OPINIO JURIS
LAW & POLITICS REVIEW

Cyber Operations in International Law.

ICT Misuses as a Threat to International Peace and Security.

Annachiara Rotondo

Cyberspace still constitutes a volatile ad unsafe domain because of its technical peculiarities, but this circumstance does not impede States from using it as an alternative battlefield, functioning both in peace time and in war time.

The reason is that cyber operations allow States to gain strategic and political results surgically and silently, i.e. avoiding collateral effects, also in terms of international exposure.

However, international law still does not provide so far any regulation in the field of computer-offences; indeed, the only legally binding multilateral instrument in force dealing with cyber operations is the 2001 Budapest Convention on Cybercrime which concerns exclusively cybercrimes by and against individuals[1]. Consequently, expressions like cyber attack, computer offences or ICT (mis)uses seem to be still neutral since these conducts have not been yet legally qualified by international law notwithstanding their strong negative characterisation from the political perspective. Then the point is whether cyber operations can be fully lawful when they are so politically questionable.

[1] CoE, Convention on Cybercrime, 2001, ETS No.185.

ISSN 2531-6931

Some scholars dealt with the theme of ICT (mis)uses trough the legal categories of unlawfulness, so referring to wrongful acts when cyber operations consists in breaches of international obligations[2], and to acts of aggression when effects of cyber-attacks may be comparable to those deriving from a conventional (military) aggression[3]. However, these attempts, although offer *prima facie* interesting solutions in terms of reactions on the part of the target State, do not seem suitable primarily because cyber offences are rarely attributable to a State, thus excluding any possibility of concrete reactions because each kind of response provided by international law presupposes the attribution of the unlawful conduct to another State.

On the contrary, other scholars retain that the negative political impact of ICT misuses could amount to a threat to international peace and security accordingly to Art. 39 of the United Nations Charter. This approach seems convincing, at least *in abstracto*, especially considering that the determination of a threat to peace has mainly a political nature. Under Art. 39 the stamp of "threat to peace" can be put only by the UNSC which, as it is well known, is responsible for maintaining international peace and security within the context of the United Nations collective security system. In ascertaining the existence of a threat to peace the Security Council enjoys considerable discretion, being able to include also situations not necessarily characterized by the use of military force. Indeed: "(t)*he absence of war and military conflicts among States does not in itself ensure international peace and security*. (So) *the*

[2] *Inter alia* SCHMITT M. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge, 2017, p. 79 ff.; WĘGLIŃSKI K., *Cyberwarfare and Responsibility of States*, in Torun International Studies, 2016, No. 1 (9), pp. 79–86; SHACKELFORD, *State Responsibility for Cyber Attacks: Competing Standard for a Growing Problem*, Conference on Cyber Conflict Proceedings 2010 C. CZOSSECK AND K. PODINS (Eds.) CCD COE Publications, 2010, Tallinn, Estonia.

[3] *Inter alia* DELERUE F., *Cyber Operations and International Law*, Cambridge, 2020, p. 328; Cameron H. Bell, *Cyber Warfare and International Law: The Need for Clarity*, in Towson University Journal of International Affairs, VOL. LI, NO. 2, 2018, p.22 ss.; ROSCINI M., *Cyber Operations and the Use of Force in International Law*, Oxford, 2014, p. 43 ff.

non-military sources of instability in the economic, social, humanitarian and ecological fields have become threats to peace and security"[4].

Actually, practice has illustrated over the years that the notion of threat to peace can be extended to any violation of an essential obligation for the safeguarding of the fundamental interests of the international community, such as nuclear proliferation [5] or the violation of democratic principles[6]. In addition, in evaluating possible threats the UNSC seems to take into consideration not only crisis situations between two States, but also those arising within the territory of a single State if able to affect international peace and security[7] .

So, considering the wide range of discretionary power UNSC enjoys in ascertaining the existence of a threat to peace and that to date cyber-operations consist in one of the most important reasons of the contemporary international in-stability, the concept of threat to peace seems to may embrace also some ICT misuses[8].

The main task of this paper is to verify international legal basis for a possible theory of a cyber-threat to peace, in order to suggest a feasible international legal framework.

Starting from the analysis of Art. 39 of UN Charter, the work will examine the practice of the UNSC and prospect possible measures against ICT misuses constituting a cyber-threat to international peace and security.

Under international law the concept of peace has been broadly interpreted because, both in the UN Charter and in the practice of UNSC, it has been linked to the existence of numerous and different conditions, such as the maintenance of friendly relations among States, the full respect of human rights, the absence of violence, as well as the respect of democratic principles, which are void of a common denominator.

---

[4] SIMMA B., KHAN D., NOLTE G., PAULUS A., *The Charter of the United Nations: A Commentary*, CH. VII, Art. 39, Oxford, 2012, § 8.

[5] SIMMA B., KHAN D., NOLTE G., PAULUS A., cit., § 16.

[6] *Ibidem*, § 28.

[7] LEANZA U., CARACCIOLO I., *Il diritto internazionale: diritto per gli Stati e diritto per gli individui,* Giappichelli, Torino, 2012, pp. 404-408.

[8] HENDERSON C., The Use of Force and International Law, 2018, Part II, § 2.1.1.

ISSN 2531-6931

Consequently, also the scope of the concept of threat to peace has been subjected to an equally wide interpretation, referring to a mere generic idea that a threat, whatever it is, may have destructive effects on international peace and security. Thus, under the Charter, the UN Security Council enjoys considerable discretion in ascertaining the existence of a threat to peace and choosing adequate measures to contain possible escalation of threats. The discretion of the Council is such that it is neither obliged in ascertaining a threat to peace, being only empowered by Art. 39 of the Charter, thus meaning that the final choice derives from a juridical/political balance based on a case by case subjective evaluation.

It is incontrovertible that a threat to peace occurs in case of imminent attacks preluding an armed conflict, as well as in the case of post-conflict situations when there are real risks of a "renewed eruption of violence", but looking at UNSC practice also weapons proliferation[9], terrorism[10], illicit exploitation of natural resources[11] have reached the threshold of a threat to peace.

So due to the broad margin of interpretation of the concept of threat to peace as well as the discretion UNSC enjoys under Art. 39[12], it seems correct, even if only *in abstracto*, to speculate on the possibility that determined (mis)uses of ICT may constitute a threat to peace, also when these misuses do not reach the threshold of an international wrongful act[13]. Indeed, UNSC practice shows that the declaration of a threat to peace is not anchored to the fact that a violation of international law occurred because the rationale of the UN collective security system is to provide preventive tools for the maintenance of

[9] SIMMA B., KHAN D., NOLTE G., PAULUS A., cit., §§ 16,17.
[10] SIMMA B., KHAN D., NOLTE G., PAULUS A., cit., § 18.
[11] SIMMA B., KHAN D., NOLTE G., PAULUS A., cit., § 31.
[12] *Inter alia* De Wet E., *The Chapter VII Powers of the United Nations Security Council*, Hart Publishing, Oxford, 2004, p. 139.
[13] ROBINSON M., JONES K., JANICKE H. AND MAGLARAS L., *An Introduction to Cyber Peacekeeping*, in Journal of Nerwork and Computer Impications, april 2018.

international peace and not to react against violations of international law[14].

If UNSC usually ascertains and declares a threat to peace with reference to very specific crises' scenarios that are territorially circumscribed, the cases of proliferation of weapons of mass destruction and international terrorism prove that Council's determinations can be referred also to transboundary and generic threats as the cyber threat.

Concerning proliferation and arms control, since 1992 the Security Council have declared that "the proliferation of all weapons of mass destruction constitutes (*per se*) a threat to international peace and security" even outside a crises situation[15] and in the Resolution n. 1467 of 2003 the Council affirmed also that trafficking in small arms by non-State actors reach the threshold of a threat to the regional peace in Africa.

So, if the mere trafficking in arms constitute a threat to peace under Art. 39 questions arise to weather cyber weapons can be considered as veritable arms and so be included in the scope of the Resolution, especially those cyber tools capable to determine indiscriminate physical damages on large scale (as *Stuxnet)* and when utilized for terrorist purposes. Actually, among authors there are some attempts of analogy between cyber weapons and weapons of mass destruction based on the conviction that both types of weapons may produce equal effects[16]. However, this analogy, although suggestive, is devoid of a concrete legal basis because it is anchored exclusively to a doctrinaire assumption: i.e. the s. c. "effect based approach".

Furthermore, the Council clearly affirmed in the Resolution n. 1373 of 2001that also "terrorism in all its forms and manifestations" (UN Doc S/Res/1373, 2001) constitutes a threat to peace under Art. 39.Then the point is whether cyber-terrorism is included in the scope of the

---

[14] SIMMA B., KHAN D., NOLTE G., PAULUS A., cit., § 10.

[15] UN Doc S/23500, 1992, UN Doc S/Res/1540, 2004; UN Doc S/Res/1977; UN Doc S/Res/1172 on Pakistan, 1998; UN Doc S/Res/1718 on North Korea, 2006.

[16] SHACKELFORD J. (2009), *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, in Berkeley Journal of International Law, Vol.27, Issue 1,195, 220.

ISSN 2531-6931

Resolution; in this respect UN's position seems favourable. Indeed, in 2015 the Group of Governmental Experts, established by the UN General Assembly for assessing Developments in the Field of Information and Telecommunications in the Context of International Security - affirmed in its official Report that "(t)he use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security". *Inter alia*, the connection between cyber tools and terrorists has been pinpointed by the UNSC with reference to the fight against terrorism when, in 2007, it underlined the urgency of protecting critical infrastructures through strategies of cybersecurity in order to prevent and contrast terrorist attacks (S/Res/2341, 2017).

If on one hand "it is incontrovertible that the UNSC has the authority" to determine that a given use of ICT constitutes a threat to the peace, on the other it is not so clear which peculiarities the cyber-operations must have to reach the threshold of a threat to peace.

Additionally, further doubts rise with reference to the possibility of a UNSC action against cyber-operations striking only individuals and not States security, because cases in which the Council acts to protect population are limited to serious violations of human rights, large scale organized violence and war crimes.

Moreover, the fact that the Council acted also with regard to pure internal situations capable to have an impact at international level allows in sustaining that the Council could intervene also when cyber-operations do not assume an international dimension. However, on this point it is not very clear if transboundary consequences and risks are requested to justify an intervention by the UNSC under art. 39,

especially considering that practice shows that only few times the Council has acted in presence of limited transboundary implications[17]. Notwithstanding doubts deriving from the circumstance that so far the Council has never determined that a cyber operation constitutes a threat to the peace the theory of a cyber threat in the terms of Art. 39 is persuasive.

Even if the UNSC has never declared a cyber-attack as a threat to peace, it is undeniably empowered to do so, especially since any specific circumstance has to occur to raise a certain act to the level of a threat to the peace.

Hypothetically speaking, in the case a cyber-threat to international peace occurs, having been declared as such by the UN Security Council, the UN Charter offers several options for containing and defeating the threat pursuant to articles 40 - 42. The latter provides enforcement measures, including the use of military force, characterized by the fact that they are carried out against the will of the State concerned. Indeed, if the State agrees with the use of force on its territory it makes the recourse to art. 42 legally unnecessary. This peculiarity limits the operability of art. 42 only to those situations in which the State openly contrasts the decision of the Council: an improbable hypothesis in the case of cyber threats considering that cyber-attacks are often (if not always) committed by private individuals with respect to whom States avoid to show any possible link, in order to escape any legal consequence in terms of responsibility. *Inter alia*, enforcement actions under art. 42 do not constitute a feasible option for response against cyber-threats also because on the basis of the principle of proportionality (which applies also in the case of measures under discussion) military force could be allowed only against cyber-attacks determining same effects of an armed attack, but, looking at the practice, except the isolated *Stuxnet* case, a cyber-attack has never been comparable, with regard to its effects, to an armed attack. On the contrary, measures provided by art. 41 seem more suitable in the cyber

[17] SIMMA B., KHAN D., NOLTE G., PAULUS A., cit., § 20.

ISSN 2531-6931

context, firstly because they never entail the use of military force. These measures are mandatory, capable to override obligations previously assumed by UN Member States and can be address against States and non-State actors: a valuable peculiarity considering the "private" nature of most cyber-operations.

Actions under Art. 41 are numerous and not limited to those listed in the Charter, e. g. they can be: embargoes, trade restrictions, interruption of means of communication, severance of diplomatic relations, creation of special Tribunals, but also targeted sanctions against private individuals deemed responsible for a threat to peace. Among actions UNSC can adopt "(t)he …'complete or partial interruption of… postal, telegraphic, radio and other means of communication' …is especially important in the cyber context" [18], even if historically UNSC avoided from intervening in the field of communications because of the involvement of human rights' protection (e.g. the freedom of expression).

In addition, sanctions against individuals also can play an essential role because "the private nature of most cyber-operations". The main categories the UNSC has developed in this respect… are financial sanctions against targets listed by the Council or identified by a sanctions committee of the Council that, for purposes under discussion, can be the main stakeholders of cyberspace as: Internet providers, intermediaries, hackers etc.

Considering the broad margins of Art. 39 of UN Charter as the hybrid nature of the cyber threat the theory of a "cyber threat to peace" seems to be at least suitable for international law. However, if a theory of cyber threats to peace seems the more feasible under international law, at the same time it strongly limits the possibilities of response entrusting the power of reaction in the solely figure of UNSC. Indeed, as it is well known, procedural obstacles to the action of the Council,

[18] SCHMITT M. (ed.), *Tallinn Manual 2.0*, *cit.*, p.358.

consisting in the presence of permanent members with the veto power, still affect the outcome of its decisions. Considering that some of permanent members are the main worldwide actors within cyberspace, is conceivable that whenever a cyber threat arise the Council will be refrain to take a determination.