Видання рекомендовано до друку рішенням вченої ради юридичного факультету Сумського державного університету (протокол № 9 від 03.04.2014 р.)

Особистість, суспільство, держава: проблеми минулого і сьогодення : зб. матер. Міжнар. наук.-практ. конф. : у 2-х част. Ч. 2 : у 2-х томах (Суми – Курськ, 18 квітня 2014 р.) / ред. колегія : В. М. Власенко, В. Б. Звагельський, Р. Камберова та ін. – Суми – Курськ : Сумський державний університет, Південно-Західний державний університет, 2014. – Ч. 2, Т. 1. – 200 с.

До збірника увійшли наукові статті та повідомлення викладачів, студентів, вчених та аспірантів ВНЗ і наукових установ, виголошені в рамках Міжнародної науково-практичної конференції «Особистість, суспільство, держава: проблеми минулого і сьогодення» (Посвідчення УкрІНТЕІ № 861 від 9 грудня 2013 р.), присвячені актуальним питанням суспільно-гуманітарних наук.

На обкладинці: Перший у світі монументальний пам'ятник Тарасу Шевченку. Встановлений у жовтні 1918 р. у м. Ромнах на Сумщині. Скульптор І. П. Кавалерідзе.

7. ДАЗО, ф.Р-4006, оп.1, спр.5.Копии приказов по отделу юстиции и заявление граждан о зачислении их на работу.
8. ДАЗО, ф.Р-4006, оп.1, спр.4.Положения о фабрично заводских комитетах. Циркуляр увоенревкома.
9. ДАЗО, ф.Р-4006, оп.1, спр.45. Постановления отдела коммунального хозяйства и переписка с ним.
10. ДАЗО, ф.Р-4006, оп.1, спр.110. Материал по снабжению сотрудников бюро юстиции продуктами питания (циркуляры, переписка, списки).
11. ДАЗО, ф.Р-4006, оп.1, спр.29. Список сотрудников юр. отдела, схема штатов, распределения участков народных судов уезда и др.
12. ДАЗО, ф.Р-4006, оп.1, спр.49. Сведения карательного подотдела о количестве мест заключения, численности служащих и вооруженного наряда.

VLASENKO V.V.

CYBER SELF-DEFENCE: «*WE ARE NOT IN A CYBER WAR YET, WE ARE IN CYBER COLD WAR*» [1]

The digital environment became an indispensable part of human activities performed in XXI century. Technological development has a great impact on the functioning of the economy, infrastructure and constitutes an important element of overall sustainable development.

Cyber space is widely used in different aspect of human life. Computer networks facilitate different aspects of international relations. Financial, educational, and health institutions, as well as telecommunication, navigation and logistics are dependent on the computer networks. Despite that cyber space has been widely applied in international warfare.

Already in 2010 the Economist recognised cyber space as the 5th domain of international warfare [2].

Before *lex specialis* that governs the use of cyber space in international warfare is adopted the states and international community refer to the core rules of public international law, international law of military operations and armed conflicts and the guiding principles of «*soft*» law - resolutions, codes of conduct, etc.

This article is devoted to the public side of cyber attacks in international warfare and covers the following matters:

1. What actions in the digital domain constitute a use of force in the sense of Article 2(4) UN Charter and what are the criteria for determining whether that acts may be qualified as armed force?

2. What acts of force constitute an armed attack giving rise to the exercise of the right of self-defence and what are the criteria for determining whether an act of «*cyber armed force*» crossed the threshold of armed attack?

3. What criteria of necessity and proportionality will be applied to regulate the response against the attack if an act constituting a cyber-armed attack has taken place?

4. If an act of cyber armed force is carried out, how can it be attributed to a particular State or non-State entity in terms of the law relating to international responsibility?

In determining the lawful use of force Article 2(4) of the UN Charter states: «*All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations*».

Attacks against critical infrastructure may cause an effect worse that economic crisis. The consequences of actions taken in cyber space may lead to horrific consequences and cause irreparable harm to the state. Attacks against national information infrastructure may end up with mass disturbances in society, economic loss and undermine political systems. Thus, one of the main questions regarding cyber use of force is whether to what extent actions performed in cyber space that resulted in the harm to state property or civil population can constitute the use of force?

It is important to make a remark the main actors in international warfare remain the states. However the role of the non-state actors is undeniable. Both states and non-state actors become involved in cyber warfare. Ralf Langner provides the definition on what can be considered as cyber war. Cyber warfare is maliscious manipulation of cyber systems (smartphones, computers, home entertainment, control/automation systems) supporting or substitution the conventional act of war where the impact that you are achieving or trying to achieve is equivalent to conventional attack [3].

The prohibition to use force is reflected in both legal instruments addressed to states – the UN Charter and in customary international law [4]. Moreover, the principle of non-use of force is established in the Declaration of Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations. The Declaration provides that all states should refrain from the use of force in their international relations, and indicates that wars of aggression are a crime against peace for which international responsibility is engaged. Furthermore, the International Law Commission in the commentaries to the Vienna Convention Law of Treaties identified the prohibition of the use of force as a jus cogens norm. Judges of the International Court of Justice in their decision, and Separate Opinions to Nicaragua case, largely supported that recognition [5]. Nevertheless, the prohibition of the use of force does not mean that war, as such, is absolutely prohibited. The UN Charter does not restrict the states to go to war. It establishes

the conditions under which the war may be permitted. There are two exceptions, which allow the UN Member States to refer to the use of force lawfully; Firstly, the Security Council may authorise an enforcement operation for maintenance of international peace and security on the basis of Chapter VII. Secondly, the states may use force in response to armed attack when exercising their right to self-defence under Article 51 [6].

It is recognized that state have the sovereign right to control cyber infrastructure and cyber activities within its territory [7]. The group of experts collaborating over the Manual emphasized two consequences of the State's sovereignty over cyber infrastructure within its territory. The state exercises legal and regulatory control over cyber infrastructure. Moreover, the state must protect its cyber infrastructure regardless whether it belongs to the government or to private sector. In addition the state will exercise the jurisdiction over its nationals and other the persons involved in cyber operation on that state's territory.

Thus, only states may consent to and facilitate cyber operations conducted from its territory. Subsequently the state will bear international responsibility for a cyber operation attributable to it.

Article 2(4) of the UN Charter prohibits the state to use force against another state's territory. International Court of Justice has stated that Article 2(4) of the United Nations Charter, regarding the prohibition of the use of force applies to «*any use of force, regardless of the weapons employed*» [8]. Hence, engagement of state's cyber capabilities in military operation that was conducted by the state's armed forces and resulted in damage scaled to the one caused by kinetic warfare will trigger the use of force in the sense of Article 2(4).

In order to define the actions performed in cyber space that can be considered as the use of force it is necessary to outline to the main instruments for such determination.

First, and the most important element with regards to determination of cyber attack as a use of force is the so-called result test. The result test, as it is implied from the name which refers to the consequences of the attack occurred [9].

The notion of the result test is greatly supported by Schmitt, who claims that cyber attack «*spans the spectrum of the consequentiality*» [10] and Y.Dinstein also agrees that determination of the use of force depends on violent consequences [11]. Taking into account the result test there must be considered two situations:

- the use of cyber attack as a part of military campaign. Computer may be used as a weapon and operate the techniques of physical attacks. During the Russia-Georgia war Russia has integrated the cyber attack as a separate element to the physical attacks against Georgia [12]. Destabilizing

the government networking systems and underpinning the reputation of the current government helped Russia to complete the attack successfully.

- the use of cyber attack for non-military means, which was reflected in physical use of force. A good example of non-military means may be an attack resulted in economic/financial losses. If attacks caused the economic losses would be equated to the use of force, that would unreasonably extend the meaning of Article 2(4). The attacks, that implicate a negative impact on financial infrastructure of the state, may not be qualified as the use of force, but rather as a cyber crime. Consequently they will be regulated by the rules of international criminal law. In order to reach the level of the use of force cyber attack must cause the consequences, graver then economic loss.

Thus, in the light of the result test, not all cyber attacks constitute violation of Act 2(4). Only those actions, which resulted in property loss and factual injury, and damages/injuries were of the same nature as the ones caused by the traditional weapons.

Another determinative condition, which can bring the cyber attack to the level of use of force in the meaning of Article 2(4) is the methods of cyber attack. In other words, while defining whether the attack was equal to armed force, attention must be drawn to the question of whether cyber was used as a weapon of warfare. Here it is important to distinguish those computer programs, which may be used as a tool of warfare and those, which are designed with a specific military objective. A computer itself is not a weapon, but if employed offensively by the military unit in order to achieve military goals, it will be constitute a part of military asset. Hence, computer data is not a weapon itself, but in certain applications may cause damage to be equated to the use of force. Stuxnet was developed solely to disrupt industrial control system of a power plant. Programs operating military aircrafts or missile launches are originally created for facilitation of its operational means. Thus computer programs and viruses, designed specifically for the military use will to be considered as weapons of warfare, and that would be taken into account during the determination of certain acts as the use of force. In order to assimilate a cyber attack to the use of force, it must be regarded through the lens of an armed attack. The damages and injuries resulted from cyber attack must be of the the same scale or even higher than damages from an armed attack. In this case the cyber attack will be recognised as a use of force and consequently constitute a violation of Article 2(4) of the UN Charter.

Another important element is military intent [13]. A cyber attack will constitute an armed attack if intended to cause direct physical damage to tangible objects or injury to human beings. Generally speaking cyber attack launched against another state myust be backed by unconditional military intention to target a specific object or to reach sertain military objective.

It is important to point out that the use of cyber attack against another state, even if the latter has not reach the scale of the use of force in the meaning of Article 2(4), for instance cyber espionage, may violate non-intervention principle, stated in Article 2(1) of the UN Charter. However it is not always clear whether espionage will be considered as intervention. Interference in cyber space of another state may reach the scale of intervention only if coercive element is at place. Determination of the coercive element requires a lot of data to be looked at, and will be defined upon each particular case.

The Security Council is the central organ of the UN and governs the use of force in cases of a threat to the peace, breach of the peace or in the event an act of aggression. In order to maintain peace and security, the Security Council has the discretionary powers to deploy armed forces, establish and authorize enforcement actions on the territory of the state and impose sanctions. By doing so, the Security Council acts in the light of objectives and principles of the UN Charter. Under no circumstances, may the aforementioned actions be qualified as those intended to defeat aggressive acts emanating from the belligerent parties. The Security Council is entrusted with the implementation of the collective security against the threat to international peace. All 197 of the UN Member States delegate their powers to the Security Council for maintenance of international peace and security [14] thus accepting its decisions as binding [15].

Likewise, the Security Council is the only body, which «*determines the existence of a threat to the peace, breach of the peace, or an act of aggression*» and «*decides what measures shall be taken...to maintain international peace and security*» [16]. The Security Council in its decision often refers to «*threat to the peace*» because this term is broader and provides more conditions to act [17]. For instance, the Security Council recognized that «*proliferation of nuclear, chemical and biological weapons, as well as their means of delivery, constitutes a threat to international peace and security*» [18]. Evidently, grave violations of human rights [19] and international terrorism [20] have been recognized as conditions, which presuppose threat to the peace. Hence, threat to the peace does not always encompass either military actions or operations where armed force was involved.

With regards to cyber attacks, Rule 18 of Tallin Manual prescribes the ability to refer to forceful measures, which may include the use of cyber force. Hence, if all peaceful means to restore a conflict have been exhausted, the Security Council may impose cyber measures against the violation. Despite the fact that Article 42 of the UN Charter outlines enforcement measure taken by air, sea or land of the states, it is accepted that this scope may be extended to cyber space [21]. Commentaries to the Rule 18 add that Security Council now may not only employ cyber operation resolution against the violating state, but authorize kinetic operation against the cyber attack emanating from that state's territory.

The Security Council would not take responsive actions against state-sponsored cyber attack producing little or no damage. However a computer network intrusion that caused large-scaled damage, economic loss, and death of civilians would well be ascertained as a reasonable factor to invoke the right to self-defence.

The fact the cyber attacks are performed without use of traditional kinetic weapons does not preclude the idea that later attack can be qualified as «*armed*» in the meaning of Article 51. Thus, it is important to determine under which conditions a cyber attack may be considered as an armed attack, giving rise to the exercise of the right to self-defence under Article 51 of the UN Charter.

An armed attack is an attack where significant armed force is used and which exceeds the level of a mere armed incident. Small-scaled attacks may constitute the use of force in the meaning of Article 2(4) but cannot be justified with self-defence. Justification is only possible if an armed attack has been committed or there is clear evidence of an impending attack [22].

Commentaries to the UN Charter stated that the purpose of Article 2(4) is to ban military force [23]. It is envisaged that in certain extreme situations, where the consequences of the use of non-military force may be equivalent to an armed attack, giving rise to referring to the right to self-defence, the scope of Article 51 may be extended. Prof. Y.Dienstein also emphasizes the existence of the situation where a violating state uses force against another state or non-state entity without an armed attack [24]. In practice states often invoke Article 51 in order to justify their use of force even when armed attack against them per se has not occurred. Armed attack occurred against the UN Member state by another state or non-state entity, infers the violation of Article 2(4). But not every breach of Article 2(4) constitutes an armed attack. The states may invoke self-defence in response to actions, which caused significant and harmful consequences with a relatively large scale of damage.

The majority of legal writers accept the possibility of self-defence in response to cyber attack, although opinions vary. Prof. Y.Dienstein noted that from the legal point of view electronic or kinetic means of the attack do not really matter if it leads to distructive results [25]. Silver considers that in case where the actions taken in cyber space have caused a disruptive effect, it will be more appropriate to apply Article 2(4) rather than Article 51 [26]. Waxman also supports this concept. He foresees proportionate countermeasures to be a reasonable response to cyber attack and argues that recourse to force is unacceptable [27]. The latter argument is also agreed by the authors of the Tallin Manual. Rule 9 allow the injured state to respond with proprtionate countermeasures, including cyber countermeasures [28]. The majority of legal writers agree that since cyber attacks results in irreparable damages, it will be ruled through the lens of

the following three elements – intent, method and consequences. The US Department of Defence in their Assessment emphasized that while taking a decision regarding invocation of Article 51, the focus will be made on the offender's intent and the consequences of the offending actions rather than on the mechanism by which the damage was done [29].

So what kind of actions will likely turn cyber attack to an armed attack?

Firstly it is important to define whether the damage resulted from a cyber attack could previously have been achieved only by a kinetic attack. Graham provides an example with power grid breakdown [30]. Today's power grids are controlled by computer systems, thus actions in cyber domain would be the easiest way to disrupt it [31]. Furthermore regarding the power grid disruption NATO recently emphasized, that «*... the risk of a large-scale attack on NATO's command and control systems or energy grids could readily warrant consultations under Article 4 and could possibly lead to collective defence measures under Article 5...*» [32].

Secondly in order to launch a military response to cyber attack, it must be determined to what extent that attack can be equated as a hostile act and whether it was launched for military purposes [33]. The cyber attack will trigger the right to self-defence if the object and purpose of the attack are equal to military acts. For example, launching Stuxnet virus is an offensive act and aimed to disrupt the power plant control system. A power plant is a tangible object and its breakdown will lead to a disadvantageous outcome. Penetration to its computer system with a purpose to change proper flow of the processes, consequent destabilization of enemy's military forces and as a result electricity is shut down across the civilian population, proves that the level of armed attack is achieved. Hence, the intrusion to the power plant computer system may be considered as an action having a hostile intent.

Thridly the consequences of the attack must reach the same scale of damage as the one from the traditional attack. Robertson supports the idea claiming that «*until a consensus develops for the need for a new normative architecture, it would appear that the most rational and practical test of whether a computer attack can be the precipitating event for the exercise of lawful self-defence, is whether the consequences are major damage to or destruction of vital military or civilian infrastructure or the loss of human life*» [34]. For example, a cyber manipulation computer network system, which controls dam functions caused significant disruptive flooding and put the local population in extreme and harsh living conditions. Despite the fact that no kinetic attack was engaged the latter would be considered an armed attack because the overall damage reaches the scale of armed attack or even worse.

Self-defence will only be lawful if it constitutes necessary and proportionate response [35] aimed to repeal prior attack and taken within reasonable period of time after the later has been performed.

Degree of necessity and proportionality is to be determined by the injured state. The Responding state will decide what [forceful or alternative non-forceful] actions will be necessary to repel or overturn a cyber attack.

The problem with regards to cyber attack is that it is not always easy to identify the effects and consequently measure the scope of proportional response against it. Firstly, they may become visible only after certain period of time. The latter may hamper a principle of immediacy. With respect to a cyber attack, application of principle of immediacy will be considered as lawful when the state became aware and got evidences that the attack has been performed. Secondly, methods of cyber attacks evolve dynamically. The Respondent state is not always fully aware about the author of the attack and the techniques used in the performance of the cyber offence. Moreover, it is possible that attack will produce greater harm than it was planned in the beginning. Disruption of power grid providing electricity to military bases may result in blackouts in the electronics used in military hospital. Where a cyber attack targets a database or denies service for important assets of the computer network or electronic infrastructure, it is up to the victim state to determine to what extent the latter can be considered as an imminent armed attack [36] and subsequently determine a proportionate response.

Lastly, it is relevant to refer to Robertson's «*3 prong test*» [37]. Firstly, response to cyber attack may be justified if subsequent attacks were part of a military campaign of the state. Secondly, cyber attack in response constitutes an irreversible step towards unavoidable armed attack. And thirdly, the defender state relies on the armed response as the last opportunity to defeat forthcoming attack. In order to repel an attack the victim state may launch a computer attack in response, intended to disable the equipment being used by the violator. The issue of proportionality will likely be minimized if a responsive cyber attack has been launched as a measure of self-defense against another cyber attack.

The question to be answered here is whether it is possible to invoke of the right to self-defence to imminent cyber attack? Indeed, with regards to current cyber capabilities timing frame may be easily hindered and a cyber attack may be identified much later than the factual attack has been launched.

Another fact that creates a problem to identification of a cyber attack is that attackers may operate from the computer, connected to the server of neutral state. This may enable them to hinder the track of original offender making determination of the source of the attack almost impossible [38]. On the other hand, the Responsive state may be in need to use computer networks owned by or passing through neutral countries and that may be considered as a violation of their sovereignty.

Furthermore, cyber attack may be a precursor to further kinetic armed attack. That means that states may exercise their right to self-defence not only against cyber attack but in order to defeat further kinetic or another graver cyber attack. The problem is that it is not always clear when a cyber attack will be an «*armed attack*», thus not conceivable what kind of responsive actions would be proportionate to such an attack, especially where the attack inflicts little or no physical damage or loss of life [39].

With respect to aforementioned the issue of anticipatory self-defence against cyber attack seems to be problematic. One of the most likely scenarios of anticipatory self-defence against cyber attack is the situation where a cyber attack constitutes a predecessor element of the upcoming physical attack [40].

Prof. Y.Dinstein states that Article 51 does not emphasize the type of weapons to be used in self-defence [41] thus the armed attack can be repelled with another cyber attack. Deployment of cyber weapons [as Stuxnet and Night Dragon], aimed to disrupt strategically important military targets and cause damage equal to the one caused by the use of force, is not internationally prohibited [42]. The status of cyber attacks has not been determined as illegal actions in international law or a forbidden method of warfare. However, such a response will be considered as lawful if the criteria of lawful self-defence are met [43].

The criteria of *jus ad bellum* which govern the fairness of war and determine whether engaging in war was lawful and properly justified, remain unchanged for years. However increasing engagement of non-state actors in present armed conflicts has brought a number of dynamic changes to the understanding of the notion of just war. International organizations and non-state entities have become an undeniable part of the international arena. Although the question of whether the non-state actors can be recognized as fully-fledged subjects to international law is still under consideration.

The use of force is a delicate question. At present we may reckon that non-state actors are bound by the prohibition of the use of force [44]. Both the UN Charter and customary international law prohibit unilateral use of force. One may argue that only states are the signing Parties to the UN Charter, therefore it is reasonable to assume that Charter provisions are only directed to states. However the prohibition of the use of force is a jus cogens norm [45], i.e. one of the fundamental principles of international law. Therefore it is reasonable to claim that non-state actors and international organisations should adhere the obligation not to recourse to force. Furthermore they must comply with the principles of international humanitarian law. Hereby, I present a few facts supporting this idea.

The Security Council in its binding resolution imposed obligations upon non-state actors and armed groups, mentioning that all parties to the conflict must comply with the provisions of international humanitarian law [46]. Indeed, the Court has already recognised international humanitarian norms as erga omnes, meaning they are addressed to all the participants in the international conflict [47]. Thus keeping in mind the fact that the Security Council once provided the binding decision upon non-state actors, it is likely that the obligation not to recourse to force under the UN charter is also applicable to them.

Another example refers to 9/11 events in New York. After 9/11 more and more legal writers recognise that a state may invoke its right to self-defence not only against states, as prescribed in Article 51, but also against the non state actors in response to a prior attack against that state.

Considering the aforementioned, non-state actors are bound with an obligation not to use force and must comply with jus ad bellum provisions.

Self-defence may be exercised on behalf of the state, meaning that only a legitimate state authority is able to declare the use of force as a legal response. The question is what my be considered as an «*authority*». One of the elements of the «*authority*» is to represent people's interests. Hence, non-state entities may fall into this category [48]. For example, rebellious movements exercising their right to seld-determination do represent the interests of the particular group of people. In order to defend themselves, they may launch an attack and that would be a reasonabe repsonse. Presumably, when this group of people, without a governing authority, is put in a threatening situation or becomes a victim of an act of aggression, a «*non-state organization ... can act as a legitimate authority and justly engage in violence on behalf of the people*» [49]. To conclude the aforementioned, the rules of jus ad bellum may be applicable to the non-state actors involved in the armed conflict, hence, must be adhered by them.

In other cases attacks that are not state-sponsored [or state-goverend] will not be justified with self-defense. The invokation of the right to self-defence will not be accpeted if malicious acts against another state have been performed by private individuals or organized groups, unless the state adopts the conduct or the conduct will be attributable to it according the the ruls of international law of states responsibilities.

Hence if the non-state actors are bound with an obligation not to use force, and only states may invoke the right to self-defence the main problem with respect to non-state actors comes with attribution. The cyber attack conducted from the territory of the state may not necessarily be attributable to that state.

The question of attribution remains one of the biggest problems in cyber warfare. It is very complicated to determine who exactly committed the attack and who exercised the control over the people involved in the

commission of the attack. Therefore, the question of who will bear responsibility for damage caused by cyber attacks remains unresolved. The issue of attributability of a cyber attacks will be reviewed through the lens of Article of State Reposnibility and, since recently, The Tallinn Manual on the International Law Applicable to Cyber Warfare.

The state will be internationally responsible for the wrongful act if that act was committed by the state organ [50] or under the direction or control of the State [51]. Hence, if the cyber attack has been performed by the state organ or private persona whose actions have been authorized by the state, the conduct of the attack will be attributable to the state. However The Tallin Manual offers an interesting approach regarding attribution of cyber attack to the state. Rule 7 states that cyber operation that has been launched from governmental cyber infrastructure will not sufficient evidence for attribution of the operation to that State. The latter will be considered as a mere indication that the operation was performed with involvement of that particular State. However the commentaries to Tallin Manual indicate that the Rule 7 will not be applied to the cyber operation originated from cyber infrastructure that was not a part of governmental cyber infrastructure even though located on the territory of that state. Moreover, Rule 8 adds that cyber operation that has been routed via the cyber infrastructure located in a State will also not be sufficient enough to attribute the operation to that State.

It is interesting to compare the aforesaid with ARSIWA's Article 4 that attributes conduct of the state body to the state. Traditional approach of the attribution of the state-generated wrongful attack to the state, prescribed in Articles on States Responsibility is supported in the Tallin Manual. The authors of the commentaries to Tallin Manual highlight that the conduct of the cyber operation launched from the state cyber infrastructure «*cannot be followed in cyber space*» [52]. The argument is defended with the possibility [fear?] of undesirable intrusion of the non-state actors into states cyber and military assets followed by their unlawful on behalf of the state.

Then, whereas the Rules 8 presumes that the state is not associated with the cyber operation, the Rule 7 refers to unconditional relation between the state and cyber attack emanating from its cyber infrastructure. Commentaries to ARSIWA note that conduct will be attributable to the state only if it «*directed or controlled the specific operation*» and was an integral part of that operation. It is added on that the principle does not extend to conduct which «*was only incidentally or peripherally associated with an operation*» and which the State was not able to direct or control [53]. Hence in the language of Rule 7 it would be reasonable perhaps not to exclude a possibility to attribute the conduct of cyber operation to the state but rather to refer to «*direction and control test*» mentioned in the commentaries to ARSIWA. Nevertheless, the disclaimer put on NATO

Cooperative Cyber Defence Centre of Excellence website states that at this moment the Tallinn Manual can not be considered as an official document or legal source.

Another controversy will arise when the attack has been launched by the non-state actor independently without any supervision by state. Even if the state adopts the conduct of that non-state actor it is absolutely unclear to what extend the rule stated in Article 11 of the Articles on State Responsibility may be applied to cyber context. Whather it would be possible to make that State responsible in the light of Rule 7 of the Tallinn Manual?

The Tallinn Manual although remain the most specific scope of rules regarding cyber warfare bring new controversies to already existing problems posed before the states, international organizations and non-state actors towards attribution of the cyber attacks and international responsibility for them.

Cyber capabilities offer the prospects of more successful and less violent warfare. States already use cyber as a multiplier of the accomplishment of kinetic operations. National policy makers of the European states concentrate on defensive cyber capabilities. Countries like the US and China actively invest in the creation and training of cyber forces. They are also engaged in the development of cyber weapons. That proves existence of such projects as Stuxnet, Flame and Red Dragon that have been created explicitly as a tool of warfare and cannot be used for other means. Hence if the computer attacks became one of the methods of international military campaigns the question arises how to define, regulate, attribute and respond to them. Today, the core international legal instruments like the UN Charter, Articles on State Responsibilities, academic researches and experts reports can be the only guides into cyber warfare regulation. In order to sum up the content of this article I would like to outline the following statements.

Firstly, not all offensive actions performed in cyber may reach the level of the use of force. In order to equate cyber attack to the cyber use of force, and subsequently be able to provide an armed response against such an attack the following criteria must be fulfilled:

- An attack is launched with a military intent; the state launched an attack with clear knowledge and intention of the consequences. By using cyber attack military commander intended to achieve the military goals.

- An attack is used as a tool of warfare; Cyber may not only be used as a tool for facilitation of aerial or naval forces. Cyber attack may be a multiplier of the whole campaign, but may be also a separate campaign.

- The method of cyber attack is developed explicitly for military purposes [or for a particular military operation] and can only be used within the operation.

- The consequences of the attack reach the level of physical attack; It is necessary to draw the line between economic, social and military consequences. Grave economic and social effects of cyber attack would not be bring the attack to the level of the use of force. Only those attacks which caused human injury, death, put national population into harsh living conditions or damaged the objects that are strategically important for state function, would be qualified as the use of force in the meaning of Article 2(4) of the UN Charter, and hence enable the injured state to recourse to armed response.

It is accepted that states may respond the cyber attack with another cyber attack or using other means to restore the conflict. Once the recourse to force becomes necessary the states may restore the conflict with the use of cyber force and vise versa, with forceful actions against the cyber attack. It is up to the injured state to decide which actions would be necessary and proportionate in order to defeat an attack. Moreover, Security Counsil may authorise cyber measure against the breach of the peace, threat to the peace of act of aggression or empower peace enforcement operation against a cyber attack of large scale.

In case cyber attack has been occured, and was qualified as a violation of the law of the use of force it remains unlcear how the matter of attribution will be resolved. Due to the lack of special rules governing international responsibility for the damages caused by cyber attacks, traditional rules on the law of state responsibility will be applied. Thus, if there is be a proof that cyber attack has been launched by the state organ, the wrong will be attributable to the state. If the state did not launch an attack itself but provided sponsor support, the attribution would be determined through the notion of effective control, ie to what extent the state exercised control over the cyber attack. The wording of the Tallinn Manual add certain ambiguities to the issue of attribution in cyber context. However having no legal power at the moment the Rules may only be considered as personal opinion of a group of independent experts. Not only states may be the actors in cyber war arena. Non-state actors also may be involved in cyber conflict. In the situation where the group of individuals launches a cyber attack that reaches the level of the use of force it must be determined to what extent the state exercised effective control over the attackers, or whether it could have known about the wrongs emanating from its territory.In the abscense of such proof the attack will not be attributable to the state.

Lastly, in order to resolve the cyber conflict the general rules of warfare, provisions of the existing public international and customary international law will be interpreted according to the factual circumstances.

---

1. *David Willson*, Attorney at Law CISSP, Security+, Active Defence: is it legal? https://www.brighttalk.com/channel/288

2. Cyberwar. War of the 5th domain, Are the mouse and keyboard the new weapons of conflict?, The Economist, 1 July 2010; http://www.economist.com/node/16478792

3. «The first deployed cyber weapon in history: Stuxnet's architecture and implications» Ralph Langner's keynote for the NATO CCD COE's International Conference on Cyber Conflict // http://vimeo.com/25710852

4. Nicaragua v US; ICJ Reports 1986, p.176.

5. Separate Opinion of President Nagendra Singh; Nicaragua v US; ICJ Reports 1986, p.143.

6. Notably, in the commentaries to the UN Charter B. Simma speaks about the third exception - Article 107 - measures against former enemy states of the Second World War, however this provision is not relevant anymore since all former enemies have become members of the UN.

7. Tallinn Manual on International Law Applicable to Cyber Warfare [Draft]. General Editor M.Schmidt; Cambridge University Press 2013; para 3, p.25.

8. Nuclear Weapons Advisory Opinion, para.39.

9. The Handbook of the international law of military operations, edited by Terry D.Gill and Dieter Fleck, Oxford University Press [2001], p.409.

10. Computer Network Attack and The Use of Force in International Law: Thoughts on a normative framework; by Michael N.Schmitt (supra fn. 54), p.912.

11. Computer Network Attacks and Self-Defense, Yoram Dinstein; International Law Studies, Vol. 76 [2002], p.103.

12. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, by J.Andress and S.Winterfels; Syngress [2011]; Chapter 1, p.14.

13. Ibid p.136.

14. Article 24(1) Charter of the United Nations.

15. Ibid, Article 25.

16. Ibid, Article 39.

17. The Law and Practice of the United Nations, by B.Conforti; Legal Aspects of International Organizations, Vol. 42; [2005] p.172.

18. Security Council Resolution 1540.

19. SC Resolution 392 (1976).

20. SC Resolution 1373 (2001).

21. The Tallinn Manual on the International Law Applicable to Cyber Warfare; para 9 at p.71.

http://www.ccdcoe.org/249.html

22. The Handbook of the international law of military operations, edited by Terry D.Gill and Dieter Fleck, Oxford University Press [2001] p.409.

23. Commentaries to the UN Charter, B.Simma.

24. War, Aggression and Self-Defence, Yoram Dinstein, 4th edition, Cambridge University Press [2004], p.193.

25. Computer Network Attacks and Self-Defense, Yoram Dinstein; International Law Studies, Vol. 76 [2002], p.103.

26. Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter by Daniel B. Silver; International Law Studies, Vol. 76 [2002], p.75.

27. Cyber Attack and the Use of Force: Back to the Future of Article 2(4) by Matthew C. Waxman, (supra fn. 51) p.430.

28. Tallinn Manual on International Law Applicable to Cyber Warfare [Draft]. General Editor M. Schmidt; Cambridge University Press 2013; para 3, p.41.

29. An Assessment of International Legal Issues in Information Operations by the US Department of Defense (May 1999), p.15.

30. Cyber Threats and the Law of War, David E.Graham, JOURNAL OF NATIONAL SECURITY LAW & POLICY [Vol. 4], p. 91.

31. International Law, Cybernetics and Cyberspace by Anthony D'Amato, (supra fn. 31), p.68.

32. International Cyber Security Legal and Policy Proceedings. Eneken Tikk, Anna-Maria Täliharm; CCD COE Publications, December 2010; Cyber security and defence from the perspeptIve of Articles 4 and 5 of the NATO treaty, Ulf Häuβler, infra fn. 254 'NATO 2020: Assured Security; Dynamic Engagement' The Report is available at http://www.nato.int/strategic-concept/expertsreport.pdf at 45.

33. Computer Network, Proportionality, and Military Operations, James. H. Doyle J., p.153.

34. Self-Defence against Computer Network Attack under International Law, by Horace B. Robertson Jr., Computer Network attack and International Law; edited by Michael N. Schmitt and Brian T.O'Donnell; International Law Studies, Vol.76 [2002], p.138.

35. The principle is supported by ICJ: Nicaragua Judgment, paras.176, 194; Nuclear Weapons Advisory Opinion, para. 41; Oil Platforms Judgment, paras.43, 73-74, 76.

36. Computer Network Attacks and Self-Defense, Yoram Dinstein; International Law Studies, Vol. 76 [2002], p.111.

37. Supra fn. 31, p.140.

38. Information Warfare and International Law by Lawrence T. Greenberg, Seymour E.Goodman and Kevin J. Soo Hoo [National Defense University Press], Chapter 3.

39. International Cyber Security Legal and Policy Proceedings. Eneken Tikk, Anna-Maria Täliharm; CCD COE Publications, December 2010; Cyber security and defence from the perspeptIve of Articles 4 and 5 of the NATO treaty, Ulf Häuβler, at p.119.

40. Self-Defence against Computer Network Attack under International Law, by Horace B. Robertson Jr., Computer Network attack and International Law; edited by Michael N.Schmitt and Brian T. O'Donnell; International Law Studies, Vol.76 [2002], p.139.

41. Computer Network Attacks and Self-Defense, Yoram Dinstein; International Law Studies, Vol.76 [2002], p.103.

42. The International Legal Implications and Limitations of Information Warfare: What Are Our Options? by LTC Bryan W. Ellis Strategy Research Project, April 2001, p. 3 infra fn. 14 International Court of Justice, «Legality of the Threat or Use of Nuclear Weapons,» Advisory Opinion, para.21; available from: http://www.icjcij.org/icjwww/idecisions/isummaries/iunanaummary960708.html; Internet; accessed 4 January 2001.

43. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law Scott J. Shackelford p.237.

44. *Nicholas Tsagourias*, Participation in the International Legal System. Multiple perspectives on non-state actors in international law. Edited by Jean d'Aspermont. Routledge Research in International law [2011], p.337.

45. Supported by the ICJ Judgement Nicaragua v US; ICJ Reports 1986, p.190.

46. SC Resolution 1214, preamble.

47. Kupreskic and others Judgement, ICTY-TPIT, 14 January 2000, para 23.

48. *Andrew Valls.* «Can Terrorism Be Justified?» in Andrew Valls ed., Ethics in International Affairs: Theories and Cases. New York: Rowman & Littlefield, Inc., 2000, Reading 57.

49. *Andrew Valls.* «Can Terrorism Be Justified?» (fn. 11), p.567.

50. ILC, Draft Articles on Responsibility of States for Internationally Wrongful Acts [2001], Art. 4.

51. ILC, Draft Articles on Responsibility of States for Internationally Wrongful Acts [2001], Art. 8.

52. Tallinn Manual on International Law Applicable to Cyber Warfare [Draft]. General Editor M. Schmidt; Cambridge University Press 2013; para 3, p.40.

53. Commentaries to the Draft Articles on Responsibility of States for Internationally Wrongful Acts [2001], p.47.