU - European Union
GA - General Assembly
ICC - International Criminal Court
ICJ - International Court of Justice
MDCD - Multinational Capability Development Campaign
NATO - North Atlantic Treaty Organisation
OHCHR - Office of the United Nations High Commissioner for Human Rights
PLO - Palestine Liberation Organization
PRC - Peoples Republic of China
RBIO - Rules Based International Order
SC - Security Council
SCS - South China Sea
UK - United Kingdom
UN - United Nations
US - United States
USA - United Staes of America
WMD - Weapons of Mass Destruction

Chapter 1: Introduction

1.1 The Background

In 2014, Russia annexed Crimea. The annexation came amid a backdrop of confusion and in the context of widespread political unrest which had spread throughout Ukraine in the preceding year, specifically after the 'Maidan' protests. After the annexation, eastern Ukraine became a conflict zone. The conflict is ongoing at the time of writing.

According to the OHCHR, by February 2020 the number of conflict-related casualties in Ukraine is estimated to be between 41,000–44,000, with an estimated 13,000-13,200 killed including the crew and passengers of Malaysian Airways flight MH17 which was shot down over eastern Ukraine in 2014[1]. There has been a corresponding negative impact on human rights. Despite the far reaching consequences of the initial political unrest and the ongoing conflict situation, Ukraine were unable exercise self defence to prevent the annexation or to stem the ongoing violence.

Whilst this sounds like an all too familiar case of civilian uprising leading to a revolution, this is not the case. In light of the annexation and subsequent occupation of Crimea by Russia and proof of Russian support to separatists in eastern Ukraine, the widely accepted truth is that that the situation in Ukraine was the culmination of a well executed Russian hybrid attack.

Since then, Hybrid warfare has become recognised as a particular form of warfare which is successful in employing a range of activities to achieve the same results as traditional kinetic warfare. These are used in combinations and in a manner which blurs the distinction between war and peace.

In the following years similar activities as those observed in Ukraine, have been reported in other countries, especially in the Baltic states, specifically Estonia and Latvia[2]. And by China in Taiwan.[3] These observations have led to concerns that hybrid warfare is a now one of the major emerging threats to global peace and security.[4]

1.2 The problem

Within the UN Charter sits what is commonly referred to as the 'armed attack' threshold. The threshold is actually the legal provision that, under current international law, the right to self defence (both unilaterally and collectively) is triggered only in the event of an 'armed attack'. The threshold has the dual purpose of deterring States from prosecuting an armed attack as well as to 'trigger' action in self defence if the armed attack threshold is breached. If the

---

[1] "Office of the United Nations High Commissioner for Human Rights Report on the human rights situation in Ukraine 16 November 2019 to 15 February 2020" (PDF). *OHCHR*.

[2] Radin, Andrew, Hybrid Warfare in the Baltics: Threats and Potential Responses. Santa Monica, CA: RAND Corporation, 2017.

[3] https://thediplomat.com/2018/01/chinas-hybrid-warfare-and-taiwan/

[4] For example, Since 2016, NATO and the EU have identified that addressing hybrid threats is a priority for cooperation https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html

threshold is obfuscated or circumvented to the point where action in self defence in the face of an attack is prevented or delayed then self defence and collective defence is weakened, or worse fails, together with a corresponding effect on its use as a deterrent. It is therefore vital to assess whether the notion of armed attack is competent to overcome the challenges that hybrid warfare poses, or if hybrid warfare does in fact give States a way to circumvent this threshold.

1.3 Research Question:

In order to address the problem identified, this thesis aims to answer the following research question:

To what extent is the notion of armed attack capable to encompass hybrid warfare?

1.4 Structure and Method:

This thesis was researched primarily using the doctrinal legal research methodology, although, due to the international nature of the law, I also utilise comparative legal methodology where appropriate[5]. The thesis proceeds in two parts:

Part one is divided into two chapters, the first of which is an analysis of the scholarly sources and legal framework on the notion of armed attack, The second researches the phenomenon of hybrid warfare, its origins, uses, component parts and not least legal implications.

In clarifying the appropriate legal framework, a wide range of relevant legislation and well case law were consulted together with academic, authoritative and official books, articles and reports.

In order to characterise hybrid warfare, academic scholarship together with military and think-tank reportage was consulted together with testimonies and case studies on the conflict in the Ukraine. Ukraine being the most relevant example of a successful use of hybrid warfare.

Part two proceeds to answer the research question by applying the relevant law on armed attack to, in chapter 5, the individual activities utilised under hybrid warfare and chapter 6, focusses on the accumulation of events theory as applied to hybrid warfare.

Chapter 6 also raises questions as to how the doctrine of accumulation of events has been understood and thus far utilised, and based upon a re-evaluation of the recent scholarship on the matter, proposes that the doctrine be understood in a broader manner.

1.5 Motivation:

---

[5] Hoecke, Mark van. Methodologies of Legal Research : Which Kind of Method for What Kind of Discipline?.Oxford: Hart Publishing, 2013.

The phenomenon of hybrid warfare and its emergence as a growing threat to peace and security and to international human rights has been recognised and studied from a military and political point of view. It has also been examined by international organisations such as NATO[6], the CoE[7], the UN[8] and national bodies, but only to a limited extent by the legal domain. This thesis aims to add to that debate, especially in drawing attention to the relevance of the accumulation of events doctrine in the context of hybrid warfare.

1.6 Delimitations:

The following activities are treated as being outside the scope of 'hybrid activities' for the purposes of the current thesis:

Nuclear/WMD - These weapons, although interrelated with the concept of hybrid warfare in the larger sense of the understanding, are covered by their own *lex specialis* and are therefore outside the scope of this thesis.

Criminal/Economic: These items are closely interrelated with hybrid warfare, and have been described by some authors as being within the Russian model of hybrid warfare[9]. However, this thesis takes the view of other authors[10] that these items fall outside the definition of warfare and fall within the ambit of normal inter-state competition, with their own regulatory frameworks and are therefore outside the scope of this thesis.

Clandestine Operations: Although closely interrelated with hybrid warfare, these operations are covered by separate legal frameworks and due to time and space considerations shall therefore not be included in this thesis.

Terrorist attacks: Hybrid warfare in the present context is understood as prosecuted by a State, this therefore excludes autonomous terrorist organisations from the scope of this thesis. State sponsored armed groups, however shall be included.

---

[6] https://www.nato.int/cps/en/natohq/topics_156338.htm

[7] https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24762&lang=en

[8] https://www.un.org/press/en/2016/sc12577.doc.htm

[9] Thiele, "The Crisis in Ukraine," 6.

[10] Wither, James K. "Making Sense of Hybrid Warfare." *Connections*, vol. 15, no. 2, 2016, pp. 73–87. *JSTOR*, www.jstor.org/stable/26326441. Accessed 18 May 2020.

Part 1: Legal Framework and Hybrid Warfare

The first part of the thesis shall proceed by outlining the legal framework pertaining to the notion of armed attack in Chapter 2 and then move on to explain the Theory of Hybrid Warfare in Chapter 3 and how it uniquely targets the armed attack threshold.

Chapter 2: The Notion of Armed Attack

2.1 Introduction

This chapter describes the legal framework surrounding the notion of armed attack that will be used in part two. It will serve as the basis for applying the relevant activities within hybrid warfare to the current understanding of the international law surrounding the notion of armed attack.
The chapter proceeds in two sections. The first section describes the right of self defence in international law and demonstrates how an armed attack is the crucial threshold in legally invoking this right in the use of force in self defence. The second section goes in depth into the elements that must be present for an attack to be considered to have reached the threshold of armed attack.

2.2 Self Defence in the *Jus ad Bellum*

The adoption of the UN Charter in 1945 reflected a desire by all the signatories to it that the horrific events that occurred during the Second World War should never happen again. The Charter formed a core part of the post war rules-based international order (RBIO). Thus the charter itself, specifically enunciated at Article 2(4), aimed to outlaw war by proclaiming a general prohibition to that effect known as the *jus contra bellum.* Article 2 of the United Nations Charter (UN Charter) states:

> 'The Organisation and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles.
> 1. The Organisation is based on the principle of the sovereign equality of all its Members.
> 2. All Members, in order to ensure to all of them the rights and benefits resulting from membership, shall fulfil in good faith the obligations assumed by them in accordance with the present Charter.
> 3. All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.
> 4. **All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.**[11]
> 5. All Members shall give the United Nations every assistance in any action it takes in accordance with the present Charter, and shall refrain from giving assistance to any state against which the United Nations is taking preventive or enforcement action.[12]'

The one exception to the general prohibition on the use of force, is found at Article 51 of the Charter. This states:

---

[11] Emphasis in bold is my own

[12] Charter of the United Nations, 24 October 1945, 1 UNTS XVI, Art. 2

> '**Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs** against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.[13]'

Together, Articles 2(4) and 51 form the general prohibition on force in International Law except in the case of self defence against an 'armed attack'. This right originates from the international customary law which preserves a states' inherent right to self defence[14] and, as stated in Art. 51, is only intended to be a temporary right which exists '…until the Security Council has taken measures necessary to maintain international peace and security.[15]' Additionally, there is a duty to report any use of force in self defence immediately to the Security Council. Failure to do so may be taken as in indication by the Court in any subsequent case that the use of force was not in fact used in self defence, as per the Courts decision against the US in *Nicaragua* demonstrates[16].

Since coming into force on 23 October 1945, there has been difficulty in achieving a unanimous agreement on the precise interpretation of Article 51, deriving from disagreements as to the specific customary origins of the right.[17] The disagreements give rise to follow on difficulties in understanding the extent to which Art. 51 exists alongside a 'general right of self defence' claimed by some to exist in customary law or, whether Art 51 and the specific requirement for an 'armed attack' superseded that right. Both understandings have some academic support with some scholars arguing that the interpretation be given an expansive understanding, and others arguing for a restrictive understanding.[18]
Judge Simma, in his more expansive view expressed in his Separate Opinion in the *Oil Platforms* Case put forward that some acts not amounting to an 'armed attack' should

---

[13] Charter of the United Nations, 24 October 1945, 1 UNTS XVI. Art. 51

[14] For an overview on the historical and customary origins of the right to self defence see Ian Brownlie, The Use of Force in Self-Defense, 37 Brit. Y. B. Int'l L. 183 (1961)

[15] ibid (At footnote18)

[16] *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits*, International Court of Justice (ICJ), 27 June 1986, para 235

[17] O Corten, 'The Controversies Over the Customary Prohibition on the Use of Force: A Methodological Debate' (2006) 16 EJIL 803

[18] Norman Menachem Feder, Reading the U.N. Charter Connotatively: Toward a New Definition of Armed Attack, 19 N.Y.U. J. Int'l L. & Pol. 395 (1987) p 403-404 Content downloaded/printed from HeinOnline Tue Mar 26 10:08:06 2019
And C Gray, International Law and the Use of Force (3rd edn, OUP 2008) p124

warrant a recourse to self defence but that the responses to such uses of force be moderated accordingly by the principles of necessity and proportionality[19]:

> '…There are two levels to be distinguished: there is, first, the level of 'armed attacks' in the substantial, massive sense of amounting to 'une agression armée', to quote the French authentic text of Article 51. Against such armed attacks, self-defence in its not infinite, but still considerable, variety would be justified. But we may encounter also a lower level of hostile military action, not reaching the threshold of an 'armed attack' within the meaning of Article 51 of the United Nations Charter. Against such hostile acts, a State may of course defend itself, but only within a more limited range and quality of responses (the main difference being that the possibility of collective self-defence does not arise, cf. Nicaragua) and bound to necessity, proportionality and immediacy in time in a particularly strict way.'[20]

On the other hand, commentators such as Nolte and Randelzhofer put forward the more restrictive understanding that:

> '[The] prevailing view considers Art. 51 to exclude any self-defence other than that in response to an armed attack, referring, above all, to the purpose of the UN Charter, ie to restrict as far as possible the use of force by individual states'[21]

The more restrictive view was confirmed in the *Nicaragua* case judgement, which is today one of the leading authorities on the matter: 'In the case of individual self-defence, the exercise of this right is subject to the State concerned having been the victim of an armed attack.'[22] the requirement also extends to when self-defence is exercised collectively: 'for one State to use force against another, on the ground that that State has committed a

---

[19] Necessity and proportionality are key limits to the right to self - defence, which was reaffirmed in The *Nicaragua* case, the *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons*, the *Oil Platforms* case and *Armed Activities on the Territory of the Congo (DRC v Uganda)*. Nolte and Randelzhofer explain the principles of necessity and proportionality as being 'what is necessary for the repelling of an armed attack and must not acquire a retaliatory, deterrent, or punitive character. The means and the extent of the defence must not be disproportionate to the gravity of the attack.' See: Nolte, G and Randelzhofer, A. Ch.VII Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Article 51. In The Charter of the United Nations - A Commentary, Volume II, OUP 2012, 3rd Edition edited by Simma, Bruno et al. Pg 1425

[20] *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America*, International Court of Justice (ICJ), 6 November 2003, available at: https://www.refworld.org/cases,ICJ,414b00604.html [accessed 10 Apr 2019] (Separate Opinion Judge Simma) para 13.

[21] Nolte, G and Randelzhofer, A. Ch.VII Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Article 51. In The Charter of the United Nations - A Commentary, Volume II, OUP 2012, 3rd Edition edited by Simma, Bruno et al. pg 1403

[22] *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits*, International Court of Justice (ICJ), 27 June 1986, para 211

wrongful act against a third State, is regarded as lawful, by way of exception, only when the wrongful act provoking the response was an armed attack… In the view of the Court, under international law in force today - whether customary international law or that of the United Nations system - States do not have a right of 'collective' armed response to acts which do not constitute an 'armed attack'.'[23]

Thus, as per the prevailing interpretation on Article 51, the key element or threshold in considering whether forcible self defence is lawful under Article 51 is the determination of whether or not an 'armed attack' has taken place as distinguished from a less serious 'act of aggression'. Use of force in self defence only being lawful if it has. Section 2.3 shall now go on to look further at what constitutes an armed attack.

2.3 Armed Attack

The elements of an 'armed attack'

The notion of 'armed attack' is far from settled[24]. As per the object and purpose of the UN Charter, it is necessarily set at a high threshold, yet encompasses a confusing range of movable and disputed requirements. It is widely accepted that there are three main elements which constitute an 'armed attack'[25]. The three elements are: 1. *ratione materie*, the material element, relating to which acts qualify as an armed attack; 2. *ratione personae,* the element dealing with whom the attack originated from; and, 3. *ratione temporis,* the temporal element determining when it can be considered that an armed attack is taking place for the purposes of using force in self defence.
The principles of 'necessity and proportionality' and the 'duty to report' to the UN Security Council, as mentioned in section 2.3, act as a check and balance as to the use of force in self defence and as such have a bearing in some elements within the notion of armed attack.
In the following sections, I shall provide a breakdown of these elements[26].

2.3.1 *Ratione Materie*

The *ratione materie* relates to the material aspect of the notion of 'armed attack' and consists of four major elements: a. The acts which qualify to be counted as an 'armed attack' according to international law. b. The gravity of these acts. c. Whether the acts must be taken in isolation or can aggregated as per the accumulation of events theory. And, finally, d. The

---

[23] ibid at para 211

[24] Gray, C. International Law and the Use of Force (4th Edition), 15 February 2018. OUP. P120

[25] Ruys, T, 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, New York. First ed Paperback 2013.

[26] It must be noted that this is an extremely large and unsettled doctrine, each element itself has tomes of literature devoted to it. This section therefore elucidates the salient points that I consider pertinent to scope of the present thesis. The selection is not exhaustive by any means and aims to serve as a starting point rather than an end point in the debate on the matter in hand.

aggressive intent of the state[27]. The law is by no means definitive in this area, however an examination of current ICJ case law gives a good starting point, which is further complemented by state practice and scholarly opinion.

a. Acts constituting an 'armed attack'.

In the *Nicaragua (merits)* case[28], the ICJ used Article 3 of the GA Res 3314 (XXIX) (14 December 1974) Definition of Aggression[29] as a blueprint to identify the acts which qualify as an act of aggression in the determination of whether or not an 'armed attack' had taken place by armed bands: "In particular, it may be considered to be agreed that an armed attack must be understood as including not merely action by regular armed forces across an international border, but also "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to (inter alia) an actual armed attack conducted by regular forces, or its substantial involvement therein". This description, contained in Art. 3 paragraph (g) of the Definition of Aggression annexed to General Assembly Resolution 3314 (XXIX), may be taken to reflect customary international law'[30]

The ICJ went on to confirm the use of the Definition of Aggression in Resolution 3314 as a source in the determination of an 'armed attack' in several subsequent cases.[31] Establishing that the resolution will serve as an authority on the future determination of acts of aggression which constitute an armed attack. The acts included within the definition are given at Article 3 of GA Resolution 3314 and are as follows:

> 'Any of the following acts, regardless of a declaration of war, shall, subject to and in accordance with the provisions of article 2, qualify as an act of aggression:
> (a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof,
> (b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State;
> (c) The blockade of the ports or coasts of a State by the armed forces of another State;

---

[27] Ruys, T, 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, New York. First ed Paperback 2013. See Chapter on 'The armed attack requirement Ratione Materie.

[28] *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits*, International Court of Justice (ICJ), 27 June 1986, available at: https://www.refworld.org/cases,ICJ,4023a44d2.html [accessed 9 Apr 2019]

[29] UN Doc A/RES/3314(XXIX)

[30] *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits*, International Court of Justice (ICJ), 27 June 1986, available at: https://www.refworld.org/cases,ICJ,4023a44d2.html para 195

[31] *Congo v Uganda* para 146; *Legal Consequences of the Construction of a Wall* para 139

> (d) An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State;
> (e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;
> (f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;
> (g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein.'[32]

The list is not exhaustive, as Article 4 states:

> 'The acts enumerated above are not exhaustive and the Security Council may determine that other acts constitute aggression under the provisions of the Charter.'[33]

In addition to its use by the ICJ, as recently as 2010, the ICC confirmed Resolution 3314 as a legal source by which to determine if an act constitutes an act of aggression upon the adoption of the Article 8 *bis* Crime of aggression in the Rome Statute[34]. Resolution 3314[35] can therefore be considered to be an authority which can be utilised in the determination of whether an act is an 'armed attack' and, as Nolte and Randelzhofer confirm, it has been accepted as such by the 'vast majority of states'[36]. Ruys interprets this as such, but unlined that it is not a restrictive or exhaustive list and that there is a 'theoretical possibility that the concept of 'armed attack' could in certain respects actually be broader that the one defined in Resolution 3314 (XXIX).'[37]
A further consideration is that whilst in most circumstances an 'armed attack' will qualify as an act of aggression, the reverse is not true[38]. Meaning that the notion of 'armed attack'

---

[32] UN Doc A/RES/3314(XXIX), Article 3

[33] UN Doc A/RES/3314(XXIX), Article 4

[34] UN General Assembly, Rome Statute of the International Criminal Court (last amended 2010), 17 July 1998

[35] UN Doc A/RES/3314(XXIX)

[36] Nolte, G and Randelzhofer, A. Ch.VII Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Article 51. In The Charter of the United Nations - A Commentary, Volume II, OUP 2012, 3rd Edition edited by Simma, Bruno et al. p 1409

[37] Ruys, T, 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, New York. First ed Paperback 2013 p139

[38] ibid p138

constitutes a narrower meaning than 'act of aggression'[39] This understanding is supported by the states parties to the draft definition of aggression provided to the Special Committee on the Question of Defining Aggression, which stated that 'armed attack (armed aggression) is the most serious form of aggression'[40] and was also reflected in the statements of the representatives of the Soviet Union[41] and the United Kingdom[42] during the course of the meetings of the Special Committee.

This implies that in order for an act to qualify as the more grave 'armed attack' there must be a way to distinguish it from being the less grave 'act of aggression'.[43] The Special Committee gave reference to the requisite 'scale and effects'[44] that would be called for in order for an act to be considered as an 'armed attack'. Thus giving rise to the next element: The 'gravity and effects' requirement.

b. The gravity and effects requirement of an 'armed attack'.

The gravity and effects requirement relates to the gravity of the act committed, for example, the severity or size of the act and what the effect, or damage, was on the victim state. As with all the other requirements, the gravity requirement meets with some divergence ranging from agreement on the minimum gravity threshold, or *de minimis* threshold, to whether the gravity requirement exists at all.

Ruys asserts that the minimum gravity threshold does not present a problem in cases such as 'large scale attacks involving massive territorial incursions, as in the case of the 1950 Korean War, the 1982 Falklands war or the 1990 Iraqi invasion of Kuwait.'[45] This suggests that the problem in determining whether an armed attack has reached the minimum gravity threshold or not is presented only in the case of smaller scale attacks.
The ICJ does not elucidate the actual point at which an attack reaches this gravity, which is decided upon in a case by case basis. However, the ICJ does distinguish between a 'mere

---

[39] Nolte, G and Randelzhofer, A. Ch.VII Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Article 51. In The Charter of the United Nations - A Commentary, Volume II, OUP 2012, 3rd Edition edited by Simma, Bruno et al. p1408

[40] UNGA 'Colombia, Cyprus, Ecuador, Ghana, Guyana, Haiti, Iran, Madagascar, Uganda and Yugoslavia: proposal' (24 March 1969) UN Doc A/AC.134/L.16. Para 2 of preamble.

[41] Statement by the Soviet representative (UNGA 'Summary Record of the 105th mtg' (9 May 1973) UN Doc A/AC.134/SR.105, 16)

[42] Statement by the United Kingdom representative (UNGA 'Summary Record of the 67th mtg' (30 July 1970) UN Doc A/AC.134/SR.67, 5)

[43] In the *Nicaragua (merits)* case, the ICJ stated that 'It is necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms.'

[44] ibid para 195

[45] ibid, 37, p152

frontier incident' and an 'armed attack'.[46] On this point, scholars such as Dinstein[47] suggest that the gravity threshold for a direct or indirect armed attack against a state, by another, is predicated by the consequences that are liable to be produced by the attack rather that the actual casualties or damage that is inflicted. Such as a missile attack, or similar which was intended to cause such damage or casualties.
When examining State practice, Ruys found that customary practice supported this view, finding that 'Even small scale bombings, artillery, naval or aerial attacks qualify as 'armed attack' activating Article 51 UN Charter, *as long as they result in or are capable of resulting in the destruction of property or loss of lives*.'[48]

In addition to this, the requisite gravity caused by an act for it to count as being an armed attack has been suggested[49] to be at a lower level when perpetrated by state actors, whereas the threshold for acts perpetrated by non-state actors is of a higher level. Something which could be a confusing factor if a state assists rebels in an attack.

The consideration of the necessity of the Gravity element was contested by the US in their submissions to the *Oil Platforms* case[50], the US argued that the minimum gravity threshold is not an issue at all for the legal characterisation of an armed attack, but instead only an issue for the determination of the proportionality calculations of any force which is used in self-defence, stating that 'Article 51 contains no qualifications regarding the size of armed attacks'[51]. It is the opinion of the present author however, when presented by the overwhelming support of State Practice, *opinio juris,* findings of the ICJ, and academic opinion that there is a difference between a use of force and a more serious 'armed attack'.

Sitting in between the argument laid out by the US and the more widely accepted argument that there be an attack of a certain gravity which is 'capable of causing damage to property or loss of life'[52] is the accumulation of events theory. The accumulation of events theory has never been successfully acknowledged as justification for use of force in self defence in court, leading to it being a somewhat neglected theory, however, it has not been directly dismissed in the courts and its existence in academic dialogue confirms its merits. As covered above, the most accepted understanding of the gravity requirement in the armed attack threshold suggests that the gravity threshold may only be reached when taking each act in isolation, and only when the said act is of a sufficient gravity to qualify. The 'accumulation of events' theory challenges this perspective. It puts forward the idea

---

[46] *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits*, International Court of Justice (ICJ), 27 June 1986, available at: https://www.refworld.org/cases,ICJ,4023a44d2.html para 195

[47] Dinstein, Y. (2017). *War, Aggression and Self-Defence*. Cambridge: Cambridge University Press. doi:10.1017/9781108120555 p193

[48] ibid, 37, p155

[49] ibid, 37, p147

[50] ICJ, Oil Platforms Case, Rejoinder submitted by the United States of America, 23 March 2001.

[51] ibid SS 5.16-5.18

[52] ibid 60

that if an act is not of sufficient gravity to qualify by itself but one of many in a series of acts of force directed against a victim state, then the effects caused by an accumulation of all the events put together could then push the overall campaign over the gravity threshold.

Famously used by Israel as a justification for a campaign against PLO strongholds in Lebanon as a response to a continuous series of PLO attacks on Israel, the accumulation of events theory or *Nadelstichtaktik* (needle prick) doctrine gives that 'each specific act of terrorism, or needle prick, may not qualify as an armed attack that entitles the victim state to respond legitimately with armed force. But the totality of the incidents may demonstrate a systematic campaign of minor terrorist activities that does rise to the intolerable level of armed attack.'[53] Thus, when invoked, the doctrine allows for lawful self defence in the face of a campaign of acts of force which do not, by themselves, amount to an 'armed attack'.

In the example given above Israel's justification was rejected by the UN Security Council, however, scholars[54] have commented that this was not necessarily due to a disagreement of the theory itself, but rather as an objection based upon a disproportionate use of force by Israel in retaliation for the attacks and as part of a general political backdrop condemning the scale of uses of force by Israel.
This indicates that in a similar situation, the accumulation of events justification could hold ground so long as any response were restrained by the coexisting rules on necessity and proportionality.
Ruys puts forward that aside from a consistent use by Israel, in examining the practice of states the theory has also been invoked by the UK, the US, China, Russia, Lebanon, Iraq, Iran, Liberia and Sudan as justification for self defence.[55] Indicating that the *opinio juris* of these countries accepts the theory.

In the courts, the ICJ have on at least two occasions, indirectly acknowledged the existence of the accumulation of events as a legal entity in two of its cases, Nicaragua (Merits)[56] and DRC v Uganda[57]. In the *Nicaragua* case, when considering if border attacks by Nicaragua into Honduras and Costa Rica could be considered as an armed attack, the ICJ said that: 'Very little information is however available to the Court as to the circumstances of these incursions or their possible motivations, which renders it difficult to decide whether they may be treated

---

[53] Norman Menachem Feder, Reading the U.N. Charter Connotatively: Toward a New Definition of Armed Attack, 19 N.Y.U. J. Int'l L. & Pol. 395 (1987) Content downloaded/ printed from HeinOnline Tue Mar 26 10:08:06 2019

[54] See Gazzini T, 'The rules and use of force at the beginning of the XXI century', 2006 11 JCSL p331; Gray, The use of force, p155; Ruys, T, 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, New York. First ed Paperback 2013. p169

[55] ibid, 37, p 171-172

[56] Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits, International Court of Justice (ICJ), 27 June 1986, available at: https://www.refworld.org/cases,ICJ,4023a44d2.html

[57]Armed Activities on the Territory of the Congo, Congo, the Democratic Republic of the v Uganda, Judgment, Merits, ICJ GL No 116, [2005] ICJ Rep 168, ICGJ 31 (ICJ 2005), 19th December 2005, International Court of Justice [ICJ]

for legal purposes as amounting, singly or collectively, to an "armed attack" by Nicaragua on either or both States.'[58]
This indicates that the Court did indeed consider that there are as yet undefined circumstances in which collective acts can indeed be considered an armed attack, yet that the justification for the case in hand failed due to a lack of factual information available to the Court.

Separately, in the *DRC v Uganda* case, the court considered if a series of attacks could be cumulative in nature: 'Even if this series of attacks could be regarded as cumulative in character, they still remained non-attributable to the DRC.'[59] While the court once again hinted that there might be a situation whereby a series of attacks could be considered as 'cumulative in character' enough to reach the sufficient gravity, the justification could not be confirmed in this case as it had already failed on the matter of attribution.

In each of these three examples (Israel, Nicaragua and Uganda) the accumulation of events was used as justification to prove that a chain of events could together fulfil the gravity requirement. Proving an armed attack had occurred triggering the right to use force in self defence. None of the arguments succeeded, yet this was demonstrably not due to a lack of 'gravity' but due to other factors. Suggesting that the 'accumulation of events' theory is accepted, yet to date, uncharted.

C. Intent

A final consideration in the material element of armed attack is that of intent. In order for an act to be classified as an 'armed attack', the case law of the ICJ requires that there must be hostile intent on the part of the attacker against a specific target state.

A 'massive' attack which clearly satisfies the gravity threshold, such as a missile attack on a neighbouring state would by its very nature imply a hostile intent. However, smaller more ambiguous attacks are harder to prove as being of a hostile intent, for example an accidental airspace incursion would likely be viewed by the court as unlikely to amount to an armed attack, but more likely to fall within the scope of a smaller 'frontier incident'. As Gray comments, 'the implication seems to be that the Court would include within 'frontier incident' episodes where there was no intent to carry out an armed attack, including accidental incursions and incidents where officials disobeyed orders'[60].

---

[58] *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits*, International Court of Justice (ICJ), 27 June 1986, available at: https://www.refworld.org/cases,ICJ,4023a44d2.html para 231

[59] ICJ, DRC v Uganda, Judgement of 19 December 2005, para 146

[60] Gray, C. International Law and the Use of Force (4th Edition), 15 February 2018. OUP. p154

The requirement for intent against the victim state was underlined in *the Oil Platforms*[61] *case* where the US had attacked Iranian offshore oil platforms, claiming to be acting in self defence after they alleged that the Iranian platforms had facilitated in 'armed attacks' against ships flagged to the US. In considering whether these acts constituted an armed attack, at paragraph 64 of the *Oil Platforms* case, the Court stated that: 'There is no evidence that the minelaying alleged to have been carried out by the *Iran Ajr*, at a time when Iran was at war with Iraq, was aimed specifically at the United States' and 'it has not been established that the mine struck by the *Bridgeton* was laid with the specific intention of harming that ship, or other United States vessel.' The court ruled that because it could not be proved that the attacks which occurred on the USA vessels were specifically aimed at US targets, then the attacks could not amount to an 'armed attack'.
Thus the prevailing law seems to imply that a host intent is indeed a prerequisite to a classification of a use of force as being an armed attack.

2.3.2 Ratione Personae

The second element in the armed attack requirement for self defence is the *ratione personae* element. This relates to 'who' conducted the illegal use of force. For example, was the use of force conducted by regular state forces or was it conducted by terrorist or non state actors? A right of self defence against an aggressor state arises only when the attack can be attributed to that state[62][63]. It is accepted that a use of force by the regular forces of a state would be attributed to that state as a direct attack. There are also some narrow circumstances whereby the indirect use of force by a state, such as private forces and non state actors, may be attributed to a state.
The characterisation of the use of private force as an act of aggression by a state emanates from Art. 3 (g) of the Definition of Aggression: 'The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein.' This was confirmed in the Nicaragua case[64] and reaffirmed in the *DRC v Uganda* case[65], when the court ruled that Uganda's actions in the DRC would only

---

[61] *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America*, International Court of Justice (ICJ), 6 November 2003, available at: https://www.refworld.org/cases,ICJ,414b00604.html

[62] Albrecht Randelzhofer, 'Article 51' in Bruno Simma et al (eds), *The Charter of the United Nations: A Commentary* (2nd edn, Oxford: Oxford University Press, 2002), 788, 802 (para 35-38)

[63] The issue of acts of force committed by armed terrorist groups not attributed to a state is a contested see: CJ Tams, 'The Use of Force against Terrorists' (2009) 20 EJIL 359, 378, and 382 outside the scope of this thesis and as such shall not be discussed in this section.

[64] *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits*, International Court of Justice (ICJ), 27 June 1986, available at: https://www.refworld.org/cases,ICJ,4023a44d2.html para 195

[65] *Armed Activities on the Territory of the Congo (DRC v. Uganda)*, Merits, Judgment of 19 Dec 2005, ICJ Rep 2005 168

qualify as self defence if there was 'satisfactory proof of the involvement in these attacks, direct or indirect, of the Government of the DRC'[66]
The test as to what qualifies as an indirect use of force falls largely to the interpretation as to the meaning of the two concepts of 'sending by or on behalf of a State' and/or 'substantial involvement' of armed groups by a State within the meaning of Art 3(g) of the Definition of Aggression.

Sending by or on behalf of a State

The general rule is that the smaller the nexus between the State and the private actor, the more likely that there will be proof of attribution. Secondary rules, codified in the Draft Articles on the Responsibility of States for Internationally Wrongful Acts (ARIWA) provide guidance in this area, as does relevant case law.

1. Complete dependency

Firstly is the 'complete dependency' category. This refers to people or groups of people who can be categorised as being so close to the State, that they act in complete dependency of the State. Case law, as established in *Nicaragua,* confirms this, holding that the status of State organ extends to 'persons, groups or entities act(ing) in "complete dependence" of the State of which they are ultimately an instrument.'[67]

This includes those that hold the status of being a 'State organ' by internal law. This derives from Article 4 of the Articles on the Responsibility of States for Internationally Wrongful Acts (ARIWA):

> 'A State organ includes 'any person or entity which has that status in accordance with the internal law of the State'[68].

2. Effective control

Second to the 'complete dependence' category is the 'effective control' category. This stems from Article 8 ARIWA:

> 'conduct of a person or group of persons shall be considered an act of a State under international law if the person or persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.'[69]

---

[66] DRC v Uganda, ibid, para 146

[67] *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits*, International Court of Justice (ICJ), 27 June 1986, available at: https://www.refworld.org/cases,ICJ,4023a44d2.html para 109

[68] Article 4(2) ARIWA

[69] Article 8 ARIWA

The relevant case law[70] has evolved so as to narrow this meaning. The appropriate test in determining conduct 'under the direction and control' of a State, is crucially whether or not that State has 'effective control' over the conduct, and specifically, only in situations whereby the State 'directed and controlled the specific operation and the conduct complained of was an integral part of that operation.'[71]

3. Acknowledges and adopts

Even if unlawful conduct is not imputable to a State because it falls outside one of the above two categories, Article 11 ARIWA provides that:

> 'Conduct which is not attributable to a State under the preceding articles shall nevertheless be considered an act of that State under international law if and to the extent that the State acknowledges and adopts the conduct in question as its own.'[72]

This was confirmed in the *Tehran Embassy*[73] case, when although acts conducted by militants had failed to be attributed to Iran thus far, the court found that official approval of the actions taken by the militants by Iran translated to attribution: 'The approval given to these facts by the Ayatollah Khomeini and other organs of the Iranian State, and the decision to perpetuate them, translated continuing occupation of the Embassy and detention of the hostages into acts of that State. The militants, authors of the invasion and jailers of the hostages, had now become agents of the Iranian State for whose acts the State itself was internationally responsible.'[74]

Substantial involvement

This prong deals with the level of involvement a State has with an unlawful conduct. The parameters of the scope of State responsibility are dictated by relevant case law, which has the effect of raising the bar in what constitutes substantial involvement by a State.

---

[70] See *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits*, International Court of Justice (ICJ), 27 June 1986, available at: https://www.refworld.org/cases,ICJ,4023a44d2.html para 195*; Prosecutor v. Dusko Tadic (Appeal Judgement), IT-94-1-A, International Criminal Tribunal for the former Yugoslavia (ICTY), 15 July 1999*

[71] ibid, 37, page 412

[72] Article 11 ARIWA

[73] *United States Diplomatic and Consular Staff in Tehran, United States v Iran*, Judgment, ICJ GL No 64, [1980] ICJ Rep 3

[74] ibid, para 74

In *Nicaragua*[75], 'the ICJ did not suggest under what circumstances an involvement must be taken to be substantial enough as to amount to an armed attack'[76] yet they 'implicitly excluded the mere tolerating of an armed group's presence within a State's territory'[77] and explicitly required assistance to amount to more than 'assistance to rebels in the form of the provision of weapons or logistical or other support'[78].

2.3.3 *Ratione temporis*

The *ratione temporis* element of the armed attack requirements is the element which deals with the determination of at what moment in time a use of force may be classified as an armed attack.
The subject is hotly contested in academic circles and the doctrine is far from a settled area of the law.
It is uncontested that the right to unilateral self defence exists when an armed attack has occurred or is in the process of occurring, derived from the plain meaning of Article 51 of the UN Charter 'Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs…'[79] The contentious issue is whether or not the use of force in self defence may be invoked in anticipation of an armed attack[80].

Anticipatory self defence

The disagreement stems from scholars on one hand claiming that Article 51 precluded any other form of self defence than that specified within it and those on the other hand pointing to the long standing customary right to self defence established in the *Caroline* case[81]. The *Caroline* test required that self defence would be lawful when 'the necessity of that self-defence is instant, overwhelming and leaving no choice of means, and no moment for deliberation.'[82]
As Nolte observes, opinion settled on the latter interpretation: 'a prevailing opinion among commentators today seems to accept that the right of self-defence entails a very narrow right

---

[75] *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits*, International Court of Justice (ICJ), 27 June 1986

[76] Albrecht Randelzhofer, 'Article 51' in Bruno Simma et al (eds), The Charter of the United Nations: A Commentary (2nd edn, Oxford: Oxford University Press, 2002), 788, 802 (para 34)

[77] ibid, 34, page 415

[78] ibid, 74, para 195

[79] Charter of the United Nations, 24 October 1945, 1 UNTS XVI Article 51

[80] Ashley S. Deeks, Ch.29 Taming the Doctrine of Pre-Emption, in Marc Weller (ed) Part III The Prohibition of the Use of Force, Self-Defence, and Other Concepts, The Oxford Handbook of the Use of Force in International Law (2015) p661

[81] The Caroline v. United States, 11 U.S. 7 (Cranch 496) (1813)

[82] Webster, Daniel. 'Letter to Henry Stephen Fox', in K.E Shewmaker (ed.). *The Papers of Daniel Webster: Diplomatic Papers, vol. 1. 1841-1843* (1983) 62. Dartmouth College Press. ISBN 978-0-87451-245-8

to anticipatory self-defence, either along the lines of the *Caroline* formula or even narrower. In a variation of the *Caroline* formula, the UN High-level Panel on Threats, Challenges and Change stated in 2004 without further qualification that 'a threatened State, according to long established international law, can take military action as long as the threat is imminent, no other means would deflect it and the action is proportionate'.[83]As such, this led to the most contested meaning in the doctrine being what constitutes an 'imminent threat'.
In the post 9/11 era, there has been an increasingly compelling argument that the customary law now extends to include pre-emptive use of force, and even more broadly, preventative use of force. Deeks defines pre-emptive self-defence as 'the use of force in self-defence to halt a particular tangible course of action that the potential victim state perceives will shortly evolve into an armed attack against it'[84] and distinguishes this from preventative self defence, which he defines as 'the use of force in self-defence to halt a serious future threat of an armed attack, without clarity about when or where that attack may emerge.'[85]
States that have adopted a broader understanding of the meaning have been headed up by the US, as demonstrated first in the US 2002 National Security Strategy[86] and by later as justifications for actions *inter alia* the use of force in self defence in Operation Iraqi Freedom[87]. A justification supported by its allies in the Operation. Other States which have also specifically expressed support for the broader understanding include: Australia, Russia, North Korea, Iran and India. Conversely, States such as Turkey, Argentina and Mexico have expressly voiced concern and opposition to the expanding doctrine.
For now, the doctrine is not settled, and is not as yet enshrined by any case law. Pointedly, the ICJ would not comment upon on the lawfulness of a 'response to the imminent threat of armed attack' in the *Nicaragua*[88] case. However, the doctrine does appear to be either directly or tacitly accepted among a growing number of States.

Repel vs Reprisal

The temporal aspect not only refers to anticipatory self defence, but also is a major factor in determining if an act of self defence is indeed necessary in order to repel an aggressor, or whether it is more likely to be classified as a reprisal. For instance, in *Nicaragua,* the court

---

[83] G Nolte, A Randelzhofer, Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Article 51, in Bruno Simma et al (eds) The Charter of the United Nations: A Commentary, Volume II (3rd Edition) page 1423 para 52

[84] Deeks, A. Ch.29 Taming the Doctrine of Pre-Emption, in Marc Weller (ed) Part III The Prohibition of the Use of Force, Self-Defence, and Other Concepts, The Oxford Handbook of the Use of Force in International Law (2015) p662

[85] ibid p663

[86] 2002 US National Security Strategy, 15. See also Sean D. Murphy, The Doctrine of Preemptive Self-Defense, 50 Vill. L. Rev. 699 (2005). Available at: https://digitalcommons.law.villanova.edu/vlr/vol50/iss3/9

[87] See Sapiro, Miriam. "Iraq: The Shifting Sands of Preemptive Self-Defense." *The American Journal of International Law*, vol. 97, no. 3, 2003, pp. 599–607. *JSTOR*, www.jstor.org/stable/3109845.

[88] *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits*, International Court of Justice (ICJ), 27 June 1986, available at: https://www.refworld.org/cases,ICJ,4023a44d2.html paras 102 - 106

stated that: ‘measures were only taken, and began to produce their effects, several months after the major offensive of the armed opposition against the Government of El Salvador had been completely repulsed (January 1981) and the actions of the opposition considerably reduced in consequence. Thus it was possible to eliminate the main danger to the Salvadorian Government without the United States embarking on activities in and against Nicaragua.'[89] Thus demonstrating that actions taken long after an alleged armed attack, would in most circumstances not be lawful.

2.4 Chapter Summary

This chapter has established that for the right of a use of force in self defence to be activated, an armed attack must first have occurred against the victim State. For an act to be considered, in international law, an armed attack, the following three elements are required:
Firstly, the *ratione materiae* element, within which the following components are required: The existence of an unlawful act of force against a state; which must meet the required gravity threshold, individually or cumulatively as per the accumulation of events theory; of which there must be a hostile intent specifically against the victim state.
Secondly, the *ratione personae* element requires the aggressor to be a State, if the aggressor is a non State actor, then the non State actors must operate in complete dependancy of the State concerned or the State must have effective control over them. Absent these conditions, conduct can be attributable to a State if it acknowledges or adopts the unlawful conduct or a non state actor as its own; there is a minimum threshold as to what constitutes substantial involvement by a State in an unlawful act which excludes the supply of weapons or logistical support including the tolerating of an armed group on its territory.
Thirdly, the *ratione temporis* element gives that use of force in self defence must be in one of the following conditions: it must be exercised only once an actual armed attack has taken place or is in the process of occurring; it may be anticipatory as long as the threat is imminent, the doctrine of pre-emptive or preventative defence is contested yet appears to have growing support in recent State practice and *opinio juris;* use of force in self defence might not be lawful if it is exercised too long after an armed attack has occurred.

[89] ibid para 237

Chapter 3: Hybrid Warfare

3.1 Introduction

This chapter will aim to understand the notion of hybrid warfare by examining its origins, uses and current academic content and commentary on the subject.
The first section examines how Russia and China have successfully developed and harnessed hybrid warfare as a means to achieve gains in recent operations. The second section extrapolates these findings, together with expert opinions in order to understand the most recently accepted characterisation of hybrid warfare. The third section in the chapter narrows down the scope of the threat that hybrid warfare poses in general to the threat that hybrid warfare poses to international law. Specifically, to the 'armed attack' threshold.

3.2. Origins and definition

Hybrid warfare is an umbrella term, increasingly used over the past two decades to describe the interchangeable conditions, strategy and tactics which have been adopted by States in recent conflicts. Frank Hoffman, one of the earliest adopters of the term, defined hybrid warfare as "Any adversary that simultaneously employs a tailored mix of conventional weapons, irregular tactics, terrorism, and criminal behaviour in the same time and battle-space to obtain their political objectives."[90]
Although it can be argued that Hybrid Warfare has always existed in the warfighters toolbox[91] the modern phenomenon is often traced back to, and thus characterised, by Russia's annexation of Crimea and by China's encroachment into the South China Sea and its operations regarding Taiwan:[92][93]

i. Russia

In 2010, Russian doctrine stated that:

> "the integrated utilization of military force and forces and resources of a nonmilitary character," and objectives such as "the prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a

---

[90] Hoffman, F. (2014) "On Not-So-New Warfare: Political Warfare vs. Hybrid Threats," War on the Rocks (blog), July 28, 2014, http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybridthreats/

[91] For examples see: Williamson Murray & Peter R. Mansoor eds., 2012. Hybrid Warfare: Fighting Complex Opponents From The Ancient World To The Present.

[92] Hybrid Warfare with Chinese Characteristics By Michael Raska at https://www.rsis.edu.sg/wp-content/uploads/2015/12/CO15262.pdf

[93] It must also be noted that the issue regarding Taiwan and China is far from settled, for an overview see https://www.cfr.org/backgrounder/china-taiwan-relations

> favorable response from the world community to the utilization of military force."[94]

Three years later, Mark Galeotti coined the phrase 'Gerasimov Doctrine' on his blog 'In Moscow's Shadows'. The blog post included the, now famous, translation by Robert Coalson of Radio Free Europe/Radio Liberty of a 2013 speech by the Russian Chief of the General Staff Valery Gerasimov[95].
Together, these examples were the first introduction to The West of a new way of Russian strategic thinking, a strategy which throws off the bonds of traditional war/peace divisions. Gerasimov's Speech has since become synonymous with describing Russian Hybrid Warfare. The speech itself is still a very important document in conceptualising, particularly for organisations such as NATO, Russian operations in previous conflicts and current activities, such as in the Baltics. The following excerpt outlines the key parts of the speech/doctrine[96]:

> *'In the 21st century we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template.*
> *The experience of military conflicts — including those connected with the so-called coloured revolutions in north Africa and the Middle East — confirm that a perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war.'...*
> *'The very "rules of war" have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness.*
> *The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other nonmilitary measures — applied in coordination with the protest potential of the population.*
> *All this is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special-operations forces.* ***The open use of forces — often under the guise of peacekeeping and crisis regulation — is resorted to only at a certain stage, primarily for the achievement of final success in the conflict****.'...*
> *'New information technologies have enabled significant reductions in the spatial, temporal, and informational gaps between forces and control organs. Frontal engagements of large formations of forces at the strategic and operational level are gradually becoming a thing of the past. Long-distance, contactless actions against the enemy are becoming the main means of achieving combat and operational goals. The defeat of the enemy's objects is conducted throughout the*

---

[94] Translated version of 2010 Russian Military doctrine "The Military Doctrine of the Russian Federation," February 5, 2010, by Carnegie available at http:carnegieendowment.org/files/2010russia_military_doctrine.pdf. (Kofman and Rojansky 2015)

[95] Original blog post by Galeotti, M, with updated prologue can be found here: https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

[96] Emphasis in bold is mine.

> *entire depth of his territory. The differences between strategic, operational, and tactical levels, as well as between offensive and defensive operations, are being erased. The application of high-precision weaponry is taking on a mass character. Weapons based on new physical principals and automatized systems are being actively incorporated into military activity.*
> *Asymmetrical actions have come into widespread use, enabling the nullification of an enemy's advantages in armed conflict.* ***Among such actions are the use of special-operations forces and internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as informational actions, devices, and means that are constantly being perfected.****'*

By making reference to a permanently operating front and to using a full range of political, economic, informational, humanitarian, and other nonmilitary measures as well as the protest potential of the population, special forces and information technology to promote informational conflict, the intent is clear. These means are meant to undermine the sovereignty of a state but without resorting to open warfare to do so.

Although not intended a formal Russian doctrine, after Russia's operations in Georgia and Ukraine, the 'Gerasimov Doctrine' has been widely cited as being a blueprint as to how Russia were to go on to conduct its operations there. To date, Russia still occupies Crimea[97] and has extended its influence in the Eastern and Southern parts of Ukraine, including parts of the Black Sea and control of access to the Sea of Azov. Its success in the region giving grounds to the belief that Russia will employ the same tactics in future conflicts. For example, in the Declaration following NATO's 2014 Wales Summit[98] NATO condemned Russia's actions in Ukraine and, specifically addressed the future threat posed by Russia by her use of Hybrid Warfare.

ii. China

The observations on the Chinese use of hybrid warfare derives from more official means. The US Department of Defense Annual Report to Congress on the Military and Security Developments involving the Peoples Republic of China (PRC) in 2011[99] recognised the official Chinese concept of 'The Three Warfares' as[100]:

> '*The Chinese concept of "three warfares" (san zhong zhanfa) refers specifically to psychological warfare, media warfare, and legal warfare. It reflects China's desire to effectively exploit these force enablers in the run up to and during hostilities. During military training and exercises, PLA troops employ the three warfares to undermine the spirit and ideological commitment of the adversary. In essence,* ***it is a non-military tool used to advance or catalyze a military objective****.*

---

[97] UN resolution A/Res/74/194 of 17 December 2019 https://undocs.org/en/A/RES/73/194

[98] https://www.nato.int/cps/en/natohq/official_texts_112964.htm

[99] Office of the Secretary of Defense. Annual Report to Congress – Military and Security Developments involving the PRC 2011. P.26.
Available here: https://dod.defense.gov/Portals/1/Documents/pubs/2011_CMPR_Final.pdf

[100] Emphasis in bold is mine.

Psychological Warfare seeks to undermine an enemy's ability to conduct combat operations through operations aimed at deterring, shocking, and demoralizing enemy military personnel and supporting civilian populations.

Media Warfare is aimed at influencing domestic and international public opinion to build support for China's military actions and dissuade an adversary from pursuing actions contrary to China's interests.

Legal Warfare uses international and domestic law to claim the legal high ground or assert Chinese interests. It can be employed to hamstring an adversary's operational freedom and shape the operational space. Legal warfare is also intended to build international support and manage possible political repercussions of China's military actions. China has attempted to employ legal warfare in the maritime domain and in international airspace in pursuit of a security buffer zone.

In 2003, the CCP Central Committee and the CMC endorsed the three warfares concept, reflecting China's recognition that as a global actor, it will benefit from learning to effectively utilize the tools of public opinion, messaging, and influence. China likely hopes to employ these three concepts in unison, particularly during the early stages of a crisis, as they have a tendency to bolster one another.'

The three warfares doctrine is a key strategic tool[101] in China's campaign to re-unite Taiwan with China[102]and also in the campaign to reclaim land in the South China Sea[103] In both cases, the Three Warfares doctrine has been successfully used to advance China's interests without triggering a conventional conflict. The Three Warfares doctrine shares the same attributes as Gerasimov's Doctrine, whereby all the components accross the political, economic, informational, legal and non-military spectrum are aimed at undermining a state's sovereignty in the support of a military campaign whilst avoiding amounting to traditional means of warfare.

iii hybrid warfare in action

Before the conflict in Crimea, hybrid warfare was widely referred as a being a model for contemporary warfare tactics amongst defence communities[104]. However, after 2014, the

---

[101] Raska, M, China and the 'Three Warfares', The Diplomat, December 18, 2015. Available here: https://thediplomat.com/2015/12/hybrid-warfare-with-chinese-characteristics-2/

[102] China has a special unit based out of the Nanjing Military Region's 311 Base (also known as the Public Opinion, Psychological Operations, and Legal Warfare Base) in Fuzhou City, Fujian Province. Ibid, Raska, M, China and the 'Three Warfares', The Diplomat, December 18, 2015. Available here: https://thediplomat.com/2015/12/hybrid-warfare-with-chinese-characteristics-2/

[103] The building in the South China sea continues contra to the ruling in the South China Sea Arbitration Case Philippines v. China (PCA Case number 2013-19)

[104] Such as NATO's own comprehensive approach.http://www.natolibguides.info/comprehensiveapproach

Crimea annexation is referred to as characterising hybrid warfare. It is therefore important to unravel how it was conducted in order to more readily understand the concept.

The annexation unfolded in an escalation from the political, through to a full occupation. BBC news reports recorded a timeline of events in Ukraine that escalated from political protests, political unrest, separatist activity, little green men and then finally overt Russian use of force[105]. In accordance with this, many post-fact testimonies have revealed a similar story, such as Damon M. Wilson[106] who submitted a testimony to the Subcommittee on Europe and Regional Security Cooperation Hearing on Russian Aggression in Eastern Europe. The testimony details a timeline of events showing a progression of activities which started with the sparking of spontaneous revolts using 'political tourists' from Russia, targeted information operations across the media and the introduction of Special Forces and intelligence operatives and 'Putin's little green men' in order to further destabilize eastern Ukraine before the final stage culminated with a full-scale invasion and support to separatists with arms and troops.

On its website, The Ministry of Foreign Affairs of Ukraine said that alongside military aggression, the following elements of hybrid warfare were used in the annexation or Crimea and subsequent operations in Ukraine: '1. Propaganda based on lies and falsifications, 2. Trade and economic pressure, 3. Energy blockade, 4. Terror and intimidation of Ukrainian citizens, 5. Cyber attacks; 6. A strong denial of the very fact of war against Ukraine despite large scope of irrefutable evidence; 7. Use of pro-russian forces and satellite states in its own interests; 8. Blaming the other side for its crimes.'[107]

Likewise, Toth[108] cites a wide range of sources which compare hybrid warfare to asymmetric warfare, however he also draws similarities between hybrid warfare and Cold War era Soviet Active Measures. 'Russian Hybrid Warfare is really nothing new in the sense that it is a revival and a modernisation of the Cold War era's Soviet Active Measures - intelligence and paramilitary operations were considered as part of a major weapons system for conducting covert warfare. Active measures were utilised to influence and manipulate events and behaviour in foreign societies through influencing the policies of

---

[105] See https://www.bbc.com/news/world-middle-east-26248275

[106] Testimony by Damon M. Wilson Executive Vice President, Atlantic Council US Senate Committee on Foreign Relations, Submitted to the Subcommittee on Europe and Regional Security Cooperation Hearing on Russian Aggression in Eastern Europe: Where Does Putin Go Next After Ukraine, Georgia and Moldova? March 4, 2015. A Transatlantic Strategy to Deter Putin's Aggression

[107] Ministry of Foreign Affairs of Ukraine website. Article: 10 facts you should know about Russian military aggression against Ukraine (19 December 2019 17:40) https://mfa.gov.ua/en/10-facts-you-should-know-about-russian-military-aggression-against-ukraine accessed 6 May 2020

[108] Gergely Toth, Legal Challenges in Hybrid Warfare Theory and Practice: Is there a Place for lLegal Norms at All? In The Use of Force against Ukraine and International Law, Jus Ad Bellum, Jus In Bello, Jus Post Bellum. TMC Asser Press, The Hague, The Netherlands, 2018

other governments, undermining or building up leaders and groups in these states, and undermining opponents through support for opposition political and armed groups.'[109]

These observations place emphasis on the use of asymmetric elements in hybrid attacks. The next section will examine how official sources have tried to define and characterise the concept of hybrid warfare.

3.3 Chacteristics vs a definition

Although a clear definition is far from settled, the examination of the key commonalities between the above two doctrines together with the a more widespread use, for instance in Ukraine, Georgia, the Baltics, has over recent years resulted in the ability to gain some clarity on what constitutes hybrid warfare overall. NATO, at the Wales Summit described Hybrid Warfare as being:

> 'where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design.'[110]

The Multinational Capability Development Campaign (MCDC)[111] headquartered within the NATO Allied Command Transformation, Operational Experimentation Branch, have devoted significant resources in developing a definition. Its project on Countering Hybrid Warfare (CHW) settled (for the time being) on describing hybrid warfare as being:

> 'the synchronised use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects'[112] with the researchers concluding that 'hybrid warfare is asymmetric and uses multiple instruments of power along a horizontal and vertical axis, and to varying degrees shares an increased emphasis on creativity, ambiguity, and the cognitive elements of war. This sets hybrid warfare apart from an attrition-based approach to warfare where one matches the strength of the other, either qualitatively or quantitatively, to degrade the opponent's capabilities.'[113]

More recently, the EEAS have expanded upon this, describing hybrid warfare as characterised (again, rather than defined) as:

---

[109] ibid page 176-177

[110] Para 13, 2014 NATO Wales Summit Declaration https://www.nato.int/cps/en/natohq/official_texts_112964.htm

[111] The Multinational Capability Development Campaign (MCDC) series is an initiative led by the United States designed to collaboratively develop and assess concepts and capabilities to address the challenges associated with conducting joint, multinational and coalition operations. https://www.act.nato.int/images/stories/media/opex/2019_MCDC_FUTLEAD.pdf

[112] Dr. Patrick J. Cullen and Erik Reichborn-Kjennerud, MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare, MCDC January 2017, Page 8 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

[113] ibid

> ‘a centrally designed and controlled use of various covert and overt tactics, enacted by military and/or non-military means, ranging from intelligence and cyber operations through economic pressure to the use of conventional forces. By employing hybrid tactics, the attacker seeks to undermine and destabilise an opponent by applying both coercive and subversive methods.’[114]

These resources, together with an analysis of the activities utilised in real life cases, allow for the extraction of three main pillars of activities from the spectrum of activities outside of the use of overt military force which comprise the hybrid warfare ‘toolbox’[115] these are:

1. Disinformation operations.
2. Cyber attacks.
3. Use of Non-State actors (proxy forces etc).

These activities shall form the basis of the application of the legal framework to hybrid warfare in the part two of this thesis.

3.4 Legal Implications.

The Council of Europe Parliamentary Assembly identified that alongside its asymmetric nature, hybrid warfare uniquely targets the legal domain. It said that successful employment of hybrid warfare relies heavily upon exploiting weaknesses within the international legal system. In its report on Legal challenges related to the hybrid war and human rights obligations[116], the Assembly stated that:

> ‘States are more and more often confronted with the phenomenon of “hybrid war”, which poses a new type of threat based on a combination of military and non-military means’… ‘hybrid war can destabilise and undermine entire societies and cause numerous casualties. The increasingly widespread use of these new tactics, especially in combination, raises concerns about the adequacy of existing legal norms…’[117]

> 'The Assembly notes that there is no universally agreed definition of “hybrid war” and there is no “law of hybrid war”. However, it is commonly agreed that the main feature of this phenomenon is “legal asymmetry”, as hybrid adversaries, as a rule, deny their responsibility for hybrid operations and try to escape the legal consequences of their actions. They exploit lacunas in the law and legal complexity, operate across legal boundaries and under-regulated spaces, exploit

---

[114] European Commission, Joint Framework on Countering Hybrid Threats: A European Union Response, JOIN(2016) 18 final (Apr. 6, 2016).

[115] Please note the delimitations on the thesis, which exclude nuclear, economic/political and espionage.

[116] Council of Europe, Parliamentary Assembly, Committee on Legal Affairs and Human Rights, Report: Legal challenges related to the hybrid war and human rights obligations

[117] ibid para 2

> legal thresholds, are prepared to commit substantial violations of the law and generate confusion and ambiguity to mask their actions.'[118]

The two main prongs of threats identified here as potentially affecting the adequacy of existing legal norms against hybrid warfare are:

1. Exploiting lacunas in the Law and exploit legal thresholds.
2. Target legal norms.

The first prong focusses on a use of the law itself by a hybrid aggressor as being permissive to allow a range of acts across the full political, economic, criminal, informational or cyber domains to shape an identified battlefield[119] without sanction by operating just under or by stretching the boundaries of legal thresholds. In armed conflict, as examined in chapter two, the relevant threshold concerned is the armed attack threshold. The determination of an armed attack being the trigger for a victim state to activate self defence measures.

The second prong concerns hybrid warfare targeting legal norms. Sari observes that 'In some cases, grave violations of international norms by hybrid actors may threaten "the rules-based international order" as a whole.'[120] This is because gross violations are considered spoiler behaviour[121], which is the practise of revisionist states who seek to change the world order to reflect their own world view.
Hybrid warfare is a direct threat in that by undermining the armed attack threshold, there is a risk that there will be a corresponding weakening of the normative value of the *jus ad bellum.*

3.5 Chapter summary

This chapter has aimed to describe what hybrid warfare is how and when it has been used.

While Hybrid warfare, as a form of warfare, can engage many levers and employ a wide range of acts. One key feature, or threat, is claimed to be the use of hybrid activities in order to exploit legal thresholds to achieve the same results as traditional warfare whilst simultaneously avoiding sanction. A second feature is that this utilisation in turn threatens the RBIS. Specifically, hybrid warfare exploits lacunas in the law around the 'armed

---

[118] Council of Europe, Parliamentary Assembly, Committee on Legal Affairs and Human Rights, Report: Legal challenges related to the hybrid war and human rights obligations, para 3

[119] For more information on the concept of shaping the battlefield or battlespace for War see Chapter 5 in MCNEILLY, M. R. (2015). Sun Tzu and the Art of Modern Warfare: Updated Edition. Oxford University Press, USA. http://www.myilibrary.com?id=642422.

[120] Sari, Aurel, Hybrid Warfare, Law and the Fulda Gap (March 5, 2017). Christopher Ford and Winston Williams (eds), Complex Battle Spaces (OUP, 2019), 161–190. Page 29

[121] For background information on spoiler behaviour see: Stedman, S. (1997). Spoiler Problems in Peace Processes. *International Security, 22*(2), 5-53

attack' threshold. The three main activities which exemplify the hybrid toolbox are: 1. Disinformation operations, 2. Cyber attacks. 3. Use of Non-State actors (proxy forces etc).

The next chapter will go on to apply the law on armed attack to hybrid warfare with reference to case examples of the activities utilised in Ukraine by Russia.

Part 2 - Analysis

As identified in first part of this thesis, hybrid warfare has been claimed to be successful in that it strategises the known legal gaps or grey areas in the doctrine of armed attack and targets the armed attack threshold in order to undermine it.

Part two of this thesis shall proceed by examining the competency of the notion of armed attack through two lenses. The first lens, examined in Chapter 4, is the single activities lens. In this lens, each individual activity utilised in hybrid attack shall be tested in turn against the legal framework in relation to case studies. The second lens, examined in Chapter 5, is the composite hybrid attack lens. This lens shall apply the doctrine of accumulation of events to hybrid activities taken together as a composite whole.

Chapter 4: Lens 1 - Individual Hybrid Warfare Elements

4.1 Introduction

This Chapter shall apply the legal framework surrounding the notion of armed attack identified in Chapter 1, against examples of case studies which fall within the categories of the individual hybrid activities identified in Chapter 3. These activities are: Information Operations; Cyber attacks; Armed groups.

4.2 Disinformation Operations.

In a report of Russian grey zone activities in Europe, Morris et al identified information operations as including the following: Attacking alternative messages and shaping public opinion to destabilize targeted states, influence local political outcomes, or both.[122] Likewise, in the same paper, the authors noted that Chinese information operations include using… 'media, and propaganda mechanisms against regional states to justify China's claims to sovereignty or to uphold the moral authority of its actions. In the international sphere, such actions include discrediting or responding to other countries' sovereignty claims over islands and maritime space in the ECS and SCS, as well as coordinating campaigns to get nonaligned countries to support China's position on disputed territory.'[123]

Cohen and Radin[124] catalogue that Russia have been, and are continuing to use information operations to conflate ethnic tensions in the Baltic States pointing to examples *inter alia* inciting riots in Estonia in 2007 and protests in Lithuania[125].

Finally, Shandra and Seely document the use of disinformation campaigns by Russia in Ukraine since before 2013 to create a 'fake reality'[126] leading up to the use of methods such as the financing of protestors by Russia in the Maidan protests in 2014 which directly contributed to the destabilisation of Ukraine government which was a key factor in the annexation of Crimea.[127]

---

[122] Morris, Lyle J., Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe, *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*, Santa Monica, Calif.: RAND Corporation, RR-2942-OSD, 2019. As of May 18, 2020: https://www.rand.org/pubs/research_reports/RR2942.html page 18

[123] ibid page 36

[124] Cohen, Raphael S. and Andrew Radin, *Russia's Hostile Measures in Europe: Understanding the Threat*, Santa Monica, Calif.: RAND Corporation, RR-1793-A, 2019. As of May 12, 2020: https://www.rand.org/pubs/research_reports/RR1793.html page 41

[125] International Center for Defense and Security, "Russia's Involvement in the Tallinn Disturbances," May 11, 2007

[126] Alya Shandra and Robert Seely, The Surkov Leaks The Inner Workings of Russia's Hybrid War in Ukraine, Published in 2019 by the Royal United Services Institute for Defence and Security Studies. Chapter 3

[127] ibid, Chapter 5

It is not therefore uncontroversial to assert that a disinformation campaign, such as the ones detailed above, which interfere with the political affairs of a target State would amount to a breach in the sovereignty[128] of that State. A breach of sovereignty is well known to be prohibited in Customary International Law[129] under the principle of non intervention[130] and was explicitly prohibited in the UN Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty[131]. However, does interference and/or intervention amount to an armed attack?

Ratione materie

As per the International law on the notion of attack, the first consideration as to whether an activity, such as a disinformation operation, would amount to an armed attack, is the *ratione materie* requirement, which requires that a use of force has occurred or is threatened.

Could a disinformation operation amount to a use of force by qualifying as an act of aggression under GA Resolution 3314?

Disinformation operations are not listed as one of the acts of aggression in Article 3 of GA Resolution 3314, although, the list is not exhaustive and as stated in Article 4 of Resolution 3314 'the Security Council may determine that other acts constitute aggression under the provisions of the Charter'.

---

[128] In the Corfu Channel Case Judge Alvarez, in his individual opinion, described sovereignty as: 'by sovereignty 'we understand the whole body of rights and attributes which a State possesses in its territory, to the exclusion of all other states, and also in its relations with other States'.
Oppenheim later described sovereignty as 'In as much as it excludes subjection to any other authority, and in particular the authority of another state, sovereignty is independence. It is external independence with regard to the liberty of action outside its borders. It is internal independence with regard to the liberty of action of a state inside its borders. As comprising the power of a state to exercise supreme authority over all persons and things within its territory, sovereignty involves territorial authority'.See Corfu Channel Case (United Kingdom v. Albania); Merits, International Court of Justice (ICJ), 9 April 1949, and Oppenheim, L. (1996), Oppenheim's International Law, Vol. 1: Peace, 9th edn, Jennings, R. Y. and Watts, A. (eds), London; New York: Longmans, p. 382.

[129] The general prohibition on intervention is widely accepted in international law, originating from Vattel. See*: The Law of Nations*, published in 1758. Oppenheim, ibid.

[130] *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits*, International Court of Justice (ICJ), 27 June 1986: 'The principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference'.

[131] UN General Assembly, Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, 21 December 1965, A/RES/2131(XX), available at: https://www.refworld.org/docid/3b00f05b22.html [accessed 20 May 2020]

However, the Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty seems to indicate that an interference or intervention cannot be considered as a use of force in that it explicitly distinguishes between armed activities and other forms of interference by way of listing each activity separately: 'no State shall organize, assist, foment, finance, incite or tolerate subversive, terrorist, or armed activities directed towards the violent overthrow of the regime of another State, or interfere in civil strife in another State.'[132]

In *Nicaragua*[133], the use of subversive activities was discussed in the context of non intervention: 'the Court defines the constitutive elements which appear relevant in this case: a prohibited intervention must be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely (for example the choice of a political, economic, social and cultural system, and formulation of foreign policy). Intervention is wrongful when it uses, in regard to such choices, methods of coercion, particularly force.' Here the court again appeared to exclude other methods of coercion by its explicit use of the word 'force'.

In this sense it would appear that a correct reading of the law is that although disinformation campaigns would be prohibited in international law by way of being a breach of sovereignty, and are a cause for serious concern in future conflicts, it is clear that they explicitly fall outside the classification of qualifying as a use of force and therefore they cannot be classified as being an 'armed attack'.

The use of disinformation campaigns specifically targets the *rationae materie* element of the armed attack threshold in that the activities fall short of being capable of classification as a use of force.

4.3 Cyber.

Jaluch and Hamulak[134] cite misuses of cyberspace as being evidenced in examples such as in the 2007 uprisings in Estonia, where distributed denial-of-service (DDoS) attacks were used to 'paralyse the web pages of important public authorities as well as some private sector providers'[135] contributing to the civil unrest in that country. The source of most of the attacks were attributed by Estonian authorities as stemming from inside Russia.
Likewise, Maurer and Janz[136] named DDoS attacks as being a critical element in the 2008 Georgia Conflict in that they 'primarily targeted Georgian government and news media

---

[132] ibid para 2

[133] *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits*, International Court of Justice (ICJ), 27 June 1986

[134] Valuch, Jozef & Hamulak, Ondrej. (2018). Cyber Operations During the Conflict in Ukraine and the Role of International Law: Jus Ad Bellum, Jus In Bello, Jus Post Bellum. Asser Press (2018) Page 223

[135] ibid p224

[136] Tim Maurer, Scott Janz, The Russia- Ukraine Conflict: Cyber and Information Warfare in a Regional Context 2014 at https://css.ethz.ch/en/services/digital-library/articles/article.html/184345/

websites, disrupting communication channels and generating confusion at a time of crisis.'[137]
In the Ukraine conflict, similar DDoS attacks occurred as well as cyber espionage and the use of malware as well as documented attacks against the Ukranian Central Election Commission.[138]

Other examples of cyber attacks include: The well documented[139] Stuxnet worm attack, which was said to originate from Israel and the USA and targeted Iranian nuclear facilities causing material damage. The Israeli 'Operation Orchard', which hacked a Syrian official's computer when in London in order to later facilitate a cyber attack in which Syrian air defences were 'blinded' (a real time air picture was replaced with an older air picture) so that an alleged nuclear complex could be bombed without detection.[140]

Does a cyber attack constitute an armed attack?

The panel of experts for the Tallinn Manual[141] confirmed with reference to the Nuclear Weapons advisory opinion[142] that 'the mere fact that a computer (rather than a more traditional weapon, weapon system, or platform) is used during an operation has no bearing on whether that operation amounts to a 'use of force' …but rather…the consequences of the operation and its surrounding circumstances.'[143] The panel of experts also stated that their analysis was based on the *lex lata* in the *jus ad bellum*[144]. Therefore it is reasonable to analyse whether a 'cyber attack' could qualify as an armed attack, as per the law laid out in Chapter 1 and with reference to the Tallinn Manual.

Ratione personae

The first factor is thus, once again, to ascertain whether the *ratione materie* element is fulfilled, firstly, the determination of whether the act is capable of being a use of force.
Although a cyber attack is not expressly mentioned in the GA Resolution 3314, the list is not exhaustive. Being that cyber attacks can manifest in a wide range of undetermined ways it appears that the authors of the Tallinn manual instead decided to concentrate on

---

[137] ibid

[138] ibid 130

[139] https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html

[140] https://www.wired.com/2009/11/mossad-hack/

[141] Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press.

[142] *Legality of the threat and use of nuclear weapons*, Advisory opinion 8 July 1996, ICJ Rep 226-67 Para 38-39

[143] Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press. page 328

[144] ibid page 329

the gravity and effects requirement to determine that a cyber attack is capable of being a use of force. As shown in Rule 69 - Definition of use of force:

> 'A cyber operation constitutes a use of force when its scale and effects are comparable to non cyber-operations rising to the level of a use of force.'[145]

In the determination of whether a cyber activity amounted to a use of force, the panel of experts utilised an approach by Michael N. Schmitt[146] which would assess the following non exhaustive factors based upon 'the level of harm inflicted and other qualitative elements of a particular cyber operation'[147]:
1. Severity of consequences involving physical harm to people or property. The greater the harm, the more likely the act is to be a use of force, (this factor is considered to be the most significant factor in the approach)[148]; 2. Immediacy of the consequences, the more immediate the results of an attack, the more likely the attack is to amount to a use of force; 3. Directness of cause and effect, the more direct the link, the more likely the act is to be a use of force; 4. Invasiveness, the higher the degree which an attack intrudes into a target State, the more likely it is to be classified as a use of force; 5. Measurability of effects, the more quantifiable and identifiable the consequences of an attack, the more likely it is to be a use of force; 6. Military character, the closer an attack represents a military operation, the more likely it is to be considered a use of force; 7, State involvement, the greater the extent of State involvement, the more likely the act is considered a use of force; 8, Presumptive legality, if the act is not *prima facie* illegal (eg, espionage, propaganda), it is less likely to be considered a use of force.[149]

When applying the first three examples of cyber attacks (above) to these factors, the fact that the DDoS attacks in Estonia, Georgia and Ukraine did not directly or immediately cause any consequences involving physical harm to people or property makes them less likely under the first three factors to be considered as a use of force. Likewise, because the attacks are not of a military character in that they do not take the form of a military action or target military installations, they will be less likely to be classified as a use of force and finally, as seen in the above section on information operations, these actions are in fact presumptively legal, making them less likely to be a use of force under the last factor. Finally, although some of the attacks can be traced back to Russian territory, there is not necessarily attribution to Russia as a State.
On the other hand, the cyber activities are all fairly invasive in nature, targeting political or government web pages and even election systems, the impact of which can be measured in

---

[145] ibid page 330

[146] Michael M. Schmitt, Computer Network and the Use of Force in International Law: Thoughts on a Normative Framework, 37 COLUM. J. TRANSNT'L L. 885, 914 (1999)

[147] Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press. page 333

[148] ibid page 334

[149] These factors have been abbreviated from the factors in the Tallinn Manual, ibid 135, pages 334-336

their effect (eg protest and uprisings), therefore, under factors four and five, these acts be classified as a use of force.
On balance, these activities would in theory not be regarded as meeting the threshold as being capable of being considered as a 'use of force'.

In contrast, when applying the same factors to the remaining two examples (The Stuxnet worm attack and the hacking activity and 'blinding' Syrian air defences in 'Operation Orchard'), the fact that in both incidences, material damage was caused to nuclear installations indicates that the consequences were more severe, the damage was manifested immediately in the Operation Orchard case, and both immediately and in further waves in the Stuxnet case, in both cases attacks were directly prosecuted against the targets, rather than incidental and were invasive in they were attacks on highly protected State nuclear facilities. The attacks were military in character and were attributed to State parties. Finally, an attack against a nuclear facility is not presumptively legal.
Under all factors, these attacks indicate that they are of a nature severe enough to be considered as a use of force.

As per chapter 2, not all attacks which constitute a use of force constitute an armed attack.

The next step in the *ratione materie* requirement and in distinguishing between a use of force and armed attack in a cyber context is that it must be discovered whether or not the gravity and effects reach the appropriate threshold as is the case in the determination of a non cyber armed attack where there must be a distinction between a frontier incident and a more 'grave' use of force.[150] Building from the use of force criteria of severity, the more severe the damage to critical infrastructure and individuals then the more likely that the attack is likely to be able to be categorised as an armed attack. In a cyber attack, being that the attack is not necessarily a kinetic attack, it is useful to consider that rather than physical damage inflicted by the attack, the severity of an attack can be judged by the consequences that are liable to be produced by the attack.[151]
Dinstein has given examples of other cyber attacks which would meet the gravity and effects to amount to an armed attack: 'Fatalities caused by loss of computer-controlled life-support systems; an extensive power grid outage (electricity blackout) creating considerable deleterious repercussions; a shutdown of computers controlling waterworks and dams, generating thereby floods of inhabited areas; deadly crashes deliberately engineered (e.g., through misinformation fed into aircraft computers), etc. The most egregious case is the wanton instigation of a core-meltdown of a reactor in a nuclear power plant, leading to the release of radioactive materials that can result in countless casualties if the neighbouring areas are densely populated'[152] Therefore, to apply this to the Stuxnet example given above, if the cyber attack had the potential to cause a nuclear

---

[150] *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits*, International Court of Justice (ICJ), 27 June 1986 para 195

[151] Dinstein, Y. (2017). *War, Aggression and Self-Defence*. Cambridge: Cambridge University Press. p193

[152] Dinstein, Y. (2002) Computer Network Attacks and Self - Defense, International Law Studies Vol 76, page 105

reactor to melt down in a Chernobyl-esque incident, with the associated damage to people, property or even to the environment then this would almost certainly meet the gravity and effects requirement to amount to push the attack from a use of force to an armed attack.
The final stage in the *ratione materie* requirement is intent. As in the *Oil Platforms*[153] case, it would be unlikely that a cyber attack that did not specifically target a victim state would demonstrate the requisite hostile intent. Indiscriminate cyber attacks are the most prolific form of attack, examples of which include: malware, ransomware, viruses, and worms[154], such attacks are often criminal or even self-proliferating, such as the Wanacry[155] randsomware and have a global reach. Due to the indiscriminate nature of these attacks, it would be hard for an affected State to prove that the attack was intended to target that State, even if it affected that State more than others.

Accumulation of events

The Tallin Manual stated that The International Group of Experts addressed the issue of accumulation of events with relation to cyber attacks and, agreed that if there is 'convincing evidence' that 'the same originator (or originators acting in concert) has carried out smaller-scale incidents that are related and taken together meet the requisite scale and effects … There are grounds for treating the incidents as a composite armed attack.'[156] Thus underlining the importance of the next element: *Ratione personae.*

Ratione personae

As laid down in Chapter 1, the *ratione personae* requires that the aggressor of an attack be attributed to a State.
In a cyber attack, the originator of an attack can, and often is, obscured easily by spoofing in incidents such as in the following example given by Roscini: 'State A attacks State B posing as State C by spoofing or manipulating transmission data to appear as if they originated from State C. In this case, State C appears to attack State B, which might take actions against an unaware State C.'[157] Therefore, in the occurrence of a Cyber attack it is arguable that the issue of attribution is of heightened importance and that due diligence in confirming the source of an attack is paramount, however, with the use of malware and

---

[153] *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America*, International Court of Justice (ICJ), 6 November 2003, available at: https://www.refworld.org/cases,ICJ,414b00604.html

[154] https://www.anomali.com/blog/targeted-vs-indiscriminate-attacks

[155] https://www.anomali.com/blog/wanacry

[156] Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press. Page 342

[157] Marco Roscini , Cyber Operations and the Use of Force in International Law . Oxford : Oxford University Press , 2014 ,page 77

spoofing techniques endemic in a in a cyber context, attribution of a cyber attack is very difficult.[158][159]

A second scenario could be that a non-State actor or a terrorist organisation could conduct spoofing operations in the same way as State A in the example above. In this case, the Tallinn manual confirmed that the same rules on attribution will be in force in the event of a cyber attack[160]. Thus, any attack which is prosecuted by a private actor who is under 'complete dependence' or under the 'effective control' of a State, can be attributed to the State in question[161]. Likewise, if the State assumes responsibility by acknowledging and adopting the attack, it will be attributable to the state in question. As Ruys highlights, attribution even in a non cyber environment is very difficult in that it is highly unlikely a State will explicitly acknowledge or adopt an armed attack by a non state actor as its own and that the standards by which to prove 'complete dependence' and 'effective control' are so high that they will almost never be reached.[162] Taking into account this, together with the integral difficulty in attribution in a cyber setting, attribution to a State by a non-State actor will be extremely difficult.

In a third scenario, State C in the above example could have explicitly allowed a State or a Non-State actor to route through it, or to use it's infrastructure to facilitate the cyber attack on state B. In this case State B would have to have been proven to have substantial involvement in the planning and execution of the attack. In *Nicaragua* this involvement was found to have to be greater than 'the mere tolerating of an armed group's presence within a State's territory'[163] and amount to more than 'assistance to rebels in the form of the provision of weapons or logistical or other support'[164]. This is widely acknowledged[165] to be a high standard to reach outside of a cyber context, and thus could prove harder to reach within a cyber context, although not impossible.

Ratione Temporis

Anticipatory self defence

---

[158] 'Perhaps the most difficult problem is that of attribution', P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar* (New York/Oxford: OUP Press, 2014, p. 73.

[159] For an in depth understanding of this, see: Thomas Rid & Ben Buchanan (2015) Attributing Cyber Attacks, Journal of Strategic Studies, 38:1-2, 4-37

[160] Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press. Page 344

[161] See section on *ratione personae* in Chapter 1 above.

[162] Ruys, T, 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, New York. First ed Paperback 2013. page 414

[163] Ibid page 415

[164] *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits*, International Court of Justice (ICJ), 27 June 1986 Para 195

[165] See Gray C, The use of force, page 130-132

If the doctrine of pre-emption was accepted (see section in chapter 1) in a non cyber context, it is equally applicable in a cyber context. The doctrine was accepted by the experts in the Tallinn manual and as per rule 73, a right of self defence arises if a cyber armed attack occurs or is imminent in the same way as it does in a non cyber attack. The experts however put extra importance on the requirement of immediacy[166].

4.4 State and Non-State actors.

Whilst the law is relatively clear on when a use of force by regular military forces (and likewise, private military contractors who operate directly on behalf of a State) is deemed an armed attack[167]. In a hybrid setting, the middle ground in between information operations and direct military use of force is less clear. This is evidenced in situations such as those that occurred in the conflict in eastern Ukraine and in the annexation of Crimea, this section shall proceed with reference to the two major 'middle ground' actors which have been evidenced to have operated in that conflict. Namely 'little green men' and separatist militias:

'Little green men'

On the morning on February 27, 2014, it was reported that 'heavily armed men wearing green uniforms with no identifying insignia stormed the regional parliament in Simferopol, the capital of Ukraine's Crimean Peninsula, and raised the Russian flag atop the building'[168]. Additional reports confirmed the existence of men with a similar description throughout Crimea and blockading Ukrainian military bases.[169] The phrase 'little green men' became synonymous with describing these mysterious forces.
Initially Russia actively denied that these were Russian troops[170], claiming they were local 'self defence groups', the denials were given by President Putin himself[171] and by high level officials such as Russian Foreign Minister Sergei Lavrov "Who are these pro-Russian forces? We have no control over them. They don't receive our orders." [172]

---

[166] Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press. Pages 350 - 354

[167] See Chapter 1

[168] https://www.rferl.org/a/from-not-us-to-why-hide-it-how-russia-denied-its-crimea-invasion-then-admitted-it/29791806.html

[169] ibid and https://www.bbc.com/news/world-europe-26532154

[170] Euronews interview with Vladimir Chizov see: https://www.youtube.com/watch?v=calO_Z1F6D4

[171] https://www.npr.org/sections/thetwo-way/2014/03/04/285653335/putin-says-those-arent-russian-forces-in-crimea?t=1590235318330

[172] https://www.ft.com/content/617b9516-a443-11e3-9cb0-00144feab7de

However, after a year of denial, in March 2015, Russia finally did admit that the 'little green men' were in fact spetsnaz[173] Although Russia claimed that they were deployed legitimately in self-defence of the Russian speaking population in Crimea.[174]

The 'little green men' events unfolded over three phases: 1. Unidentified forces on Ukrainian territory, no indication of origin, official denial by Russia of involvement. 2. Unidentified forces on Ukrainian territory, indications of Russian origin, official denial by Russia of involvement. 3. Forces on Ukrainian territory, indications of Russian origin, official Russian statement that the forces are Russian acting in self defence of Russian nationals/Russian-speaking population of Ukraine/Ethnic Russians.

Examining this from a legal perspective, the use of unidentifiable troops mostly targets the *ratione personae* aspect within the legal determination of the occurrence of an armed attack. However, because the elements are interlinked, and because the *ratione personae* aspect is targeted, this then has follow on implications for the *ratione materie* and *ratione temporis* aspects. As such this section shall proceed by examining the *ratione personae* aspect in the phases identified above:

Phase 1

Article 2(4) of the UN Charter[175] prohibits the use of force by a State upon another State. Likewise, the Advisory Opinion of the ICJ in *Legal Consequences of the Construction of a Wall* 'recognizes the existence of an inherent right of self-defence in the case of armed attack by one State against another State.[176]' Thus excluding the use of force against a non-State affiliated actor.
In the case of the 'little green men', the lack of insignia and the official denial of involvement by Russia coupled with the Russian claims that the men were 'local self defence groups' which Russia 'knew nothing about', casted doubt as to the origin of the groups. If the groups were indeed local Ukrainians then this would preclude their actions as being of an international nature and thus incapable of being a use of force, and thus unable to reach the threshold of being an armed attack.

Phase 2

---

[173] According to reports, President Putin said on a Russian language documentary "In order to block and disarm 20,000 well-armed [Ukrainian soldiers], you need a specific set of personnel. And not just in numbers, but with skill. We needed specialists who know how to do it," see: https://www.rferl.org/a/from-not-us-to-why-hide-it-how-russia-denied-its-crimea-invasion-then-admitted-it/29791806.html

[174] See speech by Russian Federation, High-Level Segment - 1st Meeting, 25th Regular Session Human Rights Council available at: http://webtv.un.org/meetings-events/human-rights-council/watch/russian-federation-high-level-segment-1st-meeting-25th-regular-session-human-rights-council/3282328996001/?term=&lan=russian

[175] Charter of the United Nations, 24 October 1945, 1 UNTS XVI, Art. 2

[176] Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion) [2004] ICJ Rep 136, para 139

As speculation and reports began to mount that the groups originated from Russia, the absence of any concrete proof of official involvement by Russia coupled with the continued denial of any official involvement in the Ukraine conflict by Russia still left open the possibility that the men could be an independent, private armed group. In this case, since International law requires that for the group to be attributable to Russia the group must have 'complete dependence' on Russia or that Russia have 'effective control'[177] of, or 'substantial involvement'[178] in the groups activities. Russia's continuing denial of any association with the group meant that this level of involvement was thrown into doubt.
The repeated denials by officials also ensured that Russia could not be held accountable for the groups actions under the 'acknowledge and adopt' exception[179].

Phase 3.

When Russia admitted that the armed groups were in fact Russian spetsnaz, they did so by claiming that they were exercising self-defence in the protection of Russian nationals, ethnic Russians and Russian speaking Ukrainians.
Russia had relied on the self defence of nationals doctrine in justifying its actions in the previous Georgia conflict[180]. After Georgia had attacked the capital city of South Ossetia, Russia intervened with the conflict reaching Abkhazia and the rest of Georgia over the next five days. Although the justification was rejected by the UN, it was based on the argument that Russia had used unnecessary and disproportionate amounts of force in going beyond South Ossetia. However, the self defence argument itself was not challenged by the UK or the USA as they had previously used the justification of self defence themselves.[181]
The legality for protection of nations in Ukraine would likely be based upon the same justification as Russia argued in their intervention in Georgia. In that case, Russia claimed to have been acting in accordance with Article 51[182], which was not contested. Any justification for Russia's intervention in Crimea would need to be proven on facts.

---

[177] *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits*, International Court of Justice (ICJ), 27 June 1986

[178] ibid

[179] *United States Diplomatic and Consular Staff in Tehran, United States v Iran*, Judgment, ICJ GL No 64, [1980] ICJ Rep 3

[180] Gray, C 'The Protection of Nationals abroad: Russia's Use of Force in Georgia', in Constantinides and Zaikos (eds), *The Diversity of International Law* (2009) 133

[181] Gray, C, International Law and the Use of Force, 4th Edition (15th February 2018), Chapter 4. Pages 165-169; For UK intervention in Suez see: 'Armed Intervention in the 1956 Suez Canal Crisis: the Legal Advice tendered to the British Government', 37 ICLQ (1988) 773; For USA intervention in Panama see 'Armed Intervention in the 1956 Suez Canal Crisis: the Legal Advice tendered to the British Government', 37 ICLQ (1988) 773

[182] Charter of the United Nations, 24 October 1945, 1 UNTS XVI Article 51

In the Georgian case, the protection of nationals was based on protecting individuals who had recently been given Russian passports. This was not considered to be legitimate as the conferral of passports was considered dubious and as a possible pretext to intervention.[183]
On the facts, being that the nationals were in fact Ukrainian, the Crimean case seems even less robust that the Georgian pretext, meaning that it would be unlikely that the justification would pass scrutiny. If this was the case then, the Russian intervention could be considered a use of force. As per the law on *ratione materie* this would likely qualify as an armed attack.

Phase three, the admittance by Russia of the fact that the 'little green men' were in fact Russian soldiers, occurred one year after the initial deployment of the 'little green men' on Ukrainian soil. Crimea was annexed in less than a month, on 18 March 2014[184]. The ambiguity successfully caused by an obfuscation of attribution of the forces to Russia when time was of the essence. This enabled a delay in the determination of the armed group which undermined Ukraine and its allies' ability to make decisions and in turn, to execute self defence.
As Malcher observes '[the use of] Spetsnaz troops created ambiguity: it allowed Russia to deny any involvement in the Ukraine conflict and was also designed to create a climate of indecision among multi-national organisations such as NATO, the EU and political systems based on the principles of consensus, when deciding on what actions to take'[185].

Separatist militias.

Mulford describes the separatist militias in eastern Ukraine as being 'known opportunists from backgrounds as organised criminals, mercenaries, Cossacks or Chechens'[186], existing since the annexation of Crimea and recruiting from both inside Ukraine, specifically eastern Ukraine as well as from Russia and acting independently of Putin[187].
The shooting down with a Russian designed BUK TELAR missile system of the MH17 Malaysian airlines flight was initially attributed to such separatists[188]. Russia denied any responsibility for the incident, or any association with the separatists. President Putin alleged that the weapons system used in the downing of the aircraft belonged to the

---

[183] Grey C, The use of force in International Law: A Case-Based Approach, ed's Tom Ruys, Olivier Corten, Alexandra Hofer, Oxford University Press, 26 Apr 2018 p723

[184] 'On March 18, Crimean and Russian officials signed the Treaty of Accession of the Republic of Crimea to Russia. Putin ratified the treaty three days later.': Pifer, S, Crimea: Six years after illegal annexation, Tuesday, March 17, 2020 at https://www.brookings.edu/blog/order-from-chaos/2020/03/17/crimea-six-years-after-illegal-annexation/

[185] Malcher, A, Russian Spetsnaz – Ukraine's Deniable 'Little Green Men' May 2105 at: https://moderndiplomacy.eu/2015/05/10/russian-spetsnaz-ukraine-s-deniable-little-green-men/

[186] Mulford, J. (2016). Non-State Actors in the Russo-Ukrainian War. *Connections, 15*(2), 89-107.

[187] ibid

[188] See Official Dutch safety report Crash MH17 17 July 2014, dated 13.10.2015 at: https://www.onderzoeksraad.nl/en/page/3546/crash-mh17-17-july-2014

Ukrainian military[189]. However, in the subsequent official investigations of the shoot down, Dutch officials released recordings[190] of intercepted phone calls between separatist leaders in Ukraine and political leaders in Russia which proved that the BUK TELAR had in fact belonged to the 53rd Anti Aircraft Missile Brigade from Kursk in Russia and was provided to the separatists complete with a crew during the period of the shooting down of MH17. The investigation also charted the transfer of the BUK TELAR system from Russia to Ukraine and back again. The investigation, in a wider sense, indicated that Russia was in fact exercising a degree of control over the separatist forces, issuing guidance and assisting with weapons and personnel.

The legal issue targeted by a hybrid aggressor by the use of armed groups is once again the *ratione personae* element in that it obscures attribution.

With the evidence of the information gained by the Dutch investigation, to what extent can the actions of the separatist groups be imputable to Russia?
The three considerations in this case are as follows: 1. The existence of armed militia acting on Ukrainian territory with possible Russian links. 2. Conversations between leaders of separatists and Russian leaders. 3. Proof of the supply of weapons and personnel to the militia in Ukraine.
I shall now proceed to discuss these considerations, under the law of attribution via firstly 'sending by on behalf of a State' to address the first two considerations, and secondly under the 'substantial involvement' method to address the final consideration[191]

'Sending by on behalf of a State.'

1. As previously confirmed in Chapter 1, for the conduct of the separatists in eastern Ukraine to be attributable to Russia, the group must either act in 'complete dependency' of Russia or Russia must have effective control over the group. Complete dependency requires that the separatists have 'that status in accordance with the internal law of the State'[192] to the extent 'which they are ultimately an instrument.'[193] since this would mainly apply to civil servants, or other such state organs does not apply to this case.

2. As per the legal framework, conduct of the militia can also be imputed to Russia if it can be proven that Russia has 'effective control' over the group. Conversations unearthed between the leaders of the separatists and Russia indicate that there is at least some influence or control over the militia. Case law restricts this to cases whereby the state 'directed and controlled the specific operation and the conduct complained of was an

---

[189] https://apnews.com/450ba5218bf24c6a9d5052cc346cbc4a/The-Latest:-Putin-denies-Russia-responsible-for-MH17-downing

[190] https://www.politie.nl/themas/flight-mh17/witness-appeal-crash-mh17-june-19.html

[191] It must be noted here that Russia has denied any involvement with the militia, thereby ensuring it has not acknowledged or adopted the unlawful conduct as its own.

[192] Article 4(2) ARIWA

[193] *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits*, International Court of Justice (ICJ), 27 June 1986

integral part of that operation.'[194] The Dutch investigation did in fact document conversations whereby a 'Suspect [named] Dubinsky asks if 'it' has come with a crew. Apparently, 'it' refers to the BUK TELAR which belonged to the 53rd Anti Aircraft Missile Brigade from Kursk in the Russian Federation.'[195] Whilst this conversation can help towards proving that weapons were supplied to the Militia by Russia, the standard which requires that the Russian leadership directed and controlled the specific operation (of the MH17 shoot-down] would require much more specific proof, in this case.

'Substantial involvement'

3. There is a very high threshold as to what constitutes substantial involvement by a State in an unlawful act. The threshold has been criticised as being almost impossible to meet[196] and it has not yet been confirmed when the threshold will be met in court. However it has ruled that involvement must amount to more than the supply of weapons or logistical support including the tolerating of an armed group on its territory.[197] Sending the BUK TELAR weapons system by itself will likely not be sufficient to cross this threshold, however by sending a crew together with the BUK TELAR system onto Ukrainian soil, would cross the minimum threshold and could be argued to push the involvement level to indicate the requisite substantial involvement by Russia.
The point is largely moot, since because both the crew and the weapon system are Russian, this would in fact amount to regular Russian forces being deployed onto Ukrainian soil and thus anyway be considered a use of force. The usual deliberations would then be taken to ascertain whether this use of force amounted to an armed attack.

As is the case with the 'little green men' it is clear that Russia is involved with separatist militias, this tactic largely enables Russia to evade attribution even in cases whereby the nexus between both actors is proven to be very small. These stringent requirements in ascertaining attribution give the advantage to an aggressor state in undermining the target state's assessments in its right to self defence.

4.5 Chapter summary

It is clear from the analysis of the above cases that the strategy of a hybrid aggressor in using a wide range of fragmented 'under threshold' activities to achieve an objective (such as the annexation of Crimea, as detailed above) can and does target specific elements within the legal framework to remain under the overall threshold in the determination of an armed attack.

As seen above, disinformation campaigns target the *ratione materie* element as they are designed so as not to reach the threshold to be considered a use of force. Cyber attacks

---

[194] Ruys, T, 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, New York. First ed Paperback 2013., page 412

[195] https://www.politie.nl/themas/flight-mh17/witness-appeal-crash-mh17-june-19.html

[196] ibid,196, pages 415-418

[197] *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits*, International Court of Justice (ICJ), 27 June 1986

target the *ratione materie* element in much the same way; cyber attacks in a hybrid sense mostly consist of DDoS attacks and other low level attacks, which in themselves do not reach the requisite gravity and effects criteria. Cyber attacks also target the *ratione personae* element in that the use of spoofing can mask attribution to an aggressor. Likewise, the use by a State of non State actors targets the *ratione personae* element in that it undermines the ability of the target State to ascertain, to the certainty required, the origin of armed groups so as to delay decision making processes and the use of force in self defence.

This section thus demonstrates that when facing a hybrid attack, the effectiveness of the notion of armed attack as a threshold in triggering the right to self defence is eroded when each of the activities are considered against it individually.

Chapter 5 : Lens 2 - Composite Hybrid Attack

5.1 Introduction

As shown in Chapter 2, Hybrid warfare uses a mix of traditional activities and non-traditional activities in combination across a vertical and horizontal axis[198]. As discovered in Chapter 3, many of the individual activities utilised, short of an overt use of force by regular forces, do not cross the threshold for reaching an armed attack, or are deliberately utilised in such a manner so as to delay the decision making process of a target state, eroding the competence of the armed attack threshold to encompass hybrid warfare.
This Chapter shall proceed to examine how the outcome would be different if the activities are taken together, as a composite whole, and utilising the accumulation of events theory.

As laid out in Chapter 1, the accumulation of events theory is accepted by a large number of States, both in practice and in *opinio juris* and by a large number of academics. In Nicaragua the wording of the court to determine if an armed attack had occurred was 'singly or collectively' confirmed that composite activities could be considered together to determine if an armed attack had occurred, this is not controversial. Its invocation has thus far never succeeded as justification for use of force taken in self defence in any case brought before a court. The doctrine remains a currently uncharted offshoot to the armed attack threshold in that no test has yet been elucidated from the courts. It is therefore necessary to look to academic sources to extract a workable framework by which to apply to the context of a hybrid attack.
Whilst it is uncontested that the accumulation of events doctrine 'deals with situations where consecutive attacks take place that are linked in time, source and cause'[199] the doctrine has grown to refer to a specific, vertical understanding which links together only activities which are described as 'less grave uses of force', whilst a simultaneous (and perhaps unintended) by-product has been to exclude the linking together of other activities for the same purpose.

This section will proceed in two parts: In the first part, I analyse hybrid warfare against this mainstream, vertical understanding of the accumulation of events doctrine. In the second part, I propose that the accumulation of events theory should also be understood in a horizontal manner and that this second understanding better applies to the conditions of a hybrid attack.

5.2 Use of Force Interpretation

This understanding of the accumulation of events doctrine has evolved in its use in amplifying the gravity or *de minimis* threshold in a vertical manner, within a specific

---

[198] Dr. Patrick J. Cullen and Erik Reichborn-Kjennerud, MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare, MCDC January 2017, Page 8 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

[199] Ruys, T, 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, New York. First ed Paperback 2013. page 168

timeframe as conducted by the same actor (or actors). The understanding is best described by Ruys who writes that the accumulation of events theory[200], 'concerns the *de minimis* threshold' for assessing when the gravity of an attack is grave enough to be considered an armed attack. Specifically, that in connecting a chain of individual incidences of 'less grave' uses of force together, they will 'qualitatively transform into an armed attack'[201]
Thus, in this understanding, the events which may be considered to be included as part of the composite whole has been funnelled down so as to include only activities which are uses of force.

In this sense, when applying the accumulation of events doctrine to the same hybrid activities as in the cases in Chapter 4, two effects are observed:
1. It would *prima facie* exclude any consideration of disinformation activities or low-level cyber attacks no matter how invasive or far reaching the effects, as they are not likely to be considered a use of force.
2. Only a high-level cyber attack or the use of little green men/militia could be taken into account as being capable of being classified as a use of force. These activities could not in practice immediately, if at all, be classified as uses of force, due to obfuscation in attribution.

In using this funnelled understanding of the theory of accumulation of events, the armed attack threshold is not likely to be triggered in a hybrid warfare scenario as it is characterised by engaging a variety of non use of force activities together with low level uses of force, rather than solely comprising multiple uses of low level acts of force such as repeated border incursions.
In this sense, the notion of armed attack would not be competent to encompass hybrid warfare.

However, it is the present author's view that this funnelled understanding exists not due to theoretical limitations but rather because it has grown incidentally based on the cases presented thus far in Court. The majority of previous cases centre on activities which by their very nature, are uses of force. Such as small border incursions, cross border bandit attacks, airspace incursions and raids[202].

5.3 Overall Campaign Interpretation

An analysis of the accumulation of events doctrine demonstrates that most academic understandings of the theory of accumulation of events specify no such restriction that all incidents should be uses of force, in fact it is often the reverse. As shall now be shown:

---

[200] Remark: Aside from its usefulness in facilitating a necessity and proportionality calculation and the potential the doctrine has for supporting arguments of pre emptive self defence

[201] ibid 201

[202] See the examples given ibid, pages 168- 175

For example, Levenfeld's formula[203], states that the doctrine applies when the series of attacks are part of a 'continuous, overall plan of attack.'[204] Although the example in question referred to small raids, there is no suggestion that the accumulation must apply solely to a *de minimis* threshold in a 'vertical' understanding, rather that the emphasis be on the proviso that the attack be continuous in nature and most importantly, the component attacks be part of an 'overall attack'.

Likewise, Feder, when describing Israels' invocation of the theory in its self defence against PLO terrorist attacks, wrote that 'the totality of the incidents may demonstrate a systematic campaign of minor terrorist activities that does rise to the intolerable level of armed attack'[205]. Emphasis in this understanding can be placed on the 'systemic campaign' requirement. Once again this does not indicate a specific requirement to link together 'uses of force' but rather that the events be linked together in an overall campaign. He also referred to 'activities' in general rather than specifying that all the activities be required to be a more narrowly understood 'use of force'.

In concert, Blum referred to 'the totality of needle pricks'[206] as being understood in 'the broader context of violence to which that state has been subjected' as well as going on to acknowledge subversive activities as being in the context of accumulation of events [207]. Once again, reference to a 'broader context of violence' indicates support for the existence of an overall campaign not limited to proving the crossing of a gravity requirement solely based on uses of force.

In reference to accumulation of events, Yoram Dinstein wrote that 'it is not required to scrutinise every single incident independently (often in vain) to show that it meets the standard of 'sufficient gravity'. A persuasive argument can be made that, should a distinctive pattern of behaviour emerge, a series of pin-prick assaults may be weighed in its totality and count as such as an armed attack.'[208] Again, here the emphasis is on a 'distinctive pattern of behaviour' and there is no exclusion of counting activities that are not a use of force.

---

[203] Levenfeld, B, Israel's Counter-Fedayeen Tactics in Lebanon: Self-Defense and Reprisal under Modern International Law, 21 Colum. J. Transnat'l L. 1 (1982-1983) page 41

[204] ibid 201 p168

[205] Feder, N: Reading the U.N. Charter Connotatively: Toward a New Definition of Armed Attack 19 N.Y.U. J. Int'l L. & Pol. 395 1987, page 415

[206] Accumulation of events theory is also referred to as the needle prick theory.

[207] 'It has also been rightly observed that a long series of subversive activities may sometimes put the target state in greater jeopardy than one single massive conventional blow'. In Blum, Y. 'State response to acts of terrorism', (1976) 19 GYBIL pg 235

[208] Dinstein, Y. (2001). *War, Aggression and Self-Defence*. Cambridge: Cambridge University Press. 3rd ed. Page 203

In the Dissenting Opinion of Judge Jennings in *Nicaragua*[209]*,* the coupling of activities which do not amount to a use of force such as 'logistical or other support' with the 'provision of arms' was mooted as having the potential to amount to an armed attack. Indicating that it could be considered that non uses of force can be applied in an accumulation of events situation when coupled with less grave uses of force such as supplying weapons.

When considering if the accumulation of events theory applied to Cyber attacks, the International Group of Experts who participated in writing the Tallinn manual agreed that 'the determinative factor is whether the same originator (or originators acting in concert) has carried out smaller scale incidents that are related and that taken together, meet the requisite scale and effects. If there is convincing evidence that this is the case, there are grounds for treating the incidents as a composite armed attack'[210]. Once again there is no requirement that the individual incidents be a 'use of force'. If this was the case, the word incidents would not have been chosen over 'use of force'.

Taken together, it is clear that there is no requirement that all of the events in an accumulation of events context need be individual uses of force. The golden thread is to prove that the activities are all part of an 'overall campaign'.
In applying this understanding, we must remain cognisant that the overall campaign must still adhere to the overall requirement in that it encompasses all of the elements of an armed attack.
As Dinstein takes pains to point out 'An armed attack postulates a use of force causing human casualties and/or serious destruction of property. When recourse to force does not engender such results, Article 51 does not come into play.[211]' In applying this, then the overall campaign must therefore engender these same results, namely causing human casualties and/or serious destruction of property.
Dinstein also points out that any recourse to self defence 'should be put to the test whether it amounts to legitimate self-defence (in response to an armed attack), satisfying the requirements of necessity, proportionality and immediacy[212].' Indicating that the usual framework for armed attack still exists around the accumulation of events. In the broader sense, if this is accepted, then an application of the doctrine would follow the same process as for individual acts. By replacing 'use of force' with 'overall campaign' within the *ratione materie* element. I propose the following framework:

1. *Ratione materie*: Act: Activities that are linked together as part of an overall campaign; Gravity and effects: That the overall campaign meets, or is capable of meeting, the requisite scale and effects of an armed attack; Intent: That the overall campaign is directed against a target State.

---

[209] *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits*, International Court of Justice (ICJ), 27 June 1986 Dissenting Opinion of Judge Jennings

[210] Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press. Page 342

[211] Dinstein, Y. (2001). *War, Aggression and Self-Defence*. Cambridge: Cambridge University Press. p174

[212] ibid p203

2. *Ratione personae*: The overall campaign is conducted by the same originator or originators.

3. *Ratione temporis*: Within an accepted timeframe.

This application still follows the accepted 'time, source, cause' descriptor, which is not disputed, however avoids an unnecessary and unhelpful funnelling of the included activities to being solely a 'use of force'. In this understanding, the application of the doctrine to hybrid warfare is practicable, the *ratione temporis* and *ratione personae* elements still provide that the armed attack threshold is held at the same high threshold so as not to be watered down, whist the *ratione materie* element is clarified so as to take into account the nature of hybrid warfare. For example, the use in concert of disinformation campaigns, cyber attacks, armed groups and little green men, all demonstrate an overall campaign exists. By taking into account the combined scale and effects of these activities, the combined cost in terms of human casualties and/or damage to property is appreciated. Any resort to force within the meaning of Article 51 is done so in line with the concomitant rules on necessity and proportionally which help to guard against abuse of the doctrine.

If this understanding of accumulation of events is accepted, then the armed attack threshold is competent to encompass hybrid warfare in this way.

5.4 Perspective

As already established in the above section on the legal implications of hybrid warfare, there are two major threats that emerge with its use. First, the hybrid nature of hybrid warfare deliberately uses multiple levers and activities underneath the armed attack threshold in order to bring about the same effects as a large scale armed attack. The aim is to do this without detection, and with impunity. The second threat is that by undermining legal thresholds, hybrid warfare targets the very legal norms that exist in the current RBIS.

Strengthening the understanding of the armed attack threshold to understand hybrid warfare as an overall campaign helps to give clarity that the use of hybrid activities to try and undercut thresholds is prohibited and will lead to consequences. This in turn provides increased resilience in this area of the law. The intention of article 51 is not to prevent states from being able to exercise self defence, but rather to allow states to do so under the qualified condition that an armed attack exists. The armed attack also has the dual function of deterring States from utilising force as there are appropriate consequences.
Conversely if hybrid warfare, in its totality, can under no circumstances be classified as an armed attack then this will mean that the armed attack threshold would prove incompetent against hybrid warfare. Encouraging its use. This would then potentially result in a more nationalistic interpretation of self defence with reference to customary law in favour of Article 51 of the UN Charter. Which could lead to a deterioration of the authority of the UN Charter in general and a real watering down of the law regulating the use of force in self defence.

As Sari warns: ‘Nations committed to a rule-based international order must contest the legal domain against hybrid adversaries in a way that safeguards the normative values embedded in the law, including the dividing line between war and peace’[213]

5.5 Chapter Summary

Accumulation of events theory is largely accepted by States, by the Courts and by academics. However, it has been funnelled down a track which only takes into account that less grave uses of force can be accumulated together in order to cumulatively be considered as an armed attack. In re-examining the doctrine of accumulation of events, it is clear that this was incidental. It is therefore proposed that the doctrine be read to understand multiple activities as part of an 'overall campaign’ applied alongside the usual requirements to ascertain the existence of an armed attack. In this way hybrid warfare is properly encompassed by the armed attack threshold.

[213] Sari, Aurel, Hybrid Warfare, Law and the Fulda Gap (March 5, 2017). Page 35

Conclusions

In the analysis above, the following conclusions were made:

Hybrid warfare is one of the emerging key threats to the international peace and security landscape. It has been deployed by both Russia and China and it is characterised by the use of various activities which are utilised as part of an overall campaign designed not to trigger key thresholds such as the armed attack threshold. The key activities were identified as being: disinformation operations, cyber attacks and utilising non-State actors.

The only exception to the prohibition on the use of force in the UN Charter is the use of force in self defence in the event of an armed attack. The notion of armed attack was therefore analysed with reference to the doctrine on self defence. The framework pertaining to the determination of an armed attack comprises the following key elements *ratione materie*, *ratione personae* and *ratione temporis,* all of which must be met if an armed attack is accepted to exist. Each element consists of a body of legislation derived from *inter alia* jurisprudence, treaties, resolutions and academia. These elements were used as a framework by which to test whether hybrid warfare could amount to an armed attack. This was achieved through viewing a hybrid attack using two lenses; an individual activities lens and a composite activities lens.

The first lens assessed to what extent the notion of armed attack was capable to encompass hybrid warfare when each individual activity was analysed in turn.

It was found that most of the individual activities in a hybrid attack were inherently incapable of being classified as a use of force, or were utilised in such a way that it was unlikely they could cross the required *de minimis* threshold. Of the activities that could be classified in this way, attribution became an obstacle as most of the activities are employed in such a way to obscure the originator of the attack.

Due to the above issues, this method revealed that very few individual activities within a hybrid attack would trigger the use of self defence.

The second lens analysed the activities together as a composite hybrid attack with relation to the accumulation of events doctrine. The doctrine has been funnelled in such a way that it is understood by many legal scholars as being the joining together of a series of less grave uses of force to push the gravity of the totality of the incidents over the requisite *de minimi*s threshold to qualify as an armed attack. The use of this doctrine in this way does enable the notion of armed attack to encompass hybrid warfare in a more robust manner than by simply dealing with each action in turn. This understanding only allows less grave uses of force to be included in the overall gravity calculation, meaning that it still does not take into account all of the activities utilised and does not take into account the gravity and effects of the entire hybrid attack.

In analysing a cross section of legal scholars in the field, I was able to identify that the doctrine should not in fact have been funnelled in this manner. The common thread in determining which activities should be joined together as a composite whole is not that all of the activities be minor uses of force, but rather that the activities to be joined together are employed as part of an overall campaign. The gravity and effects of this overall campaign being the significant factor in measuring whether or not the *de minimis* threshold is crossed.

Viewed in this way, the accumulation of events doctrine serves to ensure that the notion of armed attack is competent to encompass hybrid warfare.

From these conclusions, this thesis demonstrates that, in answer to the question, ‘To what extent is the notion of armed attack capable to encompass hybrid warfare?’ That the notion of armed attack is only capable to encompass hybrid warfare to a minimal extent if each individual activity is assessed individually. However, it encompasses it to a much greater extent when utilising the accumulation of events doctrine, specifically when utilising the proposed ‘overall campaign’ understanding.

Bibliography

Legislation and other documents

Charter of the United Nations, 24 October 1945, 1 UNTS XVI, Art. 2

Charter of the United Nations, 24 October 1945, 1 UNTS XVI. Art. 51

Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, 24 October 1970, A/RES/2625(XXV)

International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, November 2001, Supplement No. 10 (A/56/10), chp.IV.E.1 - Article 4(2)

International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, November 2001, Supplement No. 10 (A/56/10), chp.IV.E.1 - Article 8

International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, November 2001, Supplement No. 10 (A/56/10), chp.IV.E.1 - Article 11

North Atlantic Alliance (5 September 2015). Wales Summit Declaration. Meeting of the North Atlantic Council, 4–5 September 2014.

Statement by the Soviet representative (UNGA 'Summary Record of the 105th mtg' (9 May 1973) UN Doc A/AC.134/SR.105, 16)

Statement by the United Kingdom representative (UNGA 'Summary Record of the 67th mtg' (30 July 1970) UN Doc A/AC.134/SR.67, 5) UN Doc A/RES/3314(XXIX)

UN Doc A/RES/3314(XXIX), Article 3

UN Doc A/RES/3314(XXIX), Article 4

UN General Assembly, Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, 21 December 1965, A/RES/2131(XX)

UN General Assembly, Rome Statute of the International Criminal Court (last amended 2010), 17 July 1998

UN resolution A/Res/74/194 of 17 December 2019

UNGA 'Colombia, Cyprus, Ecuador, Ghana, Guyana, Haiti, Iran, Madagascar, Uganda and Yugoslavia: proposal' (24 March 1969) UN Doc A/AC.134/L.16

Cases

Armed Activities on the Territory of the Congo, Congo, the Democratic Republic of the v Uganda, Judgment, Merits, ICJ GL No 116, [2005] ICJ Rep 168, ICGJ 31 (ICJ 2005), 19th December 2005, International Court of Justice [ICJ]

Armed Intervention in the 1956 Suez Canal Crisis: the Legal Advice tendered to the British Government', 37 ICLQ (1988) 773

Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits, International Court of Justice (ICJ), 27 June 1986

Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America, International Court of Justice (ICJ), 6 November 2003,

Corfu Channel Case (United Kingdom v. Albania); Merits, International Court of Justice (ICJ), 9 April 1949

ICJ, Oil Platforms Case, Rejoinder submitted by the United States of America, 23 March 2001.

Legality of the threat and use of nuclear weapons, Advisory opinion 8 July 1996, ICJ Rep

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion) [2004] ICJ Rep

Prosecutor v. Dusko Tadic (Appeal Judgement), IT-94-1-A, International Criminal Tribunal for the former Yugoslavia (ICTY), 15 July 1999

South China Sea Arbitration Case Philippines v. China (PCA Case number 2013-19)

The Caroline v. United States, 11 U.S. 7 (Cranch 496) (1813)

United States Diplomatic and Consular Staff in Tehran, United States v Iran, Judgment, ICJ GL No 64, [1980] ICJ Rep 3

Books

Dinstein, Y. *War, Aggression and Self-Defence*. Cambridge 3rd Ed (2017) Cambridge University Press

Deeks, A. Ch.29 Taming the Doctrine of Pre-Emption, in Marc Weller (ed) Part III The Prohibition of the Use of Force, Self-Defence, and Other Concepts, The Oxford Handbook of the Use of Force in International Law (2015)

Grey C, The use of force in International Law: A Case-Based Approach, ed's Tom Ruys, Olivier Corten, Alexandra Hofer, Oxford University Press, 26 Apr 2018

Gray, C, International Law and the Use of Force (3rd edn, OUP 2008) In The Charter of The United Nations - A Commentary, Volume II, OUP 2012, 3rd Edition edited by Simma, Bruno et al.

Gray, C, International Law and the Use of Force (4th Edition), 15 February 2018. OUP.

Gray, C 'The Protection of Nationals abroad: Russia's Use of Force in Georgia', in Constantinides and Zaikos (eds), *The Diversity of International Law* (2009)

Hoecke, Mark van. Methodologies of Legal Research : Which Kind of Method for What Kind of Discipline?.Oxford: Hart Publishing, 2013.

MCNEILLY, M. R. (2015). Sun Tzu and the Art of Modern Warfare: Updated Edition. Oxford University Press, USA.

Nolte, G and Randelzhofer, A. Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Article 51. In The Charter of the United Nations - A Commentary, Volume II, OUP 2012, 3rd Edition edited by Simma, Bruno et al.

Oppenheim, L. (1996), Oppenheim's International Law, Vol. 1: Peace, 9th edn, Jennings, R. Y. and Watts, A. (eds), London; New York: Longmans.

Randelzhofer, A 'Article 51' in Bruno Simma et al (eds), in *The Charter of the United Nations: A Commentary* (2nd edn, Oxford: Oxford University Press, 2002)

Roscini, M, Cyber Operations and the Use of Force in International Law . Oxford : Oxford University Press , 2014

Ruys, T, 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, New York. First ed Paperback 2013.

Schmitt, M, Computer Network and the Use of Force in International Law: Thoughts on a Normative Framework, 37 COLUM. J. TRANSNT'L L. 885, 914 (1999)

Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press.

Singer P.W. and Allan Friedman, *Cybersecurity and Cyberwar* (New York/Oxford: OUP Press, 2014

Toth, G. Legal Challenges in Hybrid Warfare Theory and Practice: Is there a Place for lLegal Norms at All? In The Use of Force against Ukraine and International Law, Jus Ad Bellum, Jus In Bello, Jus Post Bellum. TMC Asser Press, The Hague, The Netherlands, 2018

Valuch, Jozef & Hamulak, Ondrej. (2018). Cyber Operations During the Conflict in Ukraine and the Role of International Law: Jus Ad Bellum, Jus In Bello, Jus Post Bellum. TMC Asser Press, The Hague, The Netherlands, 2018

Articles and Reports

Blum, Y. 'State response to acts of terrorism', (1976) 19 GYBIL

Brownlie, Ian, The Use of Force in Self-Defense, 37 Brit. Y. B. Int'l L. 183 (1961)

Cohen, Raphael S. and Andrew Radin, *Russia's Hostile Measures in Europe: Understanding the Threat*, Santa Monica, Calif.: RAND Corporation, RR-1793-A, 2019

Council of Europe, Parliamentary Assembly, Committee on Legal Affairs and Human Rights, Report: Legal challenges related to the hybrid war and human rights obligations

Cullen (Dr.) P. and Reichborn-Kjennerud E, MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare, MCDC January 2017

Dinstein, Y. (2002) Computer Network Attacks and Self - Defense, International Law Studies Vol 76

European Commission, Joint Framework on Countering Hybrid Threats: A European Union Response, JOIN(2016) 18 final (Apr. 6, 2016).

Feder, Norman Menachem, Reading the U.N. Charter Connotatively: Toward a New Definition of Armed Attack, 19 N.Y.U. J. Int'l L. & Pol. 395 (1987)

Gazzini T, 'The rules and use of force at the beginning of the XXI century', 2006 11 JCSL

Hoffman, F. (2014) "On Not-So-New Warfare: Political Warfare vs. Hybrid Threats," War on the Rocks (blog), July 28, 2014
Malcher, A, Russian Spetsnaz – Ukraine's Deniable 'Little Green Men' May 2105 at: https://moderndiplomacy.eu/2015/05/10/russian-spetsnaz-ukraine-s-deniable-little-green-men/

Kofman and Rojansky (2015) Translated version of 2010 Russian Military doctrine "The Military Doctrine of the Russian Federation," February 5, 2010, by Carnegie

Levenfeld, B, Israel's Counter-Fedayeen Tactics in Lebanon: Self-Defense and Reprisal under Modern International Law, 21 Colum. J. Transnat'l L. 1 (1982-1983)

Maurer, T, Janz, S, The Russia- Ukraine Conflict: Cyber and Information Warfare in a Regional Context 2014 at https://css.ethz.ch/en/services/digital-library/articles/article.html/184345/

Morris, et al *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*, Santa Monica, Calif.: RAND Corporation, RR-2942-OSD, 2019

Mulford, J. (2016). Non-State Actors in the Russo-Ukrainian War. *Connections, 15*(2), 89-107.

O Corten, 'The Controversies Over the Customary Prohibition on the Use of Force: A Methodological Debate' (2006) 16 EJIL 803

Official Dutch safety report Crash MH17 17 July 2014, dated 13.10.2015 at: https://www.onderzoeksraad.nl/en/page/3546/crash-mh17-17-july-2014

Office of the United Nations High Commissioner for Human Rights Report on the human rights situation in Ukraine 16 November 2019 to 15 February 2020 (PDF). *OHCHR*.

Office of the Secretary of Defense. Annual Report to Congress – Military and Security Developments involving the PRC 2011.

Pifer, S, Crimea: Six years after illegal annexation, Tuesday, March 17, 2020 at https://www.brookings.edu/blog/order-from-chaos/2020/03/17/crimea-six-years-after-illegal-annexation/

Radin, Andrew, Hybrid Warfare in the Baltics: Threats and Potential Responses. Santa Monica, CA: RAND Corporation, 2017.

Raska, M, Hybrid Warfare with Chinese Characteristics at https://www.rsis.edu.sg/wp-content/uploads/2015/12/CO15262.pdf

Rid T, Buchanan B (2015) Attributing Cyber Attacks, Journal of Strategic Studies, 38:1-2, 4-37

"Russia's Involvement in the Tallinn Disturbances," International Center for Defense and Security, May 11, 2007

Sapiro, Miriam. "Iraq: The Shifting Sands of Preemptive Self-Defense." *The American Journal of International Law*, vol. 97, no. 3, 2003

Sari, Aurel, Hybrid Warfare, Law and the Fulda Gap (March 5, 2017).

Shandra A and Seely R, The Surkov Leaks The Inner Workings of Russia's Hybrid War in Ukraine, Published in 2019 by the Royal United Services Institute for Defence and Security Studies. Chapter 3

Stedman, S. (1997). Spoiler Problems in Peace Processes. *International Security, 22*(2)

Tams, C 'The Use of Force against Terrorists' (2009) 20 EJIL

Thiele, Ralph D, Focus on Defense and International Security Crisis in Ukraine – The Emergence of Hybrid Warfare, ISPSW Strategy Series. 2015

Wither, James K. "Making Sense of Hybrid Warfare." *Connections*, vol. 15, no. 2, 2016, pp. 73–87. *JSTOR.*

Williamson Murray & Peter R. Mansoor *eds., 2012. Hybrid Warfare: Fighting Complex Opponents From The Ancient World To The Present.*

Military Documents

2002 US National Security Strategy, 15. See also Sean D. Murphy, The Doctrine of Preemptive Self-Defense, 50 Vill. L. Rev. 699 (2005).

Correspondence/ Testimonies

Webster, Daniel. 'Letter to Henry Stephen Fox', in K.E Shewmaker (ed.). *The Papers of Daniel Webster: Diplomatic Papers, vol. 1. 1841-1843* (1983) 62. Dartmouth College Press. ISBN 978-0-87451-245-8

Testimony by Damon M. Wilson Executive Vice President, Atlantic Council US Senate Committee on Foreign Relations, Submitted to the Subcommittee on Europe and Regional Security Cooperation Hearing on Russian Aggression in Eastern Europe: Where Does Putin Go Next After Ukraine, Georgia and Moldova? March 4, 2015. A Transatlantic Strategy to Deter Putin's Aggression

Official web pages

https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html

https://www.nato.int/cps/en/natohq/topics_156338.htm

https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24762&lang=en

https://www.un.org/press/en/2016/sc12577.doc.htm

https://undocs.org/en/A/RES/73/194

https://www.nato.int/cps/en/natohq/official_texts_112964.htm

.http://www.natolibguides.info/comprehensiveapproach

https://www.act.nato.int/images/stories/media/opex/2019_MCDC_FUTLEAD.pdf

https://www.bbc.com/news/world-middle-east-26248275

Ministry of Foreign Affairs of Ukraine website. Article: 10 facts you should know about Russian military aggression against Ukraine (19 December 2019 17:40) https://mfa.gov.ua/en/10-facts-you-should-know-about-russian-military-aggression-against-ukraine

RAND web page on Information operations at https://www.rand.org/topics/information-operations.html

Speech by Russian Federation, High-Level Segment - 1st Meeting, 25th Regular Session Human Rights Council available at: http://webtv.un.org/meetings-events/human-rights-council/watch/russian-federation-high-level-segment-1st-meeting-25th-regular-session-human-rights-council/3282328996001/?term=&lan=russian

Other online resources

Galeotti https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

https://thediplomat.com/2018/01/chinas-hybrid-warfare-and-taiwan/

https://www.cfr.org/backgrounder/china-taiwan-relations

https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html

https://www.wired.com/2009/11/mossad-hack/

https://www.anomali.com/blog/targeted-vs-indiscriminate-attacks

https://www.anomali.com/blog/wanacry

https://www.rferl.org/a/from-not-us-to-why-hide-it-how-russia-denied-its-crimea-invasion-then-admitted-it/29791806.html

https://www.npr.org/sections/thetwo-way/2014/03/04/285653335/putin-says-those-arent-russian-forces-in-crimea?t=1590235318330

https://www.ft.com/content/617b9516-a443-11e3-9cb0-00144feab7de

https://apnews.com/450ba5218bf24c6a9d5052cc346cbc4a/The-Latest:-Putin-denies-Russia-responsible-for-MH17-downing

https://www.politie.nl/themas/flight-mh17/witness-appeal-crash-mh17-june-19.html