University of Sheffield | Sheffield Centre for International & European Law

**Sheffield Centre for International and European Law**

**School of Law**

## Working Paper Series

# Digitalisation and its Systemic Impact on the Use of Force Regime: Legal Uncertainty and the Replacement of International Law

**Professor Nicholas Tsagourias**

**2023/1**

SCIEL builds on a long and distinguished tradition of international and European legal scholarship at the University of Sheffield School of Law. Research in the Centre focuses on the international and European aspects of legal issues, and more broadly draws on the School's strengths in many forms of International, European and Comparative Law to consider the wider implications of current problems and the function of law in a globalised world. As part of this mission, the Centre publishes the present Working Paper Series.



Please visit www.sheffield.ac.uk/law/sciel for more information about the Centre or contact:
Email: law@sheffield.ac.uk
Twitter: @lawsheffield

The full Working Paper Series is available at
https://www.sheffield.ac.uk/law/research/clusters/sciel/working-papers

# Digitalisation and its Systemic Impact on the Use of Force Regime: Legal Uncertainty and the Replacement of International Law

Nicholas Tsagourias

Abstract

*This article explores the systemic impact of digitalisation on the use of force regime. It identifies two types of impact: (i) legal uncertainty; and (ii) the replacement of international law. The article discusses legal uncertainty in relation to the content of the rules on the use of force and their application to digital uses of force as well as in relation to the facts that underpin digital uses of force. It then goes on to discuss the replacement of international law as a regulatory tool in the use of force by considering the impact of digitalisation on the creation of customary law, legal personhood, and international law's regulatory modality. The article's findings are not limited to the impact of digitalisation on the use of force regime but extend to international law in general.*

## 1. Digitalisation and the international law regime on the use of force

Digitalisation is currently transforming the way humans, institutions and states conduct their affairs and its impact is profound, even revolutionary.[1] Digital technologies are used for analytical, predictive, and operational purposes offering significant benefits.[2] More specifically, they can facilitate, improve, expedite, and make more efficient the decision-making process and action at the human and institutional level. They can do this by identifying, analysing, and assessing large amounts of factual patterns and data drawn from diverse and multiple sources. Digitalisation can also extend the scope and effect of decisions or actions beyond what is physically possible. Actions are not obstructed by geography, conflict, shortages of manpower or by social, economic, political, and material hurdles. At the same time, digitalisation can protect resources and minimise exposure to risks or harm because results can be attained without the need to deploy human or material resources. Digitalisation can achieve endurance and expand the reach of operations which depleted physical or human resources cannot achieve. All this means that digitalisation can scale up human,

[1] Colin B. Picker, 'A View from 40,000 Feet: International Law and the Invisible Hand of Technology', 23 *Cardoso Law Rev* (2001), 151–219. Digitalisation is used in this paper as an umbrella term to describe the use of digital technologies such as cyber technology or AI. The latter refers to technology which replicates human-like perception, cognition, planning, learning, communication, and action with minimum or no human intervention or oversight. Artificial General Intelligence (AGI) replicates but also exceeds human intelligence whereas Artificial Narrow Intelligence (ANI) includes limited cognitive tasks. For a definition see H.R.6216 – National Artificial Intelligence Initiative Act of 2020, Section 3 'Definitions'. Also see S Russell and P Norvig (2013) *Artificial intelligence: a modern approach*, 3rd edn. (Pearson Education Limited), 1-5.

[2] Chatham House, Artificial Intelligence and International Affairs (2018) https://www.chathamhouse.org/2018/06/artificial-intelligence-and-international-affairs . For an optimistic and general overview of the role of digitalisation in international law see Ashley Deeks, *High-Tech International Law*, 88 *George Wash. Law Rev*. 575–653, (2020)

institutional and state capabilities and act as force multiplier and can achieve all this without always involving human agents.

Because of these advantages, digital technology will inevitably be used to inform and support decisions involving the use of force but also the employment of force. More specifically, digitalisation can assist in the detection of actual or imminent attacks, assist in the analysis and evaluation of military data; speed up decisions and responses to attacks or automate them, assist in the accurate and targeted employment of force and in calculating proportionality, maintain constant command and control over action, pursue and maintain action over longer periods of time without the need to deploy more resources, achieve deeper reach by protecting at the same time resources and avoiding human casualties.

That having been said, digitalisation can be a vector of many risks and challenges. The speed with which decisions are made, the scaling up of capabilities and endurance can create a situation of perpetual action and reaction particularly if the ability to understand and control actions and reactions is reduced. Digitalisation can also cause unconstrained and uncontrolled overspill because digital technologies are interconnected and integrated within other technologies. In a war situation, it can automatically enlarge the area of operations or, to use Clausewitz's words, it can cause 'the utmost exertion of forces'.[3] The unpredictability of digital technology is another vector of risk. Digitalisation can produce unpredictable or unexpected results through a process of self-learning and adaptability which exceed or differ from those initially intended or anticipated by its users. This feature relates to another challenge: that of explainability. Explainability refers to the ability to understand or trace the reasoning or decisions of digital agents. Due to the complexity of the digital technology and the opacity of its reasoning in particular in the case of machine learning, [4] explainability is not always possible either from an internal or from an external point of view. The internal refers to the ability of digital agents to explain their thinking and their decision-making process whereas the external refers to the ability of an operator or a human agent to understand and explain the digital technology's reasoning and its decisional processes. This state of affairs affects the ability of humans or institutions to regulate digital technology, agents and actions. If this is combined with the inability to detect and understand errors, the possibility of manipulating and corrupting the system or what is fed into the system and the speed with which decisions and actions

[3] Carl von Clausewitz, *On War* (trans and eds. Michael Howard, Peter Paret and Beatrice Heuser) (Oxford, Oxford University Press, 2007), 5

[4] According to Chesterman 'opacity is the antithesis of legal reasoning'. S. Chesterman, *We the Robots,* (CUP, 2021), 64

are taken, unlawful or harmful actions cannot be controlled or stopped easily. Moreover, any harm caused by such actions can be more grave or widespread due to the interconnectivity of digital technology and its ability to defy borders. Another related challenge concerns that of accountability. Lacking or having limited knowledge of how decisions are made or why a particular decision was made in certain circumstances, decisions or actions cannot be challenged because giving reasons is the basis of accountability. Furthermore, identifying the entity that should bear responsibility for wrongful decisions or actions is quite difficult because of the interconnectivity of digital technology and its ability to operate with different degrees of autonomy.

The preceding discussion is not meant to be an exhaustive account of the advantages, challenges or risks of digital technology but is meant to provide the context within which the question of this article is discussed namely, how digitalisation affects the international law regime on the use of force. That said, the article will not consider the question of how digitalisation is challenging substantive rules of the use of force regime but, instead, it will consider the systemic impact of digitalisation on the use of force regime.[5] In doing so, useful insights can be drawn which are transferable to international law in general.[6]

The article will consider two issues where the systemic impact of digitalisation on the use of force regime manifests itself: the first is that of legal uncertainty which will be considered in section 2 and the second is the replacement of the international law on the use of force which will be considered in section 3.

Before continuing, some points of clarification are in order. First, I start from the premise that the international law rules on the use of force apply to digital technologies. In relation to cyber technology, the application of international law has been confirmed by the 2013, 2015 and 2021 UN

[5] For the effects of cyber technology on the use of force see chapters 14 and 15 in Nicholas Tsagourias and Russell Buchan, *Research Handbook on International Law and Cyberspace*, 2nd revised and expanded edition, Elgar, 2021; *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017). Ashley Deeks, Noam Lubell & Daragh Murray, 'Machine Learning, Artificial Intelligence, and the Use of Force by States', 10 J. *Nat'l. Secur. Law Policy* 1–25 (2019)

[6] For general overview of cyber technologies and international law see Nicholas Tsagourias and Russell Buchan, *Research Handbook on International Law and Cyberspace*, 2nd revised and expanded edition, Elgar, 2021. Regarding AI see Thomas Burri, 'International Law and Artificial Intelligence', 60 *German YBIL* 91–108 (2017); Matthijs M. Maas, 'International Law Does Not Compute: Artificial Intelligence and The Development, Displacement or Destruction of the Global Legal Order', 20 *Melb. J. Int. Law* 29–56 (2019); Liu, H-Y., Maas, M. M., Danaher, J., Scarcella, L., Lexer, M., & Van Rompaey, L. (2020). Artificial Intelligence
and Legal Disruption: A New Model for Analysis. *Law, Innovation and Technology*, *12*(2), 205-258.

GGE reports as well as by the 2021 OEWG report.[7] Many states that have made their position public have also affirmed the application of international law to cyber operations.[8] The same is true regarding AI with states having confirmed the application of international law to AI.[9]

The second point of clarification is that the referent use of force regime consists of the UN Charter rules on the use of force and customary law which runs in parallel with the Charter.[10] The three main pillars of the regime are the prohibition of the unilateral use of inter-state force; the use of force by way of individual or collective self-defence in response to an armed attack; and the use of force when authorised by the SC.[11]

The third clarification is that, because the use of force regime is organically attached to international law and share the same subjects, processes of law creation, interpretation, and application as well as the same regulatory modality, the issues I will discuss are also relevant and indeed transferrable to international law and reveal the challenges it faces by digitalisation.

---

[7] UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc A/68/98 (24 June 2013); UNGA, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc A/70/174 (22 July 2015); 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security', UN Doc A/76/135 (14 July 2021); Open-ended working group on developments in the field of information and telecommunications in the context of international security Final Substantive Report A/AC.290/2021/CRP.2 ( 10 March 2021).

[8] Indicatively see Finland, International law and cyberspace: Finland's national position (2020), https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859; Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace (July 2020) https:// www.aldiplomasy.com/en/?p=20901; République Française, Ministère des Armées, Droit International Appliqué aux Opérations dans le Cyberespace (2019); The Netherlands, Letter to the parliament on the international legal order in cyberspace (5 July 2019) https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace

[9]. EP Resolution, 2020/2013(INI) Artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice 20 January 2021. *Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects*, Final Report, CCW/MSP/2019/9, 13 December 2019

[10] Nicaragua Case paras 174- 176

[11] Articles 2(4) and 51 as well as Chapter VII of the UN Charter. UNGA Res 42/22 (18 November 1987) UN Doc A/RES/42/22. *Case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14 (*Nicaragua* Case) para 190; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory,* Advisory Opinion of 9 July 2004 (2004) ICJ Rep 136 (*Wall AdvisoryOpinion* Case) para 87; *Armed Activities on the Territory of the Congo (Democratic Republic of Congo V Uganda)* (Merits) [2005] ICJ Rep 168 (*Armed Activities* Case) para 148. R Buchan and N Tsagourias, *Regulating the Use Force: Stability and Change* (Elgar, 2021), chapters 2,3, 6.

## 2. Digitalisation and legal uncertainty in the use of force regime

Legal uncertainty has two dimensions although they are interconnected. The first refers to the indeterminacy in the scope and content of extant rules when they are called upon to apply to particular facts, what Hart calls the 'penumbra of uncertainty'.[12] Relevant international law scholarship describes this state of affairs as the existence of 'grey zones', 'legal gaps', or 'legal hybridity'. 'Grey zones' refers to situations where there are no clear normative thresholds within rules to determine whether facts fall or not within the normative space of the rule. 'Legal gaps' refers to situations where no specific rule exists to regulate a particular course of conduct. 'Legal hybridity' refers to situations where a la carte norms are developed in response to particular events or behaviours, often exhibiting hard and/or soft normativity.

The second aspect of legal uncertainty refers to indeterminacy in the ascertainment of facts which leads to uncertainty in their legal classification. Because law applies to facts, identifying, knowing, and assessing the facts is important for their legal classification and for the application of the relevant rules.[13]

### 2.1 Legal uncertainty in the use of force regime

The use of force regime is particularly prone to legal uncertainty.[14] In the first place, it is the lack of legal density that causes uncertainty. The body of primary rules on the use of force is quite thin and therefore the regime lacks the required density to regulate this area comprehensively. More specifically, in addition to the few UN Charter rules, there are also a few customary law rules on the use of force for example the rules on necessity, proportionality and imminence.[15] Second, it is the fact that the relevant rules, albeit few and apparently simple in their formulation, use vague and open-ended language in order to be inclusive of multiple fact patterns and be future proofed. This makes them subject to competing or contradictory interpretations in particular if applied to concrete

[12] H.L.A. Hart, *The Concept of Law*, 3rd ed. (Oxford, Oxford University Press, 2012), 127

[13] *Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v Uganda), Judgement (Merits) [2005] ICJ Rep 168, pars 57-58. Sir Franklin Berman QC, 'What do we expect of Lawyers in Armed Conflict?', 38 *George Washington International Law Review,* (2006), 628, 631-2

[14] For uncertainty in international law see Martti Koskenniemi, *From Apology to Utopia,* (Cambridge: Cambridge University Press, 2005)

[15] *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14 paras 176-179. Letter of US Secretary of State Daniel Webster dated 24 April 1841, in Caroline Case, 29 *British and Foreign State Papers* (1841) 1137–1138, https://avalon.law.yale.edu/19th_century/br-1842d.asp. Albrecht Randelzhofer and Georg Nolte, 'Article 51' in Bruno Simma, Daniel-Erasmus Khan, Georg Nolte and Andreas Paulus (eds), *The Charter of the United Nations: A Commentary* 3nd ed (Oxford University Press, 2012) paras 13, 63.

facts. For example, although the rule on the non-use of force or the rule on self-defence appear to be clear in their simplicity, what is force and what scale and gravity is required to amount to armed attack are not clearly defined[16] but require interpretation when applied to concrete facts. That said, as will be seen facts also need to be interpreted and what facts should be taken into consideration may also change over time as in the case of technological facts. Regarding the customary rules on imminence, proportionality, or necessity according to which the legality of the use of force is assessed,[17] they also require interpretation in light of new facts and circumstances. Third, the 'plain paradigms'[18] which led to the genesis of the particular rules on the use of force may not be relevant anymore; instead, novel situations and events and new actors may emerge which have little or no similarities with these 'plain' paradigms. For example, whereas traditionally state armies were involved in the use of force, nowadays non-state actors are prevalent or machines with digitalisation.[19] Fourth, what may cause uncertainty is states' changing perceptions of threats and their anxiety to defend themselves and their people against future but incipient threats. States are for instance concerned about asymmetric threats, a type of threat not addressed by the extant rules. Fifth, another issue that causes uncertainty is that the values promoted by the law on the use of force change or may differ between societies or eras.[20] For example, whether the regime should promote peace or justice is critical in how the rules are interpreted or applied.

Regarding the second aspect of uncertainty namely factual uncertainty, knowing and assessing the facts underpinning a use of force is important in order to establish whether there is a use of force or an armed attack, whether it has been committed by a state or a non-state actor[21], whether the use of force is imminent or necessary, or what is the target of the use of force.[22] However, identifying digital

[16] In relation to the definition of force see *Nicaragua Case,* para 195; Tom Ruys, 'The meaning of "Force" and the Boundaries of the *Jus ad bellum:* Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?' (2014) 108 *AJIL* 159. A definition of armed attack 'is not provided [for] in the Charter', *Nicaragua Case* para 176. For the Court it constitute 'the most grave forms of the use of force'. *Nicaragua Case* para 191 and 195. See also *Oil Platforms (Islamic Republic of Iran v United States of America)*, Judgment (Merits) [2003] ICJ Rep 161, para 64.

[17] *Nicaragua Case,* para 237. Dapo Akande and Thomas Liefländer, 'Clarifying Necessity, Imminence, and Proportionality in the Law of Self-Defense', 107 *The American Journal of International Law*, (2013), 564ff

[18] Hart, *Concept*,127

[19] See 'Introduction' DoD, Summary of the 2018 National Defense Strategy of the United States of America https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

[20] In general see Anthea Roberts, *Is International Law International?* (Oxford: Oxford University Press, 2017); G. Verdirame, ''The Divided West': International Lawyers in Europe and America', 18 *European Journal of International Law,* (2007),554; Prosper Weil, '"The Court Cannot Conclude Definitively..." Non Liquet Revisited', 36 *Columbia Journal of Transnational Law*, (1998), 118; E. Jouannet, 'French and American Perspectives on International Law: Legal Cultures and International Law, 58 *Maine Law Review,* (2006), 292-337

[21] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion [2004] ICJ Rep 136, para 139. République Française, Ministère des Armées, *Droit International Appliqué aux Opérations dans le Cyberespace,* p. 8

[22] Daniel Bethlehem, 'Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors', 106 *American Journal of International Law*, (2012), 769

facts is difficult because digitalisation may create new facts or no facts at all in that digital attacks may be invisible or undetected. Evaluating digital facts is also difficult because it depends on the availability, accessibility and calibre of evidence. This is particularly so regarding future and uncertain threats where the assessment of facts may lead to a host of false positives or false negatives.[23]

Another factor that contributes to factual uncertainty is the fact that there are no clear rules as to how facts and evidence can be analysed and assessed[24] or whether such assessments can be published or shared.

Factual uncertainty inevitably interacts with legal uncertainty. In the first place, factual uncertainty may cause legal uncertainty.[25] This is because facts (or their absence) and any factual inferences that are made determine whether law applies, which law applies, and which legal conclusions can be drawn. Second, legal uncertainty may lead to factual uncertainty. In the absence of clear thresholds of legality or illegality or clear definitions of the additional criteria according to which the legality of the use of force is assessed, relevant factual thresholds cannot be established. For example if the level of destruction that would make an attack a prohibited use of force or the point where an attack becomes immintent are not set out in the law, it is difficult to graft facts to these legal variables.

[23] Waxman, Matthew C, 'The use of force against states that might have weapons of mass destruction' 31 *Michigan Journal of International Law*, (2009), 1ff

[24] Anna Riddell & Brendan Plant, *Evidence Before the International Court of Justice*, (London: British Institute of International and Comparative Law, 2009); *Armed Acitivities,* para 173

[25] *The Report of the Iraq Inquiry* (London: Her Majesty's Stationery Office, 2016)

## 2.2 Digitalisation and legal uncertainty in the use of force regime

Digitalisation reproduces the aforementioned legal and factual uncertainties but can also aggravate them.[26] In the first place, there is uncertainty in the scope and application of extant rules regarding the definition of digital force and more particularly whether it includes physical and/or non-physical effects as well as whether it includes direct and/or indirect effects.[27] There is also uncertainty as to whether imminence should be defined exclusively in temporal terms considering the speed of digital force or what necessity and proportionality require in a digitally enabled operation.[28]

There is also uncertainty regarding the assessment and classification of digital facts underlying uses of force. Because digital operations are indistinguishable, this creates uncertainty as to their legal characterisation on the basis of facts. For example, the same means and methods can be used to gather information or cause damage and often all phases of digital operations such as reconnaissance, penetration, and execution, can be performed simultaneously. More critically though, digitalisation can create new facts or novel patterns of conduct for example non-tangible ones which are not included in the paradigmatic facts and behaviours assumed by existing rules or, at least, not falling neatly within these rules. For example tere may be questions as to whether direct and/or indirect facts should be taken into account to prove the gravity and scale of a digital use of force.

---

[26] 'The development and use of new technologies will inevitably raise questions both of *lex lata* and *lege ferenda*. Law will often be outpaced by scientific progress, which in turn tends to generate considerable uncertainty about the application of certain international rules. Legal uncertainty, particularly in the realm of peace and security, can lead to unwarranted insecurity and increased risks of conflict.
To the extent that interpretations of how international law applies to the use of ICT by States diverge, the risk of unpredictable behavior, misunderstandings and escalation of tensions increases. Therefore, it is important to identify convergence amongst States on this matter and, where divergences are identified, to jointly work towards increased coherence in the interpretation of existing rules. If necessary, development of additional norms should also be considered as a means to fill potential legal gaps and resolve remaining uncertainties'. Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International
Security established pursuant to General Assembly
resolution 73/266 GA, GA Doc. A /76/136* , 13 July 2021, 18

[27] Tallinn Manual 2.0 Rule 69

[28] Tallinn Manual Rules 72-73 Elizabeth Wilmshurst, 'The Chatham House Principles of International Law on the Use of Force in Self-Defence', 55 *ICLQ* 963, 967 (2006); Michael W. Doyle, *Striking First: Preemption And Prevention In International Conflict* (Princeton University Press, 2008); Abraham D. Sofaer, 'On the Necessity of Pre-Emption', 14 *EJIL* 209, 220 (2003)

Although digitalisation as was said can produce more evidence which can assist in the application of the relevant rules, such evidence can be less accessible because of security constraints or jurisdictional limitations. More critically through, it may not be possible to properly analyse and explain it.

This leads to another type of uncertainty regarding causality and how it can be proved in digital uses of force. Contrary to human reasoning, digital technologies mainly operate on the basis of correlation by performing pattern association within datasets, but this is not equivalent to causation which is about establishing how facts influence one another. A certain harm may for example be linked to a digital use of force but not necessarily caused by it.

Another area affected by digitalisation is proving the intent behind a digital use of force. For example, according to the French Government, a cyber attack must be a 'deliberate, offensive and malicious action' in order to trigger self defence[29] but how this can be established if decisions are delegated to digital agent is uncertain. Would, for example, data collected and analysed by digital agents which prove troop movements be sufficient to conclude that a use of force is imminent? Are further data needed? Can additional data regarding political, historical, psychological or other factors be collected by digital agents and analysed in context?

There is also uncertainty about the attribution of digital uses of force to states or other actors. Because of anonymity, spoofing and falsifying identities, digital agents may not be able to identify the actual authors of an attack if other variables such as intelligence information is not taken into account.[30]

The scope of legal uncertainty caused by digitalisation is not only external that is, from the point of view of those applying the law such as operators, decision-makers or adjudicators but also internal, from the point of view of the digital agents. In the absence of a stable legal and factual framework, digital agents cannot operate in a law-compliant manner because they cannot be programmed with legal precision. This is even more so in the case of digital agents with self-learning capabilities.

Uncertainty about rules and facts has reverberating effects in that it causes uncertainty about the applicable legal regime, to wit, whether it is the use of force regime or another international law regime that is implicated in a particular situation. This is because facts may fall within two or more

[29] Ministère des Armées, *Droit international appliqué aux cyberopérations dans le cyberespace* (2019) p.6

[30] Nicholas Tsagourias and Michael Farrell, 'Cyber Attribution: Technical and Legal Approaches and Challenges' 31 *EJIL* (2020), 941–967

regimes or because normative borders established by regime specific rules overlap or because which facts are legally important depends on how they are interpreted and selected. For example, uncertainty as to whether digital facts amount to an armed attack, a use of force, or intervention causes uncertainty as to whether they trigger the use of force regime or the law of state responsibility. Regime uncertainty creates another layer of uncertainty concerning the nature, scope, content, and legality of responses. For example, there can be uncertainty as to whether self-defence action should be taken which falls within the use of force regime or instead whether countermeasures should be taken which fall within the law of state responsibility.

What transpires from the above is that the use of force regime as it applies to digital uses of force is characterised by a sequence of uncertainties: uncertainty over facts; uncertainty over the identification of the applicable legal regime; and uncertainty over the content and scope of application of particular rules.

2.3 Addressing legal uncertainty

According to Hart, normative uncertainty is remedied by the existence of secondary rules namely the rule of recognition, change, and adjudication.[31] Secondary rules can address legal uncertainty by responding to the need to develop new rules to fill legal gaps. They can also respond to the need to reinterpret and clarify the content and scope of existing rules in order to regulate novel forms of conduct or agency. Secondary rules and in particular the rule of recognition can also establish criteria for the legal validity of primary rules

Regarding adjudication, according to Dworkin, legal uncertainty can be overcome through judicial interpretation where judges advance policies and principles and opt for the best justifications.[32] However, adjudication and the ensuing legal interpretation, clarification and determination of rules by judges is not a standard practice in the use of force regime or in international law in general. To a large extent, the content of the international law rules on the use of force is articulated and their validity is ascertained by states on the basis of claims and counterclaims, action and counter-action and very rarely by courts or objective third parties. This state of affairs does not offer any closure as far as the content and scope of the rules are concerned.

[31] Hart, *Concept,* Chapter V. According to Hart, primary rules stipulate obligations whereas a leal order is a union of primary and secondary rules.
[32] R. Dworkin, *A Matter of Principle*, (Oxford: Oxford University Press, 1985)

Regarding the secondary rules of recognition and change, although Hart refutes their existence in international law which according to him makes international law a primitive system, such secondary rules do in fact exist and refer to the sources of international law formulated in Article 38 of the ICJ Statute. The role of Article 38 is twofold: it lists the type of primary rules that make up international law (treaties, custom and general principles of law) but also prescribes the criteria according to which these primary rules can be introduced, changed and above all validated. In this respect Article 38 also acts as a secondary rule of recognition and change and transforms international law into a legal system than a set of primary rules.[33]

Regarding treaties, they can overcome legal uncertainty by acting as recognised law making-mechanisms. Treaties provide an institutionalised and formalised framework to introduce new law or modify and adapt existing law. Treaties can also have their own in-built mechanisms of modification, interpretation and application.[34] In this respect treaties can play the role of the Hartian rule of change but also constitute an international rule of recognition because their law-making function has been institutionalised and formalised not only procedurally but also substantively by the institution of consent.

Can treaties remedy the legal uncertainty afflicting digitally enabled uses of force? In principle they can do this by identifying which rules apply to digital uses of force, clarify how they apply or by introducing new rules. That said, there is doubt that treaties can play such a role for many reasons. In the first place, critical questions regarding definitional accuracy and precision; questions about which rules should apply to digital uses of force and the overall aims of the regime as well as questions about the scope of technical understanding of digital uses of force remain and will remain open in the future because of the opacity and inexplicability of digital technology and because of the rapid development of new technology. Secondly, digital technologies are "dual-use" without being able to demarcate in advance which aspect of the technology is peaceful and which is not or how it will be used. This affects the scope and content of regulation. Another issue that advocates against

[33] Chapter 1 Mehrdad Payandeh, 'The Concept of International Law in the Jurisprudence of H.L.A. Hart'21 *European Journal of International Law*, 2010, 967–995. David Lefkowitz, Philosophy and International Law: A Critical Introduction (CUP, 2020), ch 3.

ILC Study Group on the Fragmentation of International Law. Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law; Report of the Study Group of the International Law Commission, Finalized by Martti Koskenniemi. UN Doc A/CN.4/L.682 and Add.1 and Corr. 1, (2006), para 33

[34] See in general Vienna Convention on the Law of Treaties (1969) art. 2, Rebecca Crootof, 'Jurisprudential Space Junk: Treaties and New Technologies' in Chiara Giorgetti & Natalie Klein eds *Resolving Conflicts In The Law* 106–129 ( 2019)

treaty based law-making is the fact that digital technology is a buddle of other technologies which are at different levels of development and therefore regulating one technology or its use will be ineffective without regulating all other technologies. Furthermore, questions about the role of the private sector in treaty based law-making will definitely be raised to the extent that digital technologies are developed, produced and distributed by the private sector. Even if states enter into treaty negotiations, they may be delayed or prolonged because of states' divergent interests, resources and capabilities, and thus the concluded treaty may quickly become obsolete in view also of the rapid development and proliferation of digital technology. Finally, questions will arise about monitoring, verification and enforcement of the treaty based regime.

If consent constitutes the criterion of validity of treaty law which elevates treaties to an international rule of recognition, the question is whether states are willing to consent to a treatybased law-making regime. The challenges described above indicate that states are not ready to give their consent but there are also glaring technological disparities among states and divergent interests regarding the role and use of digital technologies or regarding the role and necessity of treaty based law-making. Even if a treaty is finally concluded, because of such disparities, states will definitely attach reservations and declarations that will dilute the scope and bindingness of such a regulatory regime.

All this means that a multilateral or universal treaty-based regime on digitalisation and the use of force is not forthcoming neither is a treaty between like-minded states more probable because it will disadvantage them in their relations with other states. Whether existing treaty law on the use of force namely the UN Charter can be amended in order to take into account digitalisation, this is in principle possible but procedurally difficult.[35]

Regarding customary law, it is presented as being more reactive to the actual needs of the international society and as a more comprehensive regulatory tool because of its universal scope and binding effect. Its formation and content however can be a cause of uncertainty. As is well known, the formative conditions of customary law are state practice and *opinio juris*.[36] Although digitalisation can increase the quantity of data and diversify their sources, there are problems with access to such data but also with understanding and analysing them due to the opacity of digital technology. This also relates to the problem of explainability as mentioned earlier. The fact that

[35] Article 108 of the UN Charter

[36] Article 38(1)(b) of the Statute of the International Court of Justice 1945. *North Sea Continental Shelf Cases*, Judgment [1969] ICJ Rep. 3, para. 72; *Nicaragua Case*, para 184. International Law Commission, *Draft Conclusions on Identification of Customary International Law, with Commentaries* (2018)

digitally enabled uses of force are often covert and undetected means that data may not exist or may be discovered years after the event. More critically through, states do not explicitly state their views on the legality or illegality of digitally enabled uses of force and do not express their views about the content and scope of specific rules, something that can affect the emergence of custom. Another problem is that of ingrained bias in the operation of digital agents, for example the inclusion of certain values in their decision making cycle which may lead to predetermined results. Furthermore, customary law is often *ex post* law which requires a quite significant time frame to mature; it will thus lag behind the pace of digital development. Granted, there are occasions where custom can develop quite rapidly and digital technology can support the rapid development of custom because of the wealth of data it can produce. However, as already said, there are problems with the analysis and evaluation of data. There is another problem as well in that a customary rule established rapidly on the basis of existing data may reflect a particular state of affairs which may become immediately obsolete in view of the rapid development of digital technology or, alternatively, it may prevent new legal developments.

All this means that uncertainty permeates not only the primary rules on the use of force but also the secondary rules which cannot thus play the role envisaged by Hart.

2.4 The impact of uncertainty on the use of force regime

Legal uncertainty can have profound effects on the use of force regime. International law is a governance tool which, by maintaining a rule-based order, fosters stability and predictability in international relations and in cyber relations in particular.[37]

Legal uncertainty is however a law regressive process which may lead to the rejection of particular rules on the use of force for example the rule on self-defence or lead to the rejection of the whole regime if states or individuals lose faith because, in their opinion, the regime is not normatively and regulatorily cost effective. If that is to happen, we will revert to a pre-legal order of naked power where norms are created, applied and enforced by political power and through political fiat without the mediating effect of the law.

Even if the consequences of legal uncertainty are not as dramatic as the ones described above, legal uncertainty can affect the intelligibility of the legal order on the use of force. It will create a

[37] See Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security', UN Doc A/76/135 (14 July 2021) and Open-ended working group on developments in the field of information and telecommunications in the context of international security Final Substantive Report A /AC.290/2021/CRP.2 (10 March 2021)

non-determinate realm of legal possibilities and legal impossibilities which will make the application of the rules on the use of force by humans, states or machines as well as their application to humans, states and machines a la carte and discretionary, contrary to the values of coherence, equality, and consistency characterising a legal order.

Such an order will be an a-legal order.[38] It will be an order where the distinction between legality and illegality will be constantly questioned by questioning the subjective, material, spatial and temporal application of the law. It will also be an order where patently unordered (outside the law) behaviour can be presented as falling within the realm of the legal order but its entry to the legal order will take place through sheer power; the power to act in a certain way and the power to force the acceptance of new conduct as one of the legal possibilities.

## 3. The replacement of international law

The second challenge I will consider concerns the replacement of international law as regulatory tool in the use of force regime.

The process according to which custom is created is a good starting point to explain this process. As is well known, States are the main actors participating in the formation of custom through their practice and *opinio juris* but digitalisation can challenge the authorship of practice and *opinio juris*. If data analysis and decisions are for instance performed by digital agents, would that constitute custom-related practice and *opinio juris* as we know it?

Although there are circumstances according to which such practice and *opinio juris* can be attributed to States, this is not the case with fully autonomous digital agents. Consider for example the case of automatic self-defence where a machine with self-learning capabilities makes determinations and decisions about the existence of an armed attack as well as about the necessity and proportionality of the self-defence action without human involvement.[39]

If autonomous digital agents become the authors of practice and *opinio juris*, they will replace states as the creators of custom. That said, digital agents are not currently recognised by international law as legal persons. If they remain unrecognised but still participate in the use of force cycle of

[38] Hans Lindahl, *Fault Lines of Globalization: Legal Order and the Politics of A-Legality* (OUP, 2013) 30-43; 156-186
[39] 'Russell Buchan and Nicholas Tsagourias, 'Automatic Cyber Defence and the Laws of War' 60 *German Yearbook of International Law* (2017), 203-237

customary law formation, the process but also its outcome to wit, the creation of customary rules on the use of force, will remain uncertain because it will not be clear what is actually state practice and *opinio juris* and what is not.

The immediate question is whether digital agents should be endowed with legal personality[40] and, consequently, be recognised as generators of customary law.

Every legal system including the international legal system defines its legal subjects that is, the entities which can create law, enforce the law and incur responsibility. Legal personhood in international law is limited to states and international organisations[41] but it is important to note that they are both artificial persons. They are legal artifacts attributed with legal personality as anthropomorphic actors. This indicates that the institution of legal personality in international law is decoupled from physicality and consciousness and, therefore, it cannot be in principle adverse to recognising digital agents as legal persons. The question then is whether there are any ingrained or functional reasons to justify the granting of legal personality to digital agents. If legal personality is ascribed to actors who are rational, certain digital entities in particular those with self-learning capabilities could be granted legal personality because they emulate rational reasoning. If legal personality is ascribed to entities which have the capacity to function in law, digital agents should be granted legal personality because they are in principle programmed to act within the law whereas their actions have legal implications. Consider for example drones or LAWS which target according to IHL and their decisions have legal implications. If legal personality is conferred to entities which are independent there are digital agents which operate without human intervention or, to use a common verbiage, operate with humans 'out of the loop'. If legal personality is granted in order to hold an entity responsible in law, then there are good reasons why digital agents should be granted legal personality; their acts can have material as well as other consequences for which they should be held responsible as in the case of autonomous weapons.[42]

---

[40] Simon Chesterman, We, the Robots? Regulating Artificial Intelligence and the Limits of the Law (CUP, 2021) ch.5; Simon Chesterman, Artificial Intelligence and the Limits of Legal Personality *69 ICLQ, 819-844 (2020)*

[41] *Reparation for Injuries Suffered in the Service of the United Nations*, Advisory Opinion, 1949 I.C.J. Rep. at 174; E. Nijman, *The Concept Of International Legal Personality: An Inquiry Into The History And Theory Of International Law* (CUP, 2004); Roland, *Legal Personality in International Law* (CUP, 2013) James R Crawford, *Brownlie's Principles of Public International Law* 9th Edition, (OUP, 2019), chapter 4

[42] European Parliament Resolution with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) (European Parliament, 16 February 2017), para 59(f)

If legal personality is granted to digital agents who can then generate customary law through their own practice and *opinio juris*, the customary law formation process on the use of force will be digitalised. The critical question is whether the process and the outcome (the customary law rules that emerge) will still be treated as falling within the scope of Article 38 of the ICJ Statute or, instead, be treated as giving rise to a heteronomous customary law called for instance customary law 1.0 or something else. If the latter is to happen, the process of customary law formation as is known in international law will be replaced by a novel digital process which will generate digital customary law rules. The consequences for the international law regime on the use of force but also for the international legal order in general will be profound. If the space, time, subjects and materials to which the legal order applies change, we can speak of the emergence of a new legal order.[43]

There is the possibility of treating this digital customary law process as part of the existing Article 38 process. In this case the use of force regime will lose its unitary character and will be divided into two subsets of processes and rules; one for the physical world and the other for the digital world. For example, different customary rules on imminence will apply to a digital armed attack from those applying to a physical attack which may justify self-defence in the first instance but not in the latter. This state of affairs can be described as the partial replacement of the extant use of force rules. Still questions will arise regarding the normative and factual boundaries separating the two subsets of rules and how or who will make decisions about which subset applies to particular facts. Would the application of the correct regime depend on whether the determination is made by digital agents or humans? Also questions will arise as to how conflicts between the two subsets can be mediated. Would the *lex specialis* rule apply? Yet the most critical question is whether the differentiated application of the use of force rules and the differentiated legal outcomes that will be produced can still preserve the viability of the regime as whole.

There is also the possibility of the two subsets (digital and physical) merging into a unitary process of customary law formation giving rise to single rules. This would most probable be the case if digital technologies inform practice and *opinio juris* rather than authoring them as in the preceding scenarios. A critical question is the extent to which digital technologies just inform or in fact replace human decision-making. This has to do with the explainability of digital reasoning mentioned earlier but also with the issue of over-reliance on digital technologies what is referred to as 'automation bias'. Human agents often defer to digital agents because of their supposed infallibility. If human

[43] Hans Kelsen , *Introduction to the Problems of Legal Theory* , 1st edn. of the Reine Rechtslehre , trans. Bonnie Litchewski Paulson and Stanley L. Paulson ( Oxford : Clarendon , 2002 )

agents for instance defer to a digital agent's determination of an armed attack but cannot understand the way such a determination has been reached, does this constitute digital or state practice and *opinio juris*? It follows that for an integrated customary law process, being able to decipher how state decision-makers and digital agents make determinations and how they interact with each other is important.

Yet, even if the process is integrated, questions about the content of the customary rules and their material and personal application will arise. What would for example be the content of the customary law rule on imminence or armed attack in an integrated (digital and physical) set of use of force rules?

The partial or total replacement of the international customary law process can also be triggered by the prominent role of private companies such as tech companies in digitalisation. These companies have taken advantage of their power, resources and global reach to fill the regulatory space left by states. They introduced norms, principles, standards and good practices to regulate digitally-enabled conduct but they have also engaged in the interpretation and application of international law.[44] However private companies do not have international legal personality and, with the exception of state owned or controlled companies, they cannot formally contribute to the formation of international customary law. Can the involvement of private companies and their regulatory norms lead to the replacement of international law? They can do so if they are recognised as legal persons, an issue discussed earlier in relation to digital agents. However, they can replace international law even if they are not recognised as legal persons. First, States and individuals may transfer their allegiance from international law and the institutions responsible for the creation, interpretation and application if international law to private companies and their regulatory frameworks. In this case international law will cease to exert its regulatory gravitational pull but it will be replaced by private regulation. Second, although the norms, principles, standards and good practices introduced by the private sector do not in principle fall within the recognised sources of international law, if they are adhered to because of their broad reach and indispensability for anyone using digital technologies, they can gradually displace international law and replace its rules with such private norms.[45] Third, although the aim of such norms, principles, standards, and good

[44] Microsoft, The need for a Digital Geneva Convention (2017) https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

[45] Alan Boyle, 'Soft law in international law-making', in M. Evans (ed.), *International Law* (Oxford, 2018, 5th ed). ch 5

practices is to order behaviour, their ordering nature and effects will not be mandatory but voluntary and discretionary. They will thus displace international law's mandatory ordering tasks and replace them with voluntary and relative ones.

Alternatively, if the international law regime on the use of force becomes a mixture of international law rules, norms, principles, standards and good practices introduced, interpreted and applied by states and private actors, this will lead to the partial replacement of international law which will cause confusion as to what is legal and what is illegal and what is expected as a matter of law or what is expected as a matter of professional or technical standards or good practice.

This leads to another form of replacement regarding international law's regulatory modality.[46] International law is a normative system which regulates behaviour, conduct and outcomes in spatial, temporal, material and subjective term and assesses the legality or illegality of such behaviour, conduct and outcomes in substantive terms.[47] Because digitalisation as explained earlier poses many challenges to the normativity of international law in all four of the aforementioned dimensions, the modality of regulation of the use of force can change to *ex ante* regulation of States' or digital agents' behaviour with a view of preventing outcomes that international law prohibits but without targeting the law prohibitive conduct and outcome (the use of force in this case).

The normative and mandatory regulatory modality of international law will thus be replaced by an administrative, managerial and technical regulatory modality whereby international law becomes the background (not the upfront applicable legal framework) to such administrative, managerial, technical regulations whose aims are to avert or neutralise as far as possible the pathways that could lead to international law violations and hold someone responsible for his/her contribution to the potentiality of a violation but they will not be concerned with the question of whether the result envisaged by the rule is achieved or whether the culprit for the wrongful result is held responsible. Consequently, instead of protecting rights and their holders from direct violations and punish perpetrators for the violations, regulation will shift responsibility to accomplices (owners, manufacturers) or to operators and decision- makers who become the subjects of responsibility for their bad choices.

[46] Lawrence Lessig, *Code, and Other Laws of Cyberspace (1999);* Lawrence Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 Harvard Law Review 501. Lessing identified law, social norms, market, and architecture/code as modalities of regulation

[47] Hans Kelsen , Introduction to the Problems of Legal Theory , 1st edn. of the Reine Rechtslehre , trans. Bonnie Litchewski Paulson and Stanley L. Paulson ( Oxford : Clarendon , 2002 )

Such a regulatory regime will for example contain due diligence[48] requirements regarding the decision-making process involving the use of force or inbuilt technical rules that regulate the operational propriety of digital agents when using force which will form the framework according to which the lawfulness of their conduct will be assessed. It would mean that even if force is actually used, there will be no assessment of its lawfulness in substantive terms but even if it is manifestly unlawful there will be no violation of the non-use of force rule if the administrative, managerial or technical regulations were followed. The only basis for holding someone responsible will be his/her failure to follow these administrative, managerial or technical standards and even in this case, ascribing responsibility may be difficult because it will be difficult to identify who was negligent in a complex decision-making process.

## 4. Conclusion

The article examined the systemic impact of digitalisation on the international law regime governing the use of force. More specifically, it identified legal uncertainty and the replacement of international law as two features of the systemic impact of digitalisation on the use of force regime.

With the inexorable advance of digitalisation, will it render the use of force regime 'at the vanishing point of international law', to use Lauterpacht's phrase?[49] If this is what digitalisation will bring about, it will be profoundly disruptive. In order to prevent this from happening, we should diversify and expand the normative context within which digital technologies are assessed to include, in addition to law, ethical, social, and political consideration. Above all however, we should rediscover the spirit of the enlightenment.[50] In the era of the enlightenment, science operated within and disseminated moral, political, legal visions of word order. Science did not create these visions. It was

[48] Heike Krieger, Anne Peters, and Leonhard Kreuzer , *Due Diligence in the International Legal Order* (OUP, 2021) in particular chapter 1

[49] H. Lauterpacht, 'The Problem of the Revision of the Law of War', 29 *British Year Book of International Law,* (1952), pp.360-382, p.382. Lauterpacht used this phrase to describe the law of war.

[50] Henry Kissinger, How the Enlightenment Ends, *The Atlantic* (June 2018) https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124/ ; Henry A. Kissinger, Eric Schmidt, and Daniel Huttenlocher, The Metamorphosis, *The Atlantic* (August 2019) https://www.theatlantic.com/magazine/archive/2019/08/henry-kissinger-the-metamorphosis-ai/592771/ ; Henry A. Kissinger, Eric Schmidt, and Daniel Huttenlocher, *The Age of AI And Our Human Future*, (Little Brown and Company, 2021)

the human mind and human consciousness that provided the explanatory power. International law is a child of the enlightenment and individuals, societies, and states should therefore maintain their power to use the law to explain and interpret the world in terms that are meaningful to them. Thus, my very modest proposal is to encourage deliberation of the political, legal, ethical, social implications of digital technologies in the use of force regime with a view of establishing an informed understanding of how they can be used and which aims they can support. Such understandings may then be included in interpretations of existing rules or the development of new rules.