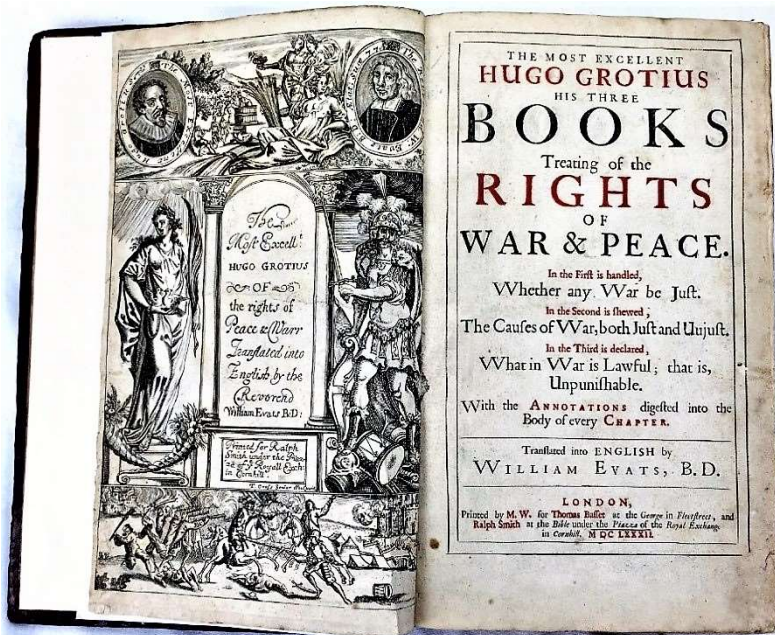


# Is Just War Theory a credible tool to explain contemporary war, globally?

by:  
Lloyd Pritchard





# Is Just War Theory a credible tool to explain contemporary war, globally?

---

by:  
Major Lloyd Pritchard RM

*Cover image:*

Hugo Grotius, *De iure belli ac pacis*, in the English translation of 1682.

The views expressed in this paper are those of the author and do not necessarily represent those of the UK Ministry of Defence or any other department of Her Britannic Majesty's Government of the United Kingdom. Furthermore such views should not be considered as constituting an official endorsement of factual accuracy, opinion, conclusion or recommendation of the UK Ministry of Defence or any other department of Her Britannic Majesty's Government of the United Kingdom.

**Is Just War Theory a credible tool to explain  
contemporary war, globally?**

---

by:  
Major Lloyd Pritchard RM

student at:  
Joint Services Command and Staff College,  
United Kingdom

The jury of EuroISME's annual prize for the best student's thesis on military ethics consists of:

1. Colonel (ret) Rev. Prof.Dr. P.J. McCormack, MBE, (chairman, United Kingdom)
  2. Lt.Col.(Ret) Dr. Daniel Beaudoin (France/Israel)
  3. Dr. Veronika Bock (Germany)
  4. MMag. Stefan Gugerel (Austria)
  5. Col. (Ret) Prof.Dr. Boris N. Kashnikov (Russia)
  6. Dr. Asta Maskaliūnaitė (Estonia)
  7. Prof.Dr. Desiree Verweij (The Netherlands)
- Ms. Ivana Gošić (Serbia, secretary)

Enquiries: [secretariat.ethicsprize@euroisme.eu](mailto:secretariat.ethicsprize@euroisme.eu)

[www.euroisme.eu](http://www.euroisme.eu)

The prize has been financially supported by:







## Table of contents

Abstract .....	11
Introduction .....	13
Section 1: Parameters of the Research Question, Literature Review and Key Concepts .....	17
Section 2: The Global Applicability of Just War <i>Theory</i> .....	25
<i>Religious Bias and Western Dominance?</i> .....	25
<i>Universally Applicable Through Law?</i> .....	28
<i>Summary</i> .....	33
<i>Subjectivity – weakness or credible strength?</i> .....	35
Section 3: Hybrid Warfare and the Contemporary <i>Limitations of Just War Theory</i> .....	39
<i>Cyber Warfare</i> .....	41
<i>Attribution</i> .....	50
<i>Misinformation Warfare</i> .....	53
<i>JWT and Hybrid Warfare in Practice</i> .....	65
Conclusion .....	69
Bibliography .....	73



## Abstract

The Just War Theory or Tradition (JWT) is fundamental to the international system, as evidenced by its codification in the UN Charter and its frequent use by state and non-state actors when justifying war. Despite this, ‘contemporary warfare’ is challenging moral, legal and intellectual frameworks, and arguably changing the very definition of war<sup>1</sup>. It is therefore imperative to examine whether JWT can continue to be credibly applied to explain contemporary war. This paper, focussed upon the explicatory function of JWT, examines *Jus Ad Bellum* in two sections. First, by analysing whether JWT can or should be considered a globally acceptable and universally applicable concept in justifications for war and conflict initiation. Second, by assessing whether JWT can credibly apply to ‘Hybrid Warfare’, a term which encompasses both an increasingly significant form of political violence and one of the more testing challenges to JWT.

The paper concludes that JWT remains a credible, global tool for explaining warfare, but one that has significant flaws, particularly in addressing non-lethal and information-based conflict. While these flaws are not significant enough to warrant discarding JWT, they do undermine its credibility to explain the full gamut of contemporary war.

---

<sup>1</sup> See: Defence Secretary R. Gates, "A Balanced Strategy: Reprogramming the Pentagon for a New Age," *Foreign Affairs*, January 2009: 28-40; General N. Carter, "Dynamic Security Threats and the British Army" (Speech, London, January 22, 2018), <https://rusi.org/event/dynamic-security-threats-and-british-army> (accessed February 1, 2018); F. Hoffman, "Hybrid Warfare and Challenges," *Joint Force Quarterly* 52 (2009): 34.



*Just War thinking provides guidance on when and how force should be used, in whatever mutation the protean monster may assume.*<sup>2</sup>

## Introduction

The notion of ‘contemporary warfare’ has attracted a wealth of analysis, but a key feature is encapsulated by former-President Obama’s observation that “it will require us to think in new ways about the notions of just war”.<sup>3</sup> That a newly appointed President made this reference indicates both the significance of Just War Theory (JWT)<sup>4</sup> in the international system and the pressures contemporary warfare is placing on all moral and intellectual frameworks. In doing so, it reveals both the value and need for examining JWT’s ability to credibly explain contemporary war. Moreover, there is a growing body of work from academics, governments and militaries suggesting that contemporary warfare is not only challenging frameworks such as JWT, but also fundamentally changing the definition of war.<sup>5</sup> In this context the impact of contemporary war on JWT is similarly contested. Fisher, for example, asserts that traditional

---

<sup>2</sup> D. Fisher, *Morality and War: Can War be Just in the 21st Century* (Oxford: OUP, 2011): 162.

<sup>3</sup> President B. Obama, “Nobel Peace Prize Acceptance” (Speech, Oslo, December 10, 2009), <http://www.whitehouse.gov/the-press-office/remarks-president-acceptance-nobel-peace-prize> (accessed February 1, 2018).

<sup>4</sup> This paper recognises the debate over whether Just War is a theory or a tradition. As the terms are often used interchangeably, this paper will not examine this any further, other than accepting that – whether a tradition or theory – it is not a fixed school of thought and will continue to evolve over time, as it has done for the last two millennia.

<sup>5</sup> Defence Secretary R. Gates, “A Balanced Strategy: Reprogramming the Pentagon for a New Age,” *Foreign Affairs*, January 2009: 28-40; General N. Carter, “Dynamic Security Threats and the British Army” (Speech, London, January 22, 2018), <https://rusi.org/event/dynamic-security-threats-and-british-army> (accessed February 1, 2018); F. Hoffman, “Hybrid Warfare and Challenges,” *Joint Force Quarterly* 52 (2009): 34.

JWT remains relevant largely unchanged, whereas others contend that it requires substantial modification or is, in fact, entirely irrelevant.<sup>6</sup>

This paper seeks to understand if and how JWT applies to contemporary warfare, how it copes with increasingly blurred definitions of war, and the identification of JWT's limitations in this context. In doing so, it analyses the contemporary international system which is derived from and influenced by JWT, as evidenced by its codification in the UN Charter and frequent employment by heads of state.<sup>7</sup> It focuses on the continued utility of the JWT, which separates into two parts: *Jus In Bello*, prescribing how a war should be fought; and *Jus Ad Bellum*, the metric by which going to war is justified. The JWT holds that a Legitimate Authority must wage war 'Proportionally', with 'Just Cause', 'Right Intentions' and only as a 'Last Resort' where there is reasonable 'Chance of Success'. As it is the decision to go to war that is currently a greater source of debate regarding 'contemporary warfare', *Jus Ad Bellum* will form the main focus of this paper.<sup>8</sup>

The analysis falls into three main sections. The first scopes the parameters of the research question, provides a brief literature

---

<sup>6</sup> Respectively: Fisher, *Morality*, 162-163; M. Gross, *Ethics Of Insurgency* (Cambridge: CUP, 2015); A. Fiala, *Just War Myth* (Lanham: Rowman, 2008).

<sup>7</sup> Prime Minister T. Blair, "Doctrine of the International Community" (Speech, Chicago, April 22, 1999), <https://www.globalpolicy.org/component/content/article/154/26026.html> (accessed February 1, 2018).

<sup>8</sup> The related JWT concept *Jus in Bello* in the context of 'contemporary warfare' remains contested (see T. Bates, *Jus In Bello* (Bloomington: AuthorHouse, 2008)). Nevertheless, the most vexed policy and academic questions surround *Jus Ad Bellum*, which provides a justification for restricting the analysis to this aspect.

review to orient the reader, and defines the key concepts employed. The second analyses the cogency of claims and counter-claims surrounding whether JWT can or should be considered a globally acceptable and universally applicable concept in justifications for war and conflict initiation. In doing so, it addresses the validity of recurring criticism that the JWT codifies religious bias, Western hegemony and subjectivity which, if true, would limit the credibility of its contemporary global application in war and conflict initiation. The third section analyses the credibility and utility of JWT principles in the context of ‘Hybrid Warfare’. The reason for focusing on ‘Hybrid Warfare’ is two-fold. First, it is an increasingly significant form of political violence in the international system, as outlined by numerous National Security documents, and therefore warrants analysis.<sup>9</sup> Second, that its key feature – non-lethal forms of aggression intended to fall below the threshold at which target states can justify a militarised response – presents one of the greatest challenges to the utility and applicability of the JWT in ‘contemporary warfare’.

The primary conclusions are fourfold. The first is that JWT retains credibility as a global framework to identify the justifications for conflict initiation, but it remains susceptible to forms of exploitation and misuse, which fosters dissent and inhibits consensus on why or how war occurs. The second

---

<sup>9</sup> *National Security Capability Review*, [no Cmd] (2018), 5-6, <https://www.gov.uk/government/publications/national-security-capability-review-nscr> (accessed May 8, 2018); *Quadrennial Defence Review Report* (Washington: Pentagon, 2010), 8, [https://www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR\\_as\\_of\\_29JAN10\\_1600.pdf](https://www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf) (accessed May 8, 2018).

conclusion is that JWT literature has been incorrectly excluding the broader forms of Information Warfare, specifically ‘misinformation’, which may, in exceptional circumstances, be capable of achieving harm and therefore be an act of war. This reflects the third conclusion, which is that in seeking to remain below the threshold for war, Hybrid Warfare nullifies the moral, linguistic and intellectual Just War (JW) apparatus used to justify and explain war. In doing so, it hinders the framing of the ‘exceptional’ conditions that are normally required to breach sovereignty and other norms, and employ extraordinary (traditionally lethal or military based) measures against another state or actor. This leads to the final conclusion, which is that any attempt to modify JWT to accommodate the challenges posed by Hybrid Warfare involves practical, moral, intellectual and legal trade-offs. Thus, the overall finding is that JWT remains a credible, global tool for explaining warfare, but one that has significant flaws, particularly in addressing non-lethal and information-based conflict. While these flaws are not significant enough to warrant discarding JWT, they do undermine its credibility to explain the full gamut of contemporary war.



## Section 1: Parameters of the Research Question, Literature Review and Key Concepts

The research question has two implications. First, it presupposes analysis of JWT and contemporary war. Thus, rather than providing a detailed description of the millennia long-history of ‘traditional’ JWT,<sup>10</sup> this review will introduce most recent developments pertinent to addressing contemporary warfare. The second implication is the use of ‘explain’, which emphasises intellectual reasons for behaviour, rather than whether it is morally correct. This paper will, therefore, focus on JWT’s ability to credibly explain war and its initiation.

This paper defines contemporary warfare using Kaldor’s conceptual framework of ‘new wars’, which emphasises non-traditional forms of political violence, presenting a number challenges to both the international system and JWT.<sup>11</sup> Therefore, this paper could have examined, amongst many issues, the challenge of: non-state actors;<sup>12</sup> secessionism;<sup>13</sup> pre-emptive and preventative war;<sup>14</sup> or justice after war (*Jus Post Bellum*).<sup>15</sup> However, as can be identified from the references, academics have already examined these in some depth. In contrast, the JWT literature has engaged with Hybrid Warfare much less, even ex-

---

<sup>10</sup> For this history, see F. Russel, *Just War In The Middle Ages* (Cambridge: CUP, 1975).

<sup>11</sup> See M. Kaldor, *New and Old Wars* (Cambridge: Polity, 2012).

<sup>12</sup> See E. Heinze and B. Steele (Eds.), *Ethics, Authority, and War: Non-State Actors And The Just War Tradition* (Basingstoke: Palgrave Macmillan, 2010).

<sup>13</sup> See B. Coppiters and R. Sakwa, *Contextualizing Secession* (Oxford: OUP, 2005).

<sup>14</sup> D. Chatterjee (Ed.), *Ethics Of Preventive War* (Cambridge: CUP, 2013).

<sup>15</sup> A concept initiated by B. Orend’s “Justice After War”, *Ethics & International Affairs* 16, no. 01 (2002): 43-56. Also: C. Stahn *et al.*, *Jus Post Bellum* (Oxford: OUP, 2014).

plicitly discounting components of it. Furthermore, Hybrid Warfare encompasses the forms of conflict that Kaldor's 'new war' framework describes. Therefore, it is one of the primary lens from which JWT and contemporary warfare will be examined. The other lens is JWT's global application in a contemporary context, centred on recurring, arguably increasingly significant themes of bias, universal application and subjectivity. For both, only the outline concepts and literature will be presented in this section, drawing on the specifics in later sections.

Following the absence of any major JWT contributions and arguably near-collapse of its relevance to the international system from the late 17<sup>th</sup> Century,<sup>16</sup> JWT was academically recovered by Ramsey and Waltz in the 1960-1970s, writing from theological and secular perspectives.<sup>17</sup> The resurgence of JWT literature since then mostly bases itself on these two works.<sup>18</sup> The result has been two streams of predominantly Western discourse: a religious one, inspired by Ramsey;<sup>19</sup> and a philosophical one, consciously drawing on Walzer's epistemic 'legalist-paradigm'.<sup>20</sup> Consequently, a large portion of JWT is subject to predominantly Western thinking and a single religion which inevitably subjects it to accusations of bias and religious or regional con-

---

<sup>16</sup> See B. Heuser, "Rise, Fall and Resurgence Of 'Just War' Thinking", in *The Art Of Creating Power: Freedman On Strategy* (London: C. Hurst, 2017), 108.

<sup>17</sup> M. Walzer, *Just And Unjust Wars* (London: Penguin, 1977); P. Ramsey, *The Just War* (New York: Scribner, 1968).

<sup>18</sup> For extensive criticism of reliance on such seminal works, see L. Calhoun, "Political Philosophers On War: Arguments Inside The "Just War" Box", *Independent Review* 15, no. 3 (2011): 447-461.

<sup>19</sup> See J. Johnson, *Ethics And The Use Of Force* (Farnham: Ashgate, 2011).

<sup>20</sup> See B. Orend, *On War and Justice* (Montreal: McGill-Queen's University Press, 2008).

straint. The detail of which will be demonstrated in section two, as a prelude to the analysis.

More recently, as contemporary warfare has presented broader challenges of war, such as that posed by new technologies, for example, it has caused a division in the literature regarding whether JWT can cope with non-traditional forms of political violence or not. Many, including Rodin and JW Revisionists like Rid, claim it cannot.<sup>21</sup> Others, such as Lucas and Whetham, counter the Walzerian legal-positivist paradigm, by drawing on an older non-Westphalian tradition, arguing JWT is evolving to credibly apply to the ever changing character of war.<sup>22</sup> This division - which is an enduring theme of JWT's approach to contemporary warfare<sup>23</sup> - is one which has yet to be resolved, requiring this paper to address both schools of thought throughout.

This JWT literature review will now focus on the second lens, Hybrid Warfare, a concept which was outlined in the introduction but will be defined in section three. The key conclusion is that there appears to be no published JWT work specifically addressing Hybrid Warfare. However, there is a growing body of literature on how JWT applies to *some* of its components, particularly *Jus Ad Vim* and 'Information Warfare',

---

<sup>21</sup> See: D. Rodin, *War and Self-Defence* (Oxford: Clarendon Press, 2002); T. Rid, *Cyber War Will Not Take Place* (Oxford: OUP, 2013).

<sup>22</sup> See: G. Lucas, "Postmodern War", *Journal of Military Ethics* 9, no. 4 (2010): 289-298; D. Whetham, *Ethics, Law And Military Operations* (Basingstoke: Palgrave Macmillan, 2011).

<sup>23</sup> See: P. Cornish *et al.*, "On Cyber Warfare", *Chatham House Report* [online] (2010), 1-2, <https://www.chathamhouse.org/publications/papers/view/109508> (accessed January 10, 2018); D. Whetham and G. Lucas, "The Relevance Of The Just War Tradition To Cyber Warfare", in *Cyber Warfare: A Multidisciplinary Analysis* (Abingdon: Routledge, 2015), 161.

which only partially fills this gap. As the literature implications and concepts of JWT's application to Hybrid Warfare are more complex, it has been afforded greater focus in this review.

Walzer introduced the term *Jus Ad Vim* in his 2006 preface to *Just and Unjust War* as meaning just force 'short-of-war'.<sup>24</sup> This notion is not only contested,<sup>25</sup> but also relatively confused, at least in the manner in which Walzer suggested it.<sup>26</sup> While *Jus Ad Vim* will be briefly examined in this paper, it is arguably becoming distinct from JWT, fused with other frameworks; and is more comprehensively applied to *In Bello* issues, such as drone strikes, neither of which are pertinent to this paper.<sup>27</sup>

'Information Warfare' is a heterogeneous phenomenon concerning the deployment of robotic weapons, cyber weapons and the use of information and communication technology in or for war.<sup>28</sup> As this concept is often non-kinetic it poses greater challenges to JWT than other forms of Hybrid Warfare, whilst still remaining (arguably) a form of war. Importantly, as Lucas contends, the issues presented by Information Warfare "are...the most representative of the common themes and ethical concerns pervading all other recently emergent military technologies combined",<sup>29</sup> allowing this paper to use it as a

---

<sup>24</sup> Walzer, *Just And Unjust Wars*, xv-xvi.

<sup>25</sup> See C. Coady, *Morality and Political Violence* (Cambridge: CUP, 2008); and H. Frowe, *The Ethics Of War And Peace*, 2nd ed. (London: Routledge, 2016).

<sup>26</sup> See S. Brandt Ford, "Jus Ad Vim And The Just Use Of Lethal Force-Short-Of-War", in *Routledge Handbook Of Ethics And War: Just War Theory In The 21St Century* (London:R outledge, 2013): 65.

<sup>27</sup> M. Gross and T. Meisels, *Soft War* (Cambridge: CUP, 2017): 3; and *ibid.*, 71.

<sup>28</sup> M. Libiki, *What Is Information Warfare?* (Washington: Defense University Press, 1998): 1-2.

<sup>29</sup> G. Lucas, "Ethics And Cyber Conflict: Response To JME 12:1 (2013)", *Journal of Military Ethics* 13, no. 1 (2014): 20-31.

platform to illustrate some of the wider impacts of contemporary warfare on JWT, beyond that of just Hybrid Warfare.

As Floridi and Taddeo contend, Information Warfare is “reshaping the concept of war itself, raising new ethical problems and challenging old solutions”.<sup>30</sup> What they fail to address is their exclusion of the psychological and perception manipulation aspect of Information Warfare – termed ‘misinformation’ in this paper – dismissing it in one unjustified sentence as simply “semantic content”.<sup>31</sup> This reflects the wider body of JWT literature, which assumes misinformation is irrelevant to JWT.<sup>32</sup> This demonstrates JWT’s limited development in the ‘broader’ forms of contemporary conflict, as noted by numerous JW theorists.<sup>33</sup> The other end of Information Warfare presents such challenges as autonomous weapons and robotics, which are primarily the remit of *Jus in Bello* and therefore not examined in this paper. The ‘middle ground’ of Information Warfare is cyberwarfare, which has a limited but growing body of JWT literature.

The term cyberwarfare was first coined by Arquilla and Ronfeldt in 1993.<sup>34</sup> The response to their notion that cyberwar was coming soon was overwhelmingly negative. As examples of

---

<sup>30</sup> L. Floridi and M. Taddeo, *Ethics Of Information Warfare* (Switzerland: Springer, 2014), v.

<sup>31</sup> *Ibid.*

<sup>32</sup> See J. Arquilla, "Twenty Years Of Cyberwar", *Journal Of Military Ethics* 12, no. 1 (2013): 80-87.

<sup>33</sup> See Cornish *et al.*, *On Cyber Warfare*, 2; G. Lucas, *Ethics and Cyberwarfare* (Oxford: OUP, 2017):102-103.

<sup>34</sup> J. Arquilla and David Ronfeldt, "Cyberwar Is Coming!", *Comparative Strategy* 12, no. 2 (1993): 141-165.

cyberwarfare increased in the 2000s, as explained by Clarke,<sup>35</sup> this response became more balanced but equally divided. This division is reflected in the seminal 2010 articles by Dipert, judging JWT as woefully deficient in cyberwarfare, and Cook, supporting JWT's applicability.<sup>36</sup> As Arquilla notes in his comprehensive review of cyber-related JWT literature, these two articles form the basis of most subsequent discussion of JWT's application to cyberwarfare, with two notable issues that frame this paper's intellectual endeavour.<sup>37</sup>

The first is the 'physical and lethal' problem. Jenkins' article on Stuxnet, and Dipert more generally, examine the difference between the physical and virtual to decipher whether cyberwarfare causes harm in the real world, crossing legal thresholds for armed attack.<sup>38</sup> This leads one to question whether increasing reliance on cyberwarfare lowers the threshold for resorting to war or encourages conflict as an easy rather than last resort.

The second area of contention is attribution: identifying who conducted the attack. As Rowe notes, the critical problem with attributing aggression is that the evidence is likely circumstantial and may not meet legal thresholds.<sup>39</sup> Schmitt disagrees noting

---

<sup>35</sup> See R. Clarke and R. Knake, *Cyber War: The Next Threat To National Security And What To Do About It* (New York: Ecco, 2010).

<sup>36</sup> R. Dipert, "The Ethics Of Cyberwarfare", *Journal Of Military Ethics* 9, no. 4 (2010): 384-410; J. Cook, "'Cyberation' And Just War Doctrine: Response To Randall Dipert", *Journal of Military Ethics* 9, no. 4 (2010): 411-423.

<sup>37</sup> Arquilla, *Twenty Years*, 80.

<sup>38</sup> R. Jenkins, "Is Stuxnet Physical? Does It Matter?", *Journal of Military Ethics* 12, no. 1 (2013): 68-79; and R. Dipert, "Other-Than-Internet (OTI) Cyberwarfare: Challenges For Ethics, Law, And Policy", *Journal of Military Ethics* 12, no. 1 (2013): 34-53.

<sup>39</sup> N. Rowe, "The Attribution Of Cyber Warfare", in *Cyber Warfare*, 69.

that “this so-called attribution problem...is neither all that big nor all that unprecedented”.<sup>40</sup> While Schmitt is correct to identify previous non-cyber problems of attribution,<sup>41</sup> his point illustrates broader relevance to contemporary warfare, while his disagreement with Rowe reflects the wider literature’s dispute regarding both the difficulty of attribution and its impact on JWT. Two issues which this paper will directly address.

The most recent, comprehensive cyber contribution is Lucas’ 2017 *Ethics and Cyberwarfare*. His book ambitiously seeks to provide a “comprehensive master narrative”,<sup>42</sup> a task he only partially achieves, as evidenced by his admission that JWT’s task “is far from finished...[asking] whether this new form of conflict requires a new ethical framework”.<sup>43</sup> A question this paper will seek to answer.

The only JWT work that seems to explicitly address the full breadth of Hybrid Warfare is Whetham’s 2016 article in the *Monist*, which argues that, by concentrating on harm in a broader sense rather than its purely lethal manifestation, JWT can be applied to hybrid attacks.<sup>44</sup> His argument draws pre-dominantly on pre-Westphalian JW thinking, identifying him as part of the contested, non-Walzerian school that apply JWT most broadly. His article poses three relevant points to this paper. First, he

---

<sup>40</sup> M. Schmitt, "Cyber Operations In International Law", in *Proceedings Of A Workshop On Detering Cyberattacks* (Washington: National Academy of Sciences, 2010), 151–178.

<sup>41</sup> See Y. Dinstein, "Cyber War And International Law", *International Law Studies* 89 (2013): 276-287.

<sup>42</sup> Lucas, *Ethics and Cyberwarfare*, 157.

<sup>43</sup> *Ibid.*, 103.

<sup>44</sup> D. Whetham, "'Are We Fighting Yet?' Can Traditional Just War Concepts Cope With Contemporary Conflict?", *The Monist* 99, no. 1 (2016): 55-69.

examines attribution but fails to fully address the fundamental problem of covert actors seeking to avoid JWT's application. Second, he poses some insightful questions but fails to fully address them, something he admits in his conclusion.<sup>45</sup> Third, where he does address these questions, he persuasively offers moral answers but, in doing so, demonstrates a subjectivity that undermines the intellectual traction of the framework. All of which are issues which this paper will confront directly.

In addition to questioning JWT's subjectivity, the reader may also note that all the literature quoted, thus far, has been from the West, perhaps causing them to question either the bias of the author or of JWT itself. Questions which will be addressed in the next section.

---

<sup>45</sup> *Ibid.*, 67.



## Section 2: The Global Applicability of Just War Theory

JWT faces repeated criticisms of religious bias and Western hegemony which, if true, would limit its potential application. Conversely, others argue JWT is universally applicable through its manifestation in international law. These claims need to be investigated to discern whether JWT can be credibly applied globally. The structure of this section will therefore commence with examination of religious bias and Western dominance, before concluding with a more detailed investigation of JWT's relationship with law. Greater emphasis has been placed upon law for two reasons. First, it is the more contemporary and complex issue. Second, it allows one to identify the more significant contemporary flaws this relationship imposes on JWT.

### *Religious Bias and Western Dominance?*

It is routine to attribute the origins of JWT to Christian thought and scholars.<sup>46</sup> For some, the Christian genesis of JWT is a fatal weakness due to the “incontrovertible” argument that a tradition rooted in a single religion cannot be globally applicable.<sup>47</sup> The typical counter-argument, as employed by Walzer, is to abstract debate to one of secular rights and norms using the ‘war

---

<sup>46</sup> N. Rengger, "On The Just War Tradition In The Twenty-First Century", *International Affairs* 78, no. 2 (2002): 353-363.

<sup>47</sup> T. Magstadt, *Understanding Politics* (Cambridge: Cengage Learning, 2016), 418 and *ibid.*, 362.

convention'.<sup>48</sup> While this counter-argument may be valid, it avoids rather than addresses the accusation of religious bias. Similarly, the rather simple atheist counter-argument regarding flawed faith rather than logic<sup>49</sup> is effectively countered by the fact that JWT does not blindly rely on faith because it is based on a distinct logic rather than recourse to scripture. The more conclusive counter-argument is to challenge the notion that religion is the source of JWT at all. While one could argue that Aristotle's first use of the term 'Just War' may be unrelated to wider JWT,<sup>50</sup> examination of his work reveals five criteria for justifying war, most of which directly correlate with JWT today.<sup>51</sup> Cicero was equally influential, describing the requirement for right intention and legitimate authority.<sup>52</sup> Heuser even suggests that Christian scholars, like Augustine, were "merely the channel through which classical enlightened thoughts were preserved for later generations"<sup>53</sup>. However, the notion that Christian scholars were merely passive recyclers of classical thought is an exaggeration, as evidenced by Augustine broadening war beyond legitimate authority<sup>54</sup>. Nevertheless, it is clear that Greek and Roman thought not only preceded Christian JWT but also informed it, as evidenced by Vitoria's referencing of such ancient scholars<sup>55</sup>. It may be that classical origins account for the growing recognition that contemporary JWT, secular and

---

<sup>48</sup> Walzer, *Just and Unjust War*, 44-47.

<sup>49</sup> See R. Dawkins, *The God Delusion* (Oxford: OUP, 2008).

<sup>50</sup> See D. Whetham, "Just War Tradition", in *Ethics, Law And Military Operations*, 70.

<sup>51</sup> Aristotle, *The Politics*, trans. E. Baker (Oxford: OUP, 1998), 199.

<sup>52</sup> Cicero, *On Duties*, bk 1, sections 34-41.

<sup>53</sup> Heuser, *Resurgence*, 102. See also A. Bellamy, *Just Wars: From Cicero to Iraq* (Cambridge: Polity Press, 2006), 17-27.

<sup>54</sup> Bellamy, *Just Wars*, 29.

<sup>55</sup> F. de Vitoria, *Political Writings*, tr. J. Lawrance (Cambridge: CUP, 1991), 307. See also Bellamy, *Just Wars*, 15-27.

Christian, correlates with (and has been arguably informed by) other religions<sup>56</sup>. On this basis, while recognising Christian scholars' considerable influence, the accusation of a fatal religious based bias in contemporary (secular) JWT is unfounded.

While there may not be such a religious bias, the considerable scale and impact of Christian based discourse in JWT reflects a wider issue, namely its association with Western hegemony. This accusation has some potential merits because of JWT's Aristotelian and Christian genesis; the growing but still limited non-Western input into JWT, with zero Russian contributions, for example;<sup>57</sup> and even recent, seminal works, such as *Just and Unjust War*, being almost exclusively based on Western conflict. By implication this provides justification for the accusation that JWT is based on and for the West, so should be considered a regional rather than a global theory. However, while JWT may not be, in Coxian terms, 'for' a non-Western country, it does not mean JWT should be discarded. Furthermore, there are three reasons which suggest JWT is globally applicable. First, an abstract framework is, by definition, universal. Evans argues that, as an abstract framework, it can eschew its origins to be universally applied.<sup>58</sup> The non-Western work on non-Western issues persuasively demonstrates this point.<sup>59</sup> Second, there is strong empirical evidence of philosophical convergence,

---

<sup>56</sup> R. Sorabji and D. Rodin, *Ethics of War: Shared Problems in Different Traditions* (Aldershot: Ashgate, 2007), 7.

<sup>57</sup> See B. Robinson, "The Justification Of War In Russian History And Philosophy", in *Just War In Comparative Perspective* (London: Routledge, 2003).

<sup>58</sup> M. Evans, "Moral Theory And The Idea Of A Just War", in *Just War Theory: Reappraisal* (Bodmin: MPG Books, 2005), 8

<sup>59</sup> For example, see E. Aboultaif, "Just War And The Lebanese Resistance to Israel", *Critical Studies On Terrorism* 9, no. 2 (2016): 334-355.

regardless of geographic area. This is evidenced by Rawls' concept of 'overlapping consensus', which demonstrates the common morality which repeatedly appears cross-culturally despite "considerable differences in citizens' conceptions of justice".<sup>60</sup> Whetham concurs,<sup>61</sup> and is further supported by evidence that JWT correlates with, and has been arguably informed by, other schools of thought.<sup>62</sup> Third, non-Western nations are both adhering to the framework in practice and making use of their own embryonic JW schools of thought.<sup>63</sup> Thus, while JWT originates from and may arguably be dominated by the West,<sup>64</sup> it remains broadly applicable to and for non-Western actors for a number of abstract, philosophical and practical reasons.

### *Universally Applicable Through Law?*

Bellamy asserts that international law is a sub-tradition of Just War itself:<sup>65</sup> a point seemingly vindicated by the codification of *Jus Ad Bellum* in the UN Charter.<sup>66</sup> It could be inferred, therefore, that JWT universally applies through the medium of international law, which increasingly applies to non-state

---

<sup>60</sup> J. Rawls, *A Theory Of Justice* (Harvard: Harvard University Press, 1971), 340; J. Rawls, *Political Liberalism* (New York: Columbia University Press, 2005).

<sup>61</sup> D. Whetham, "Ethics, Law And Conflict", in *Ethics, Law And Military Operations*, 17.

<sup>62</sup> R. Sorabji and D. Rodin, *Ethics of War*, 7.

<sup>63</sup> See S. Twiss and L. Ping-Cheung, *Chinese Just War Ethics* (Abingdon: Routledge, 2015).

<sup>64</sup> Lack of JWT focused bibliometric data does not allow one to decisively conclude this, but broader social science data may offer an indication that it is (see H. Turton, *International Relations and American Dominance* (London: Routledge, 2015), 18-21).

<sup>65</sup> Bellamy, *Just Wars*, 120.

<sup>66</sup> G. Brown, "Proportionality And Just War", *Journal of Military Ethics* 2, no. 3 (2003): 171-173.

actors.<sup>67</sup> Conversely, other academics contend that JWT forms a sphere separate from international law.<sup>68</sup> The validity of both arguments rests on whether international law is genuinely a sub-tradition of JWT or has just been informed by it. Analysing the reasoning of those who consider law to be part of JWT is therefore necessary. This reasoning is typically based on three points, as exemplified by Bellamy.<sup>69</sup> The first is that in practice, legal and moral arguments are conflated in the context of ‘just war’, rather than treated as independent entities. Second, positive and natural law are joined, as illustrated by explicit links between them in the ‘Martens Clause’ of various international treaties. Third, states morally justify war even when they are deemed legally compliant.<sup>70</sup>

There are, however, four problems with this line of argument. The first and third of Bellamy’s points, which are in effect identical,<sup>71</sup> are logically inconsistent because the existence of moral justification for war does not also make the legal argument *part* of JWT. Second, the entire argument is predicated on the connection with natural law, which is a wider body of philosophy, rather than narrowly connected to JWT alone. Third, use of the Martens Clause is unconvincing, as it is a contested and diversely interpreted article which, at best, only accepts a connection rather than dominance over positive law<sup>72</sup>. Fourth, it ignores the

---

<sup>67</sup> See, for example, the *Protocol Additional to the Geneva Conventions 1977*, <https://ihl-databases.icrc.org/ihl/INTRO/470> (accessed May 1, 2018).

<sup>68</sup> M. Byers, *War Law* (London: Atlantic Books, 2005), 2.

<sup>69</sup> Bellamy, *Just Wars*, 119-120.

<sup>70</sup> *Ibid.*

<sup>71</sup> That there are other means of justifying war beyond the legal argument.

<sup>72</sup> R. Ticehurst, "The Martens Clause And The Laws Of Armed Conflict", *International Review of The Red Cross* 37, no. 317 (1997): 125-134.

fact that international law is the product of political negotiation and compromise.<sup>73</sup> In this sense international law is the compromise between political and moral ideals, and is not merely a manifestation of JWT. Thus, while it is historically correct to note that Grotius *et al* drew on natural law (including JWT) when informing international law, and that natural law may still influence legal argument, he is incorrect to assume that JWT has exclusive possession. Moreover, as Johnson notes the “advent of positive international law significantly truncated...just war”.<sup>74</sup> Thus, whilst JWT and international law are closely aligned and connected, the universalism of the UN charter does not represent universal application of JWT.

However, one must be careful not to allow ethicists’ pursuit of ‘authentic’ JWT to down-play the importance of and connection with law, nor allow legal positivists to overlook the fact that whilst different, positive and natural law (including JWT) are still connected and mutually supporting.<sup>75</sup> This interdependence is best illustrated by states regularly employing both moral and legal arguments for war<sup>76</sup> and Orend’s point that for law to be legitimate, it must be based on ethical principles.<sup>77</sup>

However, this is not always the case. Indeed, the example of the “illegal but morally legitimate” 1998 Kosovo intervention persuasively demonstrates the distinct difference between law

---

<sup>73</sup> Biggar, *Defence*, 153. Also Rodin, *War*, x-xi.

<sup>74</sup> J. Johnson, "In Defence Of War", *Journal of Military Ethics* 13, no. 4 (2014): 386-393.

<sup>75</sup> See R. Higgins, *Problems And Process* (Oxford: Clarendon Press, 2010), 7; and Bellamy, *Right to Fight*, 231-233.

<sup>76</sup> Blair, *Doctrine of the International Community*.

<sup>77</sup> Orend, *On War and Justice*, 64.

and JWT,<sup>78</sup> and that they can even be in opposition to each other.<sup>79</sup> In the Kosovo example, Guthrie and Quinlan suggest that NATO states calculated that a proposal to the UN to authorise force in Kosovo would have been vetoed by Russia, and that a failure to secure a Security Council resolution would delegitimise any subsequent intervention.<sup>80</sup> This judgment was sound, evidenced by Russia's subsequent UN motion to prevent NATO intervention<sup>81</sup>. NATO intervened anyway, and in doing so divorced JWT from positivist law,<sup>82</sup> leading to the International Commission on Kosovo's conclusion that the intervention was "illegal but legitimate".<sup>83</sup> This legitimisation of NATO actions in JWT terms had three implications. First, the optimistic post-Cold War perception of a smoothly functioning UN Security Council was proven false, signalling a return to the Cold War era of veto and the erosion of the UN's exclusive right to legitimate authority. This provided states or coalitions with a lower threshold of legitimate authority in justifying armed interventions.<sup>84</sup> When combined with the weakened support JWT and positivist law provide each other, it subsequently hindered the role of the JWT in constraining war, evidenced by the dubiously

---

<sup>78</sup> A. Cassese, "Ex Iniuria Ius Oritur: Are We Moving Towards International Legitimation Of Forcible Humanitarian Countermeasures?", *European Journal of International Law* 10, no. 1 (1999): 23.

<sup>79</sup> Jovic, *Just War Theorist*, 98-99.

<sup>80</sup> Guthrie and Quinlan, *Just War*, 28.

<sup>81</sup> UN, "Security Council Rejects Demand for Cessation of Use of Force", March 26, 1999, <https://www.un.org/News/Press/docs/1999/19990326.sc6659.html> (accessed January 10, 2018).

<sup>82</sup> For comprehensive evidence of this point, see the Independent International Commission on Kosovo (IICK), *The Kosovo Report* (Oxford: OUP, 2000), 185-187.

<sup>83</sup> *Ibid.*, 4.

<sup>84</sup> *Ibid.*, 186. See also Higgins, *Problem and Process*, 285.

justified 2003 Iraq War and Russia's 2008 intervention in Georgia.

This Kosovo case also illustrates a second impact: the exploitation of JWT as a tool for statecraft. The bifurcation of JWT and positivist law created greater ambiguity, allowing greater debate and potential for exploitation by state actors. Stromseth optimistically contends this “very ambiguity...[provides] fertile ground for the emergence of norms”.<sup>85</sup> He neglects to point out the corollary that it also allows for exploitation and instrumental misuse of JWT. Thus Putin now conveniently states “what was done in Crimea was not in any way different from what had been done in Kosovo”<sup>86</sup>. Other academics make a similar Kosovo based argument to justify the Russo-Georgian War.<sup>87</sup> Thus, change in humanitarian precedence, using JWT, now ironically leaves JWT more open to future misuse, where JWT is used to explain the nominal rather than substantive reason for war.

These factors relate to a third impact, namely inconsistent application. For example, JWT does not explain why the Rwanda genocide in 1994 was not prevented through external intervention (seemingly because none wanted to); or why the US withdrew from Somalia in 1994 (seemingly because of ‘black hawk down’). They had compelling JWT reasons to intervene

---

<sup>85</sup> J. Stromseth, “Rethinking humanitarian intervention,” in J. Holzgrefe and R. Keohane, *Humanitarian Intervention* (Cambridge: CUP, 2003), 233.

<sup>86</sup> President V. Putin, Interview with the ‘German TV channel ARD’, November 17, 2014, transcript, Kremlin, <http://en.kremlin.ru/events/president/news/47029> (accessed February 21, 2018).

<sup>87</sup> Bellamy, *Right to Fight*, 243.



either to stop genocide or prevent a state from failing.<sup>88</sup> The explanation appears to be national self-interest, particularly as the Security Council veto argument, following Kosovo, is no longer as conclusive as it was. Far from Walzer's hubristic "triumph" of JWT,<sup>89</sup> these examples are a triumph of political interest over justice. They reflect a wider issue of JWT's selective application. Bellamy not only acknowledges selective application as a plausible flaw but even admits it is "quite correct".<sup>90</sup> When assessing his mitigation to the problem, it becomes clear he does not have one, other than blaming all nations.<sup>91</sup> Others argue such inconsistent application is more a failure of Responsibility to Protect, which offers a moral duty to protect, whereas JWT only offers moral permission should one wish to use it.<sup>92</sup> This argument is not only morally contemptible, it still leaves – even reinforces – the problem of selective application. Meaning JWT, as an intellectual tool for explaining events, is challenged by unpredictable employment of the framework.

### *Summary*

To examine JWT's global applicability, three of the more common notions regarding regional constraint, bias and universal application were investigated. First, it was concluded that the accusation of a fatal religious based flaw in contemporary (secu-

---

<sup>88</sup> See Bellamy, *Just Wars*, 199-205.

<sup>89</sup> Walzer, *Arguing*, 12.

<sup>90</sup> Bellamy, *Right to Fight*, 237.

<sup>91</sup> *Ibid.*

<sup>92</sup> H. Friberg-Fernros, "Allies In Tension: Identifying and Bridging The Rift Between R2P And Just War", *Journal of Military Ethics* 10, no. 3 (2011): 160-162.

lar) JWT is unfounded in theory and practice. Second, analysis of supposed Western bias and hegemony revealed that it remains broadly applicable to and for non-Western actors for abstract, philosophical and practical reasons. The third notion explored the claim of universal JWT application through its manifestation in international law. The 1998 Kosovo example, alongside broader analysis, demonstrated the close but distinct difference between international law and JWT. This revealed three JWT flaws. First, the absence of the, previously supporting, international law hindered JWT's ability to constrain war. Second, the JWT caused precedence change in humanitarian intervention ironically leaves JWT *increasingly open* to greater exploitation and misuse, as evidenced by employment of this precedence in Russia's war with Georgia and annexation of Crimea. Third, the subsequent lack of application of JWT to similarly unjust humanitarian crises revealed that JWT, as an intellectual tool for explaining events, is challenged by unpredictable employment of the framework. Thus, overall, JWT is predominantly absent of bias or regional constraint and is therefore applicable globally. However, flaws remain, the majority of which appear to be historic. Nevertheless, some appear to have recently increased in scale or significance. While these flaws are not sufficient to cause one to discard JWT, they do reveal a subjectivity and selective application of the framework that merits further examination in the next section.

*Subjectivity – weakness or credible strength?*

This sub-section will briefly examine theorists' views of JWT's subjectivity, before conducting more detailed analysis of what strengths and weaknesses this reveals. Many claim that subjectivity of war and JWT is a fundamental problem, as evidenced by Fiala, who contends that "those who claim wars are just are...deluded",<sup>93</sup> and Booth noting "Just War can justify anything".<sup>94</sup> One can criticise Booth for his inadequately referenced, seemingly unbalanced polemic against JWT and avoid Fiala's criticism by noting this paper's focus on the intellectual rather than moral aspect of JWT. However, their arguments are partially valid. Indeed, 16<sup>th</sup> century Vitoria recognised all protagonists would likely claim their war as just.<sup>95</sup> Even Walzer noted the problem that "there is no ready way to establish...independent views", albeit then failing to reconcile the problem.<sup>96</sup> A point demonstrated by the directly opposing views of two prominent JW theorists regarding the 2003 Iraq War.<sup>97</sup> It is this very interpretative pliability, as admitted to and demonstrated by principal JW theorists, that leads many to consider JWT as inescapably subjective, perhaps even historically so.<sup>98</sup>

---

<sup>93</sup> Fiala, *Myth*, xi.

<sup>94</sup> K. Booth, "Ten Flaws Of Just Wars", *International Journal of Human Rights* 4, no. 3-4 (2000): 314-315.

<sup>95</sup> De Vitoria, *Political Writings*, 311-313.

<sup>96</sup> Walzer, *Just and Unjust Wars*, 129.

<sup>97</sup> Bellamy, Right to Fight, 238; J. Johnson, *War to Oust Saddam Hussein* (Lanham: Rowman & Littlefield, 2005).

<sup>98</sup> D. Brown, *Continuing Challenges*, 130. See also: J. Sterba, *Justice for Here and Now* (Cambridge: CUP, 2000); and R. Werner, *Collective Self-Deception*, 42.

Having established JWT's subjectivity, it leads to the issue of whether this subjectivity makes it an inadequate framework. Werner answers with an emphatic 'yes', contending that JWT is a "dangerous moral theory" that not only allows aggressors to justify any war but also means "one can find just war theorists" to do so too, lending false legitimacy to an unjust war,<sup>99</sup> and fostering conflicting discourse. The counter is that such flexibility increases the applicability of JWT but, in doing so, it undermines its ability to deliver a clear consensus for why or how war occurred, weakening both the moral argument and its intellectual explanatory power.

Worse, the need and threshold for the more prevalent intra-state conflicts are often less clear. When combined with the uncertainty of the legal position for intervention, it places considerable burden on justification for those acting without UN authorisation.<sup>100</sup> Collectively, these failings create a substantial weakness in JWT, a "Clausewitzian centre of gravity" where subjective public opinion, based on "media-amplified moral concern", becomes crucial.<sup>101</sup> This has two impacts. First, as Walzer and Whetham separately note, when "legitimacy itself is the battleground... winning the narrative is just as significant as winning any tactical engagement".<sup>102</sup> It may even be more important, as the UK's Chief of Defence Intelligence recently noted.<sup>103</sup> Russia

---

<sup>99</sup> Werner, *Collective Self-Deception*, 42.

<sup>100</sup> Stromseth, *Rethinking*, 233.

<sup>101</sup> P. Schulte, "Just Wars Of The Future? Applying Just War Theory To Twenty-First Century Rogue Regimes", *RUSI Journal* 153, no. 4 (2008): 22.

<sup>102</sup> Whetham, *Law and Conflict*, 19; Walzer, *Arguing*, 14.

<sup>103</sup> P. Osborn, "Intelligence and Information Advantage in a Contested World" (Speech, London, May 8, 2018), <https://rusi.org/event/air-marshal-phil-osborn-intelligence-and-information-advantage-contested-world> (accessed May 9, 2018).

exemplified this point when it flew fifty journalists to Tskhinvali days before the 2008 Georgian war, seeking to dominate the international narrative.<sup>104</sup> Second, it reveals the changing nature of the Tradition, moving from an introspective moral constraint to a device susceptible to being exploited to gain support for war: where *being* just is less important than *being seen* to be just. Indeed, this point is underlined by Russia's narrative of responding to "aggressive [Georgian] acts to restore...peace"<sup>105</sup> despite years of preparation for the invasion and the well evidenced notion that Russia's action was almost entirely geo-political self-interest.<sup>106</sup>

Overall, this analysis leads to three conclusions. First, JWT's increasing subjectivity means it becomes more readily applicable and relevant but, in doing so, it fosters dissent and inhibits consensus for why or how war occurred. This has the effect of weakening both the moral argument and its intellectual explanatory power. Second, the same interpretative pliability precludes the likelihood that JWT will constrain war. Third, and as a consequence, it allows JWT to be exploited as a moral cover for immoral or self-seeking behaviours, undermining its intellectual honesty in explaining or justifying war.

---

<sup>104</sup> S. Cornell and F. Starr, *Russia's War in Georgia*, (New York: M.E. Sharpe, 2009), 3.

<sup>105</sup> UN, "Security Council Holds Emergency Meeting In Response To Russian Federation's Request" (August 8, 2008), <https://www.un.org/press/en/2008/sc9417.doc.htm> (accessed Jan 10, 2018).

<sup>106</sup> M. Light, "The Russo-Georgian War: A Conflict Announced In Advance?", *Europe-Asia Studies* 62, no. 9 (2010): 1579-1582; A. Cohen and R. Hamilton, *Russian Military and the Georgia War* [Pamphlet] (Saffron Waldron :Books Express, 2011); S. Andersen, *Analysis Of The Russo-Georgian War*, 1-7.

This reveals an issue fundamental to this paper: the relationship between the moral and intellectual function of JWT. If the number of actors who meet the substantive moral requirement reduces, the less able JWT is to intellectually explain their behaviour. Consequently, the intellectual traction of JWT is inextricably beholden to the popularity of the moral tool. Therefore, the fourth conclusion of this section is that the intellectual tool is ultimately challenged if or when actors fail to use it morally. It is particularly notable that this point appears to be unrecognised in the JWT literature.

The scale of this challenge seems significant when one notes that the World Values Survey - one of the world's largest, multi-national surveys examining over 55 countries – identified that 62% of this global cross-section do not believe in the principles of JW.<sup>107</sup> One must be cautious when using a single primary source to make sweeping JWT conclusions, particularly as many states are not democratic and may be less responsive to this individual view. Nevertheless, one can accept that it is indicative that JWT is a popular but not entirely dominant framework. Critically, while JWT remains credible, this lack of dominance limits the degree to which it can be used to explain war.

---

<sup>107</sup> R. Inglehart *et al* (eds.), *World Values Survey: Round Six* (Madrid: JDS Institute, 2014), [www.worldvaluessurvey.org/WVSDocumentationWV6.jsp](http://www.worldvaluessurvey.org/WVSDocumentationWV6.jsp) (accessed April 19, 2018).

### Section 3: Hybrid Warfare and the Contemporary Limitations of Just War Theory

Having examined the problem of subjectivity, which seems especially compounded by the contemporary scale of media and predominance of intrastate intervention, the equally contemporary problem of Hybrid Warfare will now be considered. Hybrid Warfare warrants detailed attention for four reasons. First, core attributes of Hybrid Warfare – cyberwar, misinformation and difficulties of attribution – raise vexing questions of whether and how JWT can apply.<sup>108</sup> Second, the growth in the use of Hybrid Warfare means that these questions are highly pertinent.<sup>109</sup> Third, the fact that Hybrid Warfare challenges established definitions of war means that it offers the greatest insight into JWT’s applicability and flaws, in contexts on the ‘edge of war. Finally, attribution, in particular, is reportedly “the most difficult problem” posed to those seeking to explain and justify war, and therefore relevant to contemporary warfare more broadly.<sup>110</sup>

Hybrid Warfare has been identified and categorised as a discrete form of warfare. The term is popularly used by governments, media and academics, with a broadly defined and accepted

---

<sup>108</sup> H.R. McMaster, “Atlantic Council Baltic Summit” (Speech, Washington, April 3, 2018), <https://www.whitehouse.gov/briefings-statements/remarks-ltg-h-r-mcmaster-atlantic-council-baltic-summit-dinner/> (accessed April 9, 2018).

<sup>109</sup> *Ibid.* See also *Assessing Russian Activities and Intentions in Recent US Elections*, ICA-2017-01D (ODNI, 2017), [https://www.dni.gov/files/documents/ICA\\_2017\\_01.pdf](https://www.dni.gov/files/documents/ICA_2017_01.pdf) (accessed May 8, 2018).

<sup>110</sup> P. Singer and A. Friedman, *Cybersecurity and Cyberwar* (Oxford: OUP, 2014), 73.

definition.<sup>111</sup> This paper will use Freedman's definition, whereby Hybrid Warfare is "an approach that draws upon a number of types of force from across the full spectrum, including terrorism, insurgency and regular combat, along with the extensive use of information operations",<sup>112</sup> which aligns with most academic and government definitions.<sup>113</sup> While it is important to note that Hybrid Warfare is not new,<sup>114</sup> it is equally significant to recognise that it has increased in scale, sophistication and significance over the last fifteen years.<sup>115</sup>

As this section will show, Hybrid Warfare raises particular challenges for JWT. The first challenge stems from the fact that Hybrid Warfare relies significantly on non-lethal effects – encapsulated in the notion of 'misinformation warfare' – as part of a full spectrum approach. The non-lethal nature of 'misinformation warfare', which includes any form of perception management, fake news or psychological operations, has led many analysts to conclude that JWT does not apply.<sup>116</sup> However, this paper will contend otherwise. The second challenge arises from the emphasis in Hybrid Warfare on offensive action that employs 'force short of war' (*Jus Ad Vim*) in seeking to remain below the sub-legal, sub-JWT threshold.<sup>117</sup> In doing so, Hybrid Warfare seeks to nullify the moral, linguistic and intellectual JW apparatus by hindering the framing of the

---

<sup>111</sup> See Hoffman, *Hybrid Warfare*, 34.

<sup>112</sup> L. Freedman, "Ukraine And The Art Of Limited War", *Survival* 56, no. 6 (2014): 11.

<sup>113</sup> See: Hoffman, *Hybrid*, 34; *Quadrennial Defence Review*, 8; *Putin's Asymmetric Assault on Democracy in Russia and Europe*, S.Pr.115-21, 115<sup>th</sup> Congress, Second Session (10 January 2018).

<sup>114</sup> W. Murray and P. Mansoor, *Hybrid Warfare* (Cambridge: CUP, 2012).

<sup>115</sup> *Quadrennial Defence Review*, 8.

<sup>116</sup> See: Arquilla, *Information Warfare*, 205; Floridi and Taddeo, *Information Warfare*, 2.

<sup>117</sup> Ford, *Jus Ad Vim*, 63-65.



‘exceptional’ conditions that are normally required as a justification for a target state to respond. This explains why – despite the significant outrage and political (Western) focus upon Russia’s hybrid actions – there has been such a limited military response. It is exemplified in the limited military options available to the Europe under the JWT in response to what Prime Minister May described, following Russia’s annexation of Crimea, as the “first time since the Second World War that one sovereign nation has forcibly taken territory from another”.<sup>118</sup>

The remainder of this section analyses these JWT-related challenges in the context of the key elements of the ‘full spectrum’ approach that is the hallmark of Hybrid Warfare.

### *Cyber Warfare*

As Lucas authoritatively wrote in 2017, there is no agreement on “whether cyberwarfare even exists”.<sup>119</sup> Consequently, an examination of the various definitions of cyberwarfare and their impact on JWT is necessary. This will lead to an investigation of JWT’s three schools of thought on cyberwarfare, before concluding by examining just cause and proportionality. These criteria have been chosen as they reveal two key challenges to JWT that are emblematic of Hybrid Warfare. The first is the incompatibility between Hybrid Warfare’s limited lethality

---

<sup>118</sup> Prime Minister T. May, “Lord Mayor’s Banquet” (Speech, London, November 13, 2017) <https://www.gov.uk/government/speeches/pm-speech-to-the-lord-mayors-banquet-2017> (accessed April 9, 2018).

<sup>119</sup> Lucas, *Ethics and Cyberwarfare*, 33.

versus JWT's limited ability to address non-lethal acts. The second is the key challenges posed by the embryonic evolution, limited understanding and conflicted literature on cyberwarfare, let alone the wider work of JWT. Both of which are symptomatic of the evolution of capability, understanding and literature for Hybrid Warfare, and JWT's application to it.

There are three perspectives on how cyberwarfare is defined. The first perspective is that there is no such thing as cyberwar to which JWT can apply. The most influential advocate, Rid, defines war as violent, instrumental and political, which he then uses to 'prove' that no cyber-attack has met all three criteria, judging it highly unlikely to do so in future.<sup>120</sup> He perceives cyber-conflict as "neither a crime nor war, but rather in the same category as subversion, [and] spying".<sup>121</sup> Even those who oppose his analysis accept that "cyberwar might not literally be war".<sup>122</sup> If one accepts this narrow definition of war, it suggests JWT is irrelevant to cyberwarfare. It is difficult to argue with the accuracy of this point, particularly when using a Walzerian legalist paradigm.<sup>123</sup> However, there may be exceptions to the rule, as evidenced by the Tallinn Manual – written by an authoritative and wide body of experts – unanimously agreeing that the Stuxnet attack against Iran's nuclear programme was an 'armed attack' that would have entitled armed self-defence.<sup>124</sup> By

---

<sup>120</sup> Rid, *Cyberwar Cannot*, 6. See also Eberle, *Cyberwar*, 60.

<sup>121</sup> Rid, *Cyberwar Cannot*, 5.

<sup>122</sup> Dipert, *Ethics of Cyberwarfare*, 398.

<sup>123</sup> See Walzer, *Just and Unjust Wars*, 44. Note there are those who seek to bypass this traditional use of JWT using pre-Westphalian arguments (see Whetham, *Fighting*, 55-69).

<sup>124</sup> D.Joyner, "Stuxnet an 'Act of Force'," *Arms Control Law* (March 25, 2013), <https://armscontrolaw.com/2013/03/25/stuxnet-an-act-of-force-against-iran/> (accessed May 8, 2017).

this verdict, Stuxnet was violent and instrumental, at the very least, thereby meeting two of Rid's criteria. This point is validated by the fact that, to function, Stuxnet needed to be physically destructive. This implies that Rid's argument relies upon cyber never being employed politically. Yet Stuxnet was also arguably political. Furthermore, state actors are by definition political. Proposing continued non-political cyber employment seems a foolhardy suggestion, as illustrated by numerous sources<sup>125</sup> and the fact that many militaries have elevated the significance and role of cyber capability to sit alongside physical domains<sup>126</sup>. Thus, cyberwarfare can exist, and has likely already been undertaken, even under Rid's strict definition. This paper therefore dismisses Rid's argument on these grounds and develops the premise that cyberwar is not so different that it entirely precludes JWT.

The second perspective is that JWT can apply to all forms of cyberwar, whether they meet the definition of war or not. Schmitt, as the most strident proponent of this view, states in the forward of *Cyberwar* that "all experts agree" that contemporary *Jus Ad Bellum* can unequivocally apply to all cyber conflicts, with indisputable recognition of this fact by the UN.<sup>127</sup> While such a view would indicate universal JWT application, it is decisively undermined by three points. First, Schmitt applies

---

<sup>125</sup> *Intelligence and Security Committee of Parliament Annual Report 2016–2017*, HC 655 Session 2016–2017 (20 December 2017), 30–31. C. Demchak, *Wars Of Disruption And Resilience* (Athens: University of Georgia Press, 2011), 21.

<sup>126</sup> See L. Ferdinando, "Cybercom to Elevate to Combatant Command," US Department of Defense (May 3, 2018), <https://www.defense.gov/News/Article/Article/1511959/cybercom-to-elevate-to-combatant-command/> (accessed May 15, 2018).

<sup>127</sup> C.Finkelstein *et al.*, *Cyberwar* (Oxford: OUP, 2015), v–viii.

mostly legal rather than JW justifications to sustain his argument. Second, real-world JWT application does not conform to this view, as illustrated by NATO countries rejecting Russia's 2008 cyber-attack of Estonia as a just cause for war.<sup>128</sup> Third, the evidence used by Rid above, whilst flawed, undermines Schmitt's absolutist notion. Thus, one cannot argue that JWT universally and always applies to cyberwar.

The third perspective offers a less restrictive definition of war, thereby allowing JWT to apply in some but not all forms of cyber conflict. First suggested by Cook,<sup>129</sup> it seems the most credible perspective for two reasons. First, and most compelling, is the evidence already cited above that demonstrates possible but inconsistent JWT application. Second, the notion that cyberwar can be an act of war is well evidenced in practice and theory, as definitively shown by the White House and NATO stating certain cyber-attacks are just cause for war<sup>130</sup>.

Having examined the impacts of how one defines cyberwar, we must now more specifically analyse its link to JWT. There are, broadly, three schools of thought regarding its relevance to cyberwarfare. The first school is unconvinced that cyberwarfare raises any ethical or explicatory challenges not already addressed by JWT<sup>131</sup>. The second take the opposite view, believing the

---

<sup>128</sup> Floridi and Taddeo, *Information Warfare*, 107.

<sup>129</sup> Cook, *Response*, 411.

<sup>130</sup> NATO. *Warsaw Summit Communiqué* (Brussels: NATO, 2016), 16. US. *International Strategy for Cyberspace* (np: 2011), 13, <https://obamawhitehouse.archives.gov> (accessed May 8, 2018).

<sup>131</sup> See R. Crisp, "Cyberwarfare: No New Ethics Needed", *Practical Ethics Blog* (Oxford University), 2012, <http://blog.practicaethics.ox.ac.uk/2012/06/cyberwarfare-no-new-ethics-needed/> (accessed May 1, 2018); Cook, *Response*, 411-423.

challenge posed by cyber activity is completely unaddressed by JWT, therefore requiring an entirely new meta-ethical framework of analysis.<sup>132</sup> The third, assumes a middle ground, accepting JWT as relevant but needing modification to fully address the novel challenges posed by cyber.<sup>133</sup> As can be seen by the authors cited, moderates currently hold a majority, albeit not dominant, position in the discourse. This suggests that JWT is undermined by cyber warfare somehow. However, further examination is required.

What many authors from these three schools identify but often fail to fully address is the incompatibility of cyberwarfare's limited lethality versus JWT's limited ability to encompass non-lethal acts, which resonates with the cyberwar definitional discussion above.<sup>134</sup> Even the *Journal of Military Ethics* issue dedicated to cyber war failed to address this seeming incompatibility, often assuming that JWT can apply more broadly.<sup>135</sup> This lacuna will be examined using the just cause principle.

The post-Westphalian, Walzerian just cause is based on aggression or attack by the enemy.<sup>136</sup> The UN Charter – used here as an impartial authority and because it is derived from JWT

---

<sup>132</sup> See S. Bringsjord and J. Licato, "By Disanalogy, Cyberwarfare Is Utterly New", *Philosophy & Technology* 28, no. 3 (2015): 339-358; Dipert, *Ethics of Cyberwarfare*, 384-410.

<sup>133</sup> D. Denning and B. Strawser, "Moral cyber weapons", in *Information Warfare*, 85-103; Lucas, *Ethics and Cyberwarfare*, L. Kahn, *Understanding*, M. Sleat, "Just Cyber War?: Casus Belli, Information Ethics, and The Human Perspective", *Review Of International Studies* 44, no. 02 (2017): 324-342.

<sup>134</sup> For exceptions, see: Sleat, *Just Cyber War*; and Whetham, *Fighting*.

<sup>135</sup> Vol.12, Issue 1.

<sup>136</sup> M. Walzer, *Just and Unjust Wars*, 4<sup>th</sup> edn (New York: Basic Books): 51.

– concurs and defines armed attack as “use of force against the territorial integrity or political independence of any state”.<sup>137</sup> Most JWT paradigmatically casts armed attack, and just cause, in terms of a physical invasion.<sup>138</sup> Diptert cites this as one reason why JWT is “stretched” and cannot apply to cyber warfare.<sup>139</sup> However, while this characterisation may be the ‘gold standard’ of *casus belli* it is an inaccurately narrow example of accepted just causes, which includes broader issues resulting in lethality. It is therefore perfectly reasonable to consider a cyberattack a just cause if, for example, it kills through power loss to air traffic control and hospitals. Thus, while contested, it is reasonable to assert that JWT can apply to lethal cyberwarfare.

If JWT is ‘stretched’ to apply to lethal forms of cyberwarfare, it is fundamentally challenged by non-physical forms of cyberwarfare. Orend uses hypothetical examples of a country, devastated by a neighbour refusing to trade, as having insufficient just cause for war.<sup>140</sup> There are similarities to the potential non-lethal devastation cyberwarfare poses – to the stock exchange for example – and yet still fail to meet just cause. By these terms, JWT cannot explain or justify Russia’s use of cyberwarfare in Georgia, Estonia or Syria, for example. It is for this reason - best articulated by Rousseau’s remark that it is “possible to kill a state without killing any of its members”<sup>141</sup> – that some JW theorists seek to unfix JWT from its exclusive

---

<sup>137</sup> UN. *Charter of the United Nations*. (Geneva: UN, 1945), Ch.1-Art.2-Sect.4, <http://www.un.org/en/charter-united-nations/> (accessed Jan 10, 2018).

<sup>138</sup> Heuser, *Resurgence*, 113-115.

<sup>139</sup> Diptert, *Ethics of Cyberwarfare*, 396.

<sup>140</sup> B. Orend, *Morality Of War* (Ontario: Broadview Press, 2013), 32.

<sup>141</sup> J. Rousseau, *The Social Contract* (New York: Cosimo, 2008), 20.

adherence to violence and thereby enable greater application to cyberwarfare. While such theorists are justifying this wider purview with various moral gymnastics regarding indirect harm,<sup>142</sup> it does not escape the point that the body of JWT do not agree.<sup>143</sup> Even if one accepts the moral gymnastics described above, the majority of cyber-attacks are not destructive. Stuxnet may be the only example, and even that did not cause human harm. This is not to say destructive attacks will not happen, merely that that the character of cyberwarfare is best characterized by non-destructive attack. Consequently, JWT is fundamentally challenged by and unable to explain non-violent cyber warfare, the predominant form of this warfare.<sup>144</sup> At the very least, it seems that just cause or the JW definition of force would need to be modified. However, as the moral framework is designed to constrain the exceptional condition of war, the dominant JW theorists' view of retaining a narrow definition seems appropriate, even if at cost to intellectually explaining non-lethal cyberwarfare.

Despite these limits in just cause application, it is worth continuing the examination for three reasons. First, there are a minority of JW theorists who ascribe to the loosened definition of just cause to non-destructive cyberwar. Second, there is a logical argument, however contested, to non-physical harms being included under just cause. Third, there are a larger majority that conflate or ignore this problem. These three points

---

<sup>142</sup> Kahn, *Understanding*, 387-389.

<sup>143</sup> See Walzer's discussion on the immorality of *Jus Ad Vim*, for example: Walzer, *Just and Unjust Wars* (4<sup>th</sup> edn), xiv–xviii. See also B. Orend, *Fog In The Fifth Dimension*, 27.

<sup>144</sup> The few exceptions to this will be covered in succeeding paragraphs.

highlight a key conclusion. That of JWT's conflicted and incomplete discourse on cyberwarfare, reflecting the embryonic development, use and understanding of the capability. This, in turn, resonates with the same issue facing JWT's application to wider Hybrid Warfare, as illustrated by Whetham's article on this subject posing more questions than answers<sup>145</sup>.

As noted above, JWT narrowly defines harm in physical and, typically, human, terms. When using this to apply the criteria of proportionality, non-lethal cyber-attacks are deemed ethical – or at least not applicable to JWT – as they do not constitute physical harm. By this measure, almost all cyber-attacks would be allowed, as they pose no harm. One could argue this therefore explains the prevalence of Russian cyber activities. However, this seems morally perverse, not in keeping with JWT intent, and belies Russian attempts at remaining covert in their attacks. Furthermore, such latitude is of limited use in justifying, constraining or explaining war. It is not the criteria that the 'good should be greater than the harm' that is at fault but, rather, it is the definition of good and harm that reveals its inadequacy when considering cyberwarfare.<sup>146</sup> This resonates with the definitional problem just posed regarding just cause. Therefore, as with just cause, the principle of proportionality is largely irrelevant without a broader definition of good and harm.

If one erodes the definition of proportionality to include non-physical harm, then, as with an erosion of just cause, it may more

---

<sup>145</sup> Whetham, *Fighting*, 55-69.

<sup>146</sup> M. Taddeo, "Information Warfare and Just War Theory", in *Information Warfare*, 131.



ably account for war but will also lower the threshold for war and increase the subjectivity of the framework. For example, it would allow one to morally judge and explain Russia's cyber intervention in Estonia in 2007 and the wider hybrid interventions in Ukraine since 2014. However, as the threshold for both proportionality and just cause are now more subjective, it could equally allow Russia to justify these actions. Reason, alone, may suggest Russian actions were unjustified, but the erosion of the more precisely measured physical harm exposes broader definitions to subjectivity. How does one measure the harm to national honour caused by moving an Estonian statue versus the equally imprecisely measured economic harm following a cyberattack? In this sense, it compounds the "comparison of incommensurables" problem Rodin posed 'traditional' JWT.<sup>147</sup> In layman terms, the broader definition of harm moves from an incommensurability problem of comparing 'apples and pears' to a bigger disparity of comparing, for example, apples and stock markets. Thus, the broader revisionist definition of proportionality offers greater application to cyberwarfare but, in doing so, becomes susceptible to even more subjectivity and incommensurables.

This section has disputed two of the three major JWT schools of thought: cyberwar is not so different that it entirely precludes JWT; yet it is sufficiently different to prevent universal application. Examination of the theory and practice of cyberwar revealed a less restrictive definition of war now in place, thereby allowing JWT to apply in some but not all forms of cyberwar.

---

<sup>147</sup> Rodin, *War and Self-Defense*, 115.

This analysis also identified that most authors fail to fully address the incompatibility of cyberwarfare's limited lethality versus JWT's constrained ability to encompass non-lethal acts.

This same analysis identified JWT's conflicted and incomplete discourse on cyberwarfare, reflecting the embryonic development, use and understanding of cyber, which is, in itself, microcosmic of the same issues facing JWT and Hybrid Warfare. Analysis of proportionality identified that without a broader definition, it is largely irrelevant; but with a broader definition, it becomes more flawed by incommensurability.

### *Attribution*

If definitional tensions devalue the employment of proportionality, there is a wider issue that often means JWT is entirely ignored: the problem of attribution. This equally applies to other forms of Hybrid Warfare. Therefore, this sub-section will draw on those other manifestations of Hybrid Warfare, but predominantly use the lens of cyberwarfare as the more challenging component to attribute.

The potential for achieving attribution is contested. At one extreme, US Defence Secretary Panetta stated in 2012 that "potential aggressors should be aware that...[we have] the capacity to locate and hold them accountable"<sup>148</sup>. At the other,

---

<sup>148</sup> L. Panetta, "Secretary Panetta on Cybersecurity" (Speech, New York, October 11, 2012), <http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136> (accessed February 1, 2018).

Cook asserts that achieving a trace will often be impossible, presenting a challenge that is “new in the history of warfare”.<sup>149</sup> However, neither view should be taken at face value. Panetta is more likely delivering a deterrence message than an honest explanation of capability: something *The Economist* suspected at the time.<sup>150</sup> Equally, Cook fails to address the obvious implication that without high confidence in identifying an attacker JWT is stymied, if not entirely bypassed. It is for this reason that many academics view attribution as “the most difficult problem” in identifying an aggressor upon which JWT’s principles can be employed.<sup>151</sup> A problem that is unresolvable until a technical solution is delivered.<sup>152</sup> On this basis, it constitutes a fundamental challenge to JWT, as it is unable to provide a justificatory or explanatory response to cyber-attacks. Yet, if one accepts this point, the same can be said of all other frameworks.

A more specific failing relating to JWT is revealed by those that argue there is no longer a technical challenge to attribution. Lucas’ 2017 book, *Ethics and Cyberwarfare*, only offers his view on this aspect of attribution in his footnotes when stating that huge strides in technical knowhow have overcome the “enormous obstacle...to moral and legal accountability”, making deniability implausible and JWT entirely applicable.<sup>153</sup> Yet his judgement is

---

<sup>149</sup> Cook, *Response*, 419.

<sup>150</sup> [No author], “Cyberwarfare.” *The Economist* (December 8, 2012); <https://www.economist.com/international/2012/12/08/hype-and-fear> (accessed February 15, 2018).

<sup>151</sup> Singer and Friedman, *Cybersecurity*, 73. Also Whetham, *Fighting*, 61.

<sup>152</sup> Eberle, *Just War and Cyberwar*, 57.

<sup>153</sup> Lucas, *Ethics and Cyberwarfare*, 80.

based on the belief that attribution is simply a technical hurdle. This rests on the two fundamental assumptions: that attribution is a binary outcome without equivocation; and, that when achieved, it will be readily comprehensible to a non-technical audience.<sup>154</sup> Yet attributing Stuxnet required almost unheard of commercial resources (numerous agencies and specialist companies), months to merely reveal a level of confidence, not certainty.<sup>155</sup> The US Government makes the wider point regarding Hybrid Warfare, when noting attribution is “not a simple statement of who conducted an operation, but rather a series of judgments”.<sup>156</sup> A point evidenced by two pages describing their necessary “estimative language”.<sup>157</sup> Thus, while this proves that credible attribution is possible, it counters the revisionist claim that the problem has been entirely overcome. Indeed, it leads one to the conclusion that attribution is more a matter of degree, with equivocal evidence that is difficult acquire, difficult to comprehend and open to political interpretation.

How does this difficulty and equivocation impact JWT? This paper offers one primary impact: intellectual ambiguity. One accepts Whetham *et al's* argument that lack of attribution does not prevent the cyber-attack being a cause for war,<sup>158</sup> but the problem is not certainty of an act of war but certainty of the perpetrator's identity, without which the other JWT criteria

---

<sup>154</sup> For similar more detailed argument, see T. Rid and B. Buchanan, "Attributing Cyber Attacks", *Journal of Strategic Studies* 38, no. 1-2 (2014): 4-37.

<sup>155</sup> See J. Lindsay, "Stuxnet And The Limits Of Cyberwarfare", *Security Studies* 22, no. 3 (2013): 365-404.

<sup>156</sup> *Assessing Russian Activities*, ICA-2017-01D, 2.

<sup>157</sup> *Ibid.*, 13-14.

<sup>158</sup> Lucas and Whetham, *Relevance*, 166.

cannot be applied. Where the perpetrator may be identified by circumstantial evidence, JWT cannot morally justify a response.<sup>159</sup> Even if a state is entirely certain who attacked it, the victim may be unable to persuade the international community due to the difficulty to verify or comprehend the data.<sup>160</sup> In contrast, a realist framework can provide this function as stopping the attack or future attacks is the priority, not justice. Thus, absence of attribution, the more common trait, prevents employment of JWT. Even when attribution is achieved, its ambiguity challenges JWT's ability to explain and justify a response. It is perhaps for this reason that the US Senate's Armed Forces Committee recently heard that Russia has "grown more emboldened, conducting increasingly aggressive [cyber] activities to extend their influence with limited fear of consequences".<sup>161</sup>

### *Misinformation Warfare*

Misinformation appears to be entirely discounted in JWT literature as irrelevant to war due to two fundamental challenges. This section will examine each challenge in turn, before focussing on two criteria, proportionality and just cause, which

---

<sup>159</sup> M. O'Connell, "Cyber Security Without Cyber War", *Journal Of Conflict And Security Law* 17, no. 2 (2012): 187-209.

<sup>160</sup> N. Rowe, "The Attribution of Cyber Warfare," in *Cyberwarfare*, 69.

<sup>161</sup> L. Ferdinando, "U.S. Faces Evolving, Emboldened Adversaries in Cyberspace, Officials Warn," US Department of Defense (April 11, 2018), <https://www.defense.gov/News/Article/Article/1491086/us-faces-evolving-emboldened-adversaries-in-cyberspace-officials-warn/> (accessed May 15, 2018).

show how misinformation weakens JWT application to more lethal modes of hybrid warfare.

The first challenge lies in the inability of information warfare to achieve physical harm and, therefore, the impossibility of it invoking JWT.<sup>162</sup> This perceived wisdom has become so prevalent that many do not even feel the need to address it, including in books titled *Information Warfare Ethics*, which merely discounts misinformation without justification.<sup>163</sup> Yet, it is possible to achieve lethality with misinformation. Three examples prove this. First, and most compelling, Muslim and Hindu tensions in India were exploited by misinformation in 2013. In an action designed to provoke, a still unidentified actor posted a brutal video of two men being beaten to death, with a caption identifying the victims as Hindu and the mob as Muslim, which caused mass rioting requiring 13,000 troops to quell it.<sup>164</sup> While the video did show two men being killed, it was not sectarian, as described, or even in India – it was fake news. There are similar examples of, likely non-state, misinformation either causing war, as occurred in 1898 when the US declared war on Spain,<sup>165</sup> or from the leader of the anti-Rohingya movement in

---

<sup>162</sup> Arquilla, *Twenty Years*, 205.

<sup>163</sup> See footnote 28.

<sup>164</sup> M. Magnier, “Hindu Girl’s Complaint Mushrooms into Deadly Indian Riots,” *Los Angeles Times* (September 9, 2013). <http://articles.latimes.com/2013/sep/09/world/la-fg-india-communal-20130910> See also: Senate Armed Services Committee, Subcommittee on Cybersecurity, *Testimony: The Weaponization of Information* by R. Waltzman, CT-473 (Santa Monica: RAND, 2017), 2; <https://www.armed-services.senate.gov/hearings/17-04-27-cyber-enabled-information-operations> (accessed Jan 10, 2018).

<sup>165</sup> K. Swenson, “The bloody history of April 20: Mass murders, a ‘fake news’ war and environmental disaster,” *Washington Post* (April 20, 2014), [https://www.washingtonpost.com/news/morning-mix/wp/2018/04/20/the-weird-bloody-history-of-april-20-mass-murders-a-fake-news-war-and-environmental-disaster/?noredirect=on&utm\\_term=.b890da211b7f](https://www.washingtonpost.com/news/morning-mix/wp/2018/04/20/the-weird-bloody-history-of-april-20-mass-murders-a-fake-news-war-and-environmental-disaster/?noredirect=on&utm_term=.b890da211b7f) (accessed February 15, 2018).

Myanmar using fake news to reach “100 times as many” as he did from paper leaflets. This latter example undoubtedly contributing to some (but not all) of the harm involved in, what the UN has called “textbook ethnic cleansing”.<sup>166</sup> One could argue these examples of non-state actors are irrelevant to JWT. Yet this would miss the wider point that they prove it is possible to harm with misinformation. If the capability exists then one must account for its potential use, in the same manner JW theorists argue for cyberwarfare. The only difference being that harm has been proven for misinformation but only theorised for cyberwar – a point that no other JW theorist appears to have identified. Thus, excluding misinformation from JWT is both incorrect and, as currently defined by the body of JWT literature, limits its ability to explain war. Ironically, this is arguably more a flaw with the extant theorising than the theory itself.

This leads to the second challenge, that information warfare is merely a tool to accompany conventional warfare rather than an act of war itself.<sup>167</sup> While this seems reasonable, particularly from the philosophical perspective, evidence indicates that a more nuanced, albeit contested, view is that information is rarely an act of war but that it can be. In theory, this paper has proved that misinformation can cause indirect harm at scale: *ipso facto* it can be an act of war. In practice, both US Chairmen of the

---

<sup>166</sup> M. Ingram, “In some countries, fake news on Facebook is a matter of life and death,” Columbia Journalism Review (November 21, 2017) <https://www.cjr.org/analysis/facebook-rohingya-myanmar-fake-news.php> (accessed February 15, 2018).

<sup>167</sup> J. Arquilla, “Ethics And Information Warfare”, in *Strategic Appraisal: Changing Role Of Information In Warfare* (Santa Monica: RAND, 1999), 384.

respective Houses' Foreign Affairs Committees seem to agree,<sup>168</sup> with Senator McCain even declaring the 2016 Russian information activity that affected US elections an “an act of war”<sup>169</sup>. While this may be deterrence messaging, McCain’s view is authoritative and reasonable when one considers, aside from the cyber-attacks, the significance of a foreign power breaching sovereignty to covertly contact over 129 million citizens to directly influence elections, as both the media and US Government recently recognized.<sup>170</sup> Reinforcing this point, one senior Russian official told the Russian National Security Conference that Russia was working on new strategies in the “information arena” equivalent to testing a “nuclear bomb” and which would “allow us to talk to the Americans as equals”.<sup>171</sup> Even if one accounts for hyperbole, this sounds like information activity that equates to an act of war. The fact that academics and NATO generals believe Russia “won in Crimea...based principally on information warfare”<sup>172</sup> through “the most amazing information warfare blitzkrieg we have ever seen in

---

<sup>168</sup> C. McGreal, “Vladimir Putin’s “Misinformation” Offensives Prompts US to Deploy its Cold War Propaganda Tolls,” *The Guardian* (April 25, 2015).

<https://www.theguardian.com/world/2015/apr/25/us-set-to-revive-propaganda-war-as-putin-pr-machine-undermines-baltic-states> (accessed February 15, 2018).

<sup>169</sup> T. Schleifer and D. Walsh, “McCain: Russian cyberintrusions an ‘act of war,’” *CNN* (December 31, 2016). <https://edition.cnn.com/2016/12/30/politics/mccain-cyber-hearing/index.html> (accessed February 15, 2018).

<sup>170</sup> *Assessing Russian Activities*, ICA-2017-01D. No author, “My truth against yours,” *The Economist* (January 25, 2018), <http://www.economist.com/news/special-report/21735479-power-fake-news-and-undue-influence-waging-war-disinformation?frsc=dg%7Ce> (accessed February 15, 2018).

<sup>171</sup> D. Ignatius, “Russia’s Radical New Strategy for Information Warfare,” *The Washington Post* (January 18, 2017). <https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/> (accessed April 7, 2018).

<sup>172</sup> R. Thornton, “The Changing Nature Of Modern Warfare”, *RUSI Journal* 160, no. 4 (2015): 40.



history”,<sup>173</sup> reinforces this argument, and highlights the increasing scale and significance of information warfare. This paper will avoid descending into a detailed philosophical discussion on how one defines war. Instead, it will remain epistemic, and conclude that while the ambiguity of information war inevitably makes it a contentious *casus belli*, it *may* be possible, in exceptional circumstances, that misinformation be considered an act of war. What is not clear, and what will not be covered in this essay, is how it would differ from other non-kinetic actions such as economic sanctions. Nevertheless, the growing political and military evidence above indicates that this clarity is something JWT – and a wider body of moral philosophy - needs to address rather than discount with insufficient evidence.

Having considered the overarching challenges misinformation poses JWT, the following section will examine how misinformation weakens JWT application to more lethal modes of hybrid warfare. This will be achieved by examining, proportionality and just cause, as two criteria that appear to pose the greatest challenge to JWT.

Some suggest that one of the more successful misinformation subversions of JWT by Russia was to exploit proportionality. For example, Freedman purports Russia magnified the sense of danger it presented to Europe in 2014, such as regular reminders of Russia’s nuclear strength, thereby deterring the West from

---

<sup>173</sup> J. Vandiver, “SACEUR: Allies must prepare for Russia ‘hybrid war’,” *Stars and Stripes*, (September 4, 2014) <http://www.stripes.com/news/saceuralliesmust-prepare-for-russia-hybridwar-1.301464> (accessed February 15, 2018).

supporting Ukraine as much as it might otherwise have done.<sup>174</sup> However, while Freedman may be correct that Russian misinformation warfare, supported by military activity, magnified the cost of confronting Russia in Ukraine,<sup>175</sup> one must be careful not to over-emphasise this impact on proportionality for three reasons. First, it is especially difficult, arguably impossible, to isolate and measure the impact of misinformation warfare. Second, and most importantly, it is unlikely that the West would have gone to war for Ukraine, as their treaty obligations may oblige, for the very reason that Russia poses unique ‘proportionality’ issues as a nuclear power. Preventing a small war in Ukraine is not worth the cost of potential nuclear conflict. On this basis, the JWT principle of proportionality seems fair. The third reason, which also reinforces the flaw of JWT, is that proportionality was bypassed: Russian misinformation warfare obfuscated their actions, weakening the ‘traction’ just cause could achieve, thereby precluding all other JWT criteria that routinely follow. To summarise, in explaining the limited Western response to Russian action in Ukraine, Russian use of misinformation warfare revealed a susceptibility in JWT’s proportionality principle to subjectivity, but the primary proportionate consideration appears to have been the seemingly objective fear of causing a disproportionate (worst case, nuclear) war with Russia. The greater impact of

---

<sup>174</sup> Freedman, *Ukraine*, 24.

<sup>175</sup> See M. Bodner, “Russia Hardens Military Thinking as NATO Fizzes Over Ukraine,” *Moscow Times* (September 7, 2014), <http://www.themoscowtimes.com/business/article/russia-hardens-military-thinking-as-natofizzes-over-ukraine/506570.html> (accessed May 15, 2018).

misinformation warfare, however, appears to be subverting just cause. This latter point requires further examination.

Russia appears to be subverting just cause for their own gain through reflexive control. Thomas, an authority on this subject, defines reflexive control “as a means of conveying to an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action”<sup>176</sup>. Jonsson and Seally argue an example of such control, through misinformation, was Russia provoking Georgia into conceding just cause to Russia in their 2008 war.<sup>177</sup> A point seemingly validated by UN Fact Finding Mission at first recognising Russia’s just cause, following Georgian aggression, but then noting Georgia’s actions largely originated due to months of “provocations” and mistruths from Russia.<sup>178</sup> A more compelling example is revealed by a leaked 2006 US government memo noting:

pro-Russian forces in Crimea, acting with funding and direction from Moscow, have...focused on systematically shaping public perceptions and controlling the information space...to [create pro-Russian views and] destabilize Crimea, weaken Ukraine,

---

<sup>176</sup> T. Thomas, "Russia's Reflexive Control Theory And The Military", *Journal of Slavic Military Studies* 17 (2004): 238.

<sup>177</sup> O. Jonsson and R. Seely, "Russian Full-Spectrum Conflict: An Appraisal After Ukraine", *Journal of Slavic Military Studies* 28, no. 1 (2015): 7.

<sup>178</sup> Independent International Fact-Finding Mission, *The Conflict in Georgia Report*, Vol II ([No location/publisher]: 2009), 30-33.

and prevent Ukraine's movement west into institutions like NATO.<sup>179</sup>

That this was the US view in 2006 is shockingly prescient to what happened in Crimea in 2014, particularly Russia's narrative of self-determination. A leaked Russian strategy document explicitly links such actions, secretly termed "pro-Russian drift" by the Russian Government, as aiming to "create events that will give...political legitimacy and moral justification" to annexing Crimea.<sup>180</sup> Pro-Russian drift, combined with massive amounts of misinformation, essentially "imagined Novorossiia into being" and afforded nominal legitimacy to Russia annexing Crimea. Such actions are not isolated, as indicated by the same leaked Kremlin document describing similar reflexive control in "eastern regions" and other reports of such action in the Baltics.<sup>181</sup> Thus, Russia has subverted the positive moral and explicatory framework of Just Cause by covertly provoking states into breaching Just War principles to thereby achieve nominal popular support and establish perceived Just Cause.

Subversion of just cause illustrates a wider problem that Russia poses to JWT and more generally: industrialised untruth and obfuscation. As Hellman and Wagnsson note, while Russia has

---

<sup>179</sup> US Embassy in Kyiv, *Ukraine: The Russia Factor In Crimea — Ukraine's 'Soft Underbelly'*, 06KYIV4489\_a, ([No location]: Wikileaks, 2006).

[http://www.wikileaks.org/plusd/cables/06KYIV4489\\_a.html](http://www.wikileaks.org/plusd/cables/06KYIV4489_a.html) (accessed May 8, 2018).

<sup>180</sup> Russian Federation, [*Unknown Title of Leaked Strategy Document*], trans. Google Translate, made available by A. Lipsky, "Plan for Russia's rejection of a number of Ukrainian territories, compiled in those days when Yanukovich was still the president of this country", *Novaya Gazeta* (February 24, 2015),

<https://www.novayagazeta.ru/articles/2015/02/24/63168-171-predstavlyaetsya-pravilnym-initsiirovat-prisoedinenie-vostochnyh-oblastey-ukrainy-k-rossii-187> (accessed May 8, 2018).

<sup>181</sup> *Ibid.*

a long history of deception, 21<sup>st</sup> century technology has allowed an unforeseen scale of misinformation to fuel confusion, lies and contradictory versions of events, thereby undermining the basis for rational debate.<sup>182</sup> One must recognise this as a problem for any explanatory intellectual or moral tool, yet it is a particular problem for JWT because of its particular vulnerability to subjectivity. In defence of JWT, some rightly argue that such misinformation was accurately identified as false.<sup>183</sup> However, this fails to recognise that Russia's mendacity did not aim to convince but to achieve two things. First, deliver sufficient uncertainty so that one doubts the epistemic approach, exploiting the growing Nietzschean perception that "[t]here are no facts, only interpretations".<sup>184</sup> As one US Senate Committee hearing put it, Russia is seeking to instil "distrust in all news outlets and ultimately one another".<sup>185</sup> Second, provide a *scale* of uncertainty to make it impossible to disprove claims, as illustrated by the loss of Malaysia Airlines Flight 17 over eastern Ukraine which, despite months of independent investigations,<sup>186</sup> struggled to effectively counter the "massive scale information warfare...and outright falsehood that Russia bore no responsibility", as one UK Intelligence Agency put it.<sup>187</sup> All of

---

<sup>182</sup> M. Hellman and C. Wagnsson, "How Can European States Respond To Russian Information Warfare? An Analytical Framework", *European Security* 26, no. 2 (2017): 156.

<sup>183</sup> L. Witschge, "Justice elusive 3 years from MH17 crash in east Ukraine," *Al Jazeera* (July 17, 2017). <https://www.aljazeera.com/indepth/features/2017/07/years-mh17-crash-east-ukraine-warzone-170716065152686.html> (accessed February 15, 2018).

<sup>184</sup> F. Nietzsche, *The Portable Nietzsche* (New York: Penguin Books, 2014), 458.

<sup>185</sup> House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, *Testimony by CYBERCOM Admiral M. Rogers (Apr 11, 2018)*, (Np: 2018), 5. <https://docs.house.gov/meetings/AS/AS26/20180411/108076/HHRG-115-AS26-Wstate-RogersM-20180411.pdf> (accessed May 10, 2018).

<sup>186</sup> N. Inkster, "Information Warfare And The US Presidential Election", *Survival* 58, no. 5 (2016): 23-32.

<sup>187</sup> *Intelligence Committee Report*, HC 655 Session 2016-2017, 51.

which is compounded by the Western media's professional obligation to report both sides of a story, thereby magnifying the veneer of legitimacy.<sup>188</sup> Thus, Russia's goal was not to rebut, but to obfuscate; not to determine the truth but realise many 'truths'. Indeed, this is not only achieved by overt Russian action. Part of the plausibility is use of pro-Russian influencers in media and policy circles who make no reference to their Kremlin connections.<sup>189</sup> In this sense, Russia not only subverts JWT by seeking to meet *Jus Ad Bellum* with misdirection but simultaneously seeks to bypass JWT by obfuscating their real actions and intent. In turn, this constrains the ability of states – using legal or moral frameworks – to craft common measures for countering Russia's aggressive actions<sup>190</sup>.

Such obfuscation and misdirection reveal two further issues with JWT. First, rather than constraining and explaining state employment of war, misinformation warfare weakens JWT moral and intellectual validity to the point that it merely constrains the nominal appearance rather than substantive action of states. For example, the 'BRIC' countries readily supported Russia's version of events in Crimea. Considering the broad media castigation and Western sanctions, 'BRIC' support seems better explained by Realism than JWT.<sup>191</sup> If the

---

<sup>188</sup> Ibid.

<sup>189</sup> For a comprehensive list of such influencers, see P. Pomerantsev, "How Putin Is Reinventing Warfare", *Foreign Policy*, 2014, [http://www.foreignpolicy.com/articles/2014/05/05/how\\_putin\\_is\\_reinventing\\_warfare](http://www.foreignpolicy.com/articles/2014/05/05/how_putin_is_reinventing_warfare) (accessed February 15, 2018).

<sup>190</sup> For a longer discussion and primary evidence of this issue, see: *Testimony by CYBERCOM Admiral M. Rogers*, 5.

<sup>191</sup> For a detailed, compelling argument see: O. Stuenkel, *BRICS and Future Global Order* (Lanham: Lexington Books, 2016), 147-154.

substantive action was Hobbesian, the superficial reason was explained in subverted JWT terms, as illustrated by the effort Russia took to appear “law abiding and [act as if it was] doing the right thing”, framing everything in humanitarian terms.<sup>192</sup> Such nominal explanations using JWT to mask seemingly deeper Hobbesian ones is typical of contemporary Russian action, as evidenced by the 2008 Georgian War and on-going support to Syria. However, one cannot attribute this entirely to Russia. Indeed, the already explained subjectivity of JWT illustrated this point, as did the contemporary plurality of ‘public adjudicators’ to just wars. Nevertheless, it is a separate point: that JWT’s subjectivity and global ‘court of opinion’ is exploited by the increasing scale and significance of misinformation which, when used as information warfare, is weakening JWT’s ability to constrain and intellectually explain state actions. Thereby leading to perverse applications to mask Hobbesian action. This is similar to how Heinze and Steele explain a similar subversion of JW by Islamic State (IS): “The manner in which JW can be used to provide a veneer of legitimacy for...IS to use violence, and to exclude others as illegitimate, is an exercise much more covert and effective than the outright use of force”.<sup>193</sup>

Overall, the analysis of misinformation warfare delivered three conclusions. First, that misinformation can cause indirect harm at scale, indicating that JWT literature has been incorrectly excluding misinformation. Second, while the ambiguity of misinformation war inevitably makes it a contentious *casus belli*,

---

<sup>192</sup> Thornton, *Nature*, 44.

<sup>193</sup> Heinze and Steel, *Non-State Actors*, 13.

it *may* be possible, in exceptional circumstances, that information is considered an act of war by state actors. Third, that JWT literature needs to address both points, rather than just discount them with insufficient evidence.

The second half of this section made three arguments. First, state use of reflexive control subverts JWT by manipulating other states into providing perceived just cause, whether covertly provoking belligerence or manipulating the foreign population. Second, countries such as Russia not only subvert JWT by seeking to meet *Jus Ad Bellum* with misdirection but simultaneously seek to bypass it by obfuscating their real actions and intent. In turn, this constrains the ability of states – using legal or moral frameworks – to craft common measures for countering Russia’s aggressive actions. Third, rather than constraining and explaining war, misinformation warfare weakens JWT’s moral and intellectual validity to the point that it merely constrains the nominal appearance rather than substantive action of states. Overall, this paper does not suggest that all these challenges are new or exclusive to JWT. However, lack of exclusivity does not counter the challenge posed to JWT. Furthermore, thanks to the ubiquity of modern communication, such manipulation of perception is taking place on previously unimaginable scales and significance, as made available by Moores Law and as accepted by a US Senate Committee.<sup>194</sup> Thus, the second conclusion of this section is that the use of

---

<sup>194</sup> Senate Armed Services Committee, Subcommittee on Cybersecurity, *Testimony: The Weaponization of Information* by R.Waltzman, CT-473 (Santa Monica: RAND, 2017), 2, <https://www.armed-services.senate.gov/hearings/17-04-27-cyber-enabled-information-operations> (accessed Jan 10, 2018).



information warfare is undermining, obfuscating and bypassing Just War's ability to function in contemporary, traditional (lethal) conflict in potentially more novel, more significant and more frequent ways than ever seen before.

### *JWT and Hybrid Warfare in Practice*

Having identified some substantial flaws in JWT by detailed analysis of the theory, through the lens of cyberwarfare, misinformation and attribution, it would be equally useful to briefly examine Hybrid Warfare from a practical perspective. The key JWT question is: what are states doing and what are they tolerating being done to them? Lucas adroitly answers with "both doing, and apparently tolerating, just about anything".<sup>195</sup> Russian cyber activity in the West seems a case in point. In Ukraine, it allegedly stopped banks, railways and power-stations,<sup>196</sup> even possibly destroying 80% of Ukrainian artillery.<sup>197</sup> In the Baltics, it repeatedly attacked Estonia, Lithuania and Latvia, even kidnapping an Estonian officer.<sup>198</sup> In wider Europe, Russia likely hacked President Macron's emails to affect French elections;<sup>199</sup> "attacked" all the Scandinavian governments;<sup>200</sup> and, according to the head of Germany's Protection of the Constitution, influ-

---

<sup>195</sup> Lucas, *Ethics and Cyberwarfare*, 109.

<sup>196</sup> *Putin's Asymmetric Assault on Democracy in Russia and Europe*, S.Prt.115-21, 115<sup>th</sup> Congress, Second Session (10 January 2018), 68.

<sup>197</sup> Interfax, "Ministry denies reports of alleged artillery losses," *Interfax-Ukraine* (January 6, 2017). <https://en.interfax.com.ua/news/general/395186.html> (accessed April 7, 2018).

<sup>198</sup> McMaster, *Atlantic Council Baltic Summit*.

<sup>199</sup> *Putin's Assault*, S.Prt.115-21, 115<sup>th</sup> Congress, Second Session, 121-123.

<sup>200</sup> Prime Minister T.May, "Lord Mayor's Banquet" (Speech, London, November 13, 2017) <https://www.gov.uk/government/speeches/pm-speech-to-the-lord-mayors-banquet-2017>. (accessed April 9, 2018).

enced the German election.<sup>201</sup> In the UK, it conducted over “188 major attacks against the British Government” in a mere three-months,<sup>202</sup> possibly influenced a referendum,<sup>203</sup> and probably conducted two assassinations on British soil with chemical and radioactive material.<sup>204</sup> In the US, it conducted the “bold-est...most significant escalation” yet by seeking to directly influence the 2016 US presidential election, as US agencies recently reported.<sup>205</sup> Such was the scale and significance of Hybrid Warfare that the US Senate wrote a comprehensive 2018 report titled “Putin’s Asymmetric Assault on Democracy in Russia and Europe”.<sup>206</sup> Whatever the theoretical conclusions made in previous sections, practically, Russia does not appear to adhere to JWT when using Hybrid Warfare. Yet Russia is not alone. There are equally egregious breaches of sovereignty by supposedly responsible US, UK, China, most notably in the cyber realm,<sup>207</sup> let alone Iran, Israel and North Korea.<sup>208</sup>

This global depiction of a brutish, anarchic world seems almost farcically Hobbesian, providing three pertinent challenges to JWT. First, hybrid warfare appears to sit astride and blur the

---

<sup>201</sup> No author, “Russia is trying to destabilise Germany,” *Al Jazeera* (December 8, 2016), <https://www.aljazeera.com/news/2016/12/bfv-russia-destabilise-germany-161208141856179.html> (accessed February 15, 2018).

<sup>202</sup> P. Paganini, “Britain’s Security Has Been Threatened by 188 Major Cyber Attacks,” *Security Affairs* (February 13, 2017), <http://securityaffairs.co/wordpress/56247/breaking-news/national-cyber-security-centre-hack.html> (accessed February 15, 2018).

<sup>203</sup> J. Watts, “Labour MP claims it’s ‘highly probable’ Russia interfered with Brexit referendum,” *The Independent* (December 13, 2016), <https://www.independent.co.uk/news/uk/politics/russian-interference-brexit-highly-probable-referendum-hacking-putin-a7472706.html> (accessed January 10, 2018).

<sup>204</sup> *Putin’s Assault*, S.Prt.115-21, 115<sup>th</sup> Congress, Second Session, 120.

<sup>205</sup> *Assessing Russian Activities*, ICA-2017-01D, 5.

<sup>206</sup> *Putin’s Assault*, S.Prt.115-21, 115<sup>th</sup> Congress, Second Session.

<sup>207</sup> Stuxnet being a case in point.

<sup>208</sup> *Intelligence Committee Report*, HC 655 Session 2016-2017, 30-31.

definitions of warfare, reinforcing the similar theoretical point made previously. Second, the scale and frequency of Hybrid Warfare shows that states are regularly ignoring JWT when employing Hybrid Warfare, no matter the theoretical flaws it may or may not have. This directly undermines the notion that JWT can intellectually explain Hybrid Warfare, even if it can morally judge it.

This foregrounds and reinforces two points developed in earlier sections. First, the intellectual traction of JWT is inextricably beholden to the dominant moral dimension. Second, in seeking to remain below the sub-legal threshold, *Jus Ad Vim* inadvertently seeks to nullify the moral, linguistic and intellectual JW apparatus used to justify and explain war. In so doing, it hinders the framing of the 'exceptional' conditions that are normally required to breach sovereignty and employ extraordinary (traditionally lethal or military based) measures against another state. Combined, this reveals a wider point regarding the tension between the modifications required to allow JWT to apply to the lowering threshold and definition of war versus the original requirement of JWT to morally constrain the lethal exceptionalism of war by *intentionally* not being applicable to non-lethal actions. In this sense, the non-lethal challenges posed by Hybrid Warfare force one to choose between the moral and intellectual framework. As JWT is, first and foremost, a moral framework, such challenges fundamentally diminish its ability to address Hybrid Warfare.



## Conclusion

Following a brief literature review, this paper examined two broad sections to identify JWT's ability to credibly explain contemporary warfare, globally. The first section assessed the cogency of claims and counter-claims surrounding whether JWT can or should be considered a globally acceptable and universally applicable concept in justifications for war and conflict initiation. In doing so, it addressed the validity of three recurring criticisms of religious bias, Western hegemony and subjectivity, making two conclusions. First, that JWT retains credibility as a global framework to identify the justifications for conflict initiation, but its historic flaws appear increasingly susceptible to forms of exploitation and misuse, which fosters dissent and inhibits consensus on why or how war occurs. This allows JWT to be exploited as a moral cover for immoral or self-seeking behaviours. Second, the intellectual traction of JWT is inextricably beholden to the popularity of the moral tool. Consequently, the intellectual tool is ultimately challenged if or when actors fail to use it morally. It is noticeable that this second conclusion does not appear to be recognised in the JWT literature.

The final section analysed the credibility and utility of JWT in the context of 'Hybrid Warfare' in four areas: cyberwarfare; misinformation warfare; the attribution problem; and the overall practice of Hybrid Warfare. This area yielded the most novel conclusions, arguably because it is evolving and the least

understood aspect, as intimated by the limited JWT literature on the subject. Therefore, it will be covered in some detail.

Examination of cyberwarfare offered two conclusions. First, it countered two of the three major JWT schools of thought: cyberwar is not so different that it entirely precludes JWT; yet it is sufficiently different to prevent universal application. Examination of the theory and practice of cyberwar revealed a less restrictive definition of war now in place, thereby allowing JWT to apply in some but not all forms of cyberwarfare. This analysis also identified that most authors fail to fully address the incompatibility of cyberwarfare's limited lethality versus JWT's constrained ability to encompass non-lethal acts. The second conclusion was that JWT's conflicted and incomplete discourse on cyberwarfare reflects the embryonic nature and understanding, which is illustrative of the wider JWT and Hybrid Warfare dynamic.

Analysis of misinformation warfare provided two conclusions. First, that JWT literature has been incorrectly excluding the broader forms of Information Warfare, such as 'misinformation', which may, in exceptional circumstances, be capable of achieving harm and therefore be an act of war. Second, that the use of misinformation warfare is undermining, obfuscating and bypassing Just War's ability to function in contemporary, traditional (lethal) conflict in potentially more novel, more significant and more frequent ways than ever seen before. Rather than constraining and explaining employment of war, misinformation warfare weakens JWT moral and intellectual

validity to the point that it merely constrains the nominal appearance rather than substantive action.

Examination of attribution identified absence of attribution as the more common trait of Hybrid Warfare which prevents employment of JWT. Even when attribution is achieved, its ambiguity challenges JWT's ability to explain and justify a response. The final sub-section, dealing with the overall practice of Hybrid Warfare, concluded that states are regularly ignoring JWT when employing Hybrid Warfare, no matter the theoretical flaws it may or may not have. This directly undermines the notion that JWT can intellectually explain Hybrid Warfare, even if it can morally judge it.

Throughout all these sections, a recurring theme was noted. That in seeking to remain below the threshold for war, Hybrid Warfare nullifies the moral, linguistic and intellectual Just War (JW) apparatus used to justify and explain war. In doing so, it hinders the framing of the 'exceptional' conditions that are normally required to breach sovereignty and other norms, and employ extraordinary (traditionally lethal or military based) measures against another state or actor. Yet, it is precisely the sub-threshold intent of Hybrid Warfare - and the likes of Russia going so far to be *seen* acting justly - which demonstrates that JWT does remain significant in shaping and explaining warfare. Ironically, by this measure, the recent development of Hybrid Warfare *could* be seen as a direct response and counter to the (now arguably reducing) relevance of JWT and its codification within the international system.

This leads to the final conclusion regarding the modifications required to allow JWT to apply to the lowering threshold and definition of war versus the original requirement of JWT to morally constrain the lethal exceptionalism of war by *intentionally* not being applicable to non-lethal actions. In this sense, the non-lethal challenges posed by Hybrid Warfare force one to choose between the moral and intellectual framework. As JWT is, first and foremost, a moral framework, such challenges fundamentally diminish its ability to address Hybrid Warfare.

Thus, the overall finding is that JWT remains a credible, global tool for explaining warfare without intrinsic bias. However, it has significant flaws, particularly in addressing non-lethal and information based conflict. While these flaws are not significant enough to warrant discarding JWT, they do undermine its credibility to explain the full gamut of contemporary war.



## Bibliography

### *Primary Sources*

#### *Publications and Other Reports*

Netherlands. Dutch Safety Board. *Preliminary Report: Crash Involving Malaysia Airlines Boeing 777-200 flight MH17*. The Hague: Dutch Safety Board, 2014.

<http://www.dca.gov.my/wp-content/uploads/2015/02/Preliminary-Report-MH17.pdf> (accessed Jan 10, 2018).

Independent International Commission on Kosovo, *The Kosovo Report*. Oxford: Oxford University Press, 2000.

Independent International Fact-Finding Mission. *The Conflict in Georgia Report*, Vol II. [No location or publisher] 2009. [http://www.mpil.de/files/pdf4/IIFFMCG\\_Volume\\_II1.pdf](http://www.mpil.de/files/pdf4/IIFFMCG_Volume_II1.pdf) (accessed January 10, 2018).

International Committee for the Red Cross. Protocol Additional to the Geneva Conventions. 1977. <https://ihl-databases.icrc.org/ihl/INTRO/470> (accessed May 1, 2018).

North Atlantic Treaty Organization. *Warsaw Summit Communiqué*. Brussels: North Atlantic Treaty Organization, 2016.

United Kingdom. Intelligence and Security Committee of Parliament. *Annual Report 2016–2017*. HC 655 Session 2016–2017. 20 December 2017.

<http://isc.independent.gov.uk/committee-reports/annual-reports> (accessed May 8, 2018).

United Kingdom. Cabinet Office. *National Security Capability Review*. [no cm.] March 2018.

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/705347/6.4391\\_CO\\_National-Security-Review\\_web.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf) (accessed May 8, 2018).

United Nations. *Security Council Holds Emergency Meeting In Response To Russian Federation's Request As Crisis Escalates In South Ossetia, Georgia*. Geneva: UN Press, 2008,

<https://www.un.org/press/en/2008/sc9417.doc.htm>  
(accessed January 10, 2018).

United Nations. *Charter of the United Nations*. Geneva: UN, 1945,  
<http://www.un.org/en/charter-united-nations/> (accessed January 10, 2018).

United States. Intelligence Community Assessment. *Assessing Russian Activities and Intentions in Recent US Elections*. Ref. ICA 2017-01D. ODNI: 2017.

[https://www.dni.gov/files/documents/ICA\\_2017\\_01.pdf](https://www.dni.gov/files/documents/ICA_2017_01.pdf)  
(accessed May 8, 2018).

United States. *International Strategy for Cyberspace*. No ref. Whitehouse: 2011.

[https://obamawhitehouse.archives.gov/sites/default/files/rss\\_viewer/international\\_strategy\\_for\\_cyberspace.pdf](https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf) (accessed May 8, 2018).

United States. Department of Defense. *Quadrennial Defence Review Report 2010* (Washington: Pentagon, 2010), 8. [https://www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR\\_as\\_of\\_29JAN10\\_1600.pdf](https://www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf) (accessed May 8, 2018).

United States. Senate Armed Services Committee, Subcommittee on Cybersecurity. *Testimony: The Weaponization of Information by R.Waltzman*. CT-473. Santa Monica: RAND, 2017. <https://www.armed-services.senate.gov/hearings/17-04-27-cyber-enabled-information-operations> (accessed January 10, 2018).

United States. House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, *Testimony by Admiral M.Rogers (Apr 11, 2018)*, CYBERCOM. Np: 2018. <https://docs.house.gov/meetings/AS/AS26/20180411/108076/HHRG-115-AS26-Wstate-RogersM-20180411.pdf> (accessed May 10, 2018).

United States. Congress. *Putin's Asymmetric Assault on Democracy In Russia and Europe*. S.Prt.115-21. 115<sup>th</sup> Congress, Second Session. 10 January 2018.

United States. US Embassy in Kyiv. *Ukraine: The Russia Factor In Crimea—Ukraine’s ‘Soft Underbelly’*. 06KYIV4489\_a. [No location]: Wikileaks, 2006.  
[http://www.wikileaks.org/plusd/cables/06KYIV4489\\_a.html](http://www.wikileaks.org/plusd/cables/06KYIV4489_a.html) (accessed May 8, 2018).

Russian Federation. [*Unknown Title of Leaked Strategy Document*]. Trans. GoogleTranslate. Made available by Lipsky, Andrei. “Plan for Russia's rejection of a number of Ukrainian territories, compiled in those days when Yanukovich was still the president of this country.” *Novaya Gazeta* (February 24, 2015), <https://www.novayagazeta.ru/articles/2015/02/24/63168-171-predstavlyaetsya-pravilnym-initsiirovat-prisoedinenie-vostochnyh-oblastey-ukrainy-k-rossii-187> (accessed May 8, 2018).

### *Speeches, Surveys & Interviews*

Blair, Prime Minister Tony. “Doctrine of the International Community” (Speech, Chicago, April 22, 1999), <https://www.globalpolicy.org/component/content/article/154/26026.html> (accessed February 1, 2018).

Carter, General Nick. “Dynamic Security Threats and the British Army” (Speech, London, January 22, 2018). <https://rusi.org/event/dynamic-security-threats-and-british-army> (accessed February 1, 2018).

McMaster, H.R. “Atlantic Council Baltic Summit” (Speech, Washington, April 3, 2018).

<https://www.whitehouse.gov/briefings-statements/remarks-ltg-h-r-mcmaster-atlantic-council-baltic-summit-dinner/> (accessed April 9, 2018).

Obama, President Barak. “Nobel Peace Prize Acceptance” (Speech, Oslo, December 10, 2009),

<http://www.whitehouse.gov/the-press-office/remarks-president-acceptance-nobel-peace-prize> (accessed February 1, 2018).

Osborn, Air Marshal Phil. “Intelligence and Information Advantage in a Contested World” (Speech, London, May 8, 2018), <https://rusi.org/event/air-marshall-phil-osborn-intelligence-and-information-advantage-contested-world> (accessed May 9, 2018).

Panetta, Defence Secretary Leon. “Secretary Panetta on Cybersecurity” (Speech, New York, October 11, 2012), <http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136> (accessed February 1, 2018).

Putin, President Vladimir. Interview with the ‘German TV channel ARD’, November 17, 2014, transcript, Kremlin, <http://en.kremlin.ru/events/president/news/47029> (accessed February 21, 2018).

May, Prime Minister Theresa. “Lord Mayor’s Banquet” (Speech, London, November 13, 2017)

<https://www.gov.uk/government/speeches/pm-speech-to-the-lord-mayors-banquet-2017> (accessed April 9, 2018).

### *Surveys*

Inglehart, R., Haerpfer, C., Moreno A., Welzel, C., Kizilova, K., Diez-Medrano, J., Lagos, M. Norris, P., Ponarin, E., & Puranen E., (eds.). World Values Survey: Round Six - Country-Pooled Datafile Version. Madrid: JD Systems Institute, 2014. [www.worldvaluessurvey.org/WVSDocumentationWV6.jsp](http://www.worldvaluessurvey.org/WVSDocumentationWV6.jsp) (accessed April 19, 2017).

Maliniak, Daniel, Susan Peterson, Ryan Powers, and Michael Tierney. *TRIP Journal Article Database Release (Version 3.1)*. Teaching, Research, And International Policy (TRIP) Project. Williamsburg: College of William and Mary, 2017. <https://trip.wm.edu/charts/#/fullreport/43> (accessed April 19, 2017).

## **Secondary Sources**

### *Media*

Bodner, Matthew. “Russia Hardens Military Thinking as NATO Fizzes Over Ukraine”, *Moscow Times* (September 7, 2014). <http://www.themoscowtimes.com/business/article/russia->

hardens-military-thinking-as-natofizzes-over-ukraine/506570.html (accessed May 15, 2018).

Ferdinando, Lisa. "Cybercom to Elevate to Combatant Command." *US Department of Defense* (May 3, 2018), <https://www.defense.gov/News/Article/Article/1511959/cybercom-to-elevate-to-combatant-command/> (accessed May 15, 2018).

Ferdinando, Lisa. "U.S. Faces Evolving, Emboldened Adversaries in Cyberspace, Officials Warn." *US Department of Defense* (April 11, 2018), <https://www.defense.gov/News/Article/Article/1491086/us-faces-evolving-emboldened-adversaries-in-cyberspace-officials-warn/> (accessed May 15, 2018).

Ignatius, David. "Russia's Radical New Strategy for Information Warfare." *The Washington Post* (January 18, 2017). <https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/> (accessed April 7, 2018).

Interfax. "Defense ministry denies reports of alleged artillery losses because of Russian hackers' break into software." *Interfax-Ukraine* (January 6, 2017). <https://en.interfax.com.ua/news/general/395186.html> (accessed April 7, 2018).

Ingram, Matthew. "In some countries, fake news on Facebook is a matter of life and death." *Columbia Journalism Review* (November 21, 2017) <https://www.cjr.org/analysis/facebook-rohingya-myanmar-fake-news.php> (accessed February 15, 2018).

No author. "Cyberwarfare: Hype and Fear." *The Economist* (December 8, 2012).  
<https://www.economist.com/international/2012/12/08/hype-and-fear> (accessed February 15, 2018).

No author. "My truth against yours." *The Economist* (January 25, 2018).  
<http://www.economist.com/news/special-report/21735479-power-fake-news-and-undue-influence-waging-war-disinformation?frsc=dg%7Ce> (accessed February 15, 2018).

No author. "BfV: Russia is trying to destabilise Germany." *Al Jazeera* (December 8, 2016).  
<https://www.aljazeera.com/news/2016/12/bfv-russia-destabilise-germany-161208141856179.html> (accessed February 15, 2018).

Magnier, Mark. "Hindu Girl's Complaint Mushrooms into Deadly Indian Riots." *Los Angeles Times* (September 9, 2013).  
<http://articles.latimes.com/2013/sep/09/world/la-fg-india-communal-20130910> (accessed May 15, 2018).



McGreal, Chris. "Vladimir Putin's "Misinformation" Offensives Prompts US to Deploy its Cold War Propaganda Tolls." *The Guardian* (April 25, 2015).

<https://www.theguardian.com/world/2015/apr/25/us-set-to-revive-propaganda-war-as-putin-pr-machine-undermines-baltic-states> (accessed February 15, 2018).

Paganini, Pierluigi. "Britain's Security Has Been Threatened by 188 Major Cyber Attacks." *Security Affairs* (February 13, 2017). <http://securityaffairs.co/wordpress/56247/breaking-news/national-cyber-security-centre-hack.html> (accessed February 15, 2018).

Swenson, Kyle. "The bloody history of April 20: Mass murders, a 'fake news' war and environmental disaster." *Washington Post* (April 20, 2014).

[https://www.washingtonpost.com/news/morning-mix/wp/2018/04/20/the-weird-bloody-history-of-april-20-mass-murders-a-fake-news-war-and-environmental-disaster/?noredirect=on&utm\\_term=.b890da211b7f](https://www.washingtonpost.com/news/morning-mix/wp/2018/04/20/the-weird-bloody-history-of-april-20-mass-murders-a-fake-news-war-and-environmental-disaster/?noredirect=on&utm_term=.b890da211b7f) (accessed February 15, 2018).

Schleifer, Theodore and Walsh, Deirdre. "McCain: Russian cyberintrusions an 'act of war'." *CNN* (December 31, 2016). <https://edition.cnn.com/2016/12/30/politics/mccain-cyber-hearing/index.html> (accessed February 15, 2018).

Vandiver, John. "SACEUR: Allies must prepare for Russia 'hybrid war'." *Stars and Stripes* (September 4, 2014).

<http://www.stripes.com/news/saceuralliesmust-prepare-for-russia-hybridwar-1.301464> (accessed February 15, 2018).

Witschge, Loes. "Justice elusive 3 years from MH17 crash in east Ukraine." *Al Jazeera* (July 17, 2017).

<https://www.aljazeera.com/indepth/features/2017/07/years-mh17-crash-east-ukraine-warzone-170716065152686.html> (accessed February 15, 2018).

### *Books and Periodicals*

Aboultaif, Eduardo Wassim. "Just War And The Lebanese Resistance To Israel". *Critical Studies On Terrorism* 9, no. 2 (2016): 334-355. doi:10.1080/17539153.2016.1175268.

Allhoff, Fritz, Nicholas Evans, Adam Henschke, and Allhoff. *Routledge Handbook Of Ethics And War: Just War Theory In The 21St Century*. London: Routledge, 2013.

Allhoff, Fritz. "Ethics And Cyber Warfare: The Quest For Responsible Security In The Age Of Digital Warfare, By George Lucas," *Journal of Military Ethics*, 16, no. 1-2 (2017): 124-127. doi:10.1080/15027570.2017.1352256.

Andersen, Soren. *Can War Be Just? Just War Analysis Of The Russo-Georgian War*. Norderstedt: GRIN-Verlag, 2010.

Aristotle, Ernest Barker, and R. F Stalley. *Politics*. Oxford: Oxford University Press, 1998.

Arquilla, John, and David Ronfeldt. "Cyberwar Is Coming!". *Comparative Strategy* 12, no. 2 (1993): 141-165. doi:10.1080/01495939308402915.

Arquilla, John. "Ethics And Information Warfare". In *Strategic Appraisal: Changing Role Of Information In Warfare*. Santa Monica: RAND, 1999.

Arquilla, John. "Twenty Years Of Cyberwar," *Journal of Military Ethics*, 12, no. 1 (2013): 80-87. doi:10.1080/15027570.2013.782632.

Averin, A. "Russia And Its Many Truths," in: *Fake News: A Road Map*. Riga: KCSC and NATO Strategic Communications, 2018.

Ayoob, M. "Humanitarian Intervention And State Sovereignty," *The International Journal of Human Rights* 6, no. 1 (2002): 81-102. doi:10.1080/714003751.

Barrett, Edward T. "Reliable Old Wineskins: The Applicability Of The Just War Tradition To Military Cyber Operations" *Philosophy & Technology* 28, no. 3 (2015): 387-405. doi:10.1007/s13347-014-0185-4.

Bates, Thomas. *Jus In Bello: Key Issues For A Contemporary Assessment Of Just Behaviour In War*. Bloomington: Author House, 2008.

Bellamy, Alex. *Just Wars*. Cambridge: Polity Press, 2006.

Bellamy, Alex. "When Is It Right To Fight? International Law And Jus Ad Bellum," *Journal of Military Ethics* 8, no. 3 (2009): 231-245. doi:10.1080/15027570903230299.

Betz, David J. "The More You Know, The Less You Understand: The Problem With Information Warfare" *Journal of Strategic Studies* 29, no. 3 (2006): 505-533. doi:10.1080/01402390600765900.

Biggar, Nigel. *In Defence Of War*. Oxford: Oxford University Press, 2013.

Birkett, D. J. "The Legality Of The 2011 Kenyan Invasion Of Somalia And Its Implications For The Jus Ad Bellum". *Journal Of Conflict And Security Law* 18, no. 3 (2013): 427-451. doi:10.1093/jcsl/krt014.

Booth, Ken. "NATO's Republic: Warnings From Kosovo". *Civil Wars* 2, no. 3 (1999): 89-95. doi:10.1080/13698249908402416.

Booth, Ken. "Ten Flaws Of Just Wars," *The International Journal of Human Rights* 4, no. 3-4 (2000): 314-324. doi:10.1080/13642980008406909.

Brandt Ford, S. "Jus Ad Vim And The Just Use Of Lethal Force-Short-Of-War" In *Routledge Handbook Of Ethics And War: Just War Theory In The 21St Century*. London: Routledge, 2013.

Bringsjord, Selmer, and John Licato. "By Disanalogy, Cyberwarfare Is Utterly New". *Philosophy & Technology* 28, no. 3 (2015): 339-358. doi:10.1007/s13347-015-0194-y.

Brown, Davis. "Introduction: The Just War Tradition And The Continuing Challenges To World Public Order". *Journal of Military Ethics* 10, no. 3 (2011): 125-132. doi:10.1080/15027570.2011.613161.

Brown, Gary. "Proportionality And Just War". *Journal of Military Ethics*, 2, no. 3 (2003): 171-185. doi:10.1080/15027570310000667.

Byers, M. *War Law: International Law And Armed Conflict*. London: Atlantic Books, 2005.

Calhoun, Laurie. "Arguments Inside The "Just War" Box". *The Independent Review* 15, no. 3 (2011): 447-461.

Calhoun, Laurie. "Legitimate Authority And "Just War" In The Modern World". *Peace & Change* 27, no. 1 (2002): 37-62. doi:10.1111/1468-0130.00217.

Calhoun, Laurie. "Political Philosophers On War: Arguments Inside The "Just War" Box". *The Independent Review*, 15, no. 3 (2011): 447-461.

Cassese, A. "Ex Iniuria Ius Oritur: Are We Moving Towards International Legitimation Of Forcible Humanitarian

Countermeasures In The World Community?". *European Journal Of International Law* 10, no. 1 (1999): 23-30. doi:10.1093/ejil/10.1.23.

Charap, S. "The Ghost Of Hybrid War". *Survival* 57, no. 6 (2015): 51-58. doi:10.1080/00396338.2015.1116147.

Chatterjee, D., ed. *The Ethics Of Preventive War*. Cambridge: Cambridge University Press, 2013.

Cicero, Marcus Tullius. *De Re Publica*. trans. Nial Rudd as The Republic and the Laws. Oxford: Oxford University Press, 1998.

Cicero, Marcus Tullius. *On Duties*. ed. E.M. Atkins, trans. Miriam T Griffin. Cambridge: Cambridge University Press, 1991.

Clark, Ian. "Taking 'Justness' Seriously In Just War: Who Are The 'Miserable Comforters' Now?". *International Affairs*, 93, no. 2 (2017): 327-341. doi:10.1093/ia/iix003.

Clarke, Richard, and Robert Knake. *Cyber War: The Next Threat To National Security And What To Do About It*. New York: Ecco, 2010.

Coady, C. *Morality And Political Violence*. Cambridge: Cambridge University Press, 2008.

Cohen, Ariel, and Robert Hamilton. *The Russian Military And The Georgia War: Lessons And Implications [Pamphlet]*. Saffron Waldron: Books Express, 2011.

Cook, James. "'Cyberation' And Just War Doctrine: A Response To Randall Dipert". *Journal of Military Ethics*, 9, no. 4 (2010): 411-423. doi:10.1080/15027570.2010.536406.

Cook, James. "The Future Of The Just War: New Critical Essays". *Journal of Military Ethics*, 13, no. 2 (2014): 203-210. doi:10.1080/15027570.2014.943035.

Coppieters, Bruno, and Richard Sakwa, ed. *Contextualizing Secession: Normative Studies In Comparative Perspective*. Oxford: Oxford University Press, 2005.

Cornell, S., and F. Starr. *Russia's War In Georgia*. New York: M.E.Sharpe, 2009.

Cornish, Paul. Livingstone, David. Clemente, Dave. Yorke, Claire. "On Cyber Warfare", Chatham House Report [online] (2010),  
<https://www.chathamhouse.org/publications/papers/view/109508> (accessed January 10, 2018).

Crisp, Roger. "Cyberwarfare: No New Ethics Needed". *Practical Ethics Blog (Oxford University)*, 2012.  
<http://blog.practicaethics.ox.ac.uk/2012/06/cyberwarfare-no-new-ethics-needed/>.

Dawkins, Richard. *The God Delusion*. Oxford: Oxford University Press, 2008.

De Vitoria, Francisco. *Political Writings*, tr. J.Lawrance. Cambridge: Cambridge University Press, 1991.

Demchak, Chris C. *Wars Of Disruption And Resilience*. Athens: University of Georgia Press, 2011.

Dinstein, Yoram. "Cyber War And International Law". *International Law Studies* 89 (2013): 276-287.

Dipert, Randall R. "Other-Than-Internet (OTI) Cyberwarfare: Challenges For Ethics, Law, And Policy". *Journal of Military Ethics* 12, no. 1 (2013): 34-53. doi:10.1080/15027570.2013.785126.

Dipert, Randall R. "The Ethics Of Cyberwarfare". *Journal Of Military Ethics* 9, no. 4 (2010): 384-410. doi:10.1080/15027570.2010.536404.

Dortmans, Peter J., Nitin Thakur, and Anthony Ween. "Conjectures For Framing Cyberwarfare". *Defense & Security Analysis* 31, no. 3 (2015): 172-184. doi:10.1080/14751798.2015.1056935.

Eberle, Christopher J., *Justice And The Just War Tradition: Human Worth, Moral Formation, And Armed Conflict*. New York: Routledge, 2016.



Evans, M. "Moral Theory And The Idea Of A Just War". In *Just War Theory: A Reappraisal*. Bodmin: MPG Books, 2005.

Fabre, Cecile. "Cosmopolitanism, Just War Theory And Legitimate Authority". *International Affairs* 84, no. 5 (2008): 963-976. doi:10.1111/j.1468-2346.2008.00749.x.

Fiala, Andrew. *The Just War Myth*. Lanham: Rowman & Littlefield, 2008.

Finkelstein, Claire Oakes, Jens David Ohlin, and Kevin Govern. *Cyberwar*. Oxford: Oxford University Press, 2015.

Finlay, Christopher J., Jonathan Parry, and Pål Wrangé. "Introduction: Legitimate Authority, War, And The Ethics Of Rebellion". *Ethics & International Affairs* 31, no. 02 (2017): 167-168. doi:10.1017/s0892679417000156.

Fisher, David. *Morality And War: Can War Be Just In The 21St Century*. Oxford: OUP, 2011.

Floridi, Luciano, and Mariarosaria Taddeo, ed. *The Ethics Of Information Warfare*. Switzerland: Springer, 2014.

Freedman, Lawrence. "Ukraine And The Art Of Exhaustion". *Survival* 57, no. 5 (2015): 77-106. doi:10.1080/00396338.2015.1090132.

Freedman, Lawrence. "Ukraine And The Art Of Limited War". *Survival* 56, no. 6 (2014): 7-38. doi:10.1080/00396338.2014.985432.

Friberg-Fernros, Henrik. "Allies In Tension: Identifying And Bridging The Rift Between R2P And Just War". *Journal of Military Ethics* 10, no. 3 (2011): 160-173. doi:10.1080/15027570.2011.610883.

Frowe, Helen. *The Ethics Of War And Peace*. 2<sup>nd</sup> ed. London: Routledge, 2016.

Gates, R. "A Balanced Strategy: Reprogramming The Pentagon For A New Age". *Foreign Affairs*, 2009, 28-40.

Gentry, Caron, and Amy Eckert. *The Future Of Just War*. Athens: University of Georgia Press, 2014.

German, Tracey, and Emmanuel Karagiannis. "The Ukrainian Crisis: Sub-State And Non-State Actors". *Southeast European And Black Sea Studies* 16, no. 1 (2016): 1-5. doi:10.1080/14683857.2016.1149348.

Goodin, Robert. *What's Wrong With Terrorism?*. Cambridge: Polity Press, 2006.

Green, James. "Introduction". In *Cyber Warfare: A Multidisciplinary Analysis*. Abingdon: Routledge, 2015.

Gross, Michael, and Tamar Meisels. *Soft War*. Cambridge: Cambridge University Press, 2017.

Gross, Michael L. *The Ethics Of Insurgency: A Critical Guide To Just Guerrilla Warfare*. Cambridge: Cambridge University Press, 2014.

Hedahl, Marcus, Scott Clark, and Michael Beggins. "The Changing Nature Of The Just War Tradition: How Our Changing Environment Ought To Change The Foundations Of Just War Theory". *Public Integrity* 19, no. 5 (2017): 429-443. doi:10.1080/10999922.2017.1278667.

Heinze, Eric, and Brent Steele. *Ethics, Authority, And War: Non-State Actors And The Just War Tradition*. Basingstoke: Palgrave Macmillan, 2010.

Hellman, Maria, and Charlotte Wagnsson. "How Can European States Respond To Russian Information Warfare? An Analytical Framework". *European Security* 26, no. 2 (2017): 153-170. doi:10.1080/09662839.2017.1294162.

Heuser, Beatrice. "Rise, Fall And Resurgence Of 'Just War' Thinking". In *The Art Of Creating Power: Freedman On Strategy*. London: C.Hurst, 2017.

Higgins, Rosalyn. *Problems And Process*. Oxford: Clarendon Press, 2010.

Hoffman, Frank. "Hybrid Warfare And Challenges". *Joint Force Quarterly* 52 (2009): 30-38.

Inkster, Nigel. "Information Warfare And The US Presidential Election". *Survival* 58, no. 5 (2016): 23-32. doi:10.1080/00396338.2016.1231527.

Jenkins, Ryan. "Is Stuxnet Physical? Does It Matter?". *Journal Of Military Ethics* 12, no. 1 (2013): 68-79. doi:10.1080/15027570.2013.782640.

Johnson, James Turner. *Ethics And The Use Of Force: Just War In Historical Perspective*. Farnham: Ashgate, 2011.

Johnson, James Turner. "In Defence Of War". *Journal of Military Ethics* 13, no. 4 (2014): 386-393. doi:10.1080/15027570.2014.994837.

Johnson, James Turner. "Paul Ramsey And The Recovery Of The Just War Idea". *Journal of Military Ethics* 1, no. 2 (2002): 136-144. doi:10.1080/150275702320231352.

Johnson, James Turner. *The War To Oust Saddam Hussein*. Lanham: Rowman & Littlefield, 2005.

Johnson, James Turner. "Just War, As It Was And Is". *First Things*, [online] 2018. <http://www.firstthings.com/article/2005/01/just-war-as-it-was-and-is>.

Jokic, Aleksandar. "What's A Just War Theorist?". *Journal of Theoretical And Philosophical Criminology* 4, no. 2 (2012): 91-114.

Jonsson, Oscar, and Robert Seely. "Russian Full-Spectrum Conflict: An Appraisal After Ukraine". *The Journal of Slavic Military Studies* 28, no. 1 (2015): 1-22. doi:10.1080/13518046.2015.998118.

Kahn, Leonard. "Understanding Just Cause In Cyberwarfare". In *Routledge Handbook Of Ethics And War: Routledge Handbook Of Ethics And War: Just War Theory In The Twenty-First Century*. London: Routledge, 2013.

Kaldor, Mary. *New And Old Wars*. Cambridge: Polity, 2012.

Kamm, F.M. "Failures Of Just War Theory: Terror, Harm, And Justice". *Ethics* 114, no. 4 (2004): 650-692. doi:10.1086/383441.

Kasymov, Shavkat. "Statism In Russia: The Implications For US-Russian Relations". *The Journal of Slavic Military Studies* 24, no. 3 (2011): 529-552. doi:10.1080/13518046.2011.598772.

Khalilzad, Zalmay, John White, and Andrew W. Marshall. *Strategic Appraisal: Changing Role Of Information In Warfare*. Santa Monica: RAND, 1999.

Kipp, Jacob W. "A Review Of: "Vladimir Slipchenko And Makhmut Gareev"". *The Journal of Slavic Military Studies* 20, no. 1 (2007): 147-158. doi:10.1080/13518040701205878.

Kragh, Martin, and Sebastian Åsberg. "Russia'S Strategy For Influence Through Public Diplomacy And Active Measures: The Swedish Case". *Journal of Strategic Studies* 40, no. 6 (2017): 773-816. doi:10.1080/01402390.2016.1273830.

LaCroix, W. L. *War And International Ethics*. Lanham: University Press of America, 1988.

Lang, Anthony F. "The Just War Tradition And The Question Of Authority". *Journal of Military Ethics* 8, no. 3 (2009): 202-216. doi:10.1080/15027570903230273.

Libiki, M. *What Is Information Warfare?*. Washington: National Defense University Press, 1998.

Light, Matthew. "The Russo-Georgian War Of 2008: A Conflict Announced In Advance?". *Europe-Asia Studies* 62, no. 9 (2010): 1579-1582. doi:10.1080/09668136.2010.515799.

Lindsay, Jon R. "Stuxnet And The Limits Of Cyber Warfare". *Security Studies* 22, no. 3 (2013): 365-404. doi:10.1080/09636412.2013.816122.

Lott, Alexander. "The Tagliavini Report Revisited: Jus Ad Bellum And The Legality Of The Russian Intervention In

Georgia". *Utrecht Journal of International and European Law* 28, no. 74 (2012): 4. doi:10.5334/ujiel.aw.

Lucas, George. "Ethics And Cyber Conflict: A Response To JME 12:1 (2013)". *Journal of Military Ethics* 13, no. 1 (2014): 20-31. doi:10.1080/15027570.2014.908012.

Lucas, George. *Ethics And Cyberwarfare*. Oxford: Oxford University Press, 2017.

Lucas, George. "Postmodern War". *Journal of Military Ethics*, 9, no. 4 (2010): 289-298. doi:10.1080/15027570.2010.536399.

Magstadt, Thomas. *Understanding Politics*. Cengage Learning, 2016.

Mark Mattox, John. "The Clausewitzian Trinity In The Information Age: A Just War Approach". *Journal of Military Ethics* 7, no. 3 (2008): 202-214. doi:10.1080/15027570802277755.

McMahan, Jeff. "The Sources And Status Of Just War Principles". *Journal of Military Ethics*, 6, no. 2 (2007): 91-106. doi:10.1080/15027570701381963.

Moore, Daniel, and Thomas Rid. "Cryptopolitik And The Darknet". *Survival* 58, no. 1 (2016): 7-38. doi:10.1080/00396338.2016.1142085.

Murray, Williamson, and Peter R Mansoor. *Hybrid Warfare*. New York: Cambridge University Press, 2012.

Nietzsche, Friedrich. *The Portable Nietzsche*. New York: Penguin Books, 2014.

O'Connell, M. E. "Cyber Security Without Cyber War". *Journal Of Conflict And Security Law* 17, no. 2 (2012): 187-209. doi:10.1093/jcsl/krs017.

Olivier, Marc. "Cyber Warfare: The Frontline Of 21St Century Conflict". *LBJ Journal Of Public Affairs* 20 (2018): 23-42.

Orend, Brian. "Fog In The Fifth Dimension: The Ethics Of Cyber-War". In *The Ethics of Information Warfare*. London: Springer, 2014.

Orend, Brian. "Justice After War". *Ethics & International Affairs* 16, no. 01 (2002): 43-56. doi:10.1111/j.1747-7093.2002.tb00374.x.

Orend, Brian. *Michael Walzer On War And Justice*. Montréal: McGill-Queen's University Press, 2008.

Orend, Brian. *The Morality Of War*. Ontario: Broadview Press, 2013.

Parry, Jonathan. "Legitimate Authority And The Ethics Of War: A Map Of The Terrain". *Ethics & International Affairs* 31, no. 02 (2017): 169-189. doi:10.1017/s0892679417000065.



Paskins, Barrie. "Realism And The Just War". *Journal of Military Ethics* 6, no. 2 (2007): 117-130. doi:10.1080/15027570701381971.

Pomerantsev, Peter. "How Putin Is Reinventing Warfare". *Foreign Policy*, 2014. <http://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare/>.

Purves, Duncan, and Ryan Jenkins. "Right Intention And The Ends Of War". *Journal of Military Ethics* 15, no. 1 (2016): 18-35. doi:10.1080/15027570.2016.1170385.

Ramsey, Paul. *The Just War*. New York: Scribner, 1968.

Rawls, John. *A Theory Of Justice*. Harvard: Harvard University Press, 1971.

Rawls, John. *Political Liberalism*. New York: Columbia University Press, 2005.

Reed, Charles, Charles Reed, David Ryall, and David Ryall. *The Price Of Peace: Just War In The 21St Century*. Cambridge [etc.]: Cambridge University Press, 2007.

Reichberg, Gregory M. *Thomas Aquinas On War And Peace*. Cambridge: Cambridge University Press, 2016.

Reitberger, Magnus. "License To Kill: Is Legitimate Authority A Requirement For Just War?". *International Theory* 5, no. 01 (2013): 64-93. doi:10.1017/s1752971913000122.

Rengger, N. J. *Just War And International Order*. Cambridge: Cambridge University Press, 2013.

Rengger, Nicholas. "On The Just War Tradition In The Twenty-First Century". *International Affairs* 78, no. 2 (2002): 353-363. doi:10.1111/1468-2346.00255.

Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks". *Journal of Strategic Studies* 38, no. 1-2 (2014): 4-37. doi:10.1080/01402390.2014.977382.

Rid, Thomas. "Cyber War Will Not Take Place". *Journal of Strategic Studies* 35, no. 1 (2012): 5-32. doi:10.1080/01402390.2011.608939.

Rid, Thomas. *Cyber War Will Not Take Place*. Oxford: Oxford University Press, 2013.

Robinson, B. "The Justification Of War In Russian History And Philosophy". In *Just War In Comparative Perspective*. London: Routledge, 2003.

Robinson, Paul. *Just War In Comparative Perspective*. Aldershot: Ashgate, 2003.

Rodin, David, and Richard Sorabji. *The Ethics Of War: Shared Problems In Different Traditions*. Aldershot: Ashgate, 2007.

Rodin, David. *War And Self-Defense*. Oxford: Clarendon Press, 2002.

Rousseau, Jean Jacques. *The Social Contract*. New York: Cosimo, 2008.

Rowe, N. "The Attribution Of Cyber Warfare". In *Cyber Warfare: A Multidisciplinary Analysis*. Abingdon: Routledge, 2015.

Russel, Frederick. *The Just War In The Middle Ages*. Cambridge: Cambridge University Press, 1975.

Russell, Frederick H. *The Just War In The Middle Ages*. Cambridge: Cambridge University Press, 1975.

Sakwa, R. "The Cold Peace: Russo-Western Relations As A Mimetic Cold War". *Cambridge Review Of International Affairs* 26, no. 1 (2013): 203-224. doi:10.1080/09557571.2012.710584.

Schmitt, Michael. "Cyber Operations In International Law: The Use Of Force, Collective Security, Self Defense, And Armed Conflicts". In *Proceedings Of A Workshop On Deterring Cyberattacks*. Washington: The National Academies of Science, 2010.

Schulte, Paul. "Just Wars Of The Future? Applying Just War Theory To Twenty-First Century Rogue Regimes". *The RUSI*

*Journal* 153, no. 4 (2008): 18-27.  
doi:10.1080/03071840802386158.

Schwitzgebel, Eric. "Philosophy's Western Bias And What Can Be Done About It". *New APPS: Art, Politics, Philosophy, Science*, 2018. <http://www.newappsblog.com/2014/09/philosophys-western-bias-and-what-can-be-done-about-it.html>.

Singer, Peter W, and Allan Friedman. *Cybersecurity And Cyberwar*. Oxford: Oxford University Press, 2014.

Sleat, Matt. "Just Cyber War?: Casus Belli, Information Ethics, And The Human Perspective". *Review Of International Studies* 44, no. 02 (2017): 324-342. doi:10.1017/s026021051700047x.

Sorabji, R. "Just War From Ancient Origins To The Conquistadors Debate And Its Modern Relevance". In *The Ethics Of War: Shared Problems In Different Traditions*. Farnham: Ashgate, 2006.

Stahl, Roger. "Weaponizing Speech". *Quarterly Journal Of Speech* 102, no. 4 (2016): 376-395.  
doi:10.1080/00335630.2016.1208365.

Stahn, Carsten, Jennifer S Easterday, Jens Iverson, and Freya Baetens. *Jus Post Bellum*. Oxford: Oxford University Press, 2014.

Sterba, James. *Justice For Here And Now*. Cambridge, UK: Cambridge University Press, 2000.

Strawser, Bradley J. "Guest Editor's Introduction The Ethical Debate Over Cyberwar". *Journal of Military Ethics* 12, no. 1 (2013): 1-3. doi:10.1080/15027570.2013.782639.

Stromseth, J. "Rethinking Humanitarian Intervention: The Case For Incremental Change". In *Humanitarian Intervention*. Cambridge: Cambridge University Press, 2003.

Stuenkel, Oliver. *BRICS And The Future Global Order*. Lanham: Lexington Books, 2016.

Taddeo, M. "Information Warfare And Just War Theory". In *The Ethics Of Information Warfare*. London: Springer, 2014.

Thakur, Ramesh. "Ethics, International Affairs And Western Double Standards". *Asia & The Pacific Policy Studies* 3, no. 3 (2016): 370-377. doi:10.1002/app5.140.

Thomas, Timothy. "Russia's Reflexive Control Theory And The Military". *Journal of Slavic Military Studies*, 17 (2004): 237–256.

Thomas, Timothy. "The Evolution Of Russian Military Thought: Integrating Hybrid, New-Generation, And New-Type Thinking". *The Journal of Slavic Military Studies* 29, no. 4 (2016): 554-575. doi:10.1080/13518046.2016.1232541.

Thornton, Rod. "The Changing Nature Of Modern Warfare". *The RUSI Journal* 160, no. 4 (2015): 40-48. doi:10.1080/03071847.2015.1079047.

Thornton, Rod. "The Russian Military's New 'Main Emphasis'". *The RUSI Journal* 162, no. 4 (2017): 18-28. doi:10.1080/03071847.2017.1381401.

Ticehurst, Rupert. "The Martens Clause And The Laws Of Armed Conflict". *International Review Of The Red Cross* 37, no. 317 (1997): 125-134. doi:10.1017/s002086040008503x.

Turton, Helen. *International Relations And American Dominance*. London: Routledge, 2015.

Twiss, Sumner, and Lo Ping-Cheung. *Chinese Just War Ethics: Origin, Development, And Dissent*. Abingdon: Routledge, 2015.

Waller, Michael, Bruno Coppieters, and A. V Malashenko. *Conflicting Loyalties And The State In Post-Soviet Russia And Eurasia*. London: F. Cass, 1998.

Walzer, Michael. *Arguing About War*. New Haven: Yale University Press, 2004.

Walzer, Michael. *Just And Unjust Wars*. 1<sup>st</sup> ed. London: Penguin, 1977.

Walzer, Michael. *Just And Unjust Wars*. 4<sup>th</sup> ed. London: Penguin, 2006.

Werner, Richard. "Just War Theory: Going To War And Collective Self-Deception". In *Routledge Handbook Of Ethics And War Just War Theory In The Twenty-First Century*. Abingdon: Routledge, 2013.

Whetham, D., ed. *Ethics, Law And Military Operations*. Basingstoke: Palgrave Macmillan, 2011.

Whetham, D. "Just War Tradition: A Pragmatic Compromise". In *Ethics, Law And Military Operations*. Basingstoke: Palgrave Macmillan, 2011.

Whetham, David, and George Lucas. "The Relevance Of Just War Tradition To Cyberwarfare". In *Cyber Warfare: A Multidisciplinary Analysis*. Abingdon: Routledge, 2015.

Whetham, David. "'Are We Fighting Yet?'" Can Traditional Just War Concepts Cope With Contemporary Conflict And The Changing Character Of War?". *The Monist* 99, no. 1 (2016): 55-69. doi:10.1093/monist/onv029.

Whetham, David. "Ethics, Law And Conflict". In *Ethics, Law And Military Operations*. Basingstoke: Palgrave Macmillan, 2011.

Wilkinson, B, and J Gow, ed. *The Art Of Creating Power: Freedman On Strategy*. Glasgow: Bell and Bain, 2017.

Williams, Howard. *Kant And The End Of War*. New York: Palgrave Macmillan, 2012.

Woo, Pyung-Kyun. "Russia`S Intervention In Eurasian War: The Russian-Georgian War And The Ukrainian Crisis". *The Journal of International Relations* 17, no. 2 (2014): 73. doi:10.15235/jir.2014.12.17.2.73.

Woo, Pyung-Kyun. "Russia`s Intervention In Eurasian War: The Russian-Georgian War And The Ukrainian Crisis". *The Journal of International Relations* 17, no. 2 (2014): 73. doi:10.15235/jir.2014.12.17.2.73.

Yemelianova, Galina. "Western Academic Discourse On The Post-Soviet De Facto State Phenomenon". *Caucasus Survey* 3, no. 3 (2015): 219-238. doi:10.1080/23761199.2015.1086572.

Zverev, Alexei. "Qualified Sovereignty: The Tatarstan Model For Resolving Conflicting Loyalties". In *Conflicting Loyalties And The State In Post-Soviet Russia And Eurasia*. London: Frank Cass, 1998.









The Just War Theory or Tradition (JWT) is fundamental to the international system, as evidenced by its codification in the UN Charter and its frequent use by state and non-state actors when justifying war. Despite this, ‘contemporary warfare’ is challenging moral, legal and intellectual frameworks, and arguably changing the very definition of war. It is therefore imperative to examine whether JWT can continue to be credibly applied to explain contemporary war. This paper, focussed upon the explicatory function of JWT, examines *Jus Ad Bellum* in two sections. First, by analysing whether JWT can or should be considered a globally acceptable and universally applicable concept in justifications for war and conflict initiation. Second, by assessing whether JWT can apply to ‘Hybrid Warfare’, a term which encompasses both an increasingly significant form of political violence and one of the more testing challenges to JWT.

The paper concludes that JWT remains a credible, global tool for explaining warfare, but one that has significant flaws, particularly in addressing non-lethal and information-based conflict. While these flaws are not significant enough to warrant discarding JWT, they do undermine its credibility to explain the full gamut of contemporary war.

*This thesis has been awarded the second prize of the year 2019 in EuroISME’s annual contest for the best student’s thesis. EuroIMSE will annually publish the winning theses in two or more languages. For information about the contest, please visit [www.euroisme.eu](http://www.euroisme.eu)*

