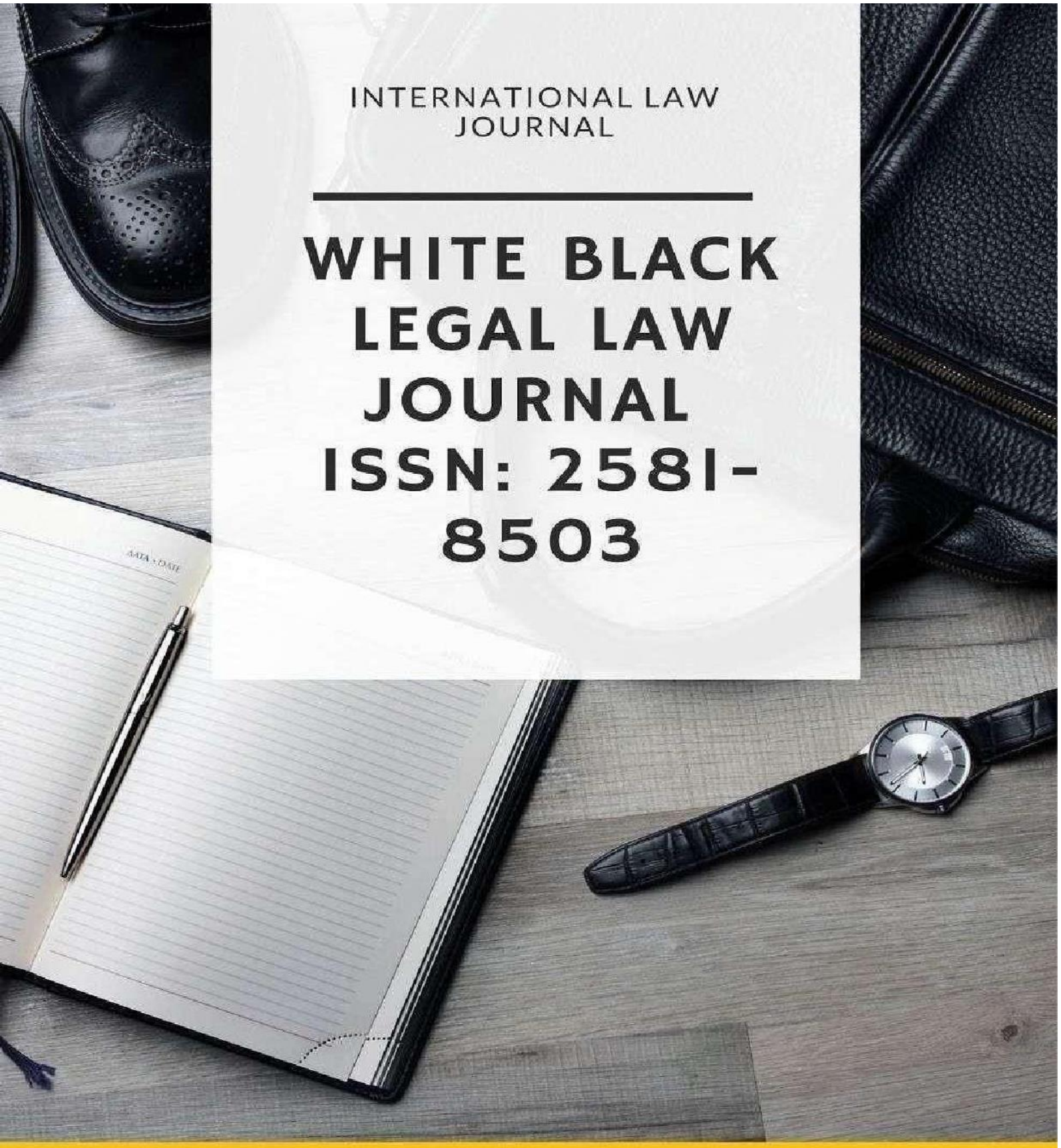


INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

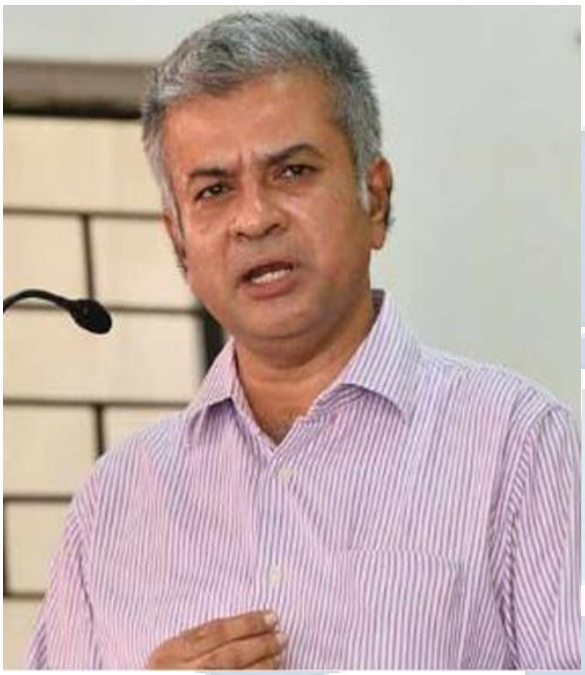
DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

WHITE BLACK
LEGAL

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer



Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and

refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | Dec 2024 ISSN: 2581-8503

TO BE (ABLE AND WILLING) OR NOT TO BE? : LEGALITY AND INEQUITIES OF 'UNABLE OR UNWILLING' DOCTRINE IN CYBER SPACE

AUTHORED BY - PALASH SRIVASTAVA

Abstract:

The regulation of non state actors has always been a complex issue for international law on use of force. The discourse around both doctrine as well as practice has been for a while trying to develop means and methods of holding States to a higher standard of accountability when it comes to non state actors operating within their territories. Post 9/11 there has been growth in the popularity of the 'unable or unwilling' doctrine, which is now being understood to apply in cyber space too. This essay seeks to establish two propositions- the application of 'unable or unwilling' doctrine in cyber space has no basis in international law, and the discursive impact of the dominant claim that 'unable or unwilling' applies in cyber space is disproportionate upon Global South States.

The first part of essay argues that the application of 'unable or unwilling' to cyber space involves an argument by analogy; and the essay unpacks the normative structure of arguments by analogy in order to establish that the specific analogy to used extend the 'unable or unwilling' doctrine to cyberspace is imperfect to the point that the argument is legally flawed. The second part of the essay examines the arguments which Third World Approaches to International Law (TWAIL) and other critical international scholars have made with respect to the 'unable or unwilling' doctrine generally, and contextualizes those arguments to argue that in cyber space, as in physical space, the presence of 'unable or unwilling' in dominant discourse pushes Global South states towards increased securitization due to the political economic currents in which these doctrinal developments are situated.

Key Words: International Law, Cyber-warfare, TWAIL

Introduction

The regulation of violence by non state actors has always presented a distinct problem in international law. The contentious nature of the *jus ad bellum* norms on non state actors came to the forefront after the 9/11 terror attack on the United States, and the resultant 'war of terror'. One important legal development of the 'war on terror' was the popularity of the 'unable or unwilling' doctrine, although many scholars argue that 9/11 was simply a catalyst while the implicit invocations of what resembles the 'unable or unwilling' test were prevalent even before 2001.[1] Simply put, the doctrine posits that if a 'victim state' faces armed attacks by a non state actor located in some other 'host state', and the attacks cannot be attributed to the host state, the victim state has the right to launch a defensive attack at the non state actors even without the consent of the host state if the host state is 'unable or unwilling' to neutralize the non state actors on its own.[2] The doctrine has been invoked multiple times in modern times including in the US military action against Osama bin Laden in Pakistani territory[3], Turkish action against Kurdish rebels in Iraq[4], and Russian military action in Ukrainian territory[5]. The legality of the test has been contested by many scholars[6], but given its continued invocation its importance cannot be denied.

Given that cyber space is increasingly seen as new avenue of vulnerability and warfare, it is hardly any surprise that there is a growing consensus about the applicability of the 'unable or unwilling' doctrine to armed attacks by non state actors in cyber space.[7] The analogies between physical space and cyber space in context of armed attacks are seen as a given. This essay seeks to interrogate the assumptions underlying the application of the 'unable or unwilling' doctrine

[1] Ntina Tzouvala, *Capitalism As Civilization: A History of International Law*, (Cambridge University Press 2020) ["Capitalism as Civilization"] 188-189

[2] Amongst many, see- Monica Hakimi, 'Defensive Force against Non-State Actors: The State of Play' (2015) 91 International Law Studies 1–31; Kimberley N. Trapp, 'Actor-Pluralism, the "Turn to Responsibility" and the Jus Ad Bellum: "Unwilling or Unable" in Context' (2015) 2 Journal on the Use of Force and International Law 199–222; Jutta Brunnée and Stephen J. Toope, 'Self-Defence against Non-State Actors: Are Powerful States Willing but Unable to Change International Law?' (2018) 67 International and Comparative Law Quarterly 263–86

[3]Elena Chacko, Ashley Deeks, 'Which States Support the Unable or Unwilling Test', *Lawfare* (10th Oct, 2016) <https://www.lawfareblog.com/which-states-support-unwilling-and-unable-test#UnitedStates > (Accessed on 6th June, 2021)

[4] ibid

[5] Ibid

[6] Corten Olivier, "The 'Unwilling or Unable' Test: Has It Been, and Could It Be, Accepted?" (2016) 29 Leiden Journal of International Law 777; Donette Murray, "Flawed and Unnecessary: the 'Unwilling or Unable' Doctrine Pertaining to States' Use of Force in Self-Defence against Non-State Actors" in Jure Vidmar (Ed), *Hague Yearbook of International Law / Annuaire de La Haye de Droit International, Vol. 30* (Brill 2017) 59-118

[7]Marco Roscini, *Cyber Operations and The Use of Force in International Law* (OUP 2014) 86-88; Ashley Deeks, "The Geography of Cyber Conflict: Through a Glass Darkly" in Michael Schmidt (Ed), *International Law Studies* (US Naval War College 2013)

to the cyber space. Without taking a position on the legality of the 'unable or unwilling' test itself, this author tries to establish that *even if* the test itself is assumed to be legal, its specific application to cyber space especially in its current form is not legal. Further, the essay examines the arguments by TWAIL and critical scholars that the 'unable or unwilling' test creates and manifests certain inequities for the Global South states, and acts as a mechanism of forceful inclusion into a particular 'anti terror' politics and political economy. The last section examines how the application of 'unable or unwilling' to cyber space to the cyber space interacts with the existing critiques, and argues that the doctrine performs the same dominating function in the cyber space.

Doctrinal Examination of 'Unable of Unwilling" in Cyber Space

There are multiple perspectives from which one can oppose and critique legal developments. One can choose to argue doctrinally, i.e. within the accepted register of law, or one can mount a critique to the very body of law and question the foundational claims of the justice and emancipation which the discipline makes. This essay seeks to critique the 'unable or unwilling' standard and its application in cyber space at every level, and so this section accepts mainstream international law on its own terms and seeks to critique the application of 'unable or unwilling' in cyber space using the tools of international legal argumentation.

The legal basis for 'unable or unwilling'

Scholars take diverging routes of international legal analysis to arrive at the 'unable or unwilling' doctrine. One of the arguments is that the doctrine results from the 'necessity and proportionality' test in the customary international law of self defence.[8] Another more complex argument is that the test has its route in the conception of 'sovereignty as responsibility'. One of the most prominent advocates for this approach, Kimberley Trapp, relies on the famous arbitral award in the *Island of Palmas* case to argue that sovereignty is not just a right but a responsibility under international law; states have a responsibility to not allow activities within their territory which cause harm to other states.[9] According to Trapp, the right to extra territorial self defence against non state actors even without the consent of the territorial state, is a logical consequence of the targeted state's responsibility to protect its own population coupled with

[8] Daniel Bethlehem, 'Principles Relevant to the Scope of a State's Right of Self-Defense against an Imminent or Actual Armed Attack by Nonstate Actors' (2012) 106 American Journal of International Law 770–7

[9]Kimberley N. Trapp, 'Actor-Pluralism, the "Turn to Responsibility" and the Jus Ad Bellum: "Unwilling or Unable" in Context' (2015) 2 Journal on the Use of Force and International Law 199–222

territorial state's failure to fulfil its obligation to prevent use of its territory for activities which cause harm to other states.[10]

Another quite different route taken to arrive at the unable or unwilling doctrine is the argument that the doctrine has its origins in the customary international law on neutrality during war. In fact the first known invocation of an argument which bears the most striking resemblance to the 'unable or unwilling' doctrine was advanced in context of belligerent use of a neutral state's territory against the opposing belligerent.[11]

In 1970, the US launched a military campaign against the communist guerrilla camps in Cambodia, which was a neutral country in the US-North Vietnam conflict. The justification for this breach of the law on neutrality was advanced by the then Legal Advisor for the US Department of State, John Stevenson. In the memo he issued, Stevenson argued that the inherent right to self defence for the US in a neutral state's territory was not limited to when the said neutral state was complicit, but also if the neutral state "cannot or will not" prevent the legal use of its territory for non-neutral purposes.[12] This was a contentious proposition from its first invocation.[13]

Some very prominent defences for the "unable and unwilling" situate it in continuity with the law of neutrality.[14] Ashley Deeks argues that there is centuries of state practice showing presence of 'unable and unwilling' doctrine in the law of neutrality.[15] She further argues that the *Caroline* case is an important example of importing the doctrine to peace time situations.[16]

Applicability in Cyber Space

Many scholars have proposed that the 'unable or unwilling' standard applies to hostile acts in cyber space which rise to the level of 'armed attack' as under the Article 51 of the UN Charter.[17]

[10] Ibid
[11] Kevin Jon Holler, 'The Earliest Invocation of "Unable or Unwilling"', *Opinio Juris* (19th March 2019) <http://opiniojuris.org/2019/03/19/the-earliest-invocation-of-unwilling-or-unable/ > (Accessed on 6th June 2021)
[12] John R. Stevenson, 'United States Military Action in Cambodia: Questions of International Law', 30
[13] Richard A. Falk, 'The Cambodian Operation and The International Law, *The American Journal of International Law* Vol 54 No. 1 (Jan 1971) 1-25
[14] Among others: Ashley Deeks, '"Unwilling or Unable": Toward a Normative Framework for Extra-territorial Self- Defense' (2012) 52 Virginia Journal of International Law 483–548; Yoram Dinstein, *War, Aggression and Self Defence* (Cambridge University Press, Originally Published in 1988, 5th Ed: 2011) 270-272
[15] Deeks, "Unable or Unwilling" 485
[16] Ibid 486
[17] Marco Roscini, *Cyber Operations and The Use of Force in International Law* (OUP 2014) 86-88; Ashley Deeks, "The Geography of Cyber Conflict: Through a Glass Darkly" in Michael Schmidt (Ed), *International Law Studies* (US Naval War College 2013)

The argument is that any rights arising out of Article 51 or in response to the armed attack do not depend upon the weapon used for the attack, but its effects.[18] This view is said to be affirmed by the ICJ's holding in the *Nuclear Weapons* Advisory Opinion.[19] The Court, in *Nuclear Weapons* observed that Article 51 "..(does) not refer to specific weapons. [it may] apply to any use of force, regardless of the weapons employed."[20]

While most scholars acknowledge that cyber space presents unique problems in attribution and evidence,[21] they nonetheless maintain that cyber space lies within the ambit of regular *jus ad bellum* norms which in their view include the 'unwilling or unable' doctrine. Acknowledging that attribution and evidence is difficult in cyber space, Yoram Dinstein argues that a similar problem is encountered in kinetic attacks by anonymous non state actors, and victim states usually have to find evidence or wait for some terror group to take credit before they act in self defence.[22] Further, according to him when computer network attacks are used as part of warfare, there would usually be a series of further attacks, which would at some point reveal the source of the attacks; and the search for such evidence would become easier with growth in new technology.[23]

The common thread across these arguments is the notion that the difference between attacks launched in and through cyber space and communication technologies are only quantitatively different from those launched kinetically, i.e. information and communication technologies are simply a different type of weapons, which are admittedly more advanced in their ability to cloak themselves, but are not *fundamentally* different in their substance. The conclusion that the 'unwilling or unable' doctrine applies to attacks in cyber space more or less the same way as in case of kinetic attacks, flows naturally from the belief in the qualitative sameness of these two modes of attack. It is however, important to investigate this assumption.

On can observe that overall, the insistence that computer network attacks trigger the 'unable or unwilling' test the same way that kinetic attacks do, follows a simple argumentative structure- the 'attack', whether by kinetic weapons or computers, is similar in its effects and the 'unable or unwilling' doctrine applies to kinetic armed attacks *ergo* it must follow that the doctrine

[18] Yoram Dinstein, 'Computer Network Attacks and Self Defence' in Michael Schmitt & Brian T. O'Donnell (eds) *International Law Studies Vol 76* (US Naval War College 2002
[19] Ibid
[20] Legality of Threat or Use of Nuclear Weapons, International Court of Justice (1994) 22
[21] Deeks, "Geography of Cyber Conflicts"; Roscini "Cyber Operations" 33-35
[22] Dinstein. "Computer Network Attacks"
[23] Ibid

shall apply to cyber attacks as well. This is a classic argument from analogy- kinetic and cyber attacks have relevant similarities, therefore norms applying to kinetic attacks shall hold true for cyber attacks.

Examining Arguments by Analogy

Law's expansion to avenues unknown is most often carried out by analogical legal arguments. Undeniably, International Law has a particular characteristic which distinguishes it from municipal law which is that judges and lawyers are arguably not the primary actors in development of International Law which is in fact developed by state practice. However, international lawyers do nonetheless play an important role in advancing International Law given that it is they who are tasked with interpretative exercises, and articulations of states' positions on international law in diplomatic arenas where development of norms take place. It is therefore important to understand the arguments international lawyers make, how they make them, and how they are accepted by international adjudicatory forums.

The reaction from lawyers and judges when confronted by a factual scenario, on which the law is not clear, is to search for another situation of fact which *is* covered by law, and has relevant similarities to the new situation at hand. However, this approach has risk of juxtaposing norms and rules meant for a different social relationship upon a new one based simply on examination of seemingly similar facts thus making law an inherently conservative practice; this risk is even more pronounced when technology is involved, because lawyers often have a tendency of readapting existing rules without examining if technology has affected qualitative changes to the social relation in question. This is why any argument by analogy must stand up to a thorough standard of scrutiny.

Scott Brewer's is the most important work when it comes to the structure of analogical arguments.[24]Brewer explained that there are three essential parts to building an argument by analogy-

i. Abduction: This is arguably the most important limb of an analogical argument. Borrowing from Charles Pierce's work on scientific discovery, Brewer saw 'abduction'

[24] Scott Brewer, 'Exemplary reasoning: semantics, pragmatics, and the rational force of legal argument by analogy' *Harvard Law Review* (1996) 109

as a hypothesis which is made possible by the truth of the premise[25]. To illustrate, if one observes a wet lawn in the morning, a person might *abduse* the hypothesis that "it rained last night"; the hypothesis is certainly not the only conclusion which can be drawn from the observation, but it can be true only if the premise, i.e. the lawn being wet, is true.[26]

In legal reasoning, one observes a situation which is not clearly covered by an existing legal rule, and then examines other examples which are similar to the case at hand, and *abduses* a rule which may resolve the case in front. The abdused rule is true only if the premise, i.e. the relevant similarity between the other cases and the case at hand is true. This rule is called 'analogy warranting rule'[27].

ii. Confirmation of Analogy Warranting Rule: Just like a scientific hypothesis is tested by experimentation, the 'analogy warranting rule' abduced in the first step is tested by examining existing legal and policy considerations for and against it. Brewer calls these considerations and arguments 'analogy warranting rationales'.[28] After examining all these rationales in detail, the legal reasoner arrives at a rule which acceptably explains the issue at hand.

iii. Application of the Analogy Warranting Rule to the facts: Once the Analogy Warranting Rule is confirmed, then all that remains is to reach a verdict by applying the rule to existing facts. This is done in just the same way as any other legal rule is applied to facts, because at this stage the Analogy Warranting Rule is essentially an existing legal rule.

'Unable or Unwilling' in cyber space: a misconstrued analogy

When confronted with cyber space, and hostile activities in taking place in and through cyber space, some states and their international lawyers tend to proceed in the standard analogical fashion. Ostensibly similar situations are examined, which are inevitably long range kinetic

[25] Ibid; Lloyd Weinreb, *Legal Reason: The Use of Analogy in an Argument* (Cambirdge University Press: 2005) 24; . For a general account of Peirce's theory of abduction ,see K. T. Fann, *Peirce's Theory of Abduction* (1970)
[26] Scott Brewer, 'Exemplary reasoning: semantics, pragmatics, and the rational force of legal argument by analogy' *Harvard Law Review* (1996) 111; Lloyd Weinreb, *Legal Reason: The Use of Analogy in an Argument* (Cambirdge University Press: 2005) 24
[27] Lloyd Weinreb, *Legal Reason: The Use of Analogy in an Argument* (Cambirdge University Press: 2005) 26
[28] Scott Brewer, 'Exemplary reasoning: semantics, pragmatics, and the rational force of legal argument by analogy' *Harvard Law Review* (1996) 111

attacks by non state actors. A rule is adduced that since the 'unable or unwilling' standard is legal say missile launches by a terror group in some country's territory, the standard is also legal for a computer generated attack. However, this view obscures the application of 'unable or unwilling'.

Effects of attacks are observed and the conclusion is reached that a particular legal standard is applicable to both internet based attacks and kinetic attacks. However, it is important to note that 'unable or unwilling' is not a legal rule which says much about the non state actors actually perpetrating the attack, in fact it is a legal limit to the sovereignty of the *state* where the attackers supposedly operated from. Yet, the facts observed to abduse the analogy warranting rule are solely about the attackers, and how their actions affect the target state. The facts which actually need to be examined in order to create a plausible analogy to apply or not to apply 'unable or unwilling' must be about what the presence of these non state actors means for the territorial state- how much control over them is realistically possibly, what are the factors involved in policing them, and what kinds of tools are needed to prevent the attacks to a foreign state, and how different or similar are all of these factors when it comes to cyber space. On examining these facts, it would be found that there is actually a distinct qualitative difference between how states deal and can deal with non state actors who can launch a kinetic attack and similar actors who launch a cyber attack.

The 'unable and unwilling' is supposedly a standard of due diligence and not an obligation upon the state to be successful, although this claim has also been disputed.[29] In *Corfu Channel*, the ICJ observed that simply the fact that a state has effective control over its territory and water, does not mean that it knew or even ought to have known of any unlawful activities being perpetrated from its territories[30]. Similarly, in *Nicaragua* the Court observed that illegal activities on a limited scale do not breach the State's obligations under international law.[31] In *Genocide* case, the Court held that the obligation to prevent genocide is not breached simply be the occurrence of genocide, because it is an obligation of conduct.[32]

[29] Waseem Ahmed Qureshi, 'International Law And The Application Of The Unwilling Or Unable Test In The Syrian Conflict' *Drexel Law Review* Vol 11:65 2018
[30] *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania),* International Court of Justice (1949) 18
[31] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, International Court of Justice (1984) Para 158
[32] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)*, Merits, Judgment, 26 February 2007, ICJ Reports 2007, para 430

In all of the articulations of due diligence, the observable nature of the internationally harmful activities is a necessary presumption of the obligation. In cyber space however, certain essential features of groups which carry out armed kinetic attacks do not apply, for instance armed attacks in cyber space can be carried out without visible militant formations, illegal weapon storage and assemblage facilities or even a localized operations base. Moreover, while a state may to link cyber attack to Non-State Actors (NSAs), there are technical difficulties in attribution of cyber-attacks to a particular NSA.

Deeks, who offers the most comprehensive view on the content of the doctrine, lays out parameters for operationalizing the 'unable or unwilling test', in which one of the standards for judging the willingness (or lack thereof) of the territorial state, is an assessment of the control the state in question exerts over its territory.[33] Even if one were to assume that there is an objective measure of control over territory apart from public image, there is certainly no method of assessing how much control a state exerts in cyber space given both its constantly changing nature and as well as its capacity to span across geographies. While Deeks does list the assessment of control over territory as one a part of the 'unable or unwilling' test for cyber space, here even she observes that given the lack of public information about a state's technological capabilities in policing cyber space, it is difficult to apply this standard.[34] Another standard Deeks lays down is an assessment of the territorial state's proposed plan to deal with the threat.[35] While applying this standard to cyber space, she again accepts the difficulties in ascertaining, and even points out that the uniquely important importance of immediacy when it comes to cyber space would make it even more difficult for the victim state to accept the plan proposed by the territorial state.[36] Given that Deeks does not resolve this tension, this assessment is then ostensibly left to the victim state to perform to its own satisfaction.

One other method of assessing whether or not a state has fulfilled its due diligence standard (and by extension "willingness") with respect to hostile non state actors in its territorial cyber space, is to assess its internal policies. A UN General Assembly Resolution in 2000, laid out ten recommendations for states most of which included internal policy changes including designing infrastructure to gather evidence for nefarious activities in cyber space, exchange of

[33]Deeks "Unable or Unwilling" 525
[34] Deeks "Geography of Cyber Conflicts" 14
[35] Ibid 15
[36] Ibid 16

information, and having mutual assistance regimes, among other points.[37] Due diligence is also said to involve adopting effective anti cyber crime domestic legislations.[38]

Even if one were to accept that a legal standard to determine when it is acceptable to breach the sovereignty of a state can possibly include a value judgment of its internal policies, there is simply still nothing to guarantee any success in these policies preventing any hostile cyber activities. In the physical sphere, there are tried and tested criminal justice and police practices, the presence of which would make it difficult for an argument to made for the territorial state's 'unwillingness'. There has never been a computer network attack which has been to the level of 'armed attack', which means that no practices or policies for preventing such attacks in cyber space have any sort of consensus in the international community.

Furthermore, in all of the other specialized legal regimes like that for the oceans or outer space, there is still a fundamental property to these areas which can be regulated by simply extending the pre existing legal frameworks while adjusting for certain specificities. This is not true for cyber space, which being a purely relational space is constituted *only* of the relation between computers- thus having no fundamental characteristics of its own. In fact, some commentators have argued that "the internet", as a unified concept with coherent characteristics is a myth, and that there are in fact multiple "internets".[39] The cyberspace is fluid and constantly changing, unlike outer space or oceans, which means that any legal regime attempting to regulate it must evolve in a completely different context than the present 'unable or unwilling' test (or other *jus ad bellum* norms). There have been commentators who have argued that the entire body of Just War Theory, needs to be modernized to fit cyber space, because there is no legitimate analogy possible between cyber space and physical space.[40] This essay sticks to the more modest claim that notwithstanding whether a larger analogy between cyber and physical warfare is possible, the analogical reasoning fails in the specific instance of 'unable or unwilling'.

To summarize- the supposed legal validity of the 'unwilling or unable' test rests upon the

[37]GA Res 55/63, 4 December 2000, para 1.
[38]Christopher E Lentz, 'A State's Duty to Prevent and Respond to Cyberterrorist Acts', *Chicago Journal of International Law* 10 (2010), 820–2
[39] See for example, Evgeny Morozov *To Save Everything, Click Here* (Penguin 2013) 120-132
[40]Selmer Bringsjord, John Licato 'By Disanalogy, Cyberwarfare is Utterly New'< http://kryten.mm.rpi.edu/SB_JL_cyberwarfare_disanalogy_112113IT.pdf>

assumption that due diligence is indeed a realistic expectation upon a state to prove itself 'willing and able', but given the qualitative differences between cyber space and physical space, the obligation is not a realistic one at all. Therefore, at least in its current form, the extension of the 'unable or unwilling' doctrine to cyber space has inadequate basis in International Law, notwithstanding its contestable legality in general.

Global South And The Application Of 'Unable Or Unwilling' To The Cyber Space

Having established that the importation of 'unable or unwilling' has questionable legality, it is nevertheless important to note that the question of legality often settles only part of any discussion about international law, especially state obligation. As discussed before, the very legality of the 'unable or unwilling' test has been questioned by a large number of scholars, and yet it is beyond doubt that the doctrine has played a significant role in providing a rhetorical justification for significant geopolitical events. Antony Anghie and B.S. Chimni have written about how indeterminacies in law are not a benign phenomenon but a structural form of inequity which furthers imperialist tendencies in International Law.[41] It is therefore, important to approach the arguments being made to apply the 'unwilling or unable' test in cyber space, *as arguments* instead of settled norms of international law and examine what drives those arguments, and the role they perform in a post colonial political economy wrought with power differentials.

The 'unwilling and unable' doctrine has generally been subject to criticism from scholars of Third World Approaches to International Law ("TWAIL"), and critical international lawyers from other schools. This section attempts to contextualize the existing scholarly criticisms of the 'unwilling or unable' doctrine for its application in cyber space, and examine how exactly the same inequities manifest in the new paradigm. These criticism generally work on two levels – application, and structure. The first kind of criticisms highlight that the application of 'unable or unwilling' generally results in disproportionate consequences for certain states because of existing power differentials in the international community, and the second kind locate the rule itself in a hierarchical structure, and insist that the rule itself instead of its consequences is a symptom of power differentials inherent international law.

[41] Anthony Anghie & BS Chimni, 'Third World Approaches to International Law and Individual Responsibility in Internal Conflicts' *Chinese Journal of International Law* Vol 11 (2003) 101

Inequities in Application

Dawood Ahmed has demonstrated quite powerfully that the 'unable or unwilling' is a doctrine which has been invoked in modern times almost only in cases where a distinct power differential exists.[42] Ahmed points out that although the doctrine is invoked mostly by Global North, predominantly white, states even when both the states involved are Global South states, the doctrine has been invoked by a regionally powerful state, for example Uganda's 2003 military incursions in Democratic Republic of Congo.[43] Arguably, the same kinds of power differentials exist in cyber space within which the 'unable or unwilling' test would presumably operate. While it may seem self evident that there is a paradoxical relationship between technological development and vulnerability to cyber threats, i.e. countries which are more dependent on digital infrastructure by the virtue of their higher technological development would be more vulnerable to cyber attacks than less developed countries, the situation is not that simple.[44] Neither vulnerability to cyber attacks nor technological capacity exist in a vacuum, consequently the capacity to respond to cyber threats is in large part a function of institutional capacity. At the end of the day, arguably 'vulnerability' is not simply a frequency of attacks (something which technologically sophisticated countries are obviously more subject to) but the capacity to respond to threats and to bounce back after an attack- something developed nations with higher institutional capacity and skilled human resource do better.

Andrea Calderaro and Anthony J. S. Craig have demonstrated with quantitative research that a country's cyber capacity level is intrinsically tied to the development of science and technology in countries, which is a function of other developmental indicators like literacy, public education, and research infrastructure.[45] Research has also shown that the most significant correlation to vulnerability in cyber space is the use of pirated software and the state of development in Information and Communication Technologies, thus making lower income countries where use of unlicensed software is prevalent, and have a low level of development in skills, and infrastructure, significantly more vulnerable to the misuse of their networks.[46] In

[42] Dawood I. Ahmad, 'Defending Weak States against the "Unwilling or Unable" Doctrine of Self Defence', *Journal of International Relations and International Law* Vol 9 (2013)
[43] ibid
[44] 'Developing countries most vulnerable to cyberattacks' (*UN News* 9 December 2011) < https://news.un.org/en/story/2011/12/397922-developing-countries-most-vulnerable-cyberattacks-un> Accessed 9th November 2021
[45] Andrea Calderaro & Anthony J. S. Craig, 'Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building', Third World Quarterly (2020)
[46] Asghari, Hadi, Michael Ciere, and Michel J. G. van Eeten. 'Post-Mortem of a Zombie: Conficker Cleanup After Six Years.' Proceedings of the 24th USENIX Conference on Security Symposium,Washington, D.C., August 12–14, (2015), 1–16

this context, the largely unequal enforcement of 'unable or unwilling' which Ahmed points at is likely to be more pronounced. The obligation of due diligence requires reasonable care, but the assessment of 'reasonability' is left to the state invoking the doctrine, i.e. more often than not, the more powerful state in the equation.

Structural inequities

The 'unable or unwilling' doctrine is unique as compared to all other expansive interpretations of Article 51 of the Charter because it makes sovereignty conditional upon internal structuring of a state, and leaves the assessment of whether the condition is fulfilled or not to another state. In this context, of particular relevance is Ntina Tzouvala's argument drawing connections between the 'unable or unwilling', and the infamous 'standard of civilization.[47]She argues that the 'unable or unwilling' is a rhetorical device which relies upon designating Global South states as fundamentally incapable of full sovereignty, while insisting that they nonetheless continue to strive towards becoming 'capable' of sovereignty, the only way of doing which is to adopt "the imperatives, political economy and aesthetics of a never-ending war on terror".[48] This idea that states need to fulfil some criteria to be 'allowed' the full enjoyment of their sovereignty is seen in Trapp's discussion on the 'unable or unwilling'-

While it is not true that some states are more sovereign than others, it is certainly true that some states are better able to meet the responsibilities of sovereignty than others. Owada therefore quite rightly argues that conceptualising sovereignty in terms of responsibility 'places the emphasis on capacity building . . . and collaboration'.[49]

Collaborative capacity building, which is essentially a practice states tend to do out of their free will, is in this vision an imposition in order to appear 'willing and able'; and thus a precondition on sovereignty itself. Deeks' framework also has similarities where she relies on 'common knowledge' to assess the 'willingness' or ability of states to deal with threats inside their own territory.[50] She relies on publically available indices and rankings, to gauge this 'common knowledge'. There have been multiple criticisms from critical scholars about indices and rankings, their methodology, and their value as indicators of state performance.[51] Yet, the

[47]Ntina Tzouvala, 'TWAIL and the Unwilling or Unable Doctrine: Continuities and Ruptures' (2015-2016) 109 AJIL Unbound 266; for more detailed argument, see Tzouvala, "Capitalism as Civilzation" 187-211
[48]Tzouvala, "Capitalism as Civilization" 209
[49]Trapp, "Actor Pluralism"120
[50] Deeks, "Unwilling or Unable"525, 526
[51] For a comprehensive critique, see: Nehal Bhuta, 'Governmentalizing Sovereignty: Indexes of State Fragility and the Calculability of Political Order' in Kevin E. Davis et al. (eds.), Governance by Indicators: Global Power

value these markers serve is of immense rhetorical value in creating public perceptions of 'failed states'. Tzouvala characterizes the use of these indices of 'performance' in order to assess a state's right to enjoyment of full sovereignty as proxies for 'civilization' since modern international lawyers do not have access to pseudo scientific theories of racial superiority which were used by 19th century international lawyers for this purpose.[52] Anghie has also argued that the 'war on terror' has a certain agenda which attempts to force Global South states to partake in the military industrial complex of defence equipment, and securitization[53], the role which according to Tzouvala 'unwilling or unable' doctrine instrumentally fulfils. It is then important to examine how the norm building processes for cyber warfare can act as markers to indicate 'unable or unwilling'.

The 4th United Nations Group of Governments Experts, tasked with formulating voluntary non binding norms on responsible state behaviour in cyber space submitted their final report in 2015.[54] The draft envisions multiple expectations for states to modify their policy structures and infrastructural development in consonance with the UNGGE recommendations; these include establishment of computer emergency response teams[55], participation in cooperative activities for confidence building[56], and take measures to protect their critical information infrastructure from malicious use.[57] Similarly, the 2019 Open Ended Working Group, under the 6th UNGGE, which recently released its first report as a result of a parallel norm developing process includes capacity development expectations similar to those the 4th UNGGE report of 2015.[58] Although these norms are voluntary and non binding, they "reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States."[59] There has been scholarly discussion about how in the norm creation process is not just an exercise in global

through Classification and Rankings
(Oxford: Oxford University Press 2012) 132–62; Francisco Gutierrez Sanin, 'Evaluating State Performance: A Critical View of State Failure and Fragility Indexes' (2011) 23 European Journal of Development Research 20–42, 24.

[52]Tzouvala, "Capitalism as Civilization" 202, 203

[53] Anthony Anghie, 'The War on Terror and Iraq in Historical Perfective, 43 *Osgood Hall Law Journal* (2005)

[54] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015

[55] Ibid 17(c)

[56] Ibid 17(d)

[57] Ibid 13(g)

[58] Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report (2021)

[59]Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Final Report (2015) para 10

cooperation but also an attempt by states to frame the standards of ideal behaviour according to their national interests.[60]

Therefore, notwithstanding the merits of states' following the norms reflected by the processes, it is important to note that in a paradigm marked with structural inequities these expectations of behaviour morph into conditions upon sovereignty itself given that it is the conformity to the model of a state in service of the 'war on terror' which arguably becomes the basis for judging whether a state is 'unable or unwilling'.

Market evaluations predict that North American firms are likely to maintain dominance in the rapidly growing market for military cyber technologies.[61] Latest evaluations put Israel's cyber security industry at $82 billion[62], which includes state of art surveillance software. As discussed above, the politics of the 'war on terror' not just includes an adoption of legal frameworks but also investment in the military industry. The way 'unwilling or unable' creates a necessity for investment in military technology, its importation to cyber space creates a necessity to invest in the growing 'military digital complex' to prove oneself as 'able and willing'. Thus the doctrine, if it does reify in cyber norms, as indeed seems to be happening, is structurally positioned to create conditions to shift the cyber security discourses and policies of Global South nations towards a particular kind of imperatives and political economy, the same way it creates an obligation of securitization in physical space. Increased penetration of the national security apparatus in the digital space, and its discursive legitimization creates conditions of erosion of privacy and digital rights.

In 2019, it came to light that Indian government had authorized targeted surveillance on activists ostensibly justified by the State's rights to limit fundamental rights on grounds of

[60]Eneken Tikk-Ringas, 'International Cyber Norms Dialogue as an Exercise of Normative Power', *Georgetown Journal of International Affairs* Vol 17(3) (2016) 47-59

[61] Research and Markets, "Global Defense Cyber Security Market Analysis, Growth, Trends, and Forecast 2019-2024: Major Players are Northrop Grumman, Thales, Boeing, IBM, Cisco System" *Intrado* (23rd Dec. 2019) < https://www.globenewswire.com/en/news-release/2019/12/23/1963921/28124/en/Global-Defense-Cyber-Security-Market-Analysis-Growth-Trends-and-Forecast-2019-2024-Major-Players-are-Northrop-Grumman-Thales-Boeing-IBM-Cisco-System.html>

[62] Kanti S, "How did Cyber security Become a $82 Billion Powerhouse in Israel" *Analytics Insight* (25th Jan 2019) < https://www.analyticsinsight.net/how-did-cybersecurity-become-a-82-billon-powerhouse-in-israel/ > (Accessed on 6th June 2021)

'national security'.[63] Recently, a new list of people has been released who were being spied upon.[64] Both of these incidents were being done by a surveillance software called Pegasus prepared by Israeli cyber arms firm called NSO Group. While the extent of its use cannot be determined, it is known that apart from India, UAE[65], Mexico[66] and Saudi Arabia[67] to conduct targeted surveillance on individuals critical of regimes. The Pegasus software is a quintessential example of the kind of technology which, as discussed above the 'unable and unwilling' standard in cyber space, promotes.

Conclusion

The discussion around heightened surveillance by governments is often situated strictly within domestic legal frameworks and internal politics of the states; while this is not inaccurate, it is important to take a step back and also look at these processes as part of a global trend, and the mechanisms which cause its growth. This essay does not deny that the relationship between securitization and global politics is complex which involves factors like regional politics, and internal political arrangements of States. To claim a simple causal connection between international law and securitization would be obviously reductionist. However, of the complex interconnected factors which form the complex web of material and social conditions for the increasingly pervasive national security apparatus, international law *is* undoubtedly an important factor. The limited objective of what has been discussed here is to examine the legal validity of applying the doctrine in cyber space, and to highlight in particular international law's role in the securitization phenomenon, and how 'unable and unwilling' standard reveals those structuring mechanisms.

Furthermore, securitization in cyber space and a push towards the *digital* economy of war on

[63] Sukanya Shantha, "Indian Activists, Lawyers Were 'Targeted' Using Israeli Spyware Pegasus", *The Wire* (31st October 2019) < https://thewire.in/tech/pegasus-spyware-bhima-koregaon-activists-warning-whatsapp > (Accessed on 15th August 2021)

[64] Aashish Aryan , Pranav Mukul, "Phones of 2 Ministers, 3 Opp leaders among many targeted for surveillance: report", *Indian Express* (19th July 2021) < https://indianexpress.com/article/india/project-pegasus-phones-of-2-ministers-3-opp-leaders-among-many-targeted-for-surveillance-report-7411027/> (Accessed on 15th August 2021)

[65] Anadolu Agency, "UAE targeted Yemen officials with Israeli Pegasus spyware: report", *Daily Sabah* (4th August 2021) < https://www.dailysabah.com/world/mid-east/uae-targeted-yemen-officials-with-israeli-pegasus-spyware-report?gallery_image=undefined#big > (Accessed on 15th August 2021)

[66] Mary Beth Sheridan, "How Mexico's traditional political espionage went high-tech", *The Washington Post* (21st July 2021), < https://www.washingtonpost.com/world/2021/07/21/mexico-nso-pegasus/> (Accessed on 15th August 2021)

[67] Devirupa Mitra, "Hacking Software Was Used to Spy on Jamal Khashoggi's Wife Months Before His Murder", *The Wire* (18th July 2021) < https://thewire.in/world/pegasus-hacking-jamal-khashoggi-wife > (Accessed on 15th August 2021)

terror involves more than just an economic dimension. Scholars have discussed how securitization and heightened surveillance are intrinsically connected.[68] Julie Cohen has noted that deep pervasiveness of surveillance culture results in corrosion of the very subject of a liberal democracy, and results in a 'modulated democracy'.[69] While a discussion upon the full extent of harms of securitization in cyber space are beyond this essay's scope, it is important to asserts for a full evaluation of what is at stake when certain States are supposed to be constantly striving towards proving themselves 'able and willing' before the international community reifies norms in cyber space.

WHITE BLACK
LEGAL

[68] Patrick Petit, 'Everywhere Surveillance': Global Surveillance Regimes as Techno-Securitization', *Science and Culture* 2020, 30-56
[69]Julie Cohen, 'What is Privacy For' 126 Harvard Law Review