**2021 13th International Conference on Cyber Conflict**
Going Viral
T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.)
2021 © NATO CCDCOE Publications, Tallinn



# Cyber Personhood

**Neal Kushwaha**
Founder and Advisor
IMPENDO Inc.
Ottawa, Canada
neal@impendo.com

**Keir Giles**
Conflict Studies Research Centre
Northamptonshire, United Kingdom
keir.giles@conflictstudies.org.uk

**Tassilo Singer**
Consultant Manager
(Cyber Security & AI)
Atos Information Technology GmbH
Munich, Germany
tassilo.singer@atos.net

**Bruce W. Watson**
Chief Scientist and Advisor
IP Blox and IMPENDO Inc.
Eindhoven, Netherlands, and Ottawa, Canada
bruce@ip-blox.com and
bruce@impendo.com

**Abstract:** In early 2020, the rapid adoption of remote working and communications tools by governments, companies, and individuals around the world increased dependency on cyber infrastructure for the normal functioning of States, businesses, and societies. For some, the urgent need to communicate whilst safeguarding human life took priority over ensuring that these communications tools were secure and resilient. But as these tools become firmly embedded in everyday life worldwide, the question arises whether they should be considered as critical infrastructure, or perhaps even something more important.

In a number of States, the critical importance of the environment for preservation of human life has been recognised by extending legal personhood – and thus, legal rights – to environmental entities. Countries such as Colombia, Ecuador, New Zealand, and India have granted legal rights to various rivers, lakes, parks, and nature in general. This paper explores the future possibility and cases where States may consider granting legal rights to other non-sentient but critically important entities. Looking into a future where human life becomes increasingly dependent upon highly interdependent systems in cyberspace, is there a possibility that these systems are granted personhood?

Remote work and its cybersecurity implications could lead to an entirely new recognition of the importance of cyberspace dependencies and, consequently, a new

legal treatment. Against the backdrop of extended debate on the legal regulation of cyberspace, including the law of armed conflict, this would raise even more complex legal considerations, especially in the light of cross-border dependencies and systems that affect multiple jurisdictions.

By way of cyber biomimicry, this paper adopts a blue-sky conceptual approach to studying policy considerations and potential implications if highly interdependent cyber systems in the distant future are granted the same protections as elements of the environment.

**Keywords:** *cyber personhood, environmental personhood, cyber attack, highly interdependent cyber systems*

## 1. INTRODUCTION

Under Canadian and U.S. environmental law, rivers, parks, and other natural resources upon which life depends do not have standing in their respective jurisdictional courts. Instead, in order for there to be standing, harm to any of these natural features must have resulted in injury to human beings. But what if natural resources were widely recognised in courts and had legal rights, with injuries to these natural resources recognised as crimes with victims in and of themselves?

If so, could this be extrapolated to a distant future where highly interdependent resources in cyberspace upon which life depends are also recognised, on the basis that these too are dynamic systems that have standing so that courts can recognise their injuries? This concept may appear unlikely, but so did the idea of environmental personhood decades ago, and today it is reality. In a world where our dependence on cyber systems is ever increasing, the idea of States granting cyber personhood to highly interdependent cyber systems of the future could be a logical progression of a number of current trends.

This paper examines environmental personhood and how a small number of States have granted it to certain natural resources. Through examples, we then describe the term "cyber personhood," align it to the precedent set by environmental personhood, present candidates for cyber personhood, and identify where we believe cyber personhood could not apply and where it may.

Finally, we examine certain policy considerations and potential implications of cyber personhood and provide our thoughts on the wider adoption of this concept.

In order to digest the content presented in this paper, we urge the reader to (1) look far into the future to help visualise these highly interdependent cyber systems and (2) not consider current cyber systems as candidates for cyber personhood. To help standardise our discussion across the political, policy, legal, and technological domains, we present the following definitions.

- Cyberspace: "The environment formed by physical and non-physical components to store, modify, and exchange data using computer networks."[1]
- Cyber infrastructure: "The communications, storage, and computing devices upon which information systems are built and operate."[2]
- Critical infrastructure:
    i. "Physical or virtual systems and assets of a State that are so vital that their incapacitation or destruction may debilitate a State's security, economy, public health or safety, or the environment."[3]
    ii. "…infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[4]
- Cyber system: "One or more interconnected computers with associated software and peripheral devices. It can include sensors and/or (programmable logic) controllers, connected over a computer network. Computer systems can be general purpose (e.g. a laptop) or specialised (e.g. the 'blue force tracking system')."[5]
- Highly interdependent cyber systems of the future: Defined by examples in the following section.

## 2. HIGHLY INTERDEPENDENT CYBER SYSTEMS

We are already on the brink of a future in which we depend so much on key cyber systems that governments, societies, corporations, and individuals are, in some cases, unable to function without them. Current trends indicate that this dependence on always-on, always-reliable cyber systems will deepen. During the coronavirus pandemic, without the ability to operate remotely, many more companies would have failed and more individuals relying on their services would have suffered. In the spring of 2020, governments and companies scrambled to increase secure remote

1 Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, (Cambridge: Cambridge University Press, 2017), 564.
2 Ibid.
3 Ibid.
4 "Critical Infrastructure Sectors," Cybersecurity Infrastructure Security Agency (CISA), https://www.cisa.gov/critical-infrastructure-sectors [accessed 8 March 2021].
5 Schmitt, *Tallinn Manual 2.0*, 564.

access capacities and adopt remote voice and video communication methods. For some, these voice and video communications systems now rely on a complicated mix of on-premise systems, service providers, cloud hosting providers, and Internet access to residences. This delicate balance of a service offering relies on the availability of each service component within and is an example of our existing dependency on always-on and always-reliable cyber systems. So far, the roles and responsibilities remain clear.

Near-future examples demonstrating this include fully autonomous vehicles (without steering wheels) and systems that are critically dependent on synchronised time signals, not only for waking you up in the morning and scheduling your day but also for key tasks such as ensuring your digital identity and encryption for connecting to your common services in cyberspace. The roles and responsibilities in such a technological system begin to blur, as they all depend on *time*. As an example, given that satellite time signals can be manipulated or jammed,[6] common services that depend on time, such as locations on maps and certificate expirations that influence identities and cryptography, could cease to function as intended. These temporary effects, described in the example, demonstrate the potential for harm to the operations of systems dependent on a synchronised time signal.

Further into the future, societies may rely on cyber systems based on emergent phenomena in complexity theory systems,[7] or cyber physical systems[8] managed entirely by artificial intelligence (AI) systems, where the original human-written algorithms of the system are regularly rewritten by the learning process of the system itself. The closer cyber systems get to sentience, the more rational it becomes to treat them as legal entities in their own right, capable not only of suffering harm but also of taking decisions that cause harm independently of human input.

Now consider multiples of these future cyber systems being highly interdependent on each other, where they feed and receive data from each other and also consume each other's deeply nested computing capacities. These systems would be managed by companies or governments and potentially poorly designed by individuals, like many

6 Peter Danilov, "GPS Jamming Still Causing Problems in Finnmark," *High North News*, 19 November 2020, https://www.highnorthnews.com/en/gps-jamming-still-causing-problems-finnmark [accessed 8 March 2021].

7 Paul Cilliers, *Critical Complexity: Collected Essays*, ed. Rika Preiser (Berlin: Walter de Gruyter GmbH, 2016). We understand Paul Cilliers' view of a complex system to be a large number of elements (which can be simple), interacting dynamically and nonlinearly using feedback loops, where the system behaviour is determined by these interactions. Such systems are adaptive, reorganising their internal structure without intervention by outside agents.

8 Claire Vishik, Mihoko Matsubara, and Audrey Plonk, "Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms," in *International Cyber Norms: Legal, Policy and Industry Perspectives*, ed. Anna-Maria Osula and Henry Rõigas (Tallinn: NATO CCD COE Publications, 2016), 228–229. Cyber physical systems are smart systems that include co-engineered interacting networks of physical and computational components. Thanks to their highly interconnected nature, they are an excellent example of complex systems in which the behavioural sum is far more than its parts.

other systems today (e.g. a great many commercial software packages). The roles and responsibilities that were once complicated will become complex. If, in the future, these highly interdependent cyber systems were to become temporarily unavailable or significantly harmed, it could impact a State's (or various States') ability to deliver healthcare or to maintain international obligations, cause a shutdown of the economy, and possibly cause civil unrest. If, as you read this, you find yourself trying to align our description of these highly interdependent cyber systems with Critical National Infrastructure or trying to align to software and/or services you may use today, then we ask that you look much further into the future and set aside any alignment to services that currently exist.

In the following section, we explore the position States have taken with respect to environmental personhood and later align this behaviour and thought to our example-based definition of highly interdependent cyber systems of the future to discuss cyber personhood.

## 3. ENVIRONMENTAL PERSONHOOD

It is simple to understand a corporation having its own rights as a legal entity, and thereby corporate personhood. These corporate entities can enter into contracts, own properties, and be recognised as legal persons in courts. But in addition to corporations, natural resources in certain States have been granted personhood rights.

The germination of environmental personhood is credited to the 1972 paper "Should Trees Have Standing? Toward Legal Rights for Natural Objects" by Christopher D. Stone.[9] The paper proposed giving legal rights to rivers, oceans, forests, or any natural environmental systems.[10] He referred back to a time when discussing rights for corporations, women, and others had seemed unthinkable.[11] He went on to describe how corporations do not have rights similar to those of a legal person and how certain persons such as inmates or children have limited rights.[12] He argued that "holders of legal rights" must satisfy all of the following three criteria:[13]

1. "[They may] institute legal actions at [their] behest;"
2. "In determining the granting of legal relief, the court must take injury to [them] into account; and"
3. "Relief must run to [their] benefit."

9 Christopher D. Stone, "Should Trees Have Standing? Toward Legal Rights for Natural Objects," *Southern California Law Review* 45 (1972): 450–501.
10 Ibid., 456.
11 Ibid., 451.
12 Ibid., 455.
13 Ibid., 458.

Stone suggested that these natural environmental systems be assigned legal guardians who could advocate for the rights of these systems.[14] In his blue-sky paper, he suggested not only rights but also liabilities, using the example of a trust fund which compensates those who suffered damages from floods.[15]

Since Stone's paper, some nations have shifted slightly from anthropocentric views toward biocentric ones, adopting environmental personhood in a number of different ways. Several papers have been published regarding the interpretation and challenges of State laws regarding environmental personhood. Examples include:

- **Bangladesh:** In 2019, Bangladesh granted legal personhood rights to all of its rivers, with legal guardianship assigned to the National River Conservation Commission.[16]

- **Bolivia:** In 2010, Bolivia passed a "Law on the Rights of Mother Earth" (Ley de Derechos de la Madre Tierra), thereby granting her, a living system, legal personhood rights.[17]

- **Colombia:** In 2016, Colombia's Constitutional Court granted legal personhood rights to the Atrato River (Rio Atrato) basin under joint guardianship of the government and the indigenous community living in the basin.[18] In 2018, Colombia's Supreme Court recognised the rights to the Amazon River and its surrounding ecosystem, reaching a unique decision involving multiple stakeholders to safeguard the life and health of Colombia's Amazon (Amazonas Colombiano).[19]

- **Ecuador:** Leading the charge in 2008, Ecuador's constitution recognises legal personhood for "Mother Nature" (Panchamama) with rights "to exist, persist, maintain and regenerate its vital cycles, structure, functions and its processes in evolution." Any person or persons can petition on her behalf.[20]

14 Ibid., 464.
15 Ibid., 481.
16 Supreme Court of Bangladesh, Human Rights and Peace for Bangladesh v. Bangladesh and Others (HRPB v. Bangladesh), Writ Petition 13989/2016 of 7 November 2016.
17 "Bolivia Law of the Rights of Mother Earth," Law 071 (2010).
18 Justice Studies et al. v. Presidency of the Republic et al., Constitutional Court of Colombia, Judgment T-622/16, https://www.corteconstitucional.gov.co/relatoria/2016/t-622-16.htm [accessed 8 March 2021].
19 Supreme Court of Colombia, Judgement STC 4360-2018 of 5 April 2018, https://cortesuprema.gov.co/corte/wp-content/uploads/2018/04/STC4360-2018-2018-00319-011.pdf [accessed 8 March 2021].
20 Constitución Politica de la República del Ecuador, Constitución 2018, Art. 71–74.

- **India:** In 2017, India's Uttarakhand High Court granted legal personhood rights to two rivers, the Ganges and the Yamuna, their respective Gangotri and Yamunotri glaciers, and other natural objects[21] in the State of Uttarakhand under the guardianship of Uttarakhand, the State in which the rivers originate. Later that same year, India's Supreme Court issued a stay of the Uttarakhand High Court's 2017 decision.[22] In March 2020, the Punjab and Haryana High Court granted Sukhna Lake personhood rights.[23]

- **New Zealand:** New Zealand granted legal personhood rights to the Te Urewera National Park in 2014,[24] the Whanganui River in 2017,[25] and Mount Taranaki in 2017,[26] with legal guardianship assigned to the Crown, the Whanganui people, and eight Māori tribes, respectively.

We recognise that with the exception of India, these States may not be globally perceived as legal opinion defining States. With the further exception of Ecuador and Bolivia, we also recognise that not all aspects of the State's environment are granted legal personhood and that only specific rivers, forests, and parks have been granted legal personhood. It is most likely for these reasons that environmental personhood is not a rule in public international law or included in customary international law.

Rather than explore the legal constructs developed to create a concept of environmental personhood, this paper builds on the established notion to consider a distant future where some States grant personhood rights to highly interdependent cyber systems. It is with this frame of reference that we propose cyber personhood.

21 High Court of Uttarakhand, Mohammad Salim vs. State of Uttarakhand & others, Writ Petition (PIL) No. 126 of 2014, 20 March 2017: "§19. Accordingly, while exercising the parens patriæ jurisdiction, the Rivers Ganga and Yamuna, all their tributaries, streams, every natural water flowing with flow continuously or intermittently of these rivers, are declared as juristic / legal persons / living entities having the status of a legal person with all corresponding rights, duties and liabilities of a living person in order to preserve and conserve river Ganga and Yamuna."
High Court of Uttarakhand, Lalit Miglani vs. State of Uttarakhand & others, Writ Petition (PIL) No. 140 of 2015, 30 March 2017: "We, by invoking our parens patriæ jurisdiction, declare the Glaciers including Gangotri & Yamunotri, rivers, streams, rivulets, lakes, air, meadows, dales, jungles, forests wetlands, grasslands, springs and waterfalls, legal entity / legal person / juristic person / juridicial person / moral person / artificial person having the status of a legal person, with all corresponding rights, duties and liabilities of a living person, in order to preserve and conserve them. They are also accorded the rights akin to fundamental rights / legal rights."

22 Supreme Court of India, State of Uttarakhand and Others v. Mohammed Salim and Others, Special Leave to Appeal (C) No. 016879/2017, Order dated 7 July 2017.

23 Punjab and Haryana High Court, Court on its own motion v. Chandigarh Administration, CWP No. 18253 of 2009 and other connected petitions of 2 March 2020.

24 Parliament of New Zealand, "Te Urewera Act 2014," Royal Assent 27 July 2014.

25 Parliament of New Zealand, "Te Awa Tupua (Whanganui River Claims Settlement) Act 2017," Royal Assent 20 March 2017.

26 "Taranaki Maunga," signed 20 December 2017, https://www.govt.nz/browse/history-culture-and-heritage/treaty-settlements/find-a-treaty-settlement/taranaki-maunga [accessed 8 March 2021].

## 4. CYBER PERSONHOOD

Our paper suggests that in the distant future, States may grant or consider granting certain highly interdependent cyber systems legal personhood rights, in a manner similar to how States have granted certain natural environment systems environmental personhood. In common with environmental personhood, the rights and liabilities of these cyber systems would, and most likely should, vary from system to system.

We propose the following definition of cyber personhood: the granting of legal-person rights to a highly interdependent cyber system under legal frameworks whereby the highly interdependent cyber system would have legal standing to claim injuries and remain accountable for any injuries it may cause.

The notion of granting legal personhood to a computer-based system may seem radical and exotic at present, but far less so than the idea of environmental personhood did in 1972. While environmental concerns have slowly achieved broad acceptance despite being stigmatised by industry-minded or politically motivated interests, dependency on cyber systems is developing much more rapidly. Where it took over 35 years for environmental personhood to take hold in Ecuador, it is possible that cyber personhood will mirror the velocity of acceptance of cyber systems, greatly reducing the time required to arrive at appropriate legal changes to recognise the new reality, or dismiss it.

### *A. Candidates for Cyber Personhood*

Just as with corporate legal entities or inmates, the highly interdependent systems of the future would probably fall into a category of their own, requiring different treatment, including in terms of their rights and obligations, as well as forms of ownership and oversight. To help understand the types of systems that may be considered for cyber personhood, we have categorised them as follows. For each scenario, our focus remains on the highly interdependent cyber systems of the future, States' and their societies' inability to function without them, and existing legal constructs that may apply, which essentially negates the concept of cyber personhood for the first two candidates described below.

1. **Individually owned cyber systems (personal):** Many people have small networks in their homes providing connections between devices within their home, such as their computers, mobile devices, and televisions, and fringe devices such as refrigerators, toasters, coffee makers, door locks, and other Internet of Things objects. This candidate is not a highly interdependent cyber system but can be impacted if it is reliant upon upstream highly interdependent cyber systems that are no longer available. Nevertheless, if

this example's services were to be unavailable, it would not gravely impact State ability to function, and any damages can be claimed by the owner. *We believe such personal systems are not candidates for cyber personhood*.

2. **Corporate- or State-owned cyber systems (single entity):** These systems are required by corporate or State entities to operate their daily business, and if they were made unusable, the impact would be localised to their operations. *These systems would likely not be granted cyber personhood*, as any damages to them can be claimed by the owner, and any damages from the system can be paid by the owner.

3. **Multi-entity-owned cyber systems in a single jurisdiction:** In this instance, several national companies combined with or without the State's owned systems leverage their respective cyber services to jointly offer services from highly interdependent cyber systems to residents of a single jurisdiction. An example of this would be a nation that is able to provide cyber services to its residents thanks to its extensive sovereign cyber capabilities at State and/or corporate levels. These interdependent cyber systems could maintain separate accountabilities, leaving each entity responsible for their portion of the system. It may also simply fall under the responsibility of the State, especially when trying to limit control from larger and more powerful corporations such as Alphabet, Facebook, Amazon, and Microsoft. Alternatively, States may implement a private-public partnered governing body to govern the system as a single unit, especially when the boundaries of the individual units within the system become difficult to ascertain. For example, what would happen if one entity or service provider within the overall highly interdependent cyber system decides to stop providing its service, thereby adversely impacting all entities and the overall service to the residents of the State? *We believe it is possible for States to grant such a system cyber personhood*.

4. **Multi-entity-owned cyber system across multiple jurisdictions:** Building upon the previous candidate, consider several multinational companies and/or several States that jointly offer a service through a highly interdependent set of cyber services to the residents of several jurisdictions, including jurisdictions beyond their own with complex and deeply nested roles and responsibilities. Depending on the public's reliance on the services of the system and the level of impact to the public when the services offered through the system are lost, *we believe such systems may be considered by some States to be deserving of cyber personhood*.

## 5. USE AND POLICY CONSIDERATIONS

In addition to candidates of cyber personhood that would require new legal treatment as described above, specific instances of actions affecting (or indeed carried out by) highly interdependent cyber systems would require careful consideration when establishing a conceptual framework for cyber personhood. Had we had the foresight to strategise or "pre-think" our handling of the coronavirus pandemic, globally we would have been in a better position than where we arrived a year later. This paper suggests that States pre-think the idea of cyber personhood to help them decide how they would respond if certain States adopt such a position.

The following is a non-exhaustive list of considerations influencing rights and obligations of legal persons that would have a distinctive impact when applied to highly interdependent cyber systems of the future that States and their societies would be unable to function without.

- **Injuries:** the nature of highly interdependent cyber systems of the future, existing in the physical world yet managing data in the virtual one, means that the potential for damage caused by cyber systems also extends across multiple domains. In the data sphere, highly interdependent cyber systems could be liable and receive relief for breach of confidentiality, damage to integrity, or breach of access, or damage or destruction of systems or data. In the physical world, harm could be caused to any system – including life support systems – which is dependent on the network for its correct functioning. Interdependencies introduce further complexity when, for instance, one entity's components of the highly interdependent cyber system cause harm to another entity's components of the same system, where one or both has been designated as a legal person.

- **Cyber attack (outside of armed conflict):** In the future, when a highly interdependent cyber system becomes the victim of a cyber attack, its rights and duties depend on the existence of an organisational body and the prevailing degree of organisation, as well as on its "legal" recognition by States on a national and international level.

    - If the highly interdependent cyber system has been granted cyber personhood by a State in which its rights can be invoked, then those rights (and duties – like a duty to notify/report authorities on serious breaches) can be exercised in front of a national jurisdiction. Furthermore, the executive branch could be asked for assistance in the form of, for example, preventive protection or services such as

attribution sourcing and security monitoring. As a result of such a legal remedy, the most basic expectation would be a return to the pre-attack status of the highly interdependent cyber system.

- On the international level, a cyber attack could result in a demand by interested parties[27] to protect the system, restore it to its pre-attack status, or to retaliate with sanctions. Additionally, if the rules of the customary law on State responsibility for States can be transferred to a highly interdependent cyber system, "third States" with common interests would be permitted to invoke them and could offer assistance.[28] Due to the necessity and/or criticality of the highly interdependent cyber system we have proposed, it is suggested that States also consider transferring these rules to such a non-State entity in order to support international laws of State responsibility.

- **Cyber attack (armed conflict):**[29] The protection under the law of armed conflict depends on how the highly interdependent cyber system is qualified. If it is equivalent to critical infrastructure, it enjoys a high standard of protection.[30] If the cyber system is used exclusively for civilian purposes, it is qualified as a civilian object and thus also protected.[31] Unfortunately, if a highly interdependent cyber system is abused by one party to an armed conflict, it could lose its status. When it becomes a civilian object used for military purposes, it can be qualified as a military objective.[32] Since an attack on a military objective results in a military advantage, a cyber attack on such a highly interdependent cyber system would be lawful. Legal reasons justifying protection could be an agreement of States on the neutrality of highly interdependent cyber systems or to qualify them as a "digital" non-defended locality.[33] Even more interestingly, due to the similar understanding

27 Examples of interested parties include, but are not limited to, (1) the recognising States, (2) the users, (3) international organisations, (4) the systems' organisational body, and the like.

28 UN ILC, "Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries" (2001), GAOR 56th Session Supp 10, 43; Art. 48: "1. Any State other than an injured State is entitled to invoke the responsibility of another State in accordance with paragraph 2 if: (a) the obligation breached is owed to a group of States including that State, and is established for the protection of a collective interest of the group; or (b) the obligation breached is owed to the international community as a whole." The cyber system could reflect the "collective interest" and/or the protection of the cyber system is "owed to the international community…" due to its criticality.

29 Schmitt, *Tallinn Manual 2.0*, 415. Rule 92 of *Tallinn Manual 2.0* defines a cyber attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects" (415).

30 Protections similar to those under Art. 54 and 56 Additional Protocol I to the Geneva Conventions, 1977.

31 "Civilian objects shall not be the object of attack or of reprisals. Civilian objects are all objects which are not military objectives": Art. 52 (1) Additional Protocol I to the Geneva Conventions, 1977.

32 As per Art. 52 (2) and within the limits of Art. 52 (3) Additional Protocol I to the Geneva Conventions, 1977; Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (Cambridge: Cambridge University Press, 2016): 104, 111–114.

33 As per Art. 59 Additional Protocol I to the Geneva Conventions, 1977.

of the wording, they could be qualified as a demilitarised zone by agreement of the State parties to the conflict.[34]

- **Obligations:** The delineation of responsibility between the creator or designer of a system and the system itself will need to be strictly determined. The system will need to demonstrate that it has a certain degree of autonomy in order for responsibility for its actions to not wholly be that of its designers, programmers, or (in the case of AI) trainers. Under a governing body, those maintaining the system will also have an ongoing degree of responsibility for any changes introduced in its functioning.

- **Liabilities:** Where injuries have been caused by a system, the question arises of how these are to be recompensed, and whence funding is to be derived in order to compensate the victim. Equivalent to legal persons and corporations, highly interdependent cyber systems of the future will have the option to purchase liability insurance (or remain self-insured) and use trust funds to support injury costs against them. Users of the highly interdependent cyber systems could be charged a fee for services and/or the highly interdependent cyber systems could receive their funding from State-collected taxes, which would fund the maintenance and operations of the services along with costs for insurance policies and trust funds.

- **Representation and/or guardianship:** Until such time as systems can argue their own cases in courts of law, they must necessarily be represented by advocates in the same way as human or corporate plaintiffs or defendants. However, it also follows logically from personhood that sentient systems may also seek representation in corporate and political as well as legal systems in the same manner as any disenfranchised group of humans has sought to organise order to ensure their own rights – whether through a guild, or trades union, or by seeking political influence at a local or State level.

  When selecting and assigning guardianship, States will likely consider the challenges of industry-driven or politically motivated interests. The system may be assigned multiple parties to act as a committee with guardianship responsibilities of the system, possibly consisting of preservation or advocacy groups, involved corporations, and a political seat (e.g. minister of the highly interdependent cyber system), similar to what has been assigned for natural environment entities. Certain international organisations could serve as a possible model.

34 As per Art. 60 Additional Protocol I to the Geneva Conventions, 1977.

- International organisations as a comparable concept: A related practice-oriented solution for multi-jurisdictional systems can be an international governing body and/or international organisation (IO) deriving from and in accordance with international law. The required pressure and/or need to organise certain IT issues on an international level is comparable and similar to the ICANN (Internet Corporation for Assigned Names and Numbers, whose duty is to maintain important databases related to namespaces and numerical spaces of the Internet) or the ISO (International Organisation for Standardization, an association under Swiss law), which, however, are not governed precisely like an IO in the international law sense. It is therefore suggested that the practical idea of ICANN et al. be merged with the concept of an IO in international law. This might be explicitly suitable for a sophisticated AI complex.

  To establish an international organisation, an agreement by at least two States in the form of an international treaty is required. In this treaty, the subject matter will be defined as well as its and the participating States' rights, duties, and funding.[35] From a practical perspective, it would be necessary to define the area of applicability precisely and thereby to determine and differentiate the highly interdependent cyber systems which are governed, guarded, and represented by the IO.

  The creation of an international entity for a particular highly interdependent cyber system would entail the need for its own governance mechanisms. Furthermore, the integration of such a legal personhood in practice (i.e. procedural and representative questions) could be challenging; it could be addressed in a similar manner to existing specific IOs. On the other hand, the IO solution offers a clear and transparent framework based on States' consensus to govern a grey area and to answer legal and practical needs. Finally, particular advantages gained by creating this international entity could be:

  - The monitoring and observance of (digital) human rights (e.g. with a view to surveillance or big data AI);
  - A fair and equal share of high-level technology (e.g. for developing States);
  - To keep critical communication and information infra-structure worldwide functioning (as a backbone);

35 Reparation for injuries suffered in the service of the United Nations (Advisory Opinion), (1949) ICJ Rep 174.

- Shared responsibility and shared burdens with a view to sustainability (to prevent environmental damage, or to foster decarbonisation); and/or
- A common control and reciprocal acceptance of a pivotal technology (sophisticated, eventually somewhat dangerous AI).

## 6. CONCLUSION

The information revolution has already brought about profound changes in the lives of most humans and in what is considered normal and natural human behaviour. The pace of this change continues to increase, and to a greater extent than in previous periods of human history, legal practice is considered only after the systems are already in place. The extent to which the development of cyber systems and capabilities has outpaced legal norms is demonstrated not only by the constant need to update domestic computer and information legislation[36] to reflect new uses and capabilities for information and communications technologies but also by the ongoing discussions of the nature of cyber activities and what constitutes a "cyber attack" between States.[37]

Our paper is written to help States pre-think the concept of cyber personhood. The example of environmental personhood cited above provides a template for consideration of whether cyber personhood is a viable means for ensuring that the legal treatment of highly interdependent cyber systems of the future remains both relevant and fit for purpose, and sufficiently flexible to accommodate as-yet-unforeseen developments in the relationships between humans and computing devices. Christopher Stone's 1972 paper first proposing environmental personhood came at a very early stage in the development of mass awareness of the vulnerability of the environment, and of its need for protection, based, not least of all, on its critical importance for sustaining human life. The process of achieving widespread acceptance of the notion that corporate profit and individual convenience needs to be balanced against environmental protection was a long one, and in some areas is still not complete. However, we believe that events such as the coronavirus pandemic will accelerate the analogous process for cyber systems by emphasising the essential and irreplaceable nature of highly interdependent cyber services for the functioning of future societies.

36 Alex Scroxton, "Security Pros Fear Prosecution under Outdated UK Laws," *Computer Weekly*, 20 November 2020, https://www.computerweekly.com/news/252492416/Security-pros-fear-prosecution-under-outdated-UK-laws [accessed 8 March 2021].

37 Sydney J. Freedberg Jr. and Theresa Hitchens, "Calling SolarWinds Hack 'Act of War' Just Makes It Worse," *Breaking Defense*, 21 December 2020, https://breakingdefense.com/2020/12/calling-solarwinds-hack-act-of-war-just-makes-it-worse [accessed 8 March 2021].

The legal regime governing actions against, through, or by computer networks will inevitably develop and change, evolving significantly from its current state. It may be that cyber personhood is not the concept through which legal mechanisms accommodate the new reality of critical human dependence on online services. But the example of environmental legislation argues strongly that this path could be considered a key means of resolving substantial challenges to applying existing legal regimes to cyber rights and responsibilities by way of cyber biomimicry.

Studying and remaining aware of potential future scenarios enables us to better position ourselves to withstand them. For many reasons, environmental personhood is not widely accepted or recognised; however, it may be that cyber personhood is embraced as highly interdependent cyber systems become indispensable to governments, societies, corporations, and individuals.

The concept of cyber personhood is not so far removed from possibility and deserves discussion, particularly as the tools to govern it are already available. The questions that remain are: which cyber systems will develop the criticality and complexity deemed to be worthy of being governed under international law, and which countries are bold enough to make this concept a reality?