



Deposited via The University of Sheffield.

White Rose Research Online URL for this paper:

<https://eprints.whiterose.ac.uk/id/eprint/105177/>

Version: Accepted Version

---

**Article:**

Tsagourias, N. (2016) Non-state actors, ungoverned spaces and international responsibility for cyber acts. *Journal of Conflict and Security Law*, 21 (3). pp. 455-474. ISSN: 1467-7954

<https://doi.org/10.1093/jcsl/krw020>

---

**Reuse**

Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

**Takedown**

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing [eprints@whiterose.ac.uk](mailto:eprints@whiterose.ac.uk) including the URL of the record and the reason for the withdrawal request.

## Non-state actors, ungoverned spaces and international responsibility for cyber acts

Nicholas Tsagourias\*

### Abstract

*This article examines the question of whether states can be held responsible for the malicious cyber activities of non-state actors operating from ungoverned spaces. After examining relevant rules of the law of state responsibility, it concludes that there is a responsibility deficit. For this reason, it puts forward a proposal for holding non-state actors that exercise effective power over territories and people directly responsible for their malicious cyber activities. In this respect, it considers the scope of their obligations, issues of attribution as well as issues concerning the implementation of their responsibility. It however acknowledges that many non-state actors including 'virtual' groups still remain outside legal regulation.*

**Words:** *responsibility, non-state actors, ungoverned spaces, virtual groups, legal personality, attribution, implementation of responsibility*

### I. Introduction

The international law literature on ungoverned spaces<sup>1</sup>, such as those in Somalia, Congo, Afghanistan, Iraq, Libya, and Syria<sup>2</sup>, is replete with warnings about the security threats that such places pose to states, people or the international society at large.<sup>3</sup> Such places are viewed as breeding grounds for non-state actors to pursue nefarious activities such as terrorist attacks, crime, or fraud with cyberspace becoming a locus or medium through which such activities are incited, facilitated, or committed.<sup>4</sup> For

---

\* Professor of International Law, University of Sheffield ([Nicholas.Tsagourias@sheffield.ac.uk](mailto:Nicholas.Tsagourias@sheffield.ac.uk)). I would like to thank Professor Michael Schmitt for his comments on a previous draft. The usual disclaimer applies.

<sup>1</sup> Anne L. Clunan and Harold A. , Trinkunas (eds), *Ungoverned Spaces. Alternatives to State Authority in an Era of Softened Sovereignty*, (Stanford University Press, 2010). Ungoverned spaces can include whole states or areas in states

<sup>2</sup> According to the World Bank's Worldwide Governance Indicators Project, in 2014, Iraq, Syria, Yemen, and Libya are placed between 11 and 5 points on a 100 (highest) points scale. <http://info.worldbank.org/governance/wgi/index.aspx#home> (accessed 31 January 2016)

<sup>3</sup> Robert D. Lamb, *Ungoverned Areas and Threats from Safe Havens: Final Report of the Ungoverned Areas Project* (Washington: Office of the Deputy Assistant Secretary of Defense for Policy Planning, 2008) [http://cissmdev.devcloud.acquia-sites.com/sites/default/files/papers/ugash\\_report\\_final.pdf](http://cissmdev.devcloud.acquia-sites.com/sites/default/files/papers/ugash_report_final.pdf) ;  
*Quadrennial Defense Review 2014* at [http://archive.defense.gov/pubs/2014\\_Quadrennial\\_Defense\\_Review.pdf](http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf) (accessed 31 December 2015)

<sup>4</sup> Cybersecurity: Jihadism and the internet, May 2015 at [http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/557006/EPRS\\_ATA%282015%29557006\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/557006/EPRS_ATA%282015%29557006_EN.pdf) (accessed 31 December 2015)

example, ISIS, a non-state actor, operates from territories that it seized in Syria and Iraq and engages in criminal activities in the physical world as well as through and in cyberspace. ISIS has been quite deft in using the internet for its own purposes and it has tried to build its own 'cyber army'. For this reason, a number of groups were created with the most prominent being the Cyber Caliphate (Caliphate Cyber Army CCA) created by the British born Junaid Hussain famed for hacking Tony Blair and killed in a drone attack; the Islamic State Hacking Division (ISHD) created by a Kosovar hacker killed by a drone; the Islamic Cyber Army (ICA); the Rabitat Al-Ansar (League of Supporters); or the Sons Caliphate Army (SCA) among others. According to recent reports, ISIS merged cyber groups into one group the United Cyber Caliphate (UCC).<sup>5</sup>

These groups are responsible for numerous cyber attacks on media, Universities, governmental departments, local authorities, military bodies, non-profit organisations, or businesses.<sup>6</sup> For example, they seized control of TV5Monde, France's international TV network, an attack that the French government dubbed an "act of terrorism",<sup>7</sup> broadcasted propaganda videos and the personal information and resumes of French soldiers fighting extremist groups; hacked Newsweek's social media accounts to issue a direct threat to the US president's wife and children; or took control of the US Central Command YouTube account to post terrorist propaganda videos.<sup>8</sup> Although none of these attacks caused any serious damage, with ISIS currently using the internet mainly for propaganda, funding and recruiting purposes, it does not mean that ISIS or other non-state actors cannot in time acquire the resources to launch damaging attacks on people or states. As George Osborne the British Chancellor said in a speech to GCHQ 'when we talk about tackling ISIS, that means tackling their cyber threat as well as the threat of their guns, bombs and knives.'<sup>9</sup> Indeed, the US has recently announced that it is

---

<sup>5</sup> See Flashpoint's report, *Hacking for ISIS: The Emergent Cyber Threat Landscape* at <https://www.flashpoint-intel.com/news/flashpoint-issues-new-report-demonstrating-advancement-of-isis-organized-cyber-capabilities/> (accessed 31 April 2016)

<sup>6</sup> For a list of such activities see Steven Stalinsky and R. Sosnow, Hacking In The Name Of The Islamic State (ISIS), Inquiry & Analysis Series No. 1183, August 21, 2015 at [http://www.memrijttm.org/hacking-in-the-name-of-the-islamic-state-isis.html#\\_ednref4](http://www.memrijttm.org/hacking-in-the-name-of-the-islamic-state-isis.html#_ednref4) (accessed 31 December 2015)

<sup>7</sup> ISIL hackers seize control of France's TV5Monde network in 'unprecedented' attack, The Telegraph (3 April 2015), <http://www.telegraph.co.uk/news/worldnews/europe/france/11525016/Isil-hackers-seize-control-of-Frances-TV5Monde-network-in-unprecedented-attack.html> (accessed 31 December 2015)

Aurelien Breeden and Alissa J, Rubin, French Broadcaster TV5 Monde Recovers After Hacking NYTimes (April 5, 2015) <http://www.nytimes.com/2015/04/10/world/europe/french-broadcaster-tv5-monde-recovers-after-hacking.html> (accessed 31 December 2015)

<sup>8</sup> *Supra* n 6

<sup>9</sup> Chancellor's speech to GCHQ on cyber security 15 November 2015. <https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security>

launching cyber attacks against ISIS. As President Obama said ‘Our cyberoperations are disrupting their command-and-control and communications’<sup>10</sup>

Ungoverned spaces are not just a security threat; they are also a systemic threat to the international legal order because they challenge certain basic principles of that order. In the first place, they challenge the concept of statehood which is a central tenet of the international legal order and following from this, they pose a challenge to the legal institutions attached to statehood and which make the international legal order operational, as for example the institution of state responsibility. The reason why ungoverned spaces pose a systemic threat to the international legal order is because they are characterised by lack or diminution of effective state power which is a necessary condition for maintaining internal as well as external order and for realising international law.

In this article I will examine the implications for the law of state responsibility of ungoverned spaces when non-state actors operating from them engage in malicious cyber activities. For this reason, I will first explain the concept of ‘ungoverned space’ and the challenges that ungoverned spaces pose to the institution of state responsibility. Reaching the uncomfortable conclusion that in such cases there is ‘responsibility deficit’, the article goes on to explore the possibilities and conditions under which responsibility can be ascribed directly to non-state actors exercising power over such spaces.

## II. The concept of ‘ungoverned space’

Since the article is concerned with ungoverned spaces, it is important to offer a definition of this concept. An ungoverned space is defined according to a RAND report as “[a]n area in which a state faces significant challenges in establishing control. Ungoverned territories can be failed or failing states, poorly controlled land or maritime borders, or areas within otherwise viable states where the central government’s authority does not extend.”<sup>11</sup> Similarly, according to a 2008 Department of Defense Report, an ungoverned space “encompasses under-governed, misgoverned, contested, and exploitable areas as well as ungoverned areas.”<sup>12</sup> In international law and relations literature there are many different terms to describe states or territories that fail to demonstrate the customary attributes of statehood in the fields of peace, security, order,

<sup>10</sup> U.S. Cyberattacks Target ISIS in a New Line of Combat, N.Y. Times, April 24, 2016 <http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html? r=0> (accessed 31 April 2016)

<sup>11</sup> A. Rabassa et al. (2007) “Ungoverned Territories: Understanding and Reducing Terrorism Risks.” *Project Air Force*. RAND Corporation, XV at [http://www.rand.org/content/dam/rand/pubs/monographs/2007/RAND\\_MG561.pdf](http://www.rand.org/content/dam/rand/pubs/monographs/2007/RAND_MG561.pdf) (accessed 31 December 2015)

<sup>12</sup> Lamb, ‘Ungoverned Areas and Threats from Safe Havens’, 3

and governance. A term that is employed quite often is that of a 'failed state'. According to Gerald Helman and Steven Ratner who coined the term 'failed state', a failed state describes a state that is 'utterly incapable of sustaining itself as a member of the international community'.<sup>13</sup> Similarly, according to Thürer, '[a] State is usually considered to have failed when the power structures providing political support for law and order have collapsed, or are non-existent to the extent that the State ceases to be an effective member of the international community.'<sup>14</sup><sup>15</sup> Ungoverned spaces and failed states share many similarities because they both refer to the erosion of state capacity but I use the term 'ungoverned space' because it is more inclusive by indicating a spectrum of ungovernability in geographic or governance terms. The concept of 'ungoverned spaces' thus includes 'failed' states or otherwise ungoverned states which describe a situation where there is total and overall loss of state capacity in geographic and governance terms but also situations where state capacity gradually or suddenly recedes from parts of an otherwise functioning state.

The preceding discussion demonstrates, first, that the concept of 'ungoverned space' is constructed against a state-centric reading of international law and relations by describing the absence or the cession of state authority and, secondly, that an 'ungoverned space' does not necessarily imply a power vacuum because there may be different forms and levels of authority exercised by non-state actors. In other words, ungoverned spaces do not preclude alternative structures and forms of authority instituted by non-state actors.<sup>16</sup>

That having been said, ungoverned spaces even if they are governed by non-state actors pose serious challenges to international law because the whole edifice of international law is premised on statehood and indeed on its effectiveness. When the institution of the state becomes ineffective or disappears, international law loses the propulsion which would allow it to function as a normative system and this is also the case when international law fails to recognise alternative forms of effective power.

### III. International law and state effectiveness

As was said in the preceding section, international law is premised on effectiveness. Effectiveness is about a set of affairs, relations or situations that exist in fact.<sup>17</sup> International law often normativises such set of affairs. For example, it recognises the demonstrations and relations of power over territory and people as a state and gives it

---

<sup>13</sup> Herald B. Helman and Steven R. Ratner's, 'Saving Failed States', 89 *Foreign Policy* 3 (Winter 1992-93), 5-6.

<sup>14</sup> D. Thürer 'Failing State' *MPEPIL*, para 4

<sup>15</sup> Netherlands Advisory Council on International Affairs Netherlands Advisory Council on Issues of Public International Law AIV/CAVV *Failing States: a Global Responsibility*, Report No. 35, May 2004, 11

<sup>16</sup> J. Keister, 'The Illusion of Chaos: Why Ungoverned Spaces Aren't Ungoverned, and Why That Matters' Cato Institute, December 9, 2014 at [http://object.cato.org/sites/cato.org/files/pubs/pdf/pa766\\_1.pdf](http://object.cato.org/sites/cato.org/files/pubs/pdf/pa766_1.pdf) (accessed 31 January 2016)

<sup>17</sup> C. De Visscher, *Les effectivités du droit international public* (Paris, Pédone, 1967)

legal status. A state is thus the recognition by international law of an effective set of relations. This is ingrained in the traditional definition of statehood according to which one of the criteria of statehood is effective government in the sense of an authority that can exercise effective power over territory and people.<sup>18</sup> As Crawford commented '[t]he proposition that statehood is a question of fact derives strong support from this equation of effectiveness and statehood. In other words, although it is admitted that effectiveness in this context is a legal requirement, it is denied that there can exist legal criteria for statehood not based on effectiveness'.<sup>19</sup> Effectiveness was also an issue in the *Aaland* Arbitration. Regarding Finland's status as a state, it was opined that '[f]or a considerable time, the conditions required for the formation of a sovereign State did not exist. In the midst of revolution and anarchy, certain elements essential to the existence of a State, even some elements of fact, were lacking for a fairly considerable period. Political and social life was disorganized; the authorities were not strong enough to assert themselves . . . the Government has been chased from the capital and forcibly prevented from carrying out its duties . . . . It is therefore difficult to say at what exact date the Finnish Republic, in the legal sense of the term, actually became a definitely constituted sovereign State. This certainly did not take place until a stable political organization had been created, and until the public authorities had become strong enough to assert themselves throughout the territories of the State without the assistance of foreign troops.'<sup>20</sup>

The state, being recognised as an effectivity (*effectivité*) and indeed as the original effectivity in international law, is also the condition for the realisation of international law. International law is a normative system; it contains postulates. International law does not possess any superimposing authority, neither does it have an ingrained factual mechanism to make it real that is, to implement it, ensure respect of its rules or enforce these rules. In international law the power that makes international law real and effective is the state and indeed an effective state. Legal effectiveness is thus dependent on state effectiveness. From that it transpires that there is a mutually reinforcing relation between effectiveness, statehood and international law in that international law recognises effectiveness in the form of statehood and (effective) statehood is a condition for the effectiveness of international law. This was alluded to in the *Isle of Palmas* case by Judge Huber who said '[i]nternational law, the structure of which is not based on any super-state organisation, cannot be presumed to reduce a right such as territorial sovereignty, with which almost all international relations are bound up, to the category of an abstract right, without concrete manifestations'.<sup>21</sup>

That having been said, it is true that in the post-colonial era a juridical notion of statehood has been promoted according to which lack of effectiveness does not prevent an entity in acceding to statehood or in retaining its status as state. Although there have been many other considerations –moral as well as political - behind such a theory, there has also been a strong presumption or expectation that the state will (re)gain effectiveness and international law proceeded on that basis to treat such entities as equal members of the international society of states.

---

<sup>18</sup> Art 1, Montevideo Convention on the Rights and Duties of States 1933

<sup>19</sup> J. Crawford, *The Creation of States in International Law*, (CUP, 2007) 106 and ch 1

<sup>20</sup> LNOJ spec supp no 4 (1920) 8–9

<sup>21</sup> *Island of Palmas* (the United States v. the Netherlands), 2 RIAA (1928) 840

It is in how international law treats effectiveness that the threat posed by ungoverned spaces to the international legal order can be revealed. When the state loses effectiveness and becomes ungoverned, it may retain its juridical character as a state with all the privileges, rights and duties attached thereto but, in effect, it is not able to fulfil the legal expectations attached to statehood, whereas when its effectiveness recedes from certain areas, it cannot fully fulfil these expectations. Moreover, other actors may exercise power over those areas but, if these actors are not recognised by international law as carriers of rights and duties, international law again loses its effectiveness. As Somalia and other similar cases show, when notions of statehood are promoted which decouple the legal from the factual aspect of statehood or when alternative forms of effective governance are not recognised, they cause serious legal problems because they create 'ghost' states and 'ghost' rulers operating below or outside the international law threshold.<sup>22</sup> For this reason, the factual and legal dimensions of authority over territories and people should correlate as for international law and the international legal order to be realised.

#### **IV. 'Ungoverned spaces' and their challenge to the institution of state responsibility**

The law of state responsibility exemplifies the correlation between legal and factual effectiveness. To explain, state responsibility arises when a state controls territory over which a wrongful act is committed or from where it emanates as the ICJ opined in its *Namibia Advisory Opinion*<sup>23</sup> or when it controls people who commit a wrongful act. As de Visscher wrote 'the operation and establishment of responsibilities largely depends on the organisation of power and the effectiveness of the control maintained in its territory by the accused State' and he went on to say that 'the extent of its [state] responsibility may then vary with the degree of effectiveness of control'.<sup>24</sup>

What are then the challenges posed to the institution of state responsibility by ungoverned spaces?

As it is well known, the law of state responsibility is premised on the distinction between primary and secondary rules with primary rules referring to international law obligations whose violation triggers the secondary rules of the law of state responsibility. When there is total lack of government, the state cannot assume international law obligations because it does not have an effective government to bind it. With no obligations, there is no responsibility. When ungovernability instead is confined to certain areas of its territory, the scope of its responsibility is accordingly circumscribed. Of course, the state as juridical person continues to be bound by existing international law but its responsibility is conterminous to its effectiveness. Moreover, as

---

<sup>22</sup> G. Kreijen, *State Failure, Sovereignty and Effectiveness: Legal lessons from the decolonization of sub-Saharan Africa*. (Leiden, Martinus Nijhoff Publishers, 2004)

<sup>23</sup> As the ICJ said 'physical control of a territory, and not sovereignty or legitimacy of title, is the basis of liability for acts affecting other States' *Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970)*, *Advisory Opinion*, I.C.J. Rep (1971), p. 16, para 118

<sup>24</sup> C. De Visscher, *Theory and reality in public international law*, trans. from the French by P.E. Corbett (Princeton, N.J., Princeton U.P., 1968) 285

will be discussed later, questions may arise as to who acts on behalf of the state when the state apparatus collapses or when its government is contested by other actors. Furthermore, even if state responsibility is established, the state may not be able to comply with Part II of the Articles on State Responsibility concerning the content of the international responsibility. For example, how can a state comply with the obligation to cease the unlawful act or to provide reparation if no functioning state apparatus exists?<sup>25</sup> In other words, there is asymmetry between formal obligations and the state's material capacity to ensure respect of those obligations.

At the same time, non-state actors that exercise power over territories and people are not bound by international law according to the prevailing opinion, with notable exceptions such as humanitarian and international criminal law. The latter obligations give rise to narrower forms of responsibility but the issue here is that the obligations and the ensuing responsibility of non-state actors who exercise power over territories and people are not coterminous to the scope and extent of their powers. One may contend that non-state actors are bound by international law through domestic law but this is not the case when a state cannot implement or enforce international law domestically. Again, respect by non-state actors of international law on the basis of the theory of legislative jurisdiction depends on state effectiveness.

To explain how this situation would affect the institution of responsibility for malicious cyber activities, a state with no functioning government cannot assume conventional obligations concerning cyberspace such as those deriving from the ITU Convention, the WTO system or from other subject-specific treaties. Even if a state becomes party to such treaties or remains bound by existing treaty law or by customary law, it cannot implement or enforce its obligations wholly or partially, if it suffers from ungovernability. Conversely, non-state actors operating from its territory and using its cyber infrastructure for their cyber activities cannot become parties to international agreements and, in any case, they are not bound by international law according to the prevailing international legal opinion. For this reason, they cannot be held responsible because they do not breach obligations incumbent on them.

Another critical feature of the law of state responsibility which affects its realisation in this instance is that it is premised on the distinction between public and private acts according to which a state is not held responsible for private or non-state conduct. This aspect of the law of state responsibility is reflected in the legal concept of attribution. Attribution 'subjectivises' a non-state act by transforming it into a public (state) act.<sup>26</sup> Attribution is based on an institutional, a functional and an agency test. The institutional test attributes the acts of a state's *de jure* or *de facto* organs to that state.<sup>27</sup> Whereas a *de jure* organ is determined by the state's institutional law, a *de facto* organ is one that is

---

<sup>25</sup> Article 30 and 31 ASR

<sup>26</sup> Art 2 ASR; Olivier de Frouville, 'Attribution of Conduct to the State: private individuals' in James Crawford, Alain Pellet and Simon Olleson (eds), *The Law of International Responsibility* (OUP 2010) 257-270. **Also see Mačák's article.**

<sup>27</sup> Art 4 ASR; *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v USA)* (Merits) [1986] ICJ Rep 14, para 109 (hereinafter referred to as *Nicaragua Case*); *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* (Judgment of 26 February 2007) [2007] ICJ Rep paras 307, 385, 390-393 (hereinafter referred to as *Bosnia Genocide Case*). J. Crawford, *State Responsibility-The general Part* (CUP, 2013) 124-126.

assimilated to or absorbed in the state apparatus. The functional test attributes acts to a state if they are committed by an entity that is empowered by that state to exercise governmental authority or if the act is committed by an organ of another state that has been placed at the disposal of the first state.<sup>28</sup> Finally, according to the agency test, an act is attributed to a state if it is committed by an individual or a group that have been instructed or directed by a state or when the act has been executed under the effective control of a state.<sup>29</sup>

It becomes apparent that the attribution standards in the law of state responsibility reflect the 'effectiveness' of statehood as an arrangement consisting of people that act on its behalf by submitting to its effective power. The state is not envisaged as a purely normative entity because, in that instance, there would be no need to establish a link between a person and a state or between specific acts and a state but a state would be held responsible for all wrongful acts committed within that state, emanating from its territory or committed by its citizens. Instead, as was commented, 'bearing in mind the important role played by the principle of effectiveness in international law, the existence of a real link between the person or group performing the act and the state machinery' is needed.<sup>30</sup> In the absence of a structured governmental and institutional apparatus or in the face of competing structures of authority some of which are not states, none of the aforementioned attribution criteria can be satisfied.

For instance, injurious physical or cyber acts by ISIS or by pro-ISIS cyber groups cannot be attributed to Syria and hold it responsible because none of the aforementioned attribution criteria can be fulfilled; they cannot also be attributed to ISIS because it is not a state or a subject of international law with international law obligations. These acts will thus be treated as private acts for purposes of state responsibility. They may of course breach domestic, Syrian, law or trigger individual criminal responsibility to the extent that they constitute international crimes but this raises the question of whether Syria has the capacity to enforce its law over ISIS and over ISIS held areas as well as whether international courts and tribunals have jurisdiction over ISIS members or the capacity to bring those responsible to justice.

The Articles on State Responsibility recognise two instances where a state can be held responsible for the acts of non-state actors without the need of attribution. According to Article 9 ASR, the conduct of a person or a group exercising elements of governmental authority of a particular state in the absence or default of the official authorities can be considered an act of that state. This covers situations where there is total or partial collapse of governmental authority and a necessity arises to exercise certain governmental functions which are performed by non-state actors.<sup>31</sup> Article 9 ASR situations do not envisage authorisation by the government but the non-state acts are considered to be state acts because of their governmental nature and because they are 'called for'. Applied to cyberspace, this provision may give rise to a number of problems.

The first challenge is to determine which functions are governmental in view of the contemporary trend to privatise or to contract out public services. One could say that

---

<sup>28</sup> Articles 5 and 6 ASR.

<sup>29</sup> Art 8 ASR. *Nicaragua Case*, paras 116-117; *Bosnia Genocide Case*, paras 398, 402-406, 413-414. [Aslo see Mačák's article](#)

<sup>30</sup> James Crawford, *The International Law Commission's Articles on State Responsibility* (CUP 2002) 110.

<sup>31</sup> Crawford, *The International Law Commission's Articles on State Responsibility*, 114-115

taxation, policing, defence and justice still remain core state functions<sup>32</sup> but this leads to the second challenge which is whether there is any space for non-state actors in the situations envisaged by Article 9 ASR. In the author's opinion there is still room for non-state actors even if governance migrates to cyber. It is true that many governmental services nowadays migrate to cyber<sup>33</sup> with Estonia being pioneer in rolling out governmental data online to allow the country to run even if it is physically occupied.<sup>34</sup> It is submitted that even in this case, the government will not be able to fulfil some of its functions, for example policing or defence, which can be performed by a non-state actor with physical presence on the territory. A non-state actor may also take over the government cloud where all governmental services or data are stored and perform various other functions, for example collect taxes or provide judicial functions. In other words, article 9 ASR can also apply to cyber governance. The third challenge is whether any involvement by the non-state actor in illegal activities such as terrorism or illegal trade will affect the application of Article 9 ASR. For instance, ISIS provides state-like services but, at the same time, engages in criminal activities and commits serious violations of international law.<sup>35</sup> There is no clear-cut answer to this question but it is the author's view that violations of *jus cogens* norms will exclude non-state actors from the purview of Article 9 ASR because these norms are the most fundamental norms of the international system. That having been said, it should be noted that Article 9 ASR covers only temporary and spontaneous assumptions of authority and not long term ones as it is the case with Hezbollah in Lebanon or the different groups that govern parts of Somalia. Furthermore, Article 9 ASR is about the voluntary assumption by non-state actors of governmental responsibilities and not about situations where they assume power by incapacitating the government. This means that even if ISIS exercises governmental powers, its governmental activities were not 'called for'.

The other instance where conduct of non-state actors is considered an act of state is contained in Article 10 ASR according to which the conduct of an insurrectional or other movements that succeed in replacing an existing government or in establishing a new state on the territory of an existing state are considered an act of that state. An 'insurrectional movement' is defined by the ILC in the light of Article 1 of Additional Protocol II (1977) as one that is organised and controls territory, usually in the same state as the government against which it has revolted.<sup>36</sup> It is not however clear whether

---

<sup>32</sup> Yeager v. Islamic Republic of Iran, Award No. 324-10199-1 (Iran-U.S. Claims Trib. Nov. 2, 1987) 104

<sup>33</sup> See HM Government, Government Cloud Strategy (March 2011) [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/266214/government-cloud-strategy\\_0.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266214/government-cloud-strategy_0.pdf) (accessed 31 December 2015)

<sup>34</sup> <https://e-estonia.com/>

<sup>35</sup> Principles in the Administration of the Islamic State <http://www.theguardian.com/world/2015/dec/07/islamic-state-document-masterplan-for-power> (accessed 31 December 2015)

Report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat, S/2016/92 (29 January 2016); Muhammad al-'Ubaydi, Nelly Lahoud, Daniel Milton, Bryan Price, The Group That Calls Itself a State: Understanding the Evolution and Challenges of the Islamic State, The Combating Terrorism Center (CTC) at West Point (December 2014) at [www.ctc.usma.edu](http://www.ctc.usma.edu)

<sup>36</sup> Article 1 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977. Article 10 ASR, commentary para 9. ICTY, *Prosecutor v Limaj, Bala and Musliu*, Judgement, IT-03-66-T, Trial Chamber II,

Article 10 ASR applies only to movements with territorial control. First, Article 10 ASR also refers to 'other movements' without defining them. One may thus say that territorial control is not necessary for those 'other' movements. Secondly, Article 10 ASR mentions insurrectional movements that act from within another state which allows for movements that do not control territory of the state they succeed in replacing. Thirdly, it mentions acts of insurrectional movements from the beginning of the insurrection at which point there may not have established territorial control. One can thus say with reason that territorial control is not necessary but what is necessary is some form of organisation.

That said, Article 10 ASR limits the scope of state responsibility. More specifically, the state will be held responsible for violations committed by the insurrectional movement as well as for those committed by the previous government when the insurrectional movement replaces the government, whereas when a new state is established by a movement, it will be held responsible only for violations committed by that movement. The scope of state responsibility is limited even further by the fact that insurrectional or other movements have limited international law obligations and by the fact that attribution is quite demanding as will be seen later. Another limitation is that Article 10 ASR does not deal with the responsibility of groups that have not been successful in forming a state and exonerates from responsibility groups that participate in a power sharing agreement.

For example, if ISIS or any of the groups fighting in Syria succeeds in establishing a new state, they will be held responsible for their previous malicious cyber activities but this will not go too far since their international law obligations are limited. It will not cover for example violations of the non-intervention norm or violations of human rights since they are not bound by these norms according to current international law doctrine.

It can thus be concluded that, although Article 9 ASR and Article 10 ASR confirm that a state is not responsible for the activities of non-state actors that govern parts of its territory, they still fail to address adequately the responsibility arising from the acts of those non-state actors.

Another major challenge posed to the law of state responsibility by ungoverned spaces is that, even if a non-state malicious act is attributed to a state, its wrongfulness may be precluded because the state may claim *force majeure*.<sup>37</sup> In order to apply this defence, the intervening events that led to loss of authority need to be unforeseen and beyond the control of the state. Ultimately, the matter turns on the question of whether the state could have foreseen its implosion or partial withdrawal of its authority. It can be argued that because there are always root causes to state implosion, this state of affairs is not caused by 'unknown causes'. Against this, it can be counter-argued that state implosion is the result of many endogenous and exogenous factors such as corruption, ethnic conflict, financial policies, repression, some of which are foreseen whereas others are not and therefore it is impossible for the state to control them as it is the case with Syria.

Finally, when a state is not effective, it cannot be held responsible for failing in its obligation of due diligence because it lacks the requisite capacity and control to

---

30 November 2005, paras 88–170; ICTY, *Prosecutor v Haradinaj, Balaj and Brahimaj*, Judgement, IT-04-84-T, Trial Chamber I, 3 April 2008, paras 37–60,

<sup>37</sup> Art 23 ASR

implement that duty.<sup>38</sup> The obligation of due diligence requires from states to ensure respect of their international law obligations and not to allow their territory to be used to the detriment of the rights of other states.<sup>39</sup> Due diligence is a corollary of the principle of state sovereignty and non-intervention. As Eagleton wrote, 'if no other state can be allowed to protect its interests therein, the territorial state must be held responsible for the protection of those interests'.<sup>40</sup> In cyberspace, it means that states should ensure the hygiene of their cyber infrastructure and prevent or punish non-state actors that use its cyber infrastructure to perpetuate malicious activities against other states. Due diligence is however an obligation of conduct.<sup>41</sup> States should have the capacity and use it in order to prevent, suppress and mitigate wrongful acts emanating from their territory. Because the obligation of due diligence is assessed by capacity, ungovernability means that there is limited or no institutional, legal or resource capacity to implement this obligation whereas non-state actors, according to the prevalent view, are not bound by any obligation of due diligence. In the case of ISIS for example neither Syria can be held responsible for violating its due diligence obligation with regard to ISIS malicious cyber activities from its territory, nor ISIS for the malicious cyber activities emanating from the territory it controls.

From the preceding exposition it can be said that, faced with ungoverned spaces, international law suffers from responsibility deficit. More specifically, in the absence of an effective state, the ingredients of international responsibility cannot be satisfied whereas international law's lack of engagement with non-state actors exercising effective control over territories and people allows them to operate with legal impunity. In such cases, it is not only non-state actors that evade responsibility but also states with non-state actors on their territory that evade responsibility for the acts of non-state actors. The problem is even more exacerbated in cyberspace because of the low entry barriers and the lack of control over a state's cyber infrastructure.

Such responsibility deficit ultimately challenges the integrity, validity, and relevance of international law as a force of order in international relations.<sup>42</sup> For this reason, the dynamics unleashed by the existence and activities of non-state actors need to be recognised and international law needs to enquire further as to whether and under what circumstances non-state actors can be carriers of duties and responsibilities. In this way, international law can fulfil its function as the normative foundation of the international order.

## **V. Non-state actor responsibility: an international law framework**

In what follows, I will propose criteria and set out conditions under which non-state actors can be held directly responsible for their malicious cyber activities.

---

<sup>38</sup> See **Buchan's article**

<sup>39</sup> *Corfu Channel case*, ICJ Rep (1949), 3, 22, *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, ICJ (1995), paras 241-2

<sup>40</sup> C. Eagleton, 'International Organisation and the Law of Responsibility', 76 *RC* (1950), 386

<sup>41</sup> *Bosnia Genocide Case*, para 430

<sup>42</sup> Michael Crawford and Jami Miscik, *The Rise of the Mezzanine Rulers: The New Frontier for International Law*, 89(6) *Foreign Affairs* 123 (2010)

The main criterion for holding non-state actors responsible is that of effectiveness. A non-state actor should exercise effective authority and control over territory and people to trigger its international law rights, duties and responsibility.<sup>43</sup> Authority is the power to decide, order, direct, delegate, and enforce compliance whereas control is the legal and material power to effectuate such authority. The effective exercise of authority and control is enabled by an organisational structure. Organisation refers to a stable arrangement that includes structures, institutions, processes and rules about activities, roles, aims, decision-making, and means of ensuring compliance. Having an organisation is critical because it provides the non-state actor with capacity to will and capacity to act and is the medium through which authority over people and territory becomes effective. Moreover, an organisation makes the non-state actor independent from its members, underpinning its separate personality.

A non-state actor that exhibits these traits of effectiveness should be recognised as a legal person. Legal personality is how international law determines that 'a certain actor [is] a separate and independent entity' for legal purposes<sup>44</sup> and consequently subject to international law rights and obligations.<sup>45</sup> Legal personality is a legal ascription superimposed on effectiveness. By granting legal personality, international law confers legal status to an effectivity that exists and operates in international relations and consequently accepts it as an actor with legal rights and obligations. Refusing to grant legal personality means that the relations between legal subjects and such effectivities or the actions of such effectivities remain outside legal regulation, even if they affect other legal subjects such states or affect the rights of the people over whom they exercise power or affect international law in general. The ICJ's response to such an eventuality was quite pragmatic as it becomes evident in its *Reparations Advisory Opinion* where the Court ascribed legal personality to the United Nations, a non-state actor, because of its functions, the capacity to possess rights and duties and the possession of organs with separate will from that of its member states. The Court also noted in its Advisory Opinion that attribution of personality relates to the 'requirements of international life' and the needs of states to interact with other actors.<sup>46</sup> The correlation between legal personality and effectiveness is also evident in the recognition of belligerency and insurgency.<sup>47</sup>

The immediate question is whether cyber groups that is, groups that are formed in cyberspace and operate only in cyberspace can exhibit these hallmarks of effectiveness in order to be recognised as legal persons. The answer is in the negative. First, notions of control over territory or people are difficult to apply in the case of cyber groups. This means that cyber groups lack the substratum of territory and people upon which effectiveness can be manifested. Secondly, concerning the element of organisation, it is true that cyber groups often act in a coordinated manner.<sup>48</sup> This can involve encouragement of members to take action, publication of lists of targets, selection of

---

<sup>43</sup> In this way, non-state actors are differentiated from criminal groups.

<sup>44</sup> Janne Nijman, *The Concept of International Legal Personality: An Inquiry into the History and Theory of International Law* (2004), 3

<sup>45</sup> Jan Klabbers, 'The Concept of Legal Personality', 11 *Ius Gentium*, (2005), 37, 47

<sup>46</sup> ICJ, *Reparation for Injuries Suffered in the Service of the United Nations, Advisory Opinion of 11 April 1949*, at 178-9

<sup>47</sup> Antonio Cassese, *International Law*, 2<sup>nd</sup> ed., (OUP, 2005), 124-131

<sup>48</sup> Tallinn Manual, 89

cyber weapons, attacks and post-attack evaluation.<sup>49</sup> The attacks on TV5Monde or on Estonia in 2007 and on Georgia in 2008 indeed followed such a pattern. Yet, coordination is not necessarily synonymous with organisation as defined above and many cyber groups are ephemeral and spontaneous formations of people or activities with loose, if any, hierarchical structures. For example *Anonymous* describes itself as 'a very loose and decentralised command structure that operates on ideas than directives'.<sup>50</sup> Even if cyber groups exhibit certain organisational characteristics,<sup>51</sup> these are not often visible or distinct as to make the group independent from its members and to transform individual actions into group actions. In virtual groups, it is often difficult to distinguish conduct committed on an individual capacity from group conduct and, moreover, membership may not be known. Thirdly, in the absence of legal or material power to enforce authority, the degree of authority and control exerted over members is quite weak and expectations of proper conduct cannot be imposed on members. Moreover, in the absence of group cohesion and of visibility of members, authority and control cannot be internalised. Even if the group excludes members or applies other virtual sanctions, such measures are more or less social sanctions and do not translate into real life consequences. Members can easily circumvent authority and control and the effectiveness of sanctions is diminished by role playing.<sup>52</sup> Fourthly, the manifestation of authority and control in cyber is not inherent to the organisation but is dependent on and is mediated by the software system; it is the software system that provides the means and determines what can be done or cannot be done. For all these reasons, it can be said that cyber groups fail the test of effectiveness which is necessary for being recognised as legal persons.

However, non-state actors that exist off-line but operate also on-line can exhibit the aforementioned traits of effectiveness but a question that may be asked is whether their character has any bearing on their recognition as a legal person. It is submitted that as long as their primary activities and the bulk of their activities are lawful, the unlawfulness of some of their activities will not have any bearing on their status. For example, an effective non-state actor that exercises authority and control over territory and people and performs functions related to such authority yet it also engages in drug trafficking will not lose its legal status but may be held responsible for its unlawful activities. To some extent, effectiveness precedes normativity. If normativity were to precede effectiveness, then we may be faced with the absurd situation of non-state actors who exercise effective control over people and territory evading responsibility because of some illegal conduct. It is only in relation to peremptory (*jus cogens*) norms that normativity precedes effectiveness. Consequently, an effective non-state actor that commits breaches of core *jus cogens* norms<sup>53</sup> will not be recognised as an international

---

<sup>49</sup> Eneken Tikk, Kadri Kaska, Liis Vihul, *International Cyber Incidents: legal considerations*, Cooperative Cyber Defence Centre of Excellence (CCD COE), 2010

<sup>50</sup> ANON OPS: A Press Release, December 10, 2010, [http://www.wired.com/images\\_blogs/threatlevel/2010/12/ANONOPS\\_The\\_Press\\_Release.pdf](http://www.wired.com/images_blogs/threatlevel/2010/12/ANONOPS_The_Press_Release.pdf) (accessed 31 January 2016)

<sup>51</sup> Rain Ottis identifies three models: Forum, Cell and Hierarchy. The last one is state organised. R. Ottis, 'Theoretical Offensive Cyber Militia Models' in *Proceedings of the 6th International Conference on Information Warfare and Security*, (Washington DC. Reading: Academic Publishing Limited, 2011), 307-313

<sup>52</sup> L. Long, 'The Prospect of Social Norms as a Governing Mechanism of Virtual Worlds', 3 *European Journal for Law and Technology* (2012)

<sup>53</sup> It is outside the scope of this paper to define *jus cogens* norms but the prohibition of aggression, genocide and of crimes against humanity are widely accepted as such norms

law person. The reason being that legal personality, as was said, is the way international law demarcates its boundaries by incorporating 'effectivities' into its domain but international law is defined by certain constitutional principles of which *jus cogens* norms form a part and which bind all international actors. Non-state actors that commit violations of *jus cogens* norms undermine its foundational principles and therefore they are not recognised by international law. It is for this reason that peremptory norms have been decoupled from the realm of effectiveness as it is seen by the sanction of non-recognition of situations brought about by a violation of these norms.<sup>54</sup> In the case at hand, it means that ISIS will fail in this respect.<sup>55</sup>

The next issue concerns the scope of international law rights and obligations incumbent upon such non-state actors. It is submitted that they have those rights and obligations that form part of international customary law<sup>56</sup> because customary law is the minimum law that applies to international law subjects and reflects international law's minimum expectations of lawful behaviour. It does not however follow that non-state actors will have the totality of international customary rights and duties but only those that relate to their functions. This has been affirmed by the ICJ in the *Reparations Advisory Opinion* where the Court introduced a differentiated system of legal rights and obligations depending on the functions of legal persons.<sup>57</sup> Legal personality is not in other words synonymous with uniformity of legal obligations. That having been said, all non-state actors that exercise some form of power over territories and people should be bound by *jus cogens* norms which constitute the fundamental principles of international law<sup>58</sup> as

---

<sup>54</sup> Article 40 and 41 ASR

<sup>55</sup> The SC or states treated ISIS as a terrorist group even if it has the hallmarks of a state. SC Res 2161 (2014); SC Res 2199 (2015); SC Res 2249 (2015); SC Res 2253 (2015). According to President Obama 'ISIL is certainly not a state. It was formerly al Qaeda's affiliate in Iraq, and has taken advantage of sectarian strife and Syria's civil war to gain territory on both sides of the Iraq-Syrian border. It is recognized by no government, nor the people it subjugates. ISIL is a terrorist organization, pure and simple.' Transcript: President Obama's Speech on Combating ISIS and Terrorism (11 September 2014) <http://edition.cnn.com/2014/09/10/politics/transcript-obama-syria-isis-speech/>

<sup>56</sup> *Interpretation of the Agreement of 25 March 1951 between the WHO and Egypt*, Advisory Opinion, ICJ Reports 1980, 73, 89-9. Human Rights Council, *Report of the independent international commission of inquiry on the Syrian Arab Republic* A/HRC/21/50 (16 August 2012), Annex II, para 11: 'Non-state actors cannot formally become parties to international human rights treaties. They must nevertheless respect the fundamental human rights of persons forming customary international law (CIL), in areas where such actors exercise *de facto* control'. U.N. H.R.C. Rep. of the International Commission of Inquiry to investigate all alleged violations of international human rights law in the Libyan Arab Jamahiriya, Feb. 25, 2011-June 1, 2011, { 72, U.N. Doc. A/17/44; GAOR, 17th Sess., Supp. No. 44 (2011) *Report of the United Nations High Commissioner for Human Rights on the situation of human rights in Mali*, UN Doc A/HRC/22/33, 7 January 2013; Ben Emmerson, the Special Rapporteur on the protection of human rights while countering terrorism A/HRC/29/51, 16 June 2015, at paras 30-31; Commission of Inquiry on Gaza (2015) A/HRC/10/22, para. 21

<sup>57</sup> *Reparations Advisory Opinion*, para 178

<sup>58</sup> *Report of the independent international commission of inquiry on the Syrian Arab Republic* A/HRC/19/69, 22 February 2012, para 106: '... the commission notes that, at a minimum, human rights obligations constituting peremptory international law (*ius cogens*) bind States, individuals and non-State collective entities, including armed groups.'

well as by those international norms relevant to their functions and the particular context.

The next issue that needs to be considered is that of attribution because attribution links the wrongful act to a subject of rights and duties for purposes of responsibility. One could apply by analogy the attribution tests found in the law of state responsibility which, as explained above, include an institutional, a functional and an agency test. In the first place, acts of their organs will automatically be attributed to the non-state actor. Such organs may be *de jure* organs, for example organs that represent the non-state actor such as its leader but also *de facto* organs that is, organs assimilated to the non-state apparatus. This shows the importance of organisation for purposes of responsibility because international law relies on internal law and regulations to make such determinations. However, non-state actors may not have or, even if they have, they may not publicise their internal organisational structure for security reasons, leading thus to inferences to be made about their organisation and, possibly, more emphasis to be placed on the concept of *de facto* organs.

This having been said, it is interesting to see how attribution plays out in the case of ISIS, a non-state actor, and of the pro-ISIS cyber groups. ISIS possesses a state-like internal organisation. It has a supreme leader, the Caliph, deputies, a Shura (consultative) council as well as councils for defence, security and intelligence, military affairs, information, judicial, and finance.<sup>59</sup> Its military force including incorporated groups of foreign fighters over whom ISIS exercises full command and control is an ISIS organ. It follows that their acts, including their cyber activities will be automatically attributed to ISIS. Concerning ISIS media people or, at least, senior media people, they can be equivalent to *de facto* organs. According to an article published in *The Washington Post* which was based on extensive interviews with a number of repentant ISIS militants, senior ISIS media people are treated as “Emirs,” of equal status to their military counterparts, they are well paid and they are directly involved in decisions on strategy and territory.<sup>60</sup> Their malicious cyberactivities will be equally attributed to ISIS. Concerning pro-ISIS cyber groups, none of these groups has received any formal recognition by ISIS, although some of them were led by persons who joined ISIS and vowed allegiance to its leader and to its cause. It can be said therefore that those

---

<sup>59</sup> Col. (ret.) Dr. Jacques Neria, ‘The Structure of the Islamic State (ISIS)’ at <http://jcpa.org/structure-of-the-islamic-state/>. Its structure can be contrasted to Al-Qaeda’s which is decentralised. Al Qaeda v ISIS: Leaders & Structure at <https://www.wilsoncenter.org/article/al-qaeda-v-isis-leaders-structure..> (accessed on 31 December 2015)

<sup>60</sup> Greg Miller and Souad Mekhennet, Inside the surreal world of the Islamic State’s propaganda machine, *The Washington Post*, 20 November 2015, [https://www.washingtonpost.com/world/national-security/inside-the-islamic-states-propaganda-machine/2015/11/20/051e997a-8ce6-11e5-acff-673ae92ddd2b\\_story.html](https://www.washingtonpost.com/world/national-security/inside-the-islamic-states-propaganda-machine/2015/11/20/051e997a-8ce6-11e5-acff-673ae92ddd2b_story.html) (accessed 31 December 2015)

individuals are *de jure* organs.<sup>61</sup> For *de facto* organ what is needed is complete dependence and control.<sup>62</sup> Whether the same can be said with regard to members of the cyber groups or the cyber group itself can be debated since members were recruited on an ad hoc basis from the hactivist world. Ideological inspiration or influence is not adequate for making them *de facto* organs or for attributing their acts to ISIS even if such acts support its aims. Also, according to US reports, Cyber Caliphate was not affiliated to ISIS neither was it endorsed by ISIS.<sup>63</sup> As for the newly formed United Cyber Caliphate (UCC), the merger was necessary to coordinate activities but there is no evidence that it is subordinated to ISIS.

Applying now the functional test of attribution to non-state actors, according to this test, if an individual or a group is not an organ of the non-state actor but is empowered to exercise elements of the authority of the non-state actor, its conduct will be attributed to the non-state actor.<sup>64</sup> If the UCC for example is empowered by ISIS to pursue the war in the cyber domain, its activities will be attributed to ISIS. There is no evidence that this is the case but it is interesting to note that this mode of attributing conduct reflects the organised and hierarchical apparatus of modern states whereas with regard to non-state actors informal and implicit modes of authorisation may be more pertinent.

The agency test of attribution will attribute to a non-state actors the wrongful acts of individuals or groups who acted on the instructions, direction or control of that non-state actor.<sup>65</sup> Instructions and direction are quite difficult to prove in the absence of formal or publicly given orders. Regarding the criterion of control, the ICJ, rejected the 'overall control' standard in the context of responsibility and opted for the more stringent 'effective control' standard which makes the possibility of attribution quite exceptional.<sup>66</sup> As far as the pro-ISIS cyber groups are concerned, there is no evidence that ISIS instructed or directed them to attack specific targets. Effective control which requires direct influence in the commission of a specific act cannot also be proven. If however ISIS provides financial assistance or training to the newly formed UCC and approves their operations, one can say that it will wield overall control over UCC but, as was said, this is not sufficient to establish responsibility.

Finally, if a non-state actor acknowledges and adopts as its own certain conduct, that conduct should be attributed to the non-state actor.<sup>67</sup> For this to happen, the non-state actor needs to adopt the conduct as its own, as if it has been committed by itself. ISIS or other non-state actors may praise, approve of or take credit of attacks for various reasons including propaganda and publicity but adoption requires engagement with the

---

<sup>61</sup> A number of them were killed in drone attacks. At a state level, the US Cyber Command and Unit 61395 of PLA may be said to constitute *de jure* organs

<sup>62</sup> *Nicaragua Case* para 109; *Bosnia Genocide Case* paras 390-391, 307.

<sup>63</sup> Cyber Caliphate Hackers Not Linked to Islamic State <http://freebeacon.com/national-security/cyber-caliphate-hackers-not-linked-to-islamic-state/> (accessed 31 December 2016)

<sup>64</sup> As per Article 5 ASR

<sup>65</sup> As per Article 8 ASR. Also see Mačák's article

<sup>66</sup> *Bosnia Genocide Case* paras 402-406.

<sup>67</sup> Article 11 ASR; *Case Concerning United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)* ICJ Rep (1980), para 74, 115

act. With regard to cyber attacks attributed to pro-ISIS groups, ISIS has praised the attacks but it did not claim them as its own, neither did it engage in furthering the attacks.

It transpires that attribution proves to be the Achilles heel of ascribing responsibility to non-state actors. At this juncture it should be noted that non-state actors exercising authority over territories and people may operate under alternative structures of authority, not corresponding to current international law standards based on western bureaucratic structures. This means that the current standards may not be able to encapsulate the reality of non-state organisation and thus different standards may need to be introduced based on more informal structures of authority or different interpretations are needed of what, for example, constitutes a *de jure* or a *de facto* organ in a non-state apparatus.

## VI. Implementation of non-state actor responsibility

Notwithstanding these difficulties, if a non-state actor is eventually found responsible for a malicious cyber activity, the means of implementing its responsibility do not give rise to many difficulties. The non-state actor has an obligation to cease the wrongful conduct, to continue performing the obligation, to offer assurances of non-repetition and to make full reparation in the form of restitution, compensation and satisfaction.<sup>68</sup> Although in principle non-state actors can easily fulfil these obligations, there are currently no formal mechanisms where non-state actors, states or individuals can apply in order to have such responsibility implemented. The only implementation mechanisms currently suited to non-state actors are arbitration, monitoring mechanisms or sanctions by states and international organisations.<sup>69</sup> The role of the Security Council in this regard is pivotal in reaffirming the obligations of non-state actors, in requesting action plans to implement obligations,<sup>70</sup> or in imposing sanctions. The SC can play the same role in relation to cyber by reminding non-state actors of the obligations attached to their cyber behaviour and conduct or by imposing sanctions for their cyber transgressions. For example the SC can instruct states and other non-state actors to freeze assets of non-state actors or not to transfer technologies or products.

A related question is whether states and international organisations or other non-state actors can take countermeasures including cyber countermeasures against a non-state actor that breached international law obligations with its cyber activities.<sup>71</sup> Countermeasures are decentralised means of enforcing international law and of implementing responsibility. Current international law confines countermeasures to states and international organisations, as the two subjects of international law. Under the proposed framework where non-state actors enjoy a measure of international personality, there is nothing to preclude the imposition of countermeasures on non-state actors provided that the acting state or international organisation and the non-state actor are bound by certain obligations. For example, if there are bilateral or multilateral agreements between states and non-state actors, for example cyber arms

---

<sup>68</sup> Articles 29-37 ASR

<sup>69</sup> SC Res 942 (1994); SC Res 1127 (1997); SC Res 1173 (1998); SC Res 1221 (1999); SC Res 1267 (1999); SC Res 1572; SC Res 1591 SC Res 1698 SC Res 2067 (2011); SC Res 2071 (2012)

<sup>70</sup> SC Res 1417; SC Res 1649 SC Res 1612 (2005); Report of the Secretary-General on Children and armed conflicts in Côte d'Ivoire\_S/2007/515, 30 August 2007, in particular Part IV.

<sup>71</sup> Articles 49-54 ASR

control agreements or cyber security agreements, breach of the agreement by the non-state actor may engage its responsibility and trigger cyber or physical countermeasures. Also breach of customary international law obligations binding states, international organisations and non-state actors would trigger countermeasures. For example, if both non-state actors and states are bound by the customary law norm of non-intervention, breach of that norm by a non-state actor by intruding into a state's cyber infrastructure would legitimise the state to take countermeasures against the responsible non-state actor. The same would hold true between non-state actors. If non-state actors are bound by bilateral or multilateral agreements or by international law obligations, breach of an obligation may trigger countermeasures by the affected non-state actors. Whether non-state actors would be able to take countermeasures against states that breached obligations towards them, the answer should be in the affirmative under the proposed framework. If a non-state actor commits violations of *jus cogens* rules, this may trigger coordinated action to put an end to such violations.<sup>72</sup> This situation is not different from existing practice where states and international organisations such as the United Nations take action against non-state actors for violations of *jus cogens* norms. Under the framework proposed here, non-state actors could also take countermeasures against other non-state actors. One may use as an example the decision of *Anonymous* to attack ISIS websites in retaliation for the Paris attacks in order for the acts not to go unpunished. For *Anonymous* it is 'uniting humanity' against ISIS.<sup>73</sup>

## VII. Conclusion

The preceding discussion has demonstrated that ungoverned spaces coupled with the existence of powerful non-state actors who operate from such territories pose serious challenges to international law and to the institution of international responsibility because, at present, neither the state nor the ruling non-state actor can be held responsible for violations of international law. The emerging state of irresponsibility can be reversed by recognising effective non-state actors as carriers of rights, duties and responsibility. Effectiveness is thus the modicum for legal recognition as well as for the realisation of international law and of international responsibility. Effectiveness will however limit the number of actors that can be thus recognised with cyber groups failing to satisfy this condition. This means that a large number of non-state actors will still evade responsibility. The answer is not thus fully satisfactory if it is also admitted that processes and forums to implement their responsibility are lacking. It is submitted that unless international law engages in a radical conceptual, institutional and structural rebooting, the place, role and consequences of non-state actors will remain uncertain.

---

<sup>72</sup> Articles 40-41 ASR

<sup>73</sup> A. Griffin, 'Paris attack: Anonymous launches 'biggest operation ever' against Isis' <http://www.independent.co.uk/life-style/gadgets-and-tech/news/paris-attacks-anonymous-launches-its-biggest-operation-ever-against-isis-promises-to-hunt-down-a6735811.html> (accessed 31 March 2016)