---

**Article:**
Tsagourias, N. (2015) The law applicable to countermeasures against low intensity cyber operations. Baltic Yearbook of International Law Online, 14. pp. 105-123. ISSN: 1569-6456

https://doi.org/10.1163/22115897-90000123

---

# The Law Applicable to Countermeasures against Low-Intensity Cyber Operations

Nicholas Tsagourias*

**Contents**



## 1. Introduction

Cyber threats appear in different forms and present different levels of seriousness. Whereas a cyber-attack amounting to armed attack is perhaps the most serious threat emanating from cyberspace, the probability of such an attack happening is quite low. Yet, legal commentators have focused their attention almost exclusively on such attacks and discussed how the rules on the use of force found in the United Nations (UN) Charter and in customary law apply to such attacks.[1] Although low-intensity cyber operations are more frequent, the legal framework that applies to them has not been fully explored.[2] Low-intensity cyber operations refer to cyber operations amounting to a use of force below the threshold of an armed attack as well as to cyber operations below the use of force threshold. Whether low-intensity cyber operations constitute uses of force depends on the harm they cause in the sense of material damage, human injury and loss or loss of functionality.[3]

* Professor of International Law, University of Sheffield. Email: Nicholas.Tsagourias@sheffield.ac.uk.

[1] *See for example The Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, Cambridge, 2013).

[2] With the exception of M. N. Schmitt, '"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law', forthcoming in 54 *Va. JIL* (2014) available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2353898

[3] *Tallinn Manual*, *supra* note 1, Rule 11. M. N. Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework', 37 *Colum. J. Transnat'l L*. (1999) p. 885, at pp. 909–912

This article will focus on countermeasures as acceptable responses to low level cyber operations and examine the legal framework within which countermeasures operate.

The article proceeds thus as follows. Part 2 will provide an account of the genealogy of countermeasures and explain the legal regime within which they operate. This is very important because, although the term countermeasures is a recent invention having specific legal connotations, the normative and legal history of countermeasures is quite rich and instructive. Identifying the target of countermeasures is critical not only for the effectiveness but also for the lawfulness of countermeasures, therefore Part 3 will examine the standards according to which low level cyber operations can be attributed to a State or to a non-State actor. Part 4 will explore the scope of the principle of proportionality in the context of countermeasures whereas Part 5 will examine the availability of third party countermeasures against low-intensity cyber operations and consider the legal effects of countermeasures on third parties.

## 2. Genealogy of Countermeasures

Countermeasures are unilateral and decentralised mechanisms of enforcing international law in view of the latter's weak enforcement mechanisms.[4] Their legality is premised on three factors: (i) the existence of a prior wrongful act; (ii) the inability or unwillingness of the wrong-doer to redress the situation; (iii) the proportionality of the measure.[5]

[4] *Institut de Droit International*, Session de Paris 1934, *Régime de répresailles en temps de paix*, Article 1; H. Kelsen, *Principles of International Law* (Rinehart & Company, New York, 1952) p. 23; A. Cassese, *International Law*, 2nd edition (Oxford University Press, 2005) p. 299; J. Crawford, *The International Law Commission's Articles on State Responsibility* (Cambridge University Press, Cambridge, 2001) p. 281.
[5] Article 22 ARSIWA and commentary in Crawford, *ibid.*, pp. 168–169. *Gabčikovo-Nagymaros Project (Hungary/Slovakia)*, Judgment, [1997] *ICJ Rep.* 7, para. 83.

Countermeasures are the modern incarnation of reprisals which as a concept and activity has a long pedigree.[6] As it was said, reprisals "existed well before law, needless to say international law. The paradox of international law as a legal order is that it allowed reprisals into the legal system itself."[7] The *locus classicus* of the law of reprisals is the *Naulilaa* arbitration of 1928. The case concerned forcible action against Portuguese forts and posts in Angola, following the killing and wounding of German officers by Portuguese soldiers.[8] Reprisals were defined there as 'an act of self-help on the part of the injured states, responding after an unsatisfied demand to an act contrary to international law on the part of the offending State . . . . They would be illegal if a previous act contrary to international law had not furnished the reason for them. They aim to impose on the offending State reparation for the offense or the return to legality in avoidance of new offenses.'[9]

Whereas traditionally forcible and non-forcible reprisals were treated as a single category[10] that could apply invariably to violations of international law regardless of whether such violations involved the use of force, arbitral awards,[11] the International Court of Justice (ICJ)[12] and later the International Law Commission (ILC) in its codification of the law of international responsibility conceptualised countermeasures as peaceful responses to violations of international law and by doing so they distinguished countermeasures from reprisals. As stated in Article 50 of the Articles on Responsibility of States for Internationally

---

[6] M. Ruffert, 'Reprisals', in *Max Planck Encyclopedia of Public International Law* (Oxford, Oxford University Press, 2012) pp. 927–930.
[7] E. Zoller, *Peacetime Unilateral Remedies: An Analysis of Countermeasures* (Transnational Publishers, Dobbs Ferry, NY, 1984) p. 35
[8] *Naulilaa Incident* Arbitration Decision *(Port.* v. *Ger)* 2 *RIAA* (1928) p. 1011.
[9] Ibid, 1017-1028
[10] O. Y. Elagab, *The Legality of Non-Forcible Counter-Measures in International Law* (Oxford University Press, Oxford, 1988) p. 85.
[11] *Case concerning the Air Service Agreement of 27 March 1946 between the United States of America and France*, decision of 9 December 1978, *R.I.A.A.*, vol. XVIII, 416, para. 80.
[12] *Case Concerning United States Diplomatic and Consular Staff in Tehran*, [1980] *ICJ Rep.* 14, para. 53; *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua* v. *United States of America)*, Judgment of 27 June 1986, [1986] *ICJ Rep.* 14 , para. 291; *Gabčikovo-Nagymaros Project*, *supra* note 8, para. 80

Wrongful Acts (ARSIWA), countermeasures should not affect the prohibition of the threat or use of force.[13] The modern concept of countermeasures thus incorporates the peaceful part of the older concept of reprisals.[14]

Yet, according to the ILC, "questions concerning the use of force in international relations … are governed by the relevant primary rules".[15] One may thus say that forcible reprisals have been consigned to the use of force regime which is separate from the law of statre responsibility. The ILC has not offered any views as to the lawfulness of forcible reprisals according to the primary rules on the use of force, so the immediate task is to ascertain their current legal status. In order to do this, it is important to explain the nature and characteristics of the use of force regime and that of international responsibility and also take into consideration any relevant State practice and *opinio juris*.

As was said, countermeasures are an institution of the law of international responsibility. This regime is constructed around the distinction between primary and secondary rules.[16] Primary rules identify the international law obligations incumbent upon the subjects of international law whereas secondary rules identify the legal consequences to be derived from violations of primary rules. The law of international responsibility contains secondary rules, that is, rules on the consequences of wrongful conduct and the modalities according to which responsibility can be engaged. Moreover, the law of international responsibility belongs to the international law of peace; it is about the peaceful enforcement of international law and the peaceful resolution of disputes. Thus, countermeasures as part of the law of international responsibility aim at enforcing international obligations and effectuating international responsibility through peaceful means.

---

[13] D. Alland, 'The Definition of Countermeasures', in J. Crawford, A. Pellet and S. Olleson (eds.), *The Law of International Responsibility* (Oxford University Press, Oxford, 2010) p. 1127, at p. 1130.
[14] Crawford, *supra* note 7, 281, para. 3.
[15] *Ibid.*, p. 282, para. 3.
[16] *Ibid.*, pp. 14–15.

Forcible reprisals operate within the use of force regime.[17] This regime contains primary rules regulating the use of force in international relations. It consists of the UN law and the customary law on the use of force. The two sources of the law on the use of force interact but exist alongside each other. [18] Central to both branches is the prohibition of the unilateral use of force and the recognition that force can be used by way of self-defence in response to an armed attack.[19] An armed attack is a grave use of force defined as such by its scale and effects.[20] The UN law on the use of force does not however contain any rule on counterforce against uses of force below the threshold of an armed attack. There is no congruence in other words between the prohibition of the use of force in Article 2(4) of the UN Charter and self-defence in Article 51 of the UN Charter. In the *Nicaragua* case the ICJ spoke of "measures which do not constitute an armed attack but may nevertheless involve a use of force"[21] against which the victim State can take proportional countermeasures but it did not provide any clarification as to whether such measures may also involve the use of force. It has been contended that such measures should not involve the use of force because, in the post-Charter era, any use of force other than in self-defence is prohibited.[22] It has also been contended that the prohibition of forcible reactions to low-intensity uses of force exists in order to prevent

---

[17] *Ibid.*, p. 282, para. 3: "Questions concerning the use of force in international relations … are governed by the relevant primary rules."
[18] *Nicaragua* case, *supra* note 11, paras. 175–178.

[19] Article 2(4) and Article 51 UN Charter.
[20] *Nicaragua* case, *supra* note 11, paras. 195, 210; *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America)*, [2003] *I.C.J. Rep.* 161, paras. 51, 64, 77; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, including in and around East Jerusalem*, Advisory Opinion of 9 July 2004, [2004] *ICJ Rep.* 136, para. 139; *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of Congo* v. *Uganda)* [2005] *ICJ Rep.*, para. 147
[21] *Nicaragua* case, *supra* note 11, para. 210.

[22] Article 2(4) UN Charter; *Tallinn Manual*, *supra* note 1, Rule 11, para. 11 and Rule 9; I. Brownlie, *International Law and the Use of Force by States* (Oxford University Press, Oxford, 1963) pp. 223, 281, 348, 431; B. Simma (ed.), *The Charter of the United Nations, A Commentary*, 2nd edition, vol. 1 (Oxford University Press, Oxford, 2002) p. 794; Declaration Concerning Friendly Relations and Cooperation Among States in Accordance with the UN Charter, General Assembly Resolution 2625 (XXV), 24 October 1970; Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, General Assembly Resolution 36/103, 9 December 1981, Section II(c); *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996, [1996] *ICJ Rep.* 227, para. 46.

further escalation of the dispute. However, in reality, if States are allowed to respond to low-intensity operations amounting to a use of force through peaceful means only, this may not provide them with adequate redress whereas offending States or non-state actors can use force more frequently when the costs to them are minimal.

It is because of the imbalance in the legal regulation of force and counterforce in the UN Charter and the serious implications such a situation has on States that forcible reprisals continue to have an enduring appeal even in the post-Charter period. For example, after a detailed study of State practice concluded in 1970, Bowett came to the conclusion that there is a trend according to which reprisals may be *de jure* illegal but accepted *de facto*.[23] Since then, reprisals acquired a greater degree of legal acceptability in the context of terrorism where criticisms centre around issues of proportionality[24] or evidence and not around the legal entitlement itself.[25] The need of equivalent reaction to low-intensity uses of force has also been recognised by certain ICJ judges. In the *Oil Platforms* case, Judge Simma and Judge Kooijmans in their Separate Opinions were of the opinion that 'proportional countermeasures' of a military nature could be taken against uses of force below the armed attack threshold.[26] In the same vein but in the cyber context, the minority view as recorded in the *Tallinn Manual* was that a State can resort to forcible reprisals.[27]

It is submitted in light of the above that forcible reprisals have a place in States' practice even if the vocabulary used is more nuanced. To explain, States often use the self-defence language when they take forcible action against uses of forces below the threshold of an

[23] D.W. Bowett, 'Reprisals Involving Recourse to Armed Force', 66 *AJIL* (1972) p. 1.

[24] B. Levenfeld, 'Israel Counter-Fedayeen Tactics in Lebanon: Self-Defence and Reprisal under Modern International Law', 21 *Col JTL* (1982) p. 1, at p. 35. With regard to the Israeli action in Gaza *see* SC Res. 1860 (2009). With regard to Israel's action in Syria in 2006 *see* statements in the Security Council S/PV.5488 (13 July 2006).

[25] 93 *AJIL* (1999) pp. 161–167.

[26] Dis. Op. Simma in *Case Concerning Oil Platforms*, *supra* note 19, para.15. Judge Koojmans is rather noncommittal. Dis. Op. Koojmans, *ibid.,* paras. 52 and 62

[27] *Tallinn Manual*, *supra* note 1, Rule 9, para. 5.

armed attack. This may be explained by the fact that certain States such as the United States do not make a distinction between a use of force and an armed attack but instead treat all uses of force irrespective of gravity as armed attacks triggering the right to self-defence. It is however interesting to follow the justification offered by the United States for their action in Sudan and Afghanistan following the bombing of their embassies in Kenya and Tanzania in 1998. Although they invoked self-defence, the reasoning is more akin to reprisals in that it invoked the wrongfulness of the prior use of force, the failed request for redress, the proportionality of the action and the lack of effective alternatives.[28] According to the US Ambassador to the United Nations:

> [T]he United States of America has exercised its right of self-defence in responding to a series of armed attacks against United States embassies and United States nationals. My Government has obtained convincing information from a variety of reliable sources that the organization of Usama Bin Ladin is responsible for the devastating bombings on 7 August 1998 of the United States embassies in Nairobi and Dar Es Salaam. … The Bin Ladin organization maintains an extensive network of camps, arsenals and training and supply facilities in Afghanistan, and support facilities in Sudan, which have been and are being used to mount terrorist attacks against American targets. … In response to these terrorist attacks, and to prevent and deter their continuation, United States armed forces today struck at a series of camps and installations used by the Bin Ladin organization to support terrorist actions against the United States and other countries. In particular, United States forces struck a facility being used to produce chemical weapons in the Sudan and terrorist training and basing camps in Afghanistan. These attacks were carried out only after repeated efforts to convince the Government of the Sudan and the Taliban regime in Afghanistan to shut these terrorist activities down and to cease their cooperation with the Bin Ladin organization.[29]

[28] It should be recalled that the attacks on the Embassy did not satisfy the criteria of an armed attack as pronounced by the ICJ in the *Nicaragua* case and accepted in customary international law although, as was said, the US does not make such a distinction.

[29] Letter dated 20 August 1998 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council, UN Doc. S/1998/780 (20 August 1998).

The same can be said with regard to the 1986 US raids in Libya in response to a terrorist attack in West Berlin which caused the killing of a US serviceman. Although the action was justified under the self-defence rubric, it is closer to reprisal even if it was disproportionate in its execution.[30]

Often the term defensive reprisals[31] is used to describe proportional counterforce to prior uses of force with the explanation that, whereas reprisals are punitive and retributive in character, defensive reprisals are purely defensive. It should be noted however that it is difficult to distinguish reprisals from self-defence on that basis because both reprisals and self-defence may have a retaliatory element or be defensive by preventing future attacks.[32] Although reprisals share a lot in common with self-defence, any 'normative drift' to stretch the meaning of self-defence is unnecessary.[33]

In the light of what was said above, it is submitted that a State can respond to low-intensity cyber operations which amount to a use of force by taking forcible reprisals. However, it should be stressed that the use of force involved in such a cyber operation should reach a certain level significance in order to justify a reprisal action.[34] If the forcible cyber operation does not satisfy the *de minimis* threshold or does not qualitatively constitute a use of force, the victim State can only take countermeasures, that is, non-forcible measures.

---

[30] G. B. Roberts, 'Self-Help In Combatting State-Sponsored Terrorism: Self Defense and Peacetime Reprisals', 19 *Case W. Res. J. Int'l L.* (1987) p. 243, at pp. 286–288.

[31] Y. Dinstein, *War, Aggression and Self-Defence*, 5th edition (Cambridge University Press, 2011) pp. 244–255; W. V. O'Brien, 'Reprisals, Deterrence and Self-Defense in Counterterror Operations', 30 *Va. J. Int'l L.* (1990) p. 421, at p. 426.

[32] Bowett, *supra* note 22, p. 3; R. Tucker, 'Reprisals and Self-Defense: The Customary Law', 66 *AJIL* (1972) p. 586.

[33] D. Bethlehem, 'International Law and the Use of Force: the Law as it is and as it Should Be' (written evidence to the Select Committee on Foreign Affairs- Minutes of Evidence, 8 June 2004), para. 21 available at: <www.publications.parliament.uk/pa/cm200304/cmselect/cmfaff/441/4060808.htm>.

[34] *Tallinn Manual*, *supra* note 1, Rule 11, paras 1, 6–7.

A related and quite interesting question in the cyber context is whether low-intensity cyber operations that do not cause material destruction or human injury and loss constitute uses of force. This issue has been debated quite extensively, and it seems that there is increased acceptance of the view that cyber operations that significantly disrupt the functionality of a State's critical national infrastructure are equivalent to a use of force.[35] A State can thus resort to forcible reprisals in response to such cyber operations, but if the opposite view that such operations are not uses of force is accepted, the victim State can resort to countermeasures.

It goes without saying that the lawfulness of the countermeasure or reprisal is premised on the existence of a prior breach of an international obligation owned to the injured State. I will not enumerate here all the obligations that low-intensity cyber operations may breach, but I will only indicatively mention the obligation enshrined in the UN Charter and in customary law not to use force, the customary law obligation not to intervene in a State's affairs or the customary law obligation to respect a State's sovereignty.

If States can resort to countermeasures or reprisals in response to low-intensity cyber operations, identifying the target of their action is crucial. As the ICJ said in relation to countermeasures, they must be directed against the State that is responsible for the wrongful act.[36] This brings into the fore the issue of attribution which will be examined in the next section.

## 3. Attribution in Low-intensity Cyber Operations

[35] W. G. Sharp, *Cyberspace and the Use of Force* (Aegis Research cooperation, Falls Church, 1999) pp. 129 *et seq*.; E. T. Jensen, 'Computer Attacks on Critical State Infrastructure: A Use of Force Invoking the Right of Self-Defence', 38 *Stan. J.Int'l L.* (2002) p. 207, at pp. 221–229. *Contra* Y. Dinstein, 'Computer Network Attack and Self-Defence', in M. N. Schmitt and B. T. O'Donnell, *Computer Network Attack and International Law* (Naval War College, 2002) at p. 105

[36] *Gabčikovo-Nagymaros Project*, *supra* note 8, para. 83; ARSIWA, p. 169.

Attribution is the assignment of an act to a particular actor. Identifying the originator of a cyber operation is a very difficult exercise because of the anonymity, the speed and the multi-stage character of such operations. It has been stated elsewhere that attribution has a technical, a political and a legal aspect.[37] The legal aspect of attribution refers to the international law criteria according to which acts can be attributed to a State.

As far as countermeasures are concerned, attribution takes place according to the standards contained in the law of international responsibility. Accordingly, a low-intensity cyber operation will be attributed to a State if it is mounted by an organ of that State,[38] by a person or entity exercising governmental authority,[39] or by a State organ placed at the disposal of another State.[40] It will also be attributed to a State if it is mounted by a person or a group of persons under the direction or control of that State, by an insurrectional movement that becomes the government of the State[41] or by a person or a group of persons acting in default of official authorities. It will finally be attributed to a State if the latter adopts it as its own.[42] In all of these cases, the victim State can take countermeasures against the wrongdoing State but it should be noted that countermeasures do not need to be qualitatively equivalent. A State may thus respond to a wrongful low-intensity cyber operation by taking cyber or physical countermeasures.

Reprisals as was said belong to the use of force regime and attribution will take place according to that regime's standards. These standards have not been codified in any specific document but international lawyers often apply *in toto* the attribution standards found in the law of international responsibility to the use of force.[43] This is not entirely correct because

[37] N. Tsagourias, 'Cyberattacks, Self-defence and the Problem of Attribution', 17 *Journal of Conflict and Security Law* (2012) pp. 229–245.
[38] Article 4 ARSIWA.
[39] Article 5 ARSIWA.
[40] Article 6 ARSIWA.
[41] Article 10 ARSIWA.
[42] Article 11 ARSIWA.
[43] *Tallinn Manual*, *supra* note 1, Rule 6.

not all of these standards correspond to the needs and particularities of the use of force regime. As a matter of fact the ICJ has accepted in the *Bosnia Genocide* case that different regimes may have different attribution criteria. As it said, "logic does not require the same test to be adopted in resolving the two issues which are very different in nature".[44] This does not mean that the two regimes cannot share certain common standards. Where the use of force regime diverges from that of international responsibility is with regard to the level of control needed in order to attribute a use of force to a State. Whereas in the law of international responsibility effective control is the applicable standard as held by the ICJ in the *Nicaragua* case[45] and was later confirmed in *Bosnia Genocide* case,[46] in the use of force regime the effective control standard can apply to individuals and unorganised groups whereas for organised groups the overall control criterion is more useful. The overall control was introduced by the International Criminal Tribunal for the former Yugoslavia (ICTY) in the *Tadić* case. According to the ICTY, a State "wields overall control over the group, not only by equipping and financing the group, but also by coordinating or helping in the general planning of its military activity" and, in that case, "it is not necessary that, in addition, the State should also issue, either to the head or to members of the group, instructions for the commission of specific acts contrary to international law".[47] Overall control covers cases where a State exerts general influence over a group and its activities and is particularly suitable in the cyber context where States and cyber groups may collude in a variety of

[44] *Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia)*, [2007] *ICJ Rep.* 43, paras. 404–405.

[45] Article 8 ARSIWA; *Nicaragua* case, *supra* note 11, paras. 116–117; *Bosnia Genocide* case, *ibid.*, para. 398.

[46] *Bosnia Genocide* case, *ibid.*, paras. 402–406.

[47] *Tadić* Appeal, para. 131.

different ways. As the ICJ said in another instance when discussing attribution, it is important to "grasp the reality of the relationship between the person taking action and the state".[48]

In addition to overall control, toleration of non-State actors and of their harmful activities or and unwillingness to suppress their harmful activities are two other standards employed by the use of force regime.[49] They have been introduced in order to respond to the complexities of State collusion with terrorists or terrorist organisations. The '9/11' attacks were the catalyst in introducing the criterion of toleration and unwillingness to the use of force regime. The US for example used force by way of self-defence against Afghanistan because it "allow[ed] … parts of Afghanistan it controls to be used by this organization as a base of operation. Despite every effort by the United States and the international community, the Taliban regime has refused to change its policy".[50] This was endorsed by the Security Council in Resolutions 1368 (2001) and 1373 (2001). Likewise, the US action in Sudan and Afghanistan in 1998 was in reaction to prior uses of force by a non-State actor hosted and tolerated by these States. In the *Congo* v. *Uganda* case, the ICJ seems to have recognised toleration as a criterion for attributing uses of force to a State.[51] Consequently, if a State tolerates non-State actors that engage in forcible cyber activities against other States or is unwilling to suppress such activities, the resulting use of force will be attributed to that State.

---

[48] *Bosnia Genocide*, *supra* note 43, para. 392.
[49] Simma, *supra* note 24, p. 802.

[50] Letter dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council, S/2001/946 (2001) and Letter dated 7 October 2001 from the Charge d'affaires a.i. of the Permanent Mission of the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the President of the Security Council, S/2006/947 (2001).

[51] *Congo* v. *Uganda*, *supra* note 22, para. 301.

It follows from the above that only when the State is not implicated at all in the forcible cyber activities of non-State actors or when the State is unable to control their activities that the use of force will not be attributed to that State. The immediate question is whether the victim State can take reprisal action against the non-State actor. The fact that the cyber operation was mounted by a non-State actor does not change its character as a use of force and does not remove the injury that has caused on the victim State. However, the crucial question is whether the non-State actor has breached any obligation towards the victim State. In international law, the prohibition not to use force formally applies to the relations between States only. Non-State actors are not bound by the obligation not to use force. Consequently, one of the reprisal conditions –that there should be a breach of an international obligation – is not met. It should be recalled that, in contrast to self-defence whose legality as will be explained later is premised on a factual occurrence (an armed attack), reprisals have maintained their normative link to an antecedent illegality. Their legality in other words is premised not on a factual situation – the use of force – but on a legal one: the violation of the obligation not to use force.

At this stage, it will be useful to remind ourselves of how the law of self-defence evolved in this respect. Nowadays there is increased acceptance of a State's right to take direct self-defence action against non-State actors.[52] This is supported by the fact that the modern

[52] *Caroline* case, 30 *British and Foreign State Papers*, pp. 196–198; Simma, *supra* note 24, p. 799; Sep. Op. Higgins in *Palestinian Wall* Advisory Opinion, *supra* note 22, paras. 33–34; Sep. Op. Kooijmans, *ibid.*, paras. 35–36 and Decl. Burgenthal, *ibid*., para. 6. Sep. Op. Simma in *Congo* v. *Uganda*, *supra* note 22, paras 4–15; Dis. Op. Kooijman, *ibid.*, paras. 25–32; Diss Op. Kateka, *ibid*., para. 34; *Institut de Droit International*, Resolution 10A 'Present Problems of the Use of Armed Force in International Law: Self-defence' (10 October 2007), para. 10. With regard to US action in Northern Pakistan *see* 'Legal Adviser Koh's Speech on the Obama Administration and International Law, March 2010', <http://www.cfr.org/international-law/legal-adviser-kohs-speech-obama-administration-international-law-march-2010/p22300>. The ICJ however maintains that only

formulation of self-defence as enshrined in Article 51 of the UN Charter has been normatively decoupled from the illegality of the initial action. To explain, normatively, the use of force by way of self-defence is a reaction to a prior violation of international law involving the use of force. As Ago put it "acting in self-defence means responding by force to forcible wrongful action carried out by another, and the only reason why such a response is not itself wrongful is that the action which provoked it was wrongful".[53] That initial violation "is not only an extremely serious one but is also of a very special kind",[54] justifying thus forcible reaction. In the process, the unlawfulness of the prior use of force lost its significance in the legal construction of self-defence which is now premised on the existence of a prior factual situation in the form of an armed attack. Under this construction, the victim State can use force by way of self-defence directly against non-State actors because the self-defence action is justified by the existence of a prior armed attack and not by the existence of a prior violation incumbent on the non-State actor not to use force, an obligation which, as was said, does not extend to non-State actors according to current international law. Moreover, the incidental breach of the host State's sovereignty when the victim State acts in self-defence against the non-State actor hosted by that State is exonerated since, according to the law of State responsibility, self-defence is also a secondary rule and as such precludes the wrongfulness of the breach.[55]

It transpires from the precedent discussion that the consequences of a formalistic approach to the use of force by non-State actors are quite serious because these actors can use force against States with relative impunity. As a matter of fact, low-intensity cyber operations by

---

states can be the authors of an armed attack. See *Palestinian Wall* Advisory Opinion, *supra* note 22, para. 139; *Congo* v. *Uganda*, *supra* note 22, para. 146.

[53] A/CN.4/318/Add.5-7 (1980), para. 88
[54] *Ibid.*, para. 89.
[55] Article 21 ARSIWA.

non-State actors are more probable due to the limited resources required whereas an armed attack by a non-State actor is perhaps a remote possibility.

It is for this reason that I have argued elsewhere that, in view of the importance of the rule on the non-use of force and the ability and willingness of non-State actors to use force, the prohibition of the use of force should extend to non-State actors.[56] They should become addressees of the rule because of their 'actorness' in the international arena. If this interpretation of the rule on the non-use of force is accepted, a low-intensity cyber operation by a non-State actor involving the use of force will be a breach of its obligation towards the victim State. However, even in this case, the State cannot respond by taking direct reprisal action against the non-State actor because of the absence of an established rule or of supporting practice. Moreover, the acting State will violate the host State's sovereignty, a wrongful act that cannot be exonerated. It should be recalled that reprisals, as opposed to countermeasures, are not circumstances precluding wrongfulness.

Thus, with regard to low-intensity cyber operations by non-State actors amounting to a use of force, the victim State cannot target them directly with reprisals either because relevant international law obligations do not extend to non-State actors or because the reprisal action, even if it is in response to a prior breach by the non-State actor of its obligation not to use force, will violate the sovereignty of the host State which is not responsible for the wrong. Likewise, the victim State cannot resort to countermeasures against non-State actors either because there is no breach of obligations by the non-State actor or because countermeasures should be directed against the responsible State only.

---

[56] N. Tsagourias, 'Non-State Actors and the Use of Force', in J. D'Aspremont (ed.), *Participants in the International Legal System: Theoretical Perspectives* (Routledge, London, 2012) p. 326.

It transpires then that the victim State is faced with the dilemma of doing nothing and continue to be exposed to uses of force by non-State actors or respond in kind and expose itself to reprisals or countermeasures by the host State whose rights have been violated. International law does not provide any answer to the dilemma but any answer will be political. The only possibility that exists is for the Security Council to impose collective sanctions on non-State actors. The Security Council has such power when it determines that there is a threat to the peace, a breach of the peace or an act of aggression[57] and it has imposed sanctions on non-State actors in the past.[58] Additionally, the Security Council can take enforcement action.

**4. Proportionality in Countermeasures**

Proportionality is an essential condition in the law of countermeasures as well as of reprisals. Because countermeasures and reprisals are decentralised mechanisms of enforcing international law, proportionality plays a restraining function by curbing excessive responses because, as was observed by one of the ILC Rapporteurs, "[a]lthough less dramatic and harmful, such measures can be equally detrimental to the preservation of friendly relations and the development of cooperation among States".[59] Proportionality in other words mediates between unilateralism and legality. However, assessing proportionality is a rather difficult exercise. This is evident by the fact that very often it is the proportionality of

[57] Article 39 UN Charter.
[58] *For example* SC Res 684 (1993) and SC Res 1127 (1997) imposed sanctions on UNITA, the rebel force in Angola.

[59] Third Report on State Responsibility, UN Doc. A/CN.4/440 (l991), 18, para. 52.

countermeasures or reprisals that has been disputed even if their legality or legitimacy has been accepted.

One way of measuring proportionality is by establishing a degree of equivalence between the initial breach and the response. As the Arbitral Tribunal opined in the *Naulilaa* case "[e]ven if one admits that international law does not require that reprisals be measured approximately by the offence, one must certainly consider as excessive, and consequently illicit, reprisals out of all proportion to the act which has motivated them".[60] It was on that basis that it opined that the German reprisals were disproportionate.

Article 51 ARSIWA is more flexible when it comes to determining the proportionality of countermeasures. According to this provision, counter measures should be "commensurate to the injury suffered and take into account the gravity of the wrongful act and the rights in question". From that it appears that quantitative as well as qualitative factors[61] relating to the injured State, the wrongdoing State, third States and perhaps individuals affected but not injured by the countermeasure are taken into consideration.

For example, if a Denial of Service Attack (DDSA) on the on-line banking system of a State affects the on-line banking systems of neighbouring countries, this should be taken into account by the State taking countermeasures as should the effects of the DDSA on individuals. It should be remembered however that the main unit of assessment is the injury suffered and this is a delimiting factor when assessing the proportionality of countermeasures.

Is this however correct? Proportionality is a general principle of law and therefore of international law and in broad terms implies a two prong test: first, whether the measure

[60] *Naulilaa Incident* Arbitration, *supra* note 6, p. 1028.
[61] These may refer to the interests protected and the seriousness of the breach. Crawford, *supra* note 7, p. 296, para. 6.

pursues a legitimate aim and, secondly, whether the measure and the means used are excessive or unnecessary in relation to the objective being pursued.[62]

What is important therefore is to identify first the purpose of the countermeasure because that will be the primary referent point against which proportionality will be assessed. Article 49 ARSIWA defines the purpose of countermeasures in instrumental terms, namely, to induce a State to cease its wrongful conduct and provide reparation. If reparation is the objective of countermeasures, then the injury is the primary unit for assessing the proportionality of the countermeasure but if inducing compliance is also one of its aims, it may involve a higher amount of compulsion compared to the injury. This immediately defies the injury – response equivalence embodied in Article 51 ARSIWA. In the *Air Service Agreement* arbitration between the US and France, the tribunal concluded that the US countermeasures were not disproportionate even if their severity was greater compared to France's initial action. As it was observed, "the real insight of the *Air Service Agreement* award was that there had to be a permissible level of escalation in response to illegal acts, or else the malefactor would simply not regard the threats made by the injured state as credible".[63]

The ARSIWA seem to subordinate the purpose of countermeasures to the proportionality calculus when it asserts that proportionality is a limitation even on measures which may be justified under Article 49 and continues by saying that a disproportionate measure may well be judged as not being necessary to induce compliance.[64] The ILC's position perhaps stems from its fear –not at all unreasonable – that countermeasures may be abused. Moreover, even if the ILC narrowed down the purposes of countermeasures, it must have been aware of the

[62] *Sunday Times* v. *United Kingdom* (1979) 2 *EHRR* 245; Case C-331/88 *Fedesa* [1990] ECR I-4023 at 4063; "the principle of proportionality … requires that measures … do not exceed the limits of what is appropriate and necessary in order to attain the objectives legitimately pursued by the legislation in question when there is a choice between several appropriate measures recourse must be had to the least onerous, and the disadvantage casued are otto be disproportionate to the aims pursued".
[63] D. J. Bederman, 'Counterintuiting Countermeasures', 96 *AJIL* (2002) p. 817, at p. 820.
[64] Crawford, *supra* note 7, p. 296, para. 7.

fact that countermeasures have always served other purposes in addition to inducing compliance and receiving reparation.[65] Depending on the declared or undeclared purpose of countermeasures, proportionality may acquire different scope. Such a graded view of proportionality in the context of countermeasures has been advocated for example by Cannizzaro. Proportionality for him has an external dimension that is about the appropriateness of the aim and function of the countermeasure as well as an internal one which is about the appropriateness of the measure in view of the result. According to Cannizzaro[66] the external proportionality of countermeasures can be assessed against their normative, retributive, coercive and executive function. Countermeasures with a normative function aim to re-establish the legal balance of the parties involved. Countermeasures with retributive function aim at inflicting a certain cost on the wrongdoer. Coercive countermeasures aim at inducing the wrongdoer to reverse the effects of its wrongful conduct and to comply with its obligation. Executive countermeasures aim at wiping out the adverse effects of the breach and securing unilaterally the benefits that would derive from the infringed obligation even without the cooperation of the wrongdoing State.

This view is shared by the present writer as far as countermeasures are concerned but it is also contended that a more nuanced view of proportionality is needed in the context of reprisals. Traditionally, reprisals have fulfilled many different purposes such as deterrence, protection, retribution, coercion or reparation and therefore proportionality should be assessed accordingly.[67] In this regard it should also be noted that linking the proportionality of a forcible measure to its goals is prevalent in the use of force regime. To give an example, it is widely accepted that the use of force by way of self-defence can be quantitatively larger

[65] "[N]o Countermeasure fulfils in reality only one function. Punitive, protective and reparative elements are mixed in the considerations of the author State and in the perception of the object State …'. K. Zemanek, 'The Unilateral Enforcement of International Obligations', *ZAORV* (1987) p. 32, at p. 35.
[66] E. Cannizzato, 'The Role of Proportionality in the Law of International Countermeasures', 12 *EJIL* (2001) p. 889
[67] E. S. Colbert, *Retaliation in International Law* (King's Cross Press, New York, 1948) pp. 60–103.

than the initial armed attack because its aim is to repel the attack and its proportionality should be commensurate to its capacity to achieve that result.[68]

The second test of the proportionality calculus concerns the suitability of the measure and of the means used to achieve the aim. Means do not necessarily need to be qualitatively similar to the initial act and therefore a State may respond to low-intensity cyber operations with cyber or physical means. That said, countermeasures should involve non-forcible measures whereas reprisals involve armed means.

There are two other issues concerning proportionality that need to be mentioned. First, in the context of low-intensity but repeated cyber operations, proportionality may be assessed against the cumulative effect of said operations. Repeated cyber operations involving the use of force may cross the threshold of an armed attack in which case the victim State can use force by way of self-defence. The proportionality of the self-defence action will then be assessed against its aim as explained above. As Ago put it, "the requirement of proportionality will certainly not mean that the victim State is not free to undertake a single armed action on a much larger scale in order to put an end to this escalating succession of attacks".[69] Yet, even if such operations do not rise to the level of an armed attack, a State may react to repeated low intensity cyber operations through a single act of reprisal or through countermeasures whose proportionality will be assessed against the cumulative effect of the prior operations as well as against the aims pursued by the reprisal or countermeasure.

Secondly, because of the fluidity of cyber operations, the lack of territorial grounding and the difficulties in identifying the authors of the attack, it has been suggested that reciprocal

[68] According to Ago, "[t]he action needed to halt and repulse the attack may well have to assume dimensions disproportionate to those of the attack suffered. What matters in this respect is the result to be achieved by the "defensive" action, and not the forms, substance and strength of the action itself." A/CN.4/318/Add.5-7 (1980), para. 120. M. S. McDougal and F. P. Feliciano, *Law and Minimum World Public Order: The Legal Regulation of International Coercion* (Yale University Press, New Haven, 1961) pp. 222–224; Dinstein, *supra* note 30, pp. 262–267; J. Gardam, *Necessity, Proportionality and the Use of Force by States* (Cambridge University Press, New York, 2004) pp. 160–161; Dis. Op. Judge Schwebel, in *Nicaragua* case, *supra* note 11, p. 368.
[69] A/CN.4/318/Add.5-7 (1980), para 121. Dinstein, *supra note 30,* 255

countermeasures are most suitable and, perhaps, more effective in the cyber context.[70] Reciprocal countermeasures are "countermeasures which involve suspension of performance of obligations towards the responsible State if such obligations correspond to, or are directly connected with, the obligation breached", and according to the ILC's commentary "countermeasures are more likely to satisfy the requirements of necessity and proportionality if they are taken in relation to the same or closely related obligation".[71] Whether reciprocal countermeasures, for example a denial of service attack (DDSA) against a previous DDSA would satisfy without more the proportionality criterion is conjectural and subject to many different factors such as the extent and density of a State's cyber infrastructure.[72] Moreover, proportionality is a wider concept than reciprocity, and it is not only about the nature of the measure. Even in the case of reprisals where action and reaction are qualitatively similar, in that they are both uses of force, the proportionality calculus takes into account other criteria as explained in this section.

### 5. Countermeasures by Third States and Countermeasures Affecting Third States

Can third States take countermeasures against a State that has launched a low-intensity operation against another State? In principle, third States cannot take countermeasures against the responsible State.[73] However the ILC has recognised the situation where third States can react to illegality. According to Article 48 ARSIWA any State other than the injured State can invoke the responsibility of another State if the obligation breached is owned to a group of States including that State and is established for the protection of a collective interest.

[70] O. A. Hathaway *et al.*, 'The Law of Cyber-Attack: Governing Legal Frameworks and How To Strengthen Them', 100 *Calif. L. Rev*. (2012) p. 817, at p. 858; Office of Gen. Counsel, Dep't of Def., An Assessment of International Legal Issues in Information Operations, 20 (1999), <http://cyber.law.harvard.edu/cybersecurity/An_Assessment_of_International_Legal_Issues_in_Information_Operations>.
[71] Crawford, *supra* note 7, p. 282, para. 5.
[72] K.C. Hinkle, 'Countermeasures in the Cyber Context: One More Thing to Worry About', 37 *The Yale Journal of International Law Online* (2011) p. 1, at pp. 19–21.
[73] *Nicaragua* case, *supra* note 11, para. 249.

Moreover, according to Article 54 ARSIWA, any State within the meaning of Article 48 ARSIWA can take 'lawful measures' against the wrongdoing State to ensure cessation of the breach and reparation in the interest of the injured State. An example is the prohibition of the use of force in the UN Charter which is for the protection of a common interest that of peace.

The question however is whether 'lawful measures' refer to countermeasures. The phrase is ambiguous, but if read in the context within which it is used, it can be reasonably inferred that it refers to countermeasures. The ILC was ambivalent in its terminology because it was not satisfied that there was sufficient State practice in this regard. It mentioned the measures taken by the European Union (EU) against Iraq following the invasion of Kuwait as well as the measures taken against Yugoslavia in view of the human rights violations committed in that country during the armed conflict in the 1990s.[74] A more recent example of such measures are those taken by the EU in response to Iran's development of nuclear capabilities[75] because "Iran continues to refuse to comply with its international obligations and to fully co-operate with the IAEA to address the concerns on its nuclear programme, and instead continues to violate those obligations".[76] Yet, according to the ILC's commentary, the availability of countermeasures in such cases is left to the future development of international law because the existing practice is scarce and mainly limited to Western States.[77] Against this, it has been argued that there is indeed sufficient practice to support the view that States can take countermeasures against third States when they violate obligations owned collectively or when they violate obligations owned to the international community and such practice is not confined to Western States only.[78]

---

[74] *Ibid.*, pp. 302–305, paras. 3 and 4.
[75] Council Decision 2012/35/CFSP of 23 January 2012; Council Regulation (EU) No 267/2012 of 23 March 2012.
[76] EU Council conclusions on Iran (3142th Foreign Affairs Council meeting, Brussels, 23 January 2012) para. 2.
[77] Crawford, *supra* note 7, pp. 302–305.
[78] L. A. Sicilianos, 'Countermeasures in Response to Grave Violations of Obligations Owed to the International Community', in Crawford, Pellet and Olleson , *supra* note 12, pp. 1137 *et seq.*

Be that as it may, even if countermeasures by third States are permitted in those cases mentioned by Article 48 ARSIWA, this does not extend to reprisals. There is no relevant practice or *opinio juris* to support the view that third and non-injured States can resort to reprisals against the wrongdoing State. The only possibility of collective reaction is either on the basis of collective self-defence if the cyber operation rises to the level of an armed attack[79] or collective action on the basis of Security Council authorisation.[80]

Another issue that is left undecided is whether reactions to such violations by third States should be channelled through institutions or whether third states can act unilaterally. The latter option entails risks whereas the former may stumble at multiple hurdles.

A different issue is whether countermeasures against a responsible State which affect other States and breach obligations owned to those States are lawful.[81] This is critical in the cyber context because, due to its interconnectedness, cyber countermeasures could incidentally and inadvertently affect third States. Although such countermeasures are lawful as far as the wrongdoing State is concerned, they may violate obligations owned to third States. Moreover, the exonerating effect of the countermeasure does not extend to third States.[82]

The immediate question is whether such countermeasures become illegal *ab initio* and therefore lose their character as a countermeasure. Countermeasures with the exception of those referred to in Article 48 ARSIWA operate in a bilateral framework involving, on the one hand, the wrongdoing State that is responsible for the breach and, on the other, the injured State which reacts to the breach. In the situation under consideration, there are two sets of bilateral relations: the first is between the State responsible for the initial wrongful act and the injured by that act State that resorts to countermeasures and the second is between the

[79] Article 51 UN Charter.
[80] Chapter VII UN Charter.
[81] M. N. Schmitt and M.C. Pitts, 'Cyber Countermeasures and Effects on Third Parties: The International Legal Regime', 14 *Baltic YBIL* (2014) .
[82] Crawford, *supra* note 7, p. 285, para. 4.

latter State and the third State injured by those countermeasure. These set of relationships give rise to different legal consequences if one also bears in mind that the obligations involved may also differ. As a result, whereas the countermeasures in the first instance are lawful provided of course that they satisfy all the other conditions, they are unlawful *vis-à-vis* the third State. The third but injured State may resort to countermeasures unless the responsible State ceases the violation and makes reparation. The reparation will cover any material or moral damage arising as a consequence of the act unless it has been too remote and unforeseeable.[83]

Countermeasures may also affect the rights of individuals located in the affected third State. For example, they may affect among others their human rights to have access to information, their right to privacy or their right to freedom of expression. However, the responsible State does not owe them any obligation, and therefore it does not breach any of their rights. The responsible State does not also breach any obligation towards the third State under whose jurisdiction those individuals reside. The immediate question is whether the affected individuals have been placed under the jurisdiction of the reacting State in relation to the countermeasure. It should be recalled that tuman rights obligations are owned by states *vis-à-vis* individuals under their jurisdiction. Human rights treaties extend a State's jurisdiction extraterritorially if the State exercises authority and control over individuals.[84] In so far as countermeasures have some physical element of authority and control, for example by injuring an individual, one may say that the State's jurisdiction extends to that individual. Such authority and control may be more difficult to establish if the countermeasure is purely cyber, although the concept of virtual control has also been introduced.[85] It has also been

[83] Crawford, *supra* note 7, para. 10; Eritrea-Ethiopia Commission, Decision No. 7, paras. 7–14.
[84] *Lopez-Burgos* v. *Uruguay*, Communication No. R.12/52, UN Doc. Supp. No. 40 (A/36/40) (1981), paras. 12.2–12.3; *Al-Skeini and others* v. *United Kingdom* [GC], App. No. 55721/07, 7 July 2011, para. 75.
[85] P. Margulies, 'The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism', 82 *Fordham. L. Rev* (2014) p. 2137. SSRN draft available at <http://ssrn.com/abstract=2383976>.

argued that extraterritorial jurisdiction is based on a State's positive obligation to respect human rights and its negative obligation to ensure respect of human rights.[86] The latter obligation is not territorially limited since a State can always prevent its organs or agents from violating human rights. Yet, even if individuals residing in a third State are placed under the jurisdiction of the responsible State on the grounds mentioned above, the violation of their rights will give rise to human rights litigation. Individuals cannot take countermeasures against States. It is only their State of nationality that may be able to take countermeasures in relation to such breaches if it exercises diplomatic protection in which case the wrongdoing State's duties are owned not to the individual but to her State of nationality.

## 6. Conclusion

From the preceding discussion it can be concluded that countermeasures are international law remedies against low-intensity cyber operations. Countermeasures are acts of self-help to enforce international obligations that compensate for international law's weak mechanisms of institutional enforcement. Yet, countermeasures conceptualized by the ILC in its Articles on the Responsibility of States as peaceful measures may not be able to deal effectively with cyber operations involving the use of force. It is for this reason that the author of this article is of the opinion that reprisals should attain full legal recognition in contemporary international law. Such a view is supported by relevant State practice as well as by academic and judicial opinion.

A problem that international law constantly fails to address and by not addressing it exposes itself to accusations of inadequacy or even irrelevance concerns the place of non-State actors in international law and more particularly in the use of force regime. Although there have

---

[86] M. Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (Oxford University Press, Oxford, 2011).

been some developments in the area of self-defence, these development have not extended to countermeasures or reprisals. It thus appears that non-State actors are not independently bound by international law although they may be the main authors of low-intensity cyber operations. One way of dealing with this problem is to expand the circumstances under which their acts can be attributed to a State but this cannot address the problem sufficiently. It is therefore imperative for international law to tackle this problem directly. Another problem that countermeasures or reprisals in the cyber context give rise to concerns their effects on third States and individuals. This implicates a host of legal issues which cannot be dealt with solely by the law of countermeasures. It is also something that depends on advancements in cyber technology.

That said, it should be noted that the problems highlighted above are not peculiar to the cyber context but perhaps the cyber context exacerbates any legal uncertainty that may exist and puts more pressure on international rules and principles.