Reflections on due diligence duties and cyberspace

Kolb, Robert

Reflections on Due Diligence Duties and Cyberspace

ROBERT KOLB*

ABSTRACT: This contribution analyses under different angles due diligence duties of States in the context of cyberattacks and cyberwarfare. After having discussed the historical evolution and peculiar content of due diligence, it tries to identify particular problems of the cyberspace in the context of the duties of prevention and suppression by States.

KEYWORDS: Due Diligence, Standard of Care, State Responsibility, Cyberspace, Cyberwar, CyberAttacks, Duty of Prevention, Duty of Cooperation

I. Introduction

During the conference which gave rise to the contributions of the present publication, I raised a series of questions on legal challenges and the cyberspace outside the context of armed conflicts. I did not provide any answers, for lack of technical knowledge of the cyber-realities. Lawyers come here quickly to their limits, as they lack the proper technical tools to assess what legal principles and rules fit the realities of cyber. In the present short text, I would like to take up only one question I had raised, and also to venture into some short analysis. The question turns around the concept of the due diligence obligations of States for activities in areas under their control and the scope it could be given in the context of that very particular space that is 'cyberspace'. I must confess that my technical knowledge of the cyberspace has not increased since the conference last year. The answers given can therefore only be at once tentative and generic. They would have to be refined in the light of tighter knowledge of and consideration of shifting technical realities.

* Professor of Public International Law at the University of Geneva.

II. The Notion of Due Diligence[1]

A. Historical Roots

Historically, the term 'due diligence' first appeared in the context of the law of neutrality in the 19th century. It was framed in the famous *Alabama Claims Arbitration.*[2] Previously, the notion had not been shaped as such. The civil law term of 'negligence' had appeared to be sufficient. In the mentioned arbitration, the question revolved around the duties of a neutral State not to allow the construction and arming of warships on its territory, when these ships were to participate in an armed conflict. The term of due diligence was inserted in the special agreement on the basis of which the Tribunal had to pronounce. In their decision, the arbitrators emphasised that the diligence due is in direct proportion to the dangers the belligerents run as a consequence of the omission and of the means a neutral State possessed to curb such private activities on its territory.[3] The term of due diligence was however also avoided in some important conventions of the same period. Thus, in Article 8 Hague Convention XIII of 1907 concerning the Rights and Duties of Neutral Powers in Naval War[4] the formulation is rather that

> [a] neutral Government is bound to employ the means at its disposal to prevent the fitting out or arming of any vessel within its jurisdiction which it has reason to believe is intended [...] to engage in hostile operations, against a Power with which that Government is at peace.[5]

The material and concrete possibilities of the State are here envisaged, but without the term of due diligence, which was judged to be too obscure.

---

[1] See the literature indicated in: *Timo Koivurova,* Due Diligence, in: Max Planck Encyclopedia of Public International Law, Vol. III (2012), 236, 246. See also *Paulos Alexandrou Zannas,* La responsabilité internationale des Etats pour des actes de négligence (1952).

[2] See *John Bassett Moore,* History and Digest of the International Arbitrations to which the United States has been a Party, Vol. 1 (1898), 495.

[3] The Tribunal stressing mainly the first aspect of the obligation, *ibid.,* 654–655.

[4] Hague Convention (XIII) concerning the Rights and Duties of Neutral Powers in Naval War, 18 October 1907, available at: https://www.icrc.org/applic/ihl/ihl.nsf/INTRO/240 (accessed on 16 October 2015).

[5] See *Dietrich Schindler/Jiři Toman,* The Laws of Armed Conflicts (4th ed. 2004), 1409.

B. Standard of Care

The due diligence formula is based on a standard of care. It is ordinarily engrafted upon a standing primary obligation under international law and can also be considered, in some cases, as a freestanding obligation of its own. In international case law, such standards of care, whether called due diligence or not, have often been mentioned since times long past. Most often, they were formulated in the context of insurrection or other situations in which foreign citizens suffered damage on the territory of a State. In the *Baldwin* case (1841), the point was to determine whether the government of Mexico had used all the means at its disposal in order to prevent the damage to foreigners from occurring.[6] In the *Prats* case (US/Mexico Claims Commission, 1868), the fulfilment of certain obligations was linked to the extent of the means available and the use of all the means effectively available[7] (*ad impossibile nemo tenetur*). In the *Spanish Zone of Morocco Claims* (1925), arbitrator *Max Huber* linked the diligence required to the means a State can dispose of. The State is not required to use means it does not possess, since that would go beyond what could be reasonably expected from it.[8] Use of all 'means at the disposal' seems to be one key requirement. It has since remained the controlling consideration. Thus, in the *Genocide* case (2007), the International Court of Justice (ICJ) considered the extent to which a State could and should act in order to prevent genocide on the territory of another State when committed by armed groups over which it displayed a degree of control, allowing influence. The Court said that what is crucial is the material capacity to influence the action of the group[9] – once more the criterion is that of the available means. Which means are available is a concrete question which has to be decided on the basis of the relevant circumstances in each case.

---

[6] *Albert Geouffre de Lapradelle/Nicolas Politis,* Recueil des arbitrages internationaux (1905), 465.

[7] *Moore* (note 2), 2893–2894.

[8] *Affaire des biens britanniques au Maroc espagnol* (Spain, Great Britain), Arbitral Award of 1 May 1925, Reports of International Arbitral Awards (RIAA) II, 644.

[9] International Court of Justice (ICJ), *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia and Herzegovina *v.* Serbia and Montenegro), Merits, Judgment of 26 February 2007, ICJ Reports 2007, 43, para. 221.

C. Definition of Due Diligence

Undue diligence is the existence of an unlawful negligence; conversely, due diligence is the absence of such a negligence. The judgement thus goes to a legally imputable difference between a conduct such as it has been and a conduct such as it should have been. The difference is based legally on the required diligence, which would, if followed, have avoided the gulf between both situations. In turn, this difference is necessarily based on a value judgement of what should reasonably have been done. Hence the definitions of (un)due diligence provided by different authors: "omission of the required standard of care";[10] "care that should have been used according to the circumstances";[11] "neglect [...] to take all reasonable measures";[12] "necessary efficiency and care";[13] "blameworthiness due to negligence";[14] *etc.* From the foregoing, it follows that: (i) due diligence is a normative prescription of a required care, it is not simply a descriptive device summing up a point of fact; (ii) due diligence is a standard of care, a general clause, not a specific rule to be immediately applied; it requires a judgement of value of what could and should have reasonably be done under the circumstances; due diligence is thus often directly linked to the concept of reasonableness, in German of *Zumutbarkeit,* and possibly also with *bona fide* duties; (iii) due diligence is essentially linked with negligence and sometimes with the maxim that the impossible cannot be required (*ad impossibile nemo tenetur*); (iv) due diligence is a relative and circumstantial term, since the judgement on it must take account of all the circumstances of the particular case; judgement thus always takes place *in concreto;* the judgement is also necessarily flexible; (v) due diligence is normally contained in primary norms requiring such a diligence, *e.g.* with respect to damages done to aliens on the territory, transboundary pollution, *etc.,* but it can also accompany any primary norm (if international

[10] *Karl Strupp,* Die völkerrechtliche Haftung des Staates, insbesondere bei Handlungen Privater (1927), 31.

[11] *Anton Roth,* Das völkerrechtliche Delikt vor und in den Verhandlungen auf der Haager Kodifikationskonferenz 1930 (1932), 177.

[12] International Law Commission (ILC), State Responsibility: Report, Yearbook of the International Law Commission, Vol. II (1956), 173, 222.

[13] *Francisco V. García-Amador/Louis Bruno Sohn/Richard Reeve Baxter,* Recent Codification of the Law of State Responsibility for Injuries to Aliens (1974), 26–27.

[14] *Koivurova* (note 1), 236.

practice establishes that) or constitute a secondary norm of State responsibility (*e.g.* the duty to mitigate the damages suffered).

D. Elements of Due Diligence

There are at least two controlling elements in any due diligence equation. The first relates to the need of a minimum of proper organisation of the State, so that it is able to face its various duties under public international law.[15] A State is not entitled to justify a lack of proper diligence by pointing to an insufficiency of legal or organisational means which are imputable to it as a culpable lack of care. To the same extent that a State may not decline international responsibility by referring to its internal laws, it also cannot escape its due diligence duties by pointing to its internal unruly organisation. This was already noted in the *Alabama Claims Arbitration* cited above.[16] Thus, a State is bound to create and maintain a proper system of internal security; it must supply it with the necessary personal, financial, and technical tools so as to allow it to properly discharge its functions; it must adapt its internal legislation to the needs of protection under international law; it must organise the system in such a way as to allow orders to be carried out effectively and quickly; it must seek to ensure an exchange of relevant information on the possible threats between the competent national services and also look for cooperation with international services; *etc.*

Second, a State must display a certain care in its dealings.[17] The degree of this diligence most often depends on the primary norms applicable and on context. It may be a diligence as in one's own dealings (*quam in suis*) or a more objectivised diligence (reasonable diligence). The objectivised diligence is of much more common use in international law: first, because it provides an equal yardstick; second, because it avoids the danger of falling beneath a minimum standard to be invariably upheld. The concrete standard of care varies according to the type of threats: abstract or general dangers, or concrete threats. In the latter case, the authorities of the State have been put on notice of the risk of a certain occurrence or have discovered that threat by their

[15] See *Zannas* (note 1), 85 *et seq.*

[16] *Moore* (note 2), 656, the Tribunal mentioning expressly lack of proper municipal legal means, which is no excuse.

[17] *Zannas* (note 1), 97 *et seq.*

own means. In such a situation, the required care is heightened.[18] This is also the case when officials of a foreign State are on an official visit in a State and due diligence duties arise for their protection.[19]

III. Due Diligence and Cyberspace

A. General Aspects

It may be recalled that the subject matter of the present contribution is not cyber-warfare but the use of cyber-techniques to perpetrate crimes or to create other nuisances during peacetime, and the related State responsibility. Reflection on this topic has not as yet developed very far,[20] especially in public international law. The question has been traditionally linked with the use of force and the laws of war.[21] We may take as a starting point Rule 5 Tallinn Manual,[22] a rule which is drafted to apply both in times of peace and of armed conflict. It relates to the control over cyber infrastructure and to due diligence duties of the State in this context. Its content is as follows: "A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States."[23] The general basis of this rule (or in other words the underlying primary rule) is the old-standing principle whereby a State is not allowed "to allow knowingly its territory to be used for acts contrary to the rights of other States."[24]

---

[18] See the cases quoted *ibid.*, 108 *et seq.*

[19] *Ibid.*, 116 *et seq.*

[20] See however *e.g. Matthew Richardson,* Cyber-Crime: Law and Practice (2014).

[21] See mainly Michael N. Schmitt (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare (2013) (Tallinn Manual). On this Manual see *e.g. Wolff Heintschel von Heinegg,* The Tallinn Manual and International Cyber Security Law, Yearbook of International Humanitarian Law 15 (2012), 3; see also *Marco Roscini,* Cyber Operations and the Use of Force in International Law (2014).

[22] See *supra,* note 21.

[23] Tallinn Manual (note 21), 26.

[24] See *e.g.* ICJ, *Corfu Channel Case* (UK *v.* Albania), Merits, Judgment of 9 April 1949, ICJ Reports 1949, 4, 22. See also the classical statement in the *Trail Smelter Case* (United States *v.* Canada), Arbitral Award of 11 March 1941, RIAA III, 1965.

B. Delimitations

The context is here one of private activities over which the State should exercise some form of control. This is indeed the classical setting of due diligence duties, as evidenced already at the time of their creation (duties of a neutral State to control the activities of private shippers). Conversely, no such duties arise when the State acts itself, *i.e.* through its organs or agents.[25] In such a case, the attribution of the actions and omissions of such organs or agents makes the conduct a conduct of the State itself. The point is then to affirm that the State must not do x or is entitled to do y; but not that it has a due diligence duty not to do x or to do y. The responsibility of the State for its own acts is always direct. It is not embedded in due diligence, the obligation being one of strict result. The responsibility for action of private individuals is conversely never direct, since these individuals are *ex hypothesi* not organs or agents of the State.[26] Thus, the responsibility of the State for their acts or omissions can be only indirect, that is for parallel actions or omissions of the State *on occasion* of such unlawful private activities. The necessary link to bridge the gulf between the private activities and State action is the due diligence duty. The State must show due diligence in this context in preventing some harm done by private individuals to other States. How far this duty of prevention reaches is a matter of discussion in the context of different sets of primary rules (diplomatic law, environmental law, crime prevention, *etc.*). We may notice that in no area of general international law there is an absolute duty of prevention of harm, in the way that the occurrence of the harmful fact would trigger itself the responsibility of the State.[27] States are not insurers for the non-commission of certain deeds.

---

[25] Thus, we will not raise questions of attribution here, even if they arise with acuteness in the cyberspace. Indeed, these questions are legally relevant only in the context of action by the State and not in the separate context of action by private individuals (which is *ex hypothesi* not attributable).

[26] See Art. 4 ILC Articles on the Responsibility of States for Internationally Wrongful Acts, GAOR, 56th Sess., Suppl. 10, 43 *et seq.* (ARS).

[27] Even if that has sometimes been claimed, see *e.g.* for injury to the rights of aliens *Manuel R. García-Mora,* International Responsibility for Hostile Acts of Private Persons against Foreign States (1962).

C. General Issues with Due Diligence in the Cyber Context

Can the classical principles and rules of due diligence apply to cyber criminality or do we need an enlarged concept of such duties? Is the novelty in this area such that the concept would indeed appear to have to be refashioned? The flexibility of due diligence would suggest that this is not the case, but the technical peculiarity of cyberspace would at the same time suggest that some significant problems may arise. Let us scroll through a series of general points, before venturing into some few special ones, more directly linked to cyberspace.

First, classical due diligence duties, under the law of neutrality or damages done to aliens, were essentially *territorially limited.* Classical international law was indeed based on a system of spaces controlled by States with their exclusive jurisdiction. At these times, there was only a limited degree of transnational activity. This has considerably changed since. Today, it is not disputed anymore that the due diligence duties follow any actual or effective control. Cyber infrastructure may be located in most diverse places. What is relevant here is who exercises control over it. The subject exercising such control is also subjected to due diligence duties. The control can be formal (*de jure*) or informal (*de facto*). Formal control creates a legal link between the controlling State and the infrastructure so that this State cannot claim to disinterest itself of what is happening there. The legally entitled State has to exercise control and to direct its legal apparatus to function correctly in such control of infrastructure. The same is true, all the more, for a State exercising mere effective control, whatever its legal entitlement. The ICJ has acknowledged important extra-territorial due diligence duties in the *Genocide* case of 2007 cited above, where it held that Serbia ought to have used its influence over armed groups in Bosnia (to which it was linked) in order to try to prevent genocidal acts.[28] Thus, there is no conceptual territorial limitation for such duties. They rather follow control. Notice that this control has neither to be effective control nor overall control. It is sufficient that there is a degree of influence, which is a question of fact; according to the ICJ, there must be a material ability to prevent. Such control is deemed to exist mainly on the territory. It is often more elusive abroad. But this is admittedly only a question of fact and of circumstances. It is not a question of law.

---

[28] ICJ, *Genocide* (note 9), paras. 425 *et seq.*

Second, due diligence duties attempt to prevent the commission of *unlawful acts.* This unlawfulness has to be reckoned mainly under international law. The (un)lawfulness of the measures taken against the dangerous private activities has however also to be taken into account. Thus, for example, activities on the internet may fall in the protected private sphere of persons or alternatively be covered by the freedom of expression.[29] To what extent this is the case depends on an assessment of the context. However, the answers to be given are not necessarily simple. This is true all the more since more than one legal order may be affected when qualifying the relevant acts. In sum, there are different unlawful acts to be considered at the same time and to be squared one with the other. A State may not engage in unlawful behaviour in order to combat another unlawful act. One unlawfulness is not to be weighed up against another unlawfulness. This also signifies that the means to which a State has recourse in order to fulfil its due diligence obligations must be compatible with international (and to a large extent also municipal) law. However, some norms of municipal law could be brushed aside if contrary norms of international law are given precedence in case of conflict.

Third, there must be a *risk of detrimental effects* of the private activities contrary to the legal rights of the other State. This may again be a matter of assessment in single cases, and could give rise to a separate issue of negligence. Conversely, no due diligence duties arise for a State to curb some private activities if there is no risk (or only a too remote risk) of unlawful damages ensuing therefrom for a foreign State. The damage need not be of a physical nature, *i.e.* damage to objects or bodily injury to persons. Conversely, to affirm that the damage may consist solely of "a negative effect"[30] for the injured State is also somewhat vague. The proper answer is that any damage giving rise to State responsibility qualifies. In other words, the question must be resolved by referring to the notion of 'damage' under the law of State responsibility.[31] The damages aggrieving a third State need not occur on the latter's territory. They can also affect a space where it has or exercises extraterritorial jurisdiction or on any other

[29] On freedom of expression under international law see *e.g. Michel Verpeaux,* Freedom of Expression in Constitutional and International Case Law (2009); see also *Merris Amos,* Freedom of Expression and the Media (2012); Deirdre Golash (ed.), Freedom of Expression in a Diverse World (2010).

[30] Tallinn Manual (note 21), 27.

[31] See the short explanation by *James Crawford,* The International Law Commission's Articles on State Responsibility (2002), 29 *et seq.*

objects protected under international law. This includes objects and rights of other subjects than States, such as international organisations or the International Committee of the Red Cross (ICRC). A delicate question is whether the duties of prevention apply also with regard to a State that unlawfully, but effectively, controls a part of a foreign territory, *e.g.* by unlawful annexation. There are two ways of arguing the point. If the principle of effectiveness is controlling, the unlawful title to that territory is irrelevant for due diligence issues (separation between due diligence and rightful title). If the principle of *ex iniuria ius non oritur* applies, the suspension of due diligence duties for the unlawfully behaving State is a form of sanction of its unlawful behaviour. The question has hitherto not been canvassed in the context of due diligence duties.[32] A relevant consideration would certainly be whether the damage to be prevented is only one for the unlawfully occupying State or one which also entails prejudice to the population in the territory, be it the population of the occupied State or perhaps even the one of the occupier. In the first situation, it would be easier to set aside the due diligence duties, in the second it would be harder.[33]

Fourth, traditionally, due diligence duties applied to each State in the context of its individual obligations to prevent certain harmful results. This is shown by the contexts in which due diligence duties developed, such as the duties of neutral States or of States with regard to aliens on their territory or with regard to environmental damage. In a context of growing interdependence and of shared jurisdictions and responsibilities, in particular in a context of activities which are not any more necessarily neatly delimited from the point of view of their territorial reach, due diligence duties must develop into duties of *proper cooperation* among the concerned States and international institutions. It may not be sufficient anymore to point out that all the feasible steps have been taken within the national sphere of jurisdiction, when the private activity at stake straddles over many territories or has detrimental effects which cannot be clearly limited in space. By analogy, many modern international régimes concerning internationally shared goods are developed around the notion of a duty of consultation, negotiation, and cooperation (instead of purely unilateral

[32] The most thorough study of consequences flowing from unlawful possession concerns Cyprus: *Stefan Talmon,* Kollektive Nichtanerkennung illegaler Staaten (2006).

[33] See by analogy the *Namibia* opinion, ICJ, *Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970),* Advisory Opinion of 21 June 1971, ICJ Reports 1971, 13, para. 56.

measures), such as, *e.g.*, the régime of international rivers.[34] It stands to reason that aspects of international cooperation must also be prominent in a resource like that of cyberspace, which is essentially unbounded from the point of vantage of classical territorial limits.

Fifth, it is unclear to what extent due diligence duties also apply to *prospective, possible, or future acts.* There is always a degree of uncertainty about the future. Private persons, possibly terrorists, might attempt to do a great variety of things (each one detrimental to the rights of other States) on the territory of the State whose due diligence duties we are considering. Must that State take (all?) reasonable measures to prevent such prospective acts? How far can the speculation into such acts reach, and what resources must the State bind for such a huge enterprise? Or does the State not have any preventive due diligence duties in such a context, the damaging conduct being still too speculative to give rise to a duty to act? The problem is particularly acute in the context of cyber-activities, due to their covert nature and their potentially broad reach. The ability to mount comprehensive defences against all possible threats would lead to unreasonable duties, going well beyond what is classically defined as *due* diligence. It comes as no surprise that the experts in the Tallinn process, who were mainly from North Atlantic Treaty Organization States, could not agree on this issue.[35] The proper answer must be to link the duties of the State to what is reasonably possible (*zumutbar*). This in turn depends on the type and gravity of the prospective threat, on the existing technical possibilities at any given moment, on the devices at the disposal of a particular State (it will be difficult to require as much from Eritrea as from the United States of America albeit there is a duty to organise the State in order to be able to fulfil international obligations), on the fact of being put on notice of a particular risk, and on other circumstantial factors. No State is obliged to do the impossible and none is obliged to venture into the unreasonable. The relation of cost and useful outcome has to be weighed.

Sixth, due diligence obligations arise normally if a State has *knowledge* of the detrimental activities or at least of the risk of such activities. The classical rule is that a

[34] See the UN Convention on the Law of Non-Navigational Uses of International Watercourses, GA Res. 51/229 of 21 May 1997, in particular Arts. 8–9. On this Convention see the commentary of *Stephen C. McCaffrey/Mpazi Sinjela,* The 1997 United Nations Convention on International Watercourses, American Journal of International Law 92 (1998), 97.

[35] Tallinn Manual (note 21), 27.

State may not 'knowingly' allow the use of its territory for activities breaching the rights of foreign States. Relevant knowledge exists when another State or institution puts a State on notice that such a detrimental activity, or the risk thereof, exists. Knowledge also exists when the intelligence services of the State, or its police forces, detect the activity or the risk thereof. In our context, this would relate essentially to credible information that a cyber attack or cyber criminality is underway from a territory.[36] This aspect triggers two further considerations. First, there is the requirement of a proper organisation of the State, so that the information is transmitted to all the competent services and shared as far as necessary. Practice shows that this is far from always being the case. The information is often sensitive and therefore some services tend to keep it aloof from other services. Or the organisation of the State is insufficient, a not infrequent occurrence in the context of inflated modern bureaucracies. Such a state of affairs would hardly be compatible with the organisational side of due diligence. Second, a careful analysis of the information must take place so as to be able to separate 'credible' information from such which is not credible. That may be an easy exercise in one situation, but it also may be a difficult one in another situation. Some degree of international cooperation may be necessary here to fully live up to the due diligence duties. The most difficult question relates to 'constructive knowledge', *i.e.* imputation to the State of what it should have known. Is any negligence, or only grave negligence, imputable to the State (perhaps itself under some due diligence standards) in order to apply the substantive due diligence duties towards another State? In other words: if a State fails to police with due care its own territory and the areas under its control and is therefore unaware of some detrimental private activities, does this State engage its responsibility? The Tallinn experts were unable to agree on this intricate matter.[37] The difficulties are indeed considerable, especially in the cyber context. As was written in the Tallinn Manual:

> Even if constructive knowledge suffices, the threshold of due care is uncertain in cyber context because of such factors as the difficulty of attribution, the challenges of correlating separate sets of events as part of a coordinated and distributed attack on one or more targets [or of criminal activity], and the ease with which deception can be mounted through cyber infrastructure.[38]

[36] *Ibid.*, 28.

[37] *Ibid.*

[38] *Ibid.*

Such difficulties suggest that a breach of due diligence duties can be affirmed only in most egregious cases, when there is a manifest negligence of the gravest nature. The test seems practically speaking to be of massive negligence, of the type: 'How could he not have done this or that ...', and not: 'It would appear that he ought better have done this or that ...'.

Seventh, the violation of due diligence duties entails the ordinary *consequences of State responsibility*. The extent to which an aggrieved State may do more than to ask for *ex post facto* reparation must be related to the applicable primary or secondary norms of international law. Thus, if the conditions for the adoption of countermeasures are met,[39] such measures may be taken. The most interesting question relates to the faculty to take direct remedial measures when a State is 'unable or unwilling' to act to curb the detrimental activity. The issue has been discussed essentially in the context of self-defence[40] but is of more general application. It would appear that in the context of the fight against criminality such measures could not be taken on the territory of another State without its consent, lest the fundamental rules on the protection of territorial sovereignty be completely subverted. However, in the cyber context measures could be taken directly from the territory of the aggrieved State, even if these measures produced some effects on the territory of another State (as the *Stuxnet* attacks in Iran show). Not implying any activity or presence on the territory of another State, these cyber-related acts are therefore not to be legally analysed as substitutive measures for a defaulting State (*Ersatzvornahme*). They are rather a category of countermeasures or simply protective measures (not limited by the conditions of countermeasures) for the violation of one's own rights and/or the concomitant violation of due diligence duties by the other State. It also stands to reason that more than one remedy may be used in parallel. Finally, the question arises as to the number of injured States. There are certainly some directly injured States in a particular context, *e.g.* the State on whose territories the detrimental and unlawful effects occur. However, since the medium of the cyberspace is unique and the routes of the internet completely inter-linked, it might be possible to consider that there is here a sort of common space. In this case each State has an interest in upholding a situation not detrimental to its security. All States of the world would to some extent be injured (jeopardised in

[39] Arts. 49 *et seq.* ARS; see *Crawford* (note 31), 281 *et seq.*

[40] See *e.g. Tom Ruys,* 'Armed Attack' and Article 51 of the UN Charter (2010), 419 *et seq.*

a common stake) by criminal activities on the net, since these activities could be routed through their territory. The only proper response to such a common interest would be to revert back to the duties of cooperation already mentioned.

D. Specific Issues with Due Diligence in Cyberspace

The particular nature of cyberspace prompts certain particular problems in the context of due diligence duties. Only two of them will be raised here because of the lack of technical knowledge of the author of these lines.

First, a State may be put on notice or acquire itself the knowledge that a harmful cyber activity is being mounted and will be routed through its territory. But that State may be unable to identify the signature and timing of the perpetrators. Should it completely block access to services on all the connections through its territory? That can hardly be expected when considering proportionality, reasonableness, and due diligence. The same is true in most cases when a State just acquires the knowledge that a cyber crime is routed through its installations or territory. It may be argued that if there is concrete knowledge of the offending operation and a parallel material ability to put an end to it (through proportional measures, it must be added), the State must exercise that ability.[41] However, the peculiarities of cyberspace will make such an operation often somewhat difficult and the result to be obtained speculative. When a transmission is blocked at one point of the network, it will usually automatically be rerouted along a different transmission path, most often through a different State. Any action of the State at one point of the network could then not have the causal effect of avoiding the detrimental result. Such action is then not due from the point of view of diligence: Due diligence is not concerned with measures which have no impact on the prevention of the unlawful outcome. The situation is different when the culprits are located within the territory of a State and there is thus a material possibility of arresting them. The situation might also be different when rerouting can be exceptionally avoided through some available technical devices. All these aspects relate to questions of fact.

Moreover, it is once more apparent that a successful fight against such activities presupposes an increased cooperation among States. To the extent the activities at

[41] This was the view of certain Tallinn experts: Tallinn Manual (note 21), 28.

stake refer to private crimes (such as trafficking of human beings, child pornography, *etc.*), there is some prospect in achieving a greater degree of cooperation. The stumbling block in this context will then not be the lack of inclination towards cooperation. However, there will be the ever-present problem of lack of resources. Conversely, when the criminal activities occur with some State involvement or State interest, such as is often the case with terrorist activities, cooperation will be limited to some States and not extend to those sympathetic to the causes of its authors.

Second, the question may arise under due diligence to what extent a State (especially poorer States) must organise and finance measures geared towards possession of a number of cyber-specialists, keeping up with the latest technical advances, and so on. As we have seen since the 19th century, due diligence concerns also the proper organisation of the State, so as to be in a position to properly react to the challenges for the rights of other States. However, the burden of organising properly to display in an orderly way the ordinary functions of a State is one thing; the burden to keep up with the pace of highly sophisticated technologies in a constantly shifting environment is another. The question cannot be easily answered (apart from the recurring point on international cooperation and possibly on transfer of technology), but it is of obvious importance. It stands indeed to reason that the criminal elements will particularly favour States and routes where the control is low or inadequate.

IV. Conclusion

One of the questions raised above was the extent to which the concept of due diligence could be applied to cyberspace activities. The answer must be that the concept is of overall usefulness in any context where the State has to monitor private activities in areas under its control so as to avoid harmful effects violating the rights of foreign States. The concept is moreover flexible enough to fit most differing contexts. At the same time, however, cyberspace presents unique characteristics. The point is not so much that due diligence is ill-adapted to such a space, but that it can be applied to such a space only when a series of parameters of the subject matter are taken into account. Due diligence is a concept flexible enough to accommodate such particular needs. To some extent, all the rules of traditional international law are to be reimagined in this unique context. International law is still essentially linked to the

exclusive jurisdiction of States over pieces of delimited territory in the world. The space of international law is fragmented; without such fragmented jurisdictional space international law would not exist at all. The paradigm of sovereignty and exclusive jurisdiction is politically cherished through self-determination and self-understanding of peoples. It will not be given up in the foreseeable future. However, the paradigm adapts with difficulty to certain activities whose nature is to be fundamentally non-territorial and ubiquitous. The virtual space is to a large extent interrelated, inseparable, and unique. Uncoordinated State actions to curb activities in such a space promise only a limited degree of success. The necessary complement can flow only from international cooperation and new legal instruments adapted to the unique nature of that peculiar space. But that is, after all, a trite truth.