*German Law Journal* (2023), **24**, pp. 494–507
doi:10.1017/glj.2023.33

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Special Issue: International Law and Digitalization

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

Nicholas Tsagourias

University of Sheffield, Sheffield, England
Email: nicholas.tsagourias@sheffield.ac.uk

(Received 11 April 2023; accepted 11 April 2023)

**Abstract**

This article explores the systemic impact of digitalization 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 of the use of force by considering the impact of digitalization 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 digitalization on the use of force regime but extend to international law in general.

**Keywords:** Digitalization; use of force; legal and factual uncertainty; replacement of international law; legal personality; customary law

## A. Digitalization and the International Law Regime on the Use of Force

Digitalization 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, analyzing, and assessing large amounts of factual patterns and data drawn from diverse and multiple sources.

[1]Colin B. Picker, *A View from 40,000 Feet: International Law and the Invisible Hand of Technology*, 23 CARDOSO L. REV. 151–219 (2001). Digitalization is used in this article as an umbrella term to describe the use of digital technologies such as cyber technology or AI. The latter refers to technology which replicates humanlike 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. *See also* STUART RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH, 1-5 (3rd ed., 2013).

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

Digitalization 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, digitalization can protect resources and minimize exposure to risks or harm because results can be attained without the need to deploy human or material resources. Digitalization can achieve endurance and expand the reach of operations which depleted physical or human resources cannot achieve. All of this means that digitalization can scale up human, institutional, and state capabilities and act as force multiplier without always involving human agents.

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

Having said that, digitalization can be a vector of many risks and challenges. The speed with which decisions are made, and 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. Digitalization 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. Digitalization 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 situation affects the ability of humans or institutions to meaningfully 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, and the speed with which decisions and actions 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 refers to 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 digitalization affects the international law regime on the use of force. That said, this article will not consider the question of how digitalization is

[3]Carl von Clausewitz, On War 5 (Michael Howard et al. eds. and trans. 2007).

[4]Simon Chesterman, We the Robots 64 (2021) (explaining opacity is the antithesis of legal reasoning).

https://doi.org/10.1017/glj.2023.33 Published online by Cambridge University Press

challenging substantive rules of the use of force regime[5], but instead, it will consider the systemic impact of digitalization on the use of force regime.

More specifically, this article considers two issues where the systemic impact of digitalization on the use of force regime manifests itself. The first is legal uncertainty, which will be considered in Section B whereas the second issue is the replacement of the international law governing the use of force, which will be considered in Section C.

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 GGE reports, as well as by the 2021 OEWG report.[6] Many states that have made their position public have also affirmed the application of international law to cyber operations.[7] The same is true regarding AI, with states having confirmed the application of international law to AI.[8]

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.[9] 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-defense in response to an armed attack, and the use of force when authorized by the Security Council.[10]

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 digitalization. [11]

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

[6]U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/68/98 (June 24, 2013); U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/70/174 (July 22, 2015); UNGA, *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 (July 14, 2021); U.N. Secretary-General, *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 (Mar. 10, 2021).

[7]*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; Press Release, Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace, Aldiplomasy (July 2020), www.aldiplomasy.com/en/?p=20901; France, *Ministère des Armées, Droit International Appliqué aux Opérations dans le Cyberespace* (2019), https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf; Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace, Gov't Netherlands (July 1, 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.

[8]*See* 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* (Jan. 20, 2021); *see also 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 (Dec. 13, 2019).

[9]*See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, paras. 174–176 (June 27).

[10]*See* U.N. Charter art. 2(4), 51, chap. 7., G.A. Res. 42/22 (Nov. 18, 1987); U.N. Doc. A/RES/42/22; *see also* Nicar. v. U.S., 1986 I.C.J. para. 190; Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 ICJ Rep. 136, para. 87 (July 9); Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 ICJ Rep. 168 para. 148 (Dec. 19); Russell Buchan & Nicholas Tsagourias, Regulating the Use Force: Stability and Change, 19–78, 132–189 (2021).

[11]For general overview of cyber technologies and international law 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*

https://doi.org/10.1017/glj.2023.33 Published online by Cambridge University Press

## B. Digitalization 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 à la carte norms are developed in response to particular events or behaviors, 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]

### *I. 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 facts. For example, although the rule on the non-use of force or the rule on self-defense 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

*Intelligence and The Development, Displacement or Destruction of the Global Legal Order*, 20 MELB. J. INT'L. L. 29–56 (2019); Hin-Yan Liu, Matthijs Mass, John Danaher & Luisa Scarcella, *Artificial Intelligence and Legal Disruption: A New Model for Analysis*, 12 LAW, INNOVATION & TECH. J. 205-258 (2020).

[12]H.L.A. HART, THE CONCEPT OF LAW 127 (3rd ed. 2012).

[13]*See* Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Merits, 2005 ICJ Rep. 168 paras. 57-58 (Dec. 19); *see also* Sir Franklin Berman QC, *What Do We Expect of Lawyers in Armed Conflict?*, 38 GEO. WASH. INT'L. L. REV., 628, 631-32 (2006).

[14]For uncertainty in international law, see MARTTI KOSKENNIEMI, FROM APOLOGY TO UTOPIA (2005).

[15]*See* Nicar. v. U.S., 1986 I.C.J. at paras. 176-179; *see also* Letter of US Secretary of State Daniel Webster in *Caroline Case*, 29 BRITISH & FOREIGN STATE PAPERS 1137–1138 (April 24, 1841), https://avalon.law.yale.edu/19th_century/br-1842d.asp; THE CHARTER OF THE UNITED NATIONS: A COMMENTARY paras. 13, 63 (Bruno Simma, Daniel-Erasmus Khan, Georg Nolte & Andreas Paulus eds., 3rd ed., 2012).

[16]In relation to the definition of force, see Nicar. v. U.S., 1986 I.C.J. at para. 195. *See also* Tom Ruys, *The Meaning of "Force" and the Boundaries of the Jus ad bellum: Are "Minimal" Uses of Force Excluded from U.N. Charter Article 2(4)?,* 108 AM. J. INT'L L. 159 (2014) (explaining a definition of armed attack is not provided for in the Charter); Nicar. v. U.S., 1986 I.C.J. paras. 176, 191, 195 (explaining for the Court it constitutes the most grave form of the use of force); Oil Platforms (Islamic Rep. of Iran v. U.S.), Judgment, 2003 I.C.J. Rep. 161, para. 64.

[17]*See* Nicar. v. U.S., 1986 I.C.J. para. 237; *see also* Dapo Akande & Thomas Liefländer, *Clarifying Necessity, Imminence, and Proportionality in the Law of Self-Defense*, 107 AM. J. OF INT'L L. 564 (2013).

[18]Hart, *supra* note 12.

https://doi.org/10.1017/glj.2023.33 Published online by Cambridge University Press

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 digitalization.[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 facts is difficult because digitalization 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 caliber 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 analyzed and assessed,[24] or whether such assessments can be published or shared.

Factual uncertainty inevitably interacts with legal uncertainty. First, 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 imminent are not set out in the law, it is difficult to graft facts to these legal variables.

## *II. Digitalization and Legal Uncertainty in the Use of Force Regime*

Digitalization not only 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

[19]Dep't Def., *Introduction, 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]*See, e.g.,* Anthea Roberts, Is International Law International? (2017); Guglielmo Verdirame, *"The Divided West": International Lawyers in Europe and America*, 18 Eur. J. Int'l L. 554 (2007); Prosper Weil, *"The Court Cannot Conclude Definitively . . ." Non Liquet Revisited*, 36 Colum. J. Transnat'l L. 118 (1998); Emmanuelle Jouannet, *French and American Perspectives on International Law: Legal Cultures and International Law*, 58 Me. L. Rev. 292-337 (2006).

[21]*See* Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 ICJ Rep. 136, para. 139 (July 9); *see also* Ministère des Armées, Droit International Appliqué aux Opérations dans le Cyberespace 8 (2019).

[22]Daniel Bethlehem, *Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors*, 106 Am. J. Int'l L. 769 (2012).

[23]Matthew C. Waxman, *The Use of Force Against States That Might Have Weapons of Mass Destruction*, 31 Mich. J. Int'l L. 1 (2009).

[24]Anna Riddell & Brendan Plant, Evidence Before the International Court of Justice (2009); Dem. Rep. Congo v. Uganda, 2005 ICJ Rep. at para. 173.

[25]House of Commons, Her Majesty's Stationery Office, The Report of the Iraq Inquiry (2016).

[26]*See* Brazil's statement in *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*

https://doi.org/10.1017/glj.2023.33 Published online by Cambridge University Press

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 characterization 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, digitalization can create new facts or novel patterns of conduct, for example non-tangible ones, which are not included in the paradigmatic facts and behaviors assumed by existing rules, or at least, not falling neatly within these rules. For example, there may be questions as to whether direct and/or indirect facts or non-destructive effects should be taken into account to prove the gravity and scale of a digital use of force.

Although one can say that digitalization can produce more evidence which can assist in the application of the relevant rules, such evidence may be less accessible because of security constraints or jurisdictional limitations. More critically though, it may not be possible to properly analyze and explain it. In both cases uncertainty remains.

Another type of uncertainty refers to the issue of 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 of uncertainty concerns 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-defense.[29] Yet exactly how this can be established if decisions are delegated to digital agents is uncertain. Would, for example, data collected and analyzed by digital agents that 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 analyzed 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 or human agents may not be able to identify the actual authors of an attack if other variables such as intelligence information are not taken into account.[30]

---

*the Context of International Security established pursuant to General Assembly Resolution 73/266* U.N. Doc. A/76/136 (July 13, 2021), 18:

> 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".

[27]Tallinn Manual, *supra* note 5 at Rule 69.

[28]Tallinn Manual, *supra* note 5 at Rules 72–73; *see also* Elizabeth Wilmshurst, *The Chatham House Principles of International Law on the Use of Force in Self-Defence*, 55 INT'L & COMPAR. L. Q. 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).

[29]Ministère des Armées, *supra* note 8, at 6.

[30]Nicholas Tsagourias & Michael Farrell, *Cyber Attribution: Technical and Legal Approaches and Challenges*, 31 EUR. J. INT'L L. 941–967 (2020).

https://doi.org/10.1017/glj.2023.33 Published online by Cambridge University Press

The scope of legal uncertainty caused by digitalization 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 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. In the example used above, there will be uncertainty as to whether self-defense 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 characterized 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.

## *III. 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 counteraction, and very rarely by courts or neutral third parties. This state of affairs does not offer any closure as far as the content and scope of the rules are concerned.

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—and it also prescribes the criteria according to which these primary rules can be introduced, changed, and

[31]Hart, *supra* note 12, Ch. 5 (explaining how primary rules stipulate obligations, whereas a legal order is a union of primary and secondary rules).

[32]Ronald Dworkin, A Matter of Principle (1985).

https://doi.org/10.1017/glj.2023.33 Published online by Cambridge University Press

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 recognized law making-mechanisms. Treaties provide an institutional and formalized framework to introduce new law or modify and adapt existing law. Treaties can also have their own built-in 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 lawmaking function has been institutionalized and formalized 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, by clarifying how they apply, or by introducing new rules. That being said, it is doubtful that treaties can play such a role for many reasons. First, critical questions remain regarding the definitional accuracy and precision of treaty rules, the relevance of existing rules to digital uses of force, as well as questions about the technical understanding of digital uses of force and thee questions will remain open in the future because of the opacity, inexplicability and complexity of digital technology. Second, digital technologies are "dual-use" technologies without being able to demarcate in advance which aspect of the technology is peaceful, which is not, or how it will be used. This affects the scope and content of any treaty-based regulation. Third, another issue that advocates against treaty-based lawmaking is the fact that digital technology is a bundle of other technologies which are at different levels of development. Therefore regulating one technology or its use will be ineffective without regulating all other technologies. Fourth, questions about the role of the private sector in treaty-based lawmaking will definitely be raised to the extent that digital technologies are developed, produced, and distributed by the private sector. Finally, questions will be asked about the monitoring, verification, and enforcement of any treaty-based regime.

The challenges described above indicate that legal uncertainty cannot be removed by concluding a treaty. States are also reluctant to regulate digital technologies via a treaty because of the glaring technological disparities that exist, their divergent interests regarding the role and use of digital technologies and their different views about the role and necessity of treaty-based lawmaking.

Even if states enter into negotiations with a view of concluding a treaty, the negotiations will be prolonged because of their divergent interests, resources, and capabilities. If a treaty is finally concluded, for the same reasons, states will attach reservations and declarations that will dilute the scope and bindingness of its provisions. Moreover, because of the prolonged negotiations, the concluded treaty may quickly become obsolete in view of the rapid development and proliferation of digital technology.

In short, a multilateral or universal treaty-based regime on digitalization and the use of force to remove uncertainty is not forthcoming, and 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 digitally enabled uses of force is in principle possible but procedurally difficult.[35]

Regarding customary law, it is usually presented as being more reactive to the actual needs of the international society and as a more comprehensive regulatory tool because of its universal

[33]Mehrdad Payandeh, *The Concept of International Law in the Jurisprudence of H.L.A. Hart*, 21 Eur. J. Int'l L. 967–995 (2010); *see also* David Lefkowitz, Philosophy and International Law: A Critical Introduction ch. 3 (2020); U.N. Int'l Law Comm'n, *Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law*, *Report of the Study Group of the International Law Commission*, para. 33, U.N. Doc. A/CN.4/L.682 (July 18, 2006).

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

[35]U.N. Charter art. 108.

https://doi.org/10.1017/glj.2023.33 Published online by Cambridge University Press

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 digitalization can increase, as was said, the quantity of data tah can be taken into account for the formation of custom and diversify their sources, it does not mean that customary law can be easily established. First, there are problems with access to such data but also with understanding and analyzing them due to the opacity of digital technology. This relates to the problem of explainability mentioned earlier. Second, the fact that digitally enabled uses of force will most probably be covert and undetected means that data may not exist or may be discovered years after the event. This affects the material element of custom formation namely, state practice. Third, states are reluctant to make their views public about the content of international law rules as they apply to the digital world and refrain from pronouncing on the legality or illegality of digital operations. The digitally enabled use of force will not be an exception to such reticence. Such lack of opinions will affect the content of subjective element of custom.

Another problem with customary law is the ingrained bias in the operation of digital agents if they become the source of practice and *opinio juris*. The inclusion for instance of certain values in their decision-making cycle may lead to predetermined results. As a result, practice and *opinio juris* can be manipulated.

Finally, it should be recalled that customary law is often *ex post facto* law which requires a quite significant time frame to mature. It will thus lag behind the pace of digital developments. 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 in order to decipher the underlying practice and *opinio juris*. Also, if a customary rule is established rapidly on the basis of existing data, it may reflect a particular state of affairs and thus prevent new legal developments.

All of 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.

## IV. The Impact of Uncertainty on the Use of Force Regime

Legal uncertainty can have profound effects on the international law regime governing the use of force including digitally enabled use of force.

International law is a governance tool, which by maintaining a rule-based order, fosters stability and predictability in international relations.[37] Legal uncertainty is, however, a law regressive process that may lead to the rejection of particular rules on the use of force—for example, the rule on self-defense—or lead to the rejection of the whole regime if states or individuals conclude that 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 and order is maintained 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. The use of force regime will become an indeterminate legal order where the application of its rules by humans, states, or machines as well as their application to humans, states, and machines will be à la carte and discretionary, contrary to the values of coherence, equality, and consistency characterizing a legal order.

[36]I.C.J. Statute, Article 38(1)(b) (1945); North Sea Continental Shelf Cases (Fed. Rep. of Ger. V. Den.; Fed. Rep. of Ger. v. Neth.), Judgment, 1969 I.C.J. Rep. 3, para. 72 (Feb. 20); Nicar. v. U.S., 1986 I.C.J. para. 184; U.N. Int'l Law Comm'n, *Draft Conclusions on Identification of Customary International Law, With Commentaries* (2018).

[37]*See* Rep. of the S.C., *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, U.N. Doc. A/76/135 (July 14, 2021); *see also* Rep. of the S.C., *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Final Substantive Report*, U.N. Doc. A /AC.290/2021/CRP.2 (Mar. 10, 2021).

https://doi.org/10.1017/glj.2023.33 Published online by Cambridge University Press

Such an order can be described as 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. In such an order, new conduct can be presented as falling within the realm of the legal order through sheer power—the power to act in a certain way and the power to force its acceptance as the law. To give an example, the question of whether or under what circumstances digital attacks on critical state infrastructure constitute a violation of the rule prohibiting the use of force will remain open by questioning the content and scope of the rule, the meaning of 'force', the underlying facts over which the rule applies or by introducing qualifiers to such determination with power, referring to the ability of certain states to compel or influence the process of rule development, acting as the final arbiter of the legality or illegality of such conduct.

## C. The Replacement of International Law

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

The process according to which custom is created is a good starting point to explain this phenomenon. As is well known, states are the main actors participating in the formation of custom through their practice and *opinio juris*, but digitalization 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-defense 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-defense 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 being said, digital agents are not currently recognized by international law as legal persons. If they remain unrecognized, but still participate in the use of force cycle of customary law formation, the process and 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* as opposed to what is not.

The immediate question is whether digital agents should be endowed with legal personality[40] and, consequently, be recognized 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 organizations[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 recognizing digital agents as legal persons. The question then is whether there are

[38]Hans Lindahl, Fault Lines of Globalization: Legal Order and the Politics of A-Legality 30–43, 156–186 (2013).

[39]Russell Buchan & Nicholas Tsagourias, *Automatic Cyber Defence and the Laws of War*, 60 German Y.B. Int'l L. 203-237 (2017).

[40]Simon Chesterman, We, the Robots? Regulating Artificial Intelligence and the Limits of the Law (2021); Simon Chesterman, *Artificial Intelligence and the Limits of Legal Personality,* 69 Int'l Compar. L. Q. 819-844 (2020).

[41]Reparation for Injuries Suffered in the Service of the United Nations, Advisory Opinion, 1949 I.C.J. 174; Janne Elisabeth Nijman, The Concept Of International Legal Personality: An Inquiry Into The History And Theory Of International Law (2004); Roland Portmann, Legal Personality in International Law (2013); James Crawford, Brownlie's Principles of Public International Law (9th ed., 2019).

https://doi.org/10.1017/glj.2023.33 Published online by Cambridge University Press

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 agents, 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 that 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]

In view of the above, 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 digitalized. 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-defense 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 be the most probable 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 overreliance on digital technologies—what is referred to as "automation bias". Human agents often defer to digital agents because of their supposed infallibility. If human agents, for instance, defer to a digital agent's determination of an armed attack because of an ingrained belief in their accuracy but at the same time they cannot understand

[42]Recommendations to the Commission on Civil Law Rules on Robotics, Eur. Parl. Res., O.J. (2015/2103, INL), para. 59(f) (Feb. 16, 2017).

[43]Hans Kelsen, Introduction to the Problems of Legal Theory: A Translation of the First Edition of the Reine Rechtslehre or Pure Theory of Law (Bonnie Litchewski Paulson & Stanley L. Paulson trans., 2002).

https://doi.org/10.1017/glj.2023.33 Published online by Cambridge University Press

the way such a determination has been reached, does this constitute digital or state practice and *opinio juris*? What transpires is 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 digitalization. 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, and 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 with their regulatory norms lead to the replacement of international law? It can do so if companies are recognized as legal persons, an issue discussed earlier in relation to digital agents. However, their involvement can lead to the replacement of international law even if companies are not recognized as legal persons. First, states and individuals may transfer their allegiance from international law and the institutions responsible for the creation, interpretation, and application of 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 recognized 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 practices is to order behavior, 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, what is illegal, what is expected as a matter of law, and what is expected as a matter of professional or technical standards or good practice.

This leads to another form of replacement concerning international law's regulatory modality.[46] International law is a normative system that regulates behavior, conduct, and outcomes in spatial, temporal, material, and subjective terms and assesses the legality or illegality of such behavior, conduct, and outcomes in substantive terms.[47] Because digitalization, 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' behavior with a view of preventing outcomes that

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

[45]Alan Boyle, *Soft Law in International Lawmaking*, *in* INTERNATIONAL LAW (M. Evans ed., 5th ed., 2018).

[46]LAWRENCE LESSIG, CODE, AND OTHER LAWS OF CYBERSPACE (1999); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach* 113 HARV. L. REV. 501 (1999) (identifying law, social norms, market, and architecture/code as modalities of regulation).

[47]Kelsen, *supra* note 43.

https://doi.org/10.1017/glj.2023.33 Published online by Cambridge University Press

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 neutralize 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. However, 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 such as owners and manufacturers or to operators and decisionmakers who will become the subjects of responsibility for their bad choices.

Such a regulatory regime will, for example, contain due diligence[48] requirements regarding the decision-making process involving the use of force or built-in 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. This would mean that even if force is actually used, there will be no assessment of its lawfulness in substantive terms and 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 their failure to follow these administrative, managerial, or technical standards. 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.

## D. Conclusion

This article examined the systemic impact of digitalization 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 digitalization on the use of force regime. In doing so, useful insights were drawn which are also transferrable to international law in general.

The question that can be asked at this point is whether the inexorable advance of digitalization, will render the use of force regime "at the vanishing point of international law", to use Lauterpacht's phrase?[49] If this is what digitalization will bring about, it will be profoundly disruptive. In order to prevent this from happening and in order to preserve the governing authority of international law, we should diversify and expand the normative context within which digital technologies are assessed to include, in addition to law, ethical, social, and political considerations. Above all however, we should rediscover the spirit of the enlightenment as advocated by Henry Kissinger.[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 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

[48]Heike Krieger, Anne Peters, & Leonard Kreuzer, Due Diligence in the International Legal Order ch. 1 (2021).

[49]Hersch Lauterpacht, *The Problem of the Revision of the Law of War*, 29 British Y.B. Int'l L. 360–82 (1952) (using this phrase to describe the law of war).

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

https://doi.org/10.1017/glj.2023.33 Published online by Cambridge University Press

modest proposal is to encourage deliberation of the political, legal, ethical, social implications of digital technologies in the use of force regime and more generally 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.

**Competing Interests.** The author declares none.

**Funding Statement.** No specific funding has been declared in relation to this article.

**Cite this article:** Tsagourias N (2023). Digitalization and its Systemic Impact on the Use of Force Regime: Legal Uncertainty and the Replacement of International Law. *German Law Journal* **24**, 494–507. https://doi.org/10.1017/glj.2023.33