INTERNATIONAL responsibility of a state for certain unlawful behaviour is currently determined by actual attribution of this behaviour to the state. However, international cyberspace is a special environment in which certain operations are usually hardly attributable to specific actors. As a result, the question arises how to establish the responsibility of the state for unlawful operations in cyberspace and whether to establish state’s responsibility for the operations that merely stem out of the computers on its territory. In order to understand the impacts of special character of cyberspace on state responsibility, this paper deeply examines the notions of “unlawful behaviour” and “responsibility of states”. It distinguishes different models of state responsibility from the historical perspective and applies this distinction on cyberspace. Consequently, it claims that the character of cyberspace could summon the older and more primitive form of state responsibility.

INTRODUCTION

The increasing number of incidents in cyberspace has intensified the debate on cyber war\(^1\). Following acts are often discussed as manifestations of ongoing conflict in this virtual environment. In 2007, infamous cyber-attack on Estonia overloaded the webpages of the government and many private institutions. Estonian Minister of defense asked the crucial question – what is the difference between a military naval blockade and such a massive cyber strike. In the same year, during the operation Orchard, the Israeli forces used cyber-strike to successfully eliminate Syrian air defense. Three years later the virus Stuxnet was revealed. Supposedly originating in the US, it is blamed for damaging the Iranian nuclear power-plant in Natanz. In an alleged retaliation, cyber-strike on Saudi Aramco attacked thousands of

\(^1\) See e.g. Farwell and Rohozinsky 2012, Stone 2013.
computers of the oil company, disrupted its activities and lowered the value of its stocks and shares on the market.\(^2\)

Regardless the discussion on the warlike character of those acts, the behavior of states in cyberspace is determined by the following questions: Under what circumstances is a state responsible for certain behavior in cyberspace? Do the norms of public international law apply on states due to their responsibility? On the one hand, there is the opinion that cyberspace is entirely subject to current international law regulations. On the other hand, the opposing standpoint claims that cyberspace shall become rather anarchical environment without any regulations. This paper contributes to the ongoing debate and combines two perspectives – legal analysis and constructivist approach to international relations and law. Public international law and its institute of state responsibility are analyzed as a social constructs, a phenomenon consensually created in discourses and practices. The first part of the paper analyzes the notion “responsibility of states” and identifies different modes of this responsibility. The second part tackles the international legal norms possibly applicable on cyberspace. It argues that the character of cyberspace influences the responsibility of states in a special way. Cyber environment, allowing the actors to hide their identity, causes the inapplicability of the most important *erga omnes* norms\(^3\) of international public law. Nevertheless, there is still a possibility to apply different norms of international law on the bilateral level. Therefore, the key point of this paper is that the denial of universal norms and strengthening of the importance of bilateral state relations summon older and more primitive form of state responsibility.

For the analytical clarity, we can list the simplified definitions of two basic notions. No widely accepted definition of cyberspace has been provided by the legal scholars or technical specialists. Nonetheless, it may be regarded as the network created by the means of telecommunications, including the Internet, or more specifically the computers interconnected through certain protocol. The computers cooperate and create the system of data exchange, which exists separately of the outer world (Schaap 2009, 125 – 126). Due to the special characteristics of this environment, it is very difficult to verify the identity of the actor. The costs of verifying the identity of a person that actually acted in cyberspace are very high, while the costs of disguising this identity are relatively low (Lessig 1999, 24).

\(^2\) (for more detailed information on those attacks and further reference to other strikes see Centre for Strategic and International Studies 2014)

\(^3\) Norms applicable on every state of the international community, although it did not ratify any special convention etc.
From the variety of different descriptions of cyber-attack, we may use the definition of American Department of Defense (Joint Doctrine for information operations 1998, 141). It provides that a cyber-attack is an “actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.”

RESPONSIBILITY AND ITS MODELS

According to current public international law, the international responsibility of a state is invoked every time when the state commits internationally wrongful act. This general maxim of customary law is embodied e.g. as the grounding principle of Draft Articles on Responsibility of States for Internationally Wrongful Acts. Subsequently, the international wrongful act is described in the following way (Draft Articles 2001, Rule 2 Elements of Internationally Wrongful Act, p. 34):

“There is an internationally wrongful act of a State when conduct consisting of an action or omission:

(a) is attributable to the State under international law; and

(b) constitutes a breach of an international obligation of the State.”

Thus, the responsibility of states includes two elements. Firstly, the objective element means the breach of certain obligation (particular and concrete violated norm). Secondly, the subjective element means that the perpetrator of the behavior can be identified – the act may be attributed to him. In other words, the state is responsible for certain act or failure to act only if this act breaches an identifiable international law norm and is provably committed by this state.

Nevertheless, the notion of state responsibility is subject to different interpretations. At this point, we may use the constructivist perspective. This approach allows us to perceive the state responsibility as something that is rather articulated in discourses and created by practices than objectively given (for further conceptualization of social construction, see Berger and Luckman 1966). Therefore the legal doctrine of state responsibility serves here not as a

---

4 Further referred to as Draft Articles (2001). This document itself, prepared by the UN International Law Commission, is not legally binding. However, it is a codification of customary law. Therefore the legal customs described in this codification are legally binding.
starting point, but rather as an object of analysis. By examining the legal discourses, one may identify different models of state responsibility that loosely correspond with the *constructed* character of international system of states. The key distinctive characteristic of each model is to whom is the state responsible.

*Schemes of models of state responsibility:*

**Vertical (“communitarian”) model:**
- International Community
- State A
- “People”: Residents on state’s territory

**Horizontal (“bilateral”) model:**
- State A
- State B

*Vertical model of state responsibility*

The difference between the perceptions of responsibility was remarked already by the former member of UN International Law Commission Martti Koskenniemi (2010, 47 – 48). The vertical model, or as Koskenniemi calls it “communitarian doctrine”, establishes the state responsibility towards the international community as well as towards the state’s citizens, or all people under its jurisdiction. This model connects state responsibility with so called peremptory rules⁵, thus making certain behavior mandatory *erga omnes* (towards all other members of the community). The breach of the norms which are crucially important for the international community represents *international crime* (Šturma 2007, 52). This approach also demands that the responsibility should express the interests of the people rather than states (Allot 1988: 26) and serve as the mean for their protection. Koskenniemi (Ibid.) describes the roots of this model within the legal discourse, mentioning Island of Palmas arbitration in 1928, when the customary rule was articulated by the arbiter that sovereignty involves the

---

⁵ So called *ius congens*. Those are e.g. prohibition of genocide, torture and inhuman treatment, slavery etc. The International Court of Justice identified those obligations in *The Barcelona Traction Case* (see also Šturma, 2007).
duty to protect the population of the state, making the state responsible towards its own population. As Koskenniemi (Ibid. 47) further explains, “already in the 1950s García Amador viewed State responsibility in general terms as an instrument for the protection of the ‘essential rights of man’”. Latter spreading and wide recognition of human rights strengthened this construct of responsibility.

Other peremptory *erga omnes* norms established responsibility of states towards international community of other states. Especially the prohibition of the use of force embedded in article 2(4) of the UN Charter founded a strong commitment of every state towards the group of all other countries of the world. In the same way, the obligation not to intervene in the affairs of other states became important part of peremptory rules in international system. The vertical model of state responsibility prevailed and gained vital importance within the framework of the modern international law during the last century.

*Horizontal model of state responsibility*

On the contrary, according to the horizontal model, the responsibility of state may be understood only in terms of bilateral relationships of states. This model analogically resembles the domestic level. We may imagine two citizens that are in certain legal relationship. This means that they have obligations and rights towards each other. In the same way, this model presupposes that the states are responsible only to their counterparties – other states – in bilateral relationships.

According to this model, the responsibility is the natural result of the state existence. At the same time it represents the ability to face (*respond to*) the consequences of breach of the state’s obligation in bilateral relationship. This approach was favored by classical theorists of the international law. Lauterpacht (1944) claimed that once a state is powerful enough to secure its own existence, other states should recognize it. Thus, this state is able to enter into agreements with other states. In the same way, it is responsible to them for possible unlawful or harmful behavior. Vattel (1883) asserted that states (nations) have their rights that can be claimed in mutual relationship. He stressed that the states are entitled to do whatever is necessary to protect their sovereignty and to preserve their existence: “Since then a nation is obliged to preserve itself, it has a right to everything necessary for its preservation (Ibid. §
Consequently, the states may resort to offensive war as a tool in the international relations, which represents their right to do justice themselves (Ibid. § 68).

Because of the application of norms in bilateral relationship only, this model of responsibility was also called liability. The important feature of traditional international law that favored this model was that no particular sanction existed that would punish the perpetrator of the norm or set the secondary obligation for the perpetrator to compensate the damages. The perpetrator was simply regarded as a party uninterested in any legal regulation. The damaged party thus could also refuse the regulation provided by concerned norm. It was entitled to so called freedom of action. This means that it could undertake any steps against the perpetrator that it deemed appropriate (Čepelka and Šturma 2008, 574 - 575).

As a result, the situation usually developed according to one of following scenarios. Firstly, the state-perpetrator was not willing to redress his behavior and thus the state-victim could resort to possible coercion through power-politics. Secondly, the state-victim was not even interested in reparations and preferred other solution (armed conflict etc.). Thirdly, the state-perpetrator willingly accepted new obligation, e.g. to provide the state-victim with remedies. (David, Sladký, Zbořil, 2008: 309).

Those two models of state responsibility can be perceived as competing constructions or as Weber ideal types. Their distinctive features appear and reappear in different legal discourses; sometimes they may be mixed. Even the quintessential legal document for the field of state responsibility, the above mentioned Draft articles on Responsibility of States for Internationally Wrongful Acts, may be subject to horizontal (“bilateralist”) or vertical (“communitarian”) interpretation of responsibility (Koskenniemi 2010, 50). Generally, while the traditional international law favored the horizontal bilateral model, the modern international law operates rather with the communitarian model.

At this point, the models could be interconnected with the constructed levels of anarchy proposed by Alexander Wendt (1999, 246 - 311). Wendt claimed that international anarchy is a construct, which may be established differently according to perception and attitude of involved states towards each other. He introduced three cultures of this anarchy – Hobbesian (deep enmity of states, continuous war), Lockean (rivalry of states, war as acceptable optional behavior) and Kantian (friendship of states, war is prohibited).
The vertical or the “communitarian” model resembles the Kantian anarchy. States, being responsible to their population and international community, are supposed not to break certain rules – peremptory norms. If those rules are breached, the sanction should follow, guaranteed by the authority of international community. The prohibition of the use of force is the most important norm *erga omnes*.

Older horizontal or the “bilateral” model of state responsibility (liability) could loosely correlate with the Lockean anarchy. States are recognized units, they may choose their course of action freely and manifest their rivalry, but they are liable to other state if they violate certain mutual obligation. Their legal existence means they must and are able to face the consequences of their behavior. It is also up to the states whether the legal regulation should apply.

This part of the paper may be summarized in the following way. The responsibility for internationally wrongful act may be legally defined in terms of objective elements (breached norms) and subjective elements (attribution). However, there are different models of this state responsibility, differentiated according to the fact towards who is the state responsible. After setting this basic theoretical framework, we may investigate the impacts of cyberspace on the responsibility of states.

(IR) RESPONSIBILITY OF STATES IN CYBERSPACE

Taking into account the above mentioned elements of internationally wrongful act, two conditions must be fulfilled if the state should be responsible for certain (unlawful) behavior in cyberspace. Firstly, the behavior must violate particular norm of international law. Secondly, it must be attributable to the state.

In case of cyber-attacks, two norms could possibly be violated. Firstly, it is the norm prohibiting the use of force, embedded in customary law and articulated also in the article 2(4) of the UN Charter. Under what conditions could cyber-attack constitute the use of force? According to current doctrinal interpretation, the scale and effects of this cyber-attack must be analogic to the scale and effects of possible non cyber (conventional) attack (CCDCOE 2013, Rule 11, 47). This condition is based on the application of so called Schmitt criteria (Schmitt 2001, 53 – 85) that specify what is meant by the scale and effects. Those criteria consist of *severity, immediacy, directness, invasiveness* and *measurability of concerned* strike. If the
cyber-attack evaluated through those criteria reaches the threshold of conventional attack, it does constitute the use of force. Otherwise, it could constitute a breach of sovereignty and violate the obligation not to intervene in internal affairs of other states⁶ (see also Buchan 2012, 212 or Shackelford 2009, 212 – 216).

Both the above mentioned norms – prohibition of the use of force and of the intervention – are peremptory. And as far as objective element of internationally wrongful act is concerned, they could be possibly applicable to cyberspace. However, the problem arises with the subjective element – the attribution of the behavior breaching those norms to particular state. It is recognized by the doctrine that “[t]he fact that a cyber operation has been routed via the cyber infrastructure located in a State is not sufficient evidence for attributing the operation to that State” (CCDCOE 2013, Rule 8, p. 40). Generally speaking⁷, it is very hard to verify the real identity of an actor in cyberspace. If certain behavior should be attributable to the state, the state has to exercise so called effective control over it. This means it has to factually lead and command the operation. This condition was used by the International Court of Justice in Nicaragua case. It is included also in Draft Articles (2001, see Article 8 and following).

Considering the anonymous character of cyberspace, it would be very hard to prove this effective control through any kind of investigation. Moreover, the unwillingness to cooperate or just reluctant assistance of the state-perpetrator may significantly aggravate the situation. In the specific cyber-environment, the state may simply deny its responsibility for active involvement in cyber-attack and refuse or just merely pretend further investigation, sovereignty principle serving as effective shield. As a result, the attribution on the basis of effective control is impossible. Consequently, the responsibility of a state for use of force in cyberspace or for violation of sovereignty in cyberspace can hardly be established.

Jason Healey (2011:57) proposes to move beyond the attribution fixation to the point when “nations are held responsible for major attacks from their national territory or citizens”. He outlines ten categories of state responsibility for cyber-attacks according to the intensity of involvement of the state from the infrastructure of which the attack originates:

- state prohibited cyber-attacks;
- state prohibited but inadequate;
- state ignored;

---

⁶ This customary obligation was articulated e.g. in ICJ Case Nicaragua.
⁷ The technical aspects of this statement are omitted in order to leave more space for societal analysis.
- state encouraged;
- state shaped;
- state coordinated;
- state ordered;
- state rogue conducted;
- state executed;
- state integrated (Ibid., 57 – 62).

However, those levels are oriented rather on policy-making. If we want to move beyond direct attribution also in legal realm, we have to search for other norms that can be violated through cyber-attack and that do not require direct attribution provable through effective control over the operation.

Those are the obligations outlined in points 3 to 6 in the following table. While the norms 1 and 2 may establish the responsibility according to Healey’s categories of state-coordinated and state-executed attacks, the other norms 3 – 6 may be used as a legal basis how to constitute the responsibility of state for other Healey’s categories.

Table of possible norms violated by cyber-attack

<table>
<thead>
<tr>
<th>Breached international obligation (objective element):</th>
<th>Attribution of the act to the state (subjective element):</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Prohibition of the use of force (Art. 2(4) of UN Charter)</td>
<td>In case of effective control over the activity</td>
</tr>
<tr>
<td>2. Non-interference (articulated in ICJ case Nicaragua)</td>
<td>In case of effective control over the activity</td>
</tr>
<tr>
<td>3. Obligation to warn the victim-state of possible danger (ICJ case Corfu Channel)</td>
<td>in case of negligence</td>
</tr>
<tr>
<td>4. Obligation to prevent unlawful activities stemming from the territory of the state (ICJ case Namibia)</td>
<td>in case of negligence</td>
</tr>
<tr>
<td>5. Obligation to secure own territory and obligation not to acknowledge the results of unlawful acts (ICJ case Tehran)</td>
<td>in case of negligence</td>
</tr>
<tr>
<td>6. Obligation to prevent harmful (though legal, not wrongful) activities stemming from the territory of the state (Trail Smelter Case)</td>
<td>in case of negligence</td>
</tr>
</tbody>
</table>
The international legal norms 3 – 6 were expressed within the decisions of international judiciary bodies\(^8\), most frequently International Court of Justice. The attribution as a subjective element of unlawful behavior can be proved without actual test of effective control in those cases. The character of concerned norms 3 – 6 enables us to make the state responsible for omission – no action or failure to act. In other words, there is no action to be attributable to state, but the state may be blamed for simple failure to act. This conception enables us to apply the legal regulations without the direct attribution of the action to the state – beyond the attribution on the basis of effective control.

Let us explain the problem on an example. We may imagine that there is the cyber-attack from the computer network of the state A against the state B. If the state A is aware of this attack, it has to warn the state B immediately (norm 3). This could cover the Healey’s category of responsibility for state ignored attack. Moreover, every state should reasonably secure its own network so that no unlawful actions stem from it (norm 4). In addition, the state should not acknowledge the cyber-attacks as legitimate (norm 5). This norm should cover the state-encouraged cyber-attacks and cut off possible public support of individual hackers. Finally, even if the cyber-attack is conducted in the way that is not explicitly illegal, the state A should stop it in case it causes damage to the state B (norm 6). The state A could possibly deny its responsibility only if it proved that every possible measure had been undertaken to avert the cyber-attacks but in spite of this effort the attacks had occurred.

We may observe that the norms 3 – 6 have rather bilateral character. The active involvement of victim-state is needed and the ability of international community to act is rather limited. In cases 4 – 6, the state perpetrator must be previously notified of the fact that there are the cyber-attacks emanating from the computer network under its jurisdiction. Only then it is obliged to act and its responsibility for the failure to act may be established.

The victim state may demand that the state from the network of which the cyber-attacks originate stops and prevents further attacks (cessation), apologizes (satisfaction) or pays the damages (compensation). This may be achieved through international arbitration. However, the other state may simply refuse the claim of the victim state. The situation may turn into protracted legal dispute or simple continuation of the perpetrator’s ignorance.

---

\(^8\) Judicial decisions have the special position as sources of international law; they may articulate existing legal custom and establish the precedent.
In that case, it is up to the victim state, whether it will stay within the boundaries of legal solution or organize appropriate cyber defense. The cyber defender – more or less anonymous in the cyber environment – may even strike back at the state perpetrator in retaliation.

In this way, the older, bilateral or horizontal model of state responsibility may prevail again. There are three basic reasons of the revival of this older model. Firstly, *erga omnes* norms (prohibition of the use force and of intervention) are inapplicable in cyberspace. Secondly, the other norms shall be applicable only in bilateral relationship, on the dyadic level of two states. Thirdly, the states may simply refuse to apply international law and rather resort to cyber retaliation in a more or less anonymous way. Those distinctive features move the international responsibility of state closer to the older, horizontal model of state responsibility.

CONCLUSION AND DISCUSSION

As the cyberspace largely disguises and blurs the identity of individual actors and makes direct attribution impossible, the older model of state responsibility returns. We have interconnected this model with the second Lockean culture of anarchy of Alexander Wend. However, the construction is a process rather than a definite outcome and there is no guarantee that the state responsibility in cyberspace may forever work according to rules of this second model. This model hugely relies on territorialization and monopoly of state on coercive use of force. While the system of Westphalia brought *formula for peace* (Slaughter 1995, 38) in division on outside and inside of the state territory, cyberspace may significantly erode this partition and turn the physical borders obsolete. Can the cyberspace also deny the state monopoly on coercive use of (cyber-)force to that extent that the state would be just one of many important actors in this environment? Will the states attempt to “fight back” and strengthen their authority in cyberspace, even for the price of shortening civic liberties? Can the Lockean anarchy fall to Hobbesian anarchy, where entities – individual, corporate and governmental – rise to fight with each other? And can the model of responsibility concerning cyberspace spread to other realms regulated by public international law? The return of the older form of the state responsibility due to cyberspace environment may well indicate that we are in the middle of such processes.

---

9 With a possible result of cyberspace opened for business, but not to ideas (Lewis 2010, 63).
REFERENCES:

**Doctrinal codifications of international customary law:**


**Judiciary Cases:**


**Bibliography:**


