

# *Ius ad bellum* in Cyberspace – Some Thoughts on the “Schmitt- Criteria” for Use of Force

**Katharina Ziolkowski**

Legal & Policy Branch

NATO CCD COE

Tallinn, Estonia

katharina.ziolkowski@ccdcoe.org

**Abstract:** The term “cyber-attack” has become a synonym for any malicious cyber-activity. Given the martial semantics and the hype of “cyberwar” in the media and non-legal disciplines, as well as the political sabre-rattling partly perceivable in international relations, the present article endeavours to augment the academic discussion in regard to the criteria used for the legal assessment of malicious cyber-activities as “use of force” pursuant to Article 2(4) of the UN Charter and, at the same time, in regard to the closely related term of “armed attack” in the meaning of Article 51 of the UN-Charter and Article 5 of the North Atlantic Treaty. The importance of the discussion of such criteria lies in the fact that “use of force” in international relations enables the victim State to undertake a range of unfriendly (retorsions) and otherwise illegal actions (counter-measures), and that an “armed attack” triggers the right to self-defence of the victim State and justifies its resort to forceful self-defence measures – all situations with potentially severe consequences for international peace and security. First, the traditional meaning of the terms “use of force” and “armed attack” will be presented. Without replicating the relevant scholarly writings, it will be shown which categories of malicious cyber-activities can be considered “use of [armed] force” and – given a certain threshold of severity in scale and effects – as an “armed attack”. In this context, the so-called “Schmitt-Criteria” for the classification of malicious cyber-activities as “use of force”, established by Professor Michael N. Schmitt over a decade ago and hitherto not analysed in depth within scholarly writings, will be elaborated upon. These criteria contain a range of significant aspects and refer to complex matters; therefore, they deserve a substantial discussion. Due to the focus and the limited scope of the present paper, the discussion of the *ius ad bellum* aspects related to Chapter VI and VII of the UN Charter will be deliberately omitted.

**Keywords:** *cyberspace, use of force, armed attack, Art. 2(4) UN Charter, Art. 51 UN Charter, Art. 5 North Atlantic Treaty, Schmitt-Criteria*

# 1. INTRODUCTION

Since the term “cyber-attack” has become a synonym for any malevolent activity conducted by the means of the Internet or other information and communication technologies (in the following referred to as “malicious cyber-activity”), a martial connotation can be perceived in the respective semantics describing cyber-threats and malicious cyber-activities. Especially media and non-legal disciplines use the term “attack” without the necessary sensitivity, which would be desirable, given the cognitive association of the term in the context of international peace and security. Additionally, the different meanings of the legal term “attack” being a term of art for both, the *ius ad bellum* and in the *ius in bello*, are not always clearly distinguished<sup>1</sup>.

Given the confusion in terminology, and bearing in mind the aforementioned martial semantics, the media-hype of “cyberwar” and the political sabre-rattling partly perceivable in international relations<sup>2</sup> – clearly to be seen in the context of deterrence policy efforts –, the present article endeavours to augment the academic discussion in regard to the criteria used for the legal assessment of malicious cyber-activities as “use of force” pursuant to Article 2(4) of the UN Charter, enabling States to undertake a range of unfriendly (retorsions) and otherwise illegal actions (counter-measures), and in regard to the closely related term of an “armed attack”, justifying a State’s resort to self-defence measures in the meaning of Article 51 of the UN Charter and Article 5 of the North Atlantic Treaty. In particular, the so-called “Schmitt-Criteria” for the classification of malicious cyber-activities as “use of force”, established by Professor Michael N. Schmitt over a decade ago and – pursuant to the knowledge of the author – hitherto not analysed in depth within scholarly writings, will be elaborated upon. The criteria contain a range of significant aspects and refer to complex matters; therefore, they deserve a substantial discussion. The assessment will, *inter alia*, show differences in the approach of the common law system and the civil law system in regard to lines of legal argumentation.

However, it shall be emphasised that the decision about undertaking retorsions or counter-measures, as well as about the existence of a self-defence situation and the resort to use of force in international relations will always be a political one, which will be taken at the highest levels of a State’s governmental structure and which will always depend on the overall political context of the particular political crisis. The legal discipline can only support governmental decision-makers by providing in advance abstract criteria and – in the case of governmental legal advisors – concrete *ad hoc* legal counsel affecting the overall assessment and judgment.

It shall be only mentioned that, due to the focus and the limited scope of the present survey, the discussion of the *ius ad bellum* aspects related to Chapter VI and VII of the UN Charter is deliberately omitted.

<sup>1</sup> See M. N. Schmitt, “‘Attack’ as a Term of Art in International Law: The Cyber Operations Context” in this volume.

<sup>2</sup> See e.g. S. Gorman & J. E. Barnes, “Cyber Combat: Act of War Pentagon Sets Stage for U.S. to Respond to Computer Sabotage With Military Force”, in *The Wall Street Journal* online of 31 May 2011, available at <http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html> (last visited 16 April 2012).

## 2. "USE OF FORCE" AND "ARMED ATTACK" IN PUBLIC INTERNATIONAL LAW

Currently, neither a legal definition nor a universally accepted definition of the terms "use of force" (Article 2(4) of the UN Charter) and "armed attack" (Article 51 of the UN Charter, Article 5 of the North Atlantic Treaty) exist. However, the meaning of the terms can be clarified to a certain degree by substantial interpretive work, an endeavour challenged by the fact that the core meanings of the treaty norms are recognised to constitute norms of international customary law at the same time.

As indicated by Articles 31-33 of the Vienna Convention on the Law of Treaties and the corresponding<sup>3</sup> international customary law, and by Article 38(1) of the Statute of the International Court of Justice (ICJ), the interpretation of a term should include, *inter alia*, the preparatory work of the treaty and the ordinary meaning of the term in its context of the treaty and in the light of its object and purpose. These aspects reflect the canon of legal interpretation, stated by the German lawyer Friedrich Carl von Savigny<sup>4</sup> in the early 19th century and still forming an elementary component of legal teaching in continental-Europe: the historic, the textual, the systematic and the teleological interpretation. Corresponding to the nature of public international law, the aforementioned norms designate further aspects to be taken into account when interpreting international norms. Those are, among others, subsequent State practice or international custom, judicial decisions and, according to Article 38(1)(d) of the ICJ-Statute, "the teachings of the most highly qualified publicists of the various nations". It shall be mentioned that in regard to *ius ad bellum* as applicable to cyberspace, it is the work of academia which currently importantly influences the development of a common understanding within the international community. Potential State practice is not perceivable in the public, declarations of *opinio iuris* by States are rare and general<sup>5</sup> in nature, and respective national or international jurisdiction does not yet exist on the matter.

In the following, first, the traditional meaning of the terms will be presented, before its application to acts conducted by means of the Internet or other information and communication technologies will be elaborated upon.

Although disputed in detail, it can be stated that – generally speaking – an "armed attack" is given in most severe cases of "use of force" in international relations (in the meaning of Article 2(4) of the UN-Charter) of significant scale and effects. This finding is supported by the

<sup>3</sup> Despite being highly political documents, the UN Charter and the North Atlantic Treaty are subject to the rules of interpretation of international treaties. Although, according to its Article 4, the Convention of 1969 does not apply retroactively (to the UN Charter of 1945 and to the North Atlantic Treaty of 1949), the provisions on interpretation of treaties are a valuable reference as they reflect international customary law. See: G. Ress, "The Interpretation of the Charter", in B. Simma (ed.), *The Charter of the United Nations. A Commentary* (Oxford / New York, Oxford University Press, 2002, 2nd ed.), at para. 2 et seq.; ICJ, *Oil Platforms (Islamic Republic of Iran v. United States of America)*, Merits, ICJ Rep. 1996, at p. 823 para. 41.

<sup>4</sup> For more information on von Savigny see "Friedrich Karl von Savigny", in *Encyclopedia Britannica Online*, available at <http://www.britannica.com/EBchecked/topic/525746/Friedrich-Karl-von-Savigny> (last visited 16 April 2012).

<sup>5</sup> See Gorman & Barnes, *supra* note 2.

jurisdiction of the ICJ<sup>6</sup> as well as by a vast amount of scholarly writings<sup>7</sup>, of which the mere repetition will be abstained from in this survey.

Thus, the two terms “use of force” and “armed attack” are closely related. In order to identify which situations would comprise an “armed attack” and trigger the right of the victim State to undertake self-defence measures it must first be established in which situations “force” in the meaning of Article 2(4) of the UN Charter is used in international relations. Thus, the term “use of force” can be deemed as the nucleus of all *ius ad bellum* deliberations.

Illustrating the different lines of arguments concerning a further specification of the term “force” within international jurisdiction and scholarly writings would certainly exceed the scope of this paper. In addition, there is no benefit in their mere replication. Therefore, without further explanation, in the following it will be assumed that “force” in the meaning of Article 2(4) of the UN Charter is to be understood as “armed force”.<sup>8</sup> Hereby, two aspects are of importance for further deliberations: On the one hand, pursuant to the historical, systematic and teleological interpretation of the norm, “use of [armed] force” does not include measures of mere coercion, be it political or economic in nature.<sup>9</sup> On the other hand, however, the term “use of [armed] force” is not limited to the employment of military weaponry: The ICJ stated over 25 years ago the possibility of an “indirect” use of armed force<sup>10</sup> (e.g. by arming and training insurgents) and scholarly writings<sup>11</sup> describe e.g. spreading fire over the border or flooding another State’s territory as violating the prohibition of “use of [armed] force”.

In order to specify the meaning of “use of [armed] force” conducted by the means of the Internet or other information and communication technologies, an effects-based approach inherent to public international law is surely to be considered appropriate (ruling out other possible approaches, e.g. focusing the target of the malicious activities, the intent of the malevolent actor, or the designation of the means used). Hereby, the comparison of the effects indirectly caused or intended by malicious cyber-activities with the effects usually caused or intended by conventional, biological or chemical weapons (BC-weapons) plays a paramount role<sup>12</sup>.

Again, in order not to replicate the legal arguments presented in diverse scholarly writings, it

<sup>6</sup> The ICJ held in the *Nicaragua Case* that only “the most grave forms” of use of force “[...] of significant scale [...]”, which “[...] because of its scale and effects, would have been classified as an armed attack rather than a mere frontier incident [...]” could trigger the right to self-defence; see ICJ, *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, Merits, ICJ Rep. 1986, pp. 14–150, at pp. 101 and 103 paras. 191 and 195; see also ICJ, *Oil Platforms (Islamic Republic of Iran v. United States of America)*, ICJ Rep. 2003, at p. 161 para. 51.

<sup>7</sup> See A. Randelzhofer, “Article 51”, in B. Simma (ed.), *supra* note 3, at paras. 4 and 20; M. Bothe, “Völkerrechtliche Verhinderung von Gewalt (*ius contra bellum*)”, in W. Graf Vitzthum, *Völkerrecht* (Berlin, De Gruyter, 2001), Section 8, at para. 10; R. Higgins, *Problems and Process: International Law and How We Use It* (Oxford, Oxford University Press, 1994), at p. 250.

<sup>8</sup> A good overview on the discussion is given by M. Roscini, “Word Wide Warfare – Jus ad bellum and the Use of Cyber Force”, Vol. 14 *Max Planck Yearbook of United Nations Law* 2010, pp. 85–130, at pp. 104–106; see also A. Randelzhofer, “Article 2(4)”, in B. Simma (ed.), *supra* note 3; Th. Bruha, “Use of Force, Prohibition of”, in R. Wolfrum & Ch. Philipp (eds.), *United Nations: Law, Policies and Practice*, (Vol. II., München, Springer, 1995), at pp. 1387 *et seq.*

<sup>9</sup> Randelzhofer, *supra* note 8, at para. 21.

<sup>10</sup> ICJ, *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, ICJ Rep. 1986, pp. 14–150, at p. 118 *et seq.* para. 228.

<sup>11</sup> See e.g. Randelzhofer, *supra* note 8.

<sup>12</sup> For detailed discussion see K. Ziolkowski, “Computer Network Operations and the Law of Armed Conflict”, Vol. 49 *Military Law and the Law of War Review* 2010, pp. 47–94, at pp. 69–75.

can be assumed that malicious cyber activities can be considered “use of [armed] force” in the meaning of Article 2(4) of the UN Charter if they – indirectly – result in<sup>13</sup>:

- Deaths or physical injuries of living beings and/or the destruction of property.<sup>14</sup>
- Massive, medium to long-term disruption of critical infrastructure systems of a State (if in its effects equal to the physical destruction of the respective systems).<sup>15</sup>

Neither the destruction of data (even of substantial importance, e.g. classified data, or of significant economical value, e.g. symbolising assets)<sup>16</sup> nor the “theft”<sup>17</sup> (rather: illegal copying) of data (being nothing more than modern espionage<sup>18</sup> not generally forbidden under public international law) can be considered “use of [armed] force”.<sup>19</sup> Such effects cannot be equated to the effects usually caused or intended by conventional or BC-weapons, especially not to the physical destruction of objects.<sup>20</sup> Furthermore, it is agreed by the vast majority of scholars, that malicious cyber-activities targeted at critical infrastructure systems of a State, which do not exceed the threshold of merely minimally affecting the population’s quality of life or going beyond a mere inconvenience, are not showing effects of disruption of the public life

<sup>13</sup> *Ibid.*

<sup>14</sup> Y. Dinstein, “Computer Network Attack and Self-Defense”, in M.N. Schmitt & B.T. O’Donnell (eds.), *Computer Network Attack and International Law* (Newport / Rhode Island, US Naval War College, 2002), pp. 59–71, at p. 103; D.B. Silver, “Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter”, in Schmitt & O’Donnell, at p. 85; J. Barkham, “Information Warfare and International Law on the Use of Force”, Vol. 34 *New York University Journal of International Law & Politics* 2001, at p. 80; T. Morth, “Considering Our Position. Viewing Information Warfare as Use of Force Prohibited by Article 2(4) of the U.N. Charter”, Vol. 30 *Case Western Reserve Journal of International Law* 1998, at p. 591; T. Stein & T. Marauhn, “Völkerrechtliche Aspekte von Informationsoperationen”, Vol. 60 *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* 2000, pp. 1–60, at p. 7; C.C. Joyner & C. Lotrionte, “Information Warfare as International Coercion: Elements of a Legal Framework”, Vol. 12 *European Journal of International Law* 2001, at pp. 846 and 850; M.N. Schmitt, “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework”, Vol. 37 No. 3 *Columbia Journal of Transnational Law* 1999, at pp. 914 *et seq.*; W.G. Sharp, *Cyberspace and the Use of Force* (Falls Church, Aegis Research Cooperation, 1999), at p. 102; and L.T. Greenberg, S.E. Goodman & K.J. Soo Hoo, *Information Warfare and International Law* (Washington, National Defence University, 1998), at pp. 19 and 32.

<sup>15</sup> Ziolkowski, *supra* note 12, at pp. 69–75; J.P. Terry, “Responding to Attacks on Critical Computer Infrastructure. What Targets? What Rules of Engagement?”, in Schmitt & O’Donnell (eds.), *supra* note 14, at pp. 428 *et seq.*; Morth, *supra* note 14, at p. 599; Sharp, *supra* note 14, at pp. 129 *et seq.* *Contra*: Dinstein, *supra* note 14, at p. 105; and Stein & Marauhn, *supra* note 14, at p. 8, who demand the occurrence of physical damage outside the targeted computer networks in order to qualify CNO as use of force.

<sup>16</sup> See Barkham, *supra* note 14, at p. 88.; M.N. Schmitt, D.H.A. Harrison & Th.C. Wingfield, *Computers and War: The Legal Battlespace* (International Humanitarian Law Research Institute, Background Paper, 2004), at pp. 5 *et seq.*

<sup>17</sup> Joyner & Lotrionte, *supra* note 14, at pp. 846, 855 *et seq.*; *contra*: Stein & Marauhn, *supra* note 14, at p. 10.

<sup>18</sup> A. D’Amato, “International Law, Cybernetics, and Cyberspace”, in M.N. Schmitt & B.T. O’Donnell (eds.), *supra* note 14, pp. 59–71, at p. 67; and Stein & Marauhn, *supra* note 14, at p. 32 with further references. In regard to cyber-activities as a modern form of espionage see W.H. von Heinegg, “Informationskrieg und Völkerrecht. Angriffe auf Computernetzwerke in der Grauzone zwischen nachweisbarem Recht und rechtspolitischer Forderung”, in V. Epping, H. Fischer & W.H. von Heinegg (Hrsg.), *Brücken bauen und begehen. Festschrift für Knut Ipsen zum 65. Geburtstag* (München, C.H. Beck, 2000), at p. 134. Apart from the penalisation of espionage resulting from respective national law systems, spying is restrained by certain provisions of public international law, e.g. the taboos stated by the diplomatic and consular law protecting diplomatic and consular archives and correspondence, i.e. respective electronic databases and communication via the Internet.

<sup>19</sup> Ziolkowski, *supra* note 12, at pp. 69–75.

<sup>20</sup> For detailed discussion see *ibid.*

and *ordre public* similar to physical destruction by e.g. a bombardment and, therefore, do not amount to “use of [armed] force”.

### 3. THE “SCHMITT-CRITERIA”

“Use of [armed] force” in the meaning of Article 2(4) of the UN Charter is to be distinguished especially from measures of mere (economic or political) coercion<sup>21</sup> in international relations, a task that can pose considerable challenges upon decision-makers in practice. For facilitating such a distinction, in 1999<sup>22</sup> Professor Schmitt developed and recently reinforced<sup>23</sup> a set of criteria for the determination of “use of [armed] force” (amending their descriptions over time). The factors shall serve as indicators which States are likely to take into consideration when assessing whether specific malicious cyber-activities qualify as “use of [armed] force”.<sup>24</sup>

These criteria are:<sup>25</sup>

“1) *Severity*: Consequences involving physical harm to individuals or property will alone amount to a use of force. Those generating only minor inconvenience or irritation will never do so. Between the extremes, the more consequences impinge on critical national interests, the more they will contribute to the depiction of a cyber operation as a use of force. In this regard, the scale, scope, and duration of the consequences will have great bearing on the appraisal of their severity. Severity is self-evidently the most significant factor in the analysis.

2) *Immediacy*: The sooner consequences manifest, the less opportunity states have to seek peaceful accommodation of a dispute or to otherwise forestall their harmful effects. Therefore, states harbor a greater concern about immediate consequences than those that are delayed or build slowly over time.

3) *Directness*: The greater the attenuation between the initial act and the resulting consequences, the less likely states will be to deem the actor responsible for violating the prohibition on the use of force. Whereas the immediacy factor focused on the temporal aspect of the consequences in question, directness examines the chain of causation. For instance, the eventual consequences of economic coercion (economic downturn) are determined by market forces, access to markets, and so forth. The causal connection between the initial acts and their effects tends to be indirect. In armed actions, by contrast, cause and effect are closely related—an explosion, for example, directly harms people or objects.

4) *Invasiveness*: The more secure a targeted system, the greater the concern as to its penetration. By way of illustration, economic coercion may involve no intrusion at all

<sup>21</sup> See representatively: Ranzelzhofer, *supra* note 8, at para. 21.

<sup>22</sup> Schmitt, *supra* note 14, at pp. 913 *et seq.*

<sup>23</sup> M.N. Schmitt, “Cyber Operations and the *Jus Ad Bellum* Revised”, Vol. 56 *Villanova Law Review* 2011, at pp. 576 *et seq.* The criterion of “responsibility” was mentioned already in the 1999 publication, although only in a footnote, see Schmitt, *supra* note 14, at p. 915, footnote 81.

<sup>24</sup> *Id.*, at p. 605.

<sup>25</sup> *Id.*, at pp. 576 *et seq.*

(trade with the target state is simply cut off), whereas in combat the forces of one state cross into another in violation of its sovereignty. The former is undeniably not a use of force, whereas the latter always qualifies as such (absent legal justification, such as evacuation of nationals abroad during times of unrest). In the cyber context, this factor must be cautiously applied. In particular, cyber exploitation is a pervasive tool of modern espionage. Although highly invasive, espionage does not constitute a use of force (or armed attack) under international law absent a nonconsensual physical penetration of the target state's territory, as in the case of a warship or military aircraft which collects intelligence from within its territorial sea or airspace. Thus, actions such as disabling cyber security mechanisms to monitor keystrokes would, despite their invasiveness, be unlikely to be seen as a use of force.

5) *Measurability*: The more quantifiable and identifiable a set of consequences, the more a state's interest will be deemed to have been affected. On the one hand, international law does not view economic coercion as a use of force even though it may cause significant suffering. On the other, a military attack that causes only a limited degree of destruction clearly qualifies. It is difficult to identify or quantify the harm caused by the former (e.g., economic opportunity costs), while doing so is straightforward in the latter (X deaths, Y buildings destroyed, etc).

6) *Presumptive legitimacy*: At the risk of oversimplification, international law is generally prohibitory in nature. In other words, acts which are not forbidden are permitted; absent an express prohibition, an act is presumptively legitimate.[...] For instance, it is well accepted that the international law governing the use of force does not prohibit propaganda, psychological warfare, or espionage. To the extent such activities are conducted through cyber operations, they are presumptively legitimate.

7) *Responsibility*: The law of state responsibility [...] governs when a state will be responsible for cyber operations. But it must be understood that responsibility lies along a continuum from operations conducted by a state itself to those in which it is merely involved in some fashion. The closer the nexus between a state and the operations, the more likely other states will be inclined to characterize them as uses of force, for the greater the risk posed to international stability.”

#### 4. SOME THOUGHTS ON THE “SCHMITT-CRITERIA”

The criteria, which – pursuant to the knowledge of the author – hitherto have not been analysed in depth within academic writings, contain a range of significant aspects and refer to complex matters; therefore, they deserve a substantial discussion. The following considerations aim to initiate such a debate.

##### *Severity*

As Professor Schmitt states, the criterion of “severity” is the most significant in the analysis of malicious cyber-activities. Insofar as the criterion refers to “physical harm to individuals or property”, it is congruent with the above presented view that malicious cyber activities indirectly

resulting in “deaths or physical injuries of living beings and/or the destruction of property” can be considered “use of [armed] force” in the meaning of Article 2(4) of the UN Charter. The author of the present survey would argue that the “massive, medium to long-term disruption of critical infrastructure systems of a State (if in its effects equal to the physical destruction of the respective systems)” would also be covered by the “Schmitt-Criterion” of “severity”. Disabling critical infrastructure systems, massive in scope and duration, can be equated to “physical harm to property” in the sense of eliminating the functionality of the targeted systems. In either the case of kinetic destruction of the components of a critical infrastructure system or in the case of total disabling of the system, the system in question cannot serve its purpose and must be – in whatever way – repaired in order to function.

The author of the present survey subscribes to the criterion of “severity” and its importance, except for the aspect of the relevance of “critical national interests” (“Between the extremes, the more consequences impinge on critical national interests, the more they will contribute to the depiction of a cyber operation as a use of force”). The prohibition of the “use of [armed] force” in international relations in the meaning of Article 2(4) of the UN Charter (and the right to self-defence, given in most severe cases of “use of [armed] force”) does not protect the national interests – which can be manifold, including e.g. economic interests – but rather the (physical) security of a State and its population. This threshold is high and, for the sake of international peace and security, should not be diluted.

As a final thought on the criterion of “severity” of the effects of malicious cyber-activities, the author of the present survey argues that in the future a debate on the so-called “accumulation of events” or “Nadelstichtaktik” doctrine will present a necessary part of the discussion in regard to cyberspace. The abovementioned approaches were elaborated in the legal literature in order to categorise the “hit and run” or guerrilla tactics within the *ius ad bellum* and where used in the political practice of the USA and Israel in the course of justifications of forceful measures conducted against “terrorists” in the past (partly condemned by the UN Security Council as “retaliation”).<sup>26</sup> This thought is based on a certain tendency visible in cyberspace. Malevolent data-streams, accumulating to a malicious code at its destination, are being deliberately sent in an extremely slow manner and in small pieces in order to be classified by the security-sensors of the targeted computer systems as “background noise” and not as a danger. It is conceivable that in the future such a segmented course of action could also be conducted in regard to the (physical) effects caused by malicious cyber-activities. For example, the malfunctioning of a few critical infrastructure systems of a State could be caused by and by, each of which would rather be classified as a mere nuisance than “use of [armed] force” – a finding which could turn out differently if the malfunctioning of the different systems at different times were judged in terms of their “accumulation”.

### *Immediacy*

The explanatory text to the criterion suggests that “immediacy” of consequences of malicious cyber-activities is an aspect but not a requirement for their classification as “use of [armed] force”.

<sup>26</sup> See examples of State practice, UN Security Council resolutions and a discussion in K. Ziolkowski, *Gerechtigkeitspostulate als Rechtfertigung von Kriegen* (Baden-Baden, Nomos, 2008), at pp. 229-231.

This is of importance because it is very likely that the consequences of malicious cyber-activities – even if immediately given – will mostly not be recognisable or not recognised as such for a certain period of time. This is based on the complexity of modern computer systems and the large number of possible errors, which can lead to the malfunctioning of the systems. In the case of malfunctioning of computer systems it will always be investigated first whether the problem is caused by a programming error of the software-producer, by a malfunction of outsourced computer services providers, by mal-configuration of the systems by the own system administrators, or by errors of the users of the system. Additionally, it is conceivable that in cases of malicious cyber-activities against critical infrastructure systems of a State, a vast majority of which is owned and operated by private industry, both intrusions into the computer systems and their perceptible effects would be covered in order to not lose confidence in the security of the respective services and to preserve the own reputation and the customers' trust. A long period of time can pass by before malicious data-streams will be discovered and analysed and finally brought into context with the negative effects on governmental levels dealing with questions of national security and foreign policy. For example, the worm Stuxnet was discovered in July 2010 in the computer systems of Iranian nuclear power installations, “but is confirmed to have existed at least one year prior and likely even before”<sup>27</sup>. By February 2010 the IT-security company *Symantec* – monitoring the command and control traffic of the worm – had gathered 3,280 unique samples representing three different variants of *Stuxnet*.<sup>28</sup> Media reports of the replacement<sup>29</sup> of a remarkable number of centrifuges in the nuclear enrichment facility at *Natanz* could – although hitherto not confirmed<sup>30</sup> by Iranian officials – indicate that the effects of the malicious codes were conceivable in the past but not brought into context with a possible computer system problem. However, as e.g. border intrusions by military forces of a neighbouring State in a (geographically) remote area of a victim State's territory would constitute a “use of [armed] force”, although not recognisable to the victim State immediately, malicious cyber-activities, although their perceptible (physical) effects are not recognisable yet as such, can also theoretically be classified as “use of [armed] force”.

Thus, given the complexity of cyberspace and the large number of possible reasons for malfunctioning of computer systems, the recognition of the connection between malicious cyber-activities and their perceivable (physical) effects cannot be expected to occur immediately. Therefore, the relevance of the criterion of “immediacy” – although perfectly logical as such – could be minimised in hacking-cases showing a scope of sophistication that raises the political concern of a State in terms of *ius ad bellum*.

### *Directness*

The criterion of “directness” describes the direct casual connection between the initial act and the resulting consequences of malicious cyber-activities. The explanatory text contrasts

<sup>27</sup> N. Falliere, L.O. Murchu & E. Chien, *W32.Stuxnet Dossier* (Symantec Publication, Version 1.4, February 2011), at pp. 2 and 4, available at [http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_stuxnet\\_dossier.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf) (last visited 18 April 2012).

<sup>28</sup> *Id.*, at p. 7.

<sup>29</sup> See D. Albright, P. Brannan & Ch. Walrond, *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report* (ISIS Report of 15 February 2011), at p. 3, available at [http://isis-online.org/uploads/isis-reports/documents/stuxnet\\_update\\_15Feb2011.pdf](http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf) (last visited 16 April 2012); Y. Katz, “Stuxnet may have destroyed 1,000 centrifuges at Natanz”, in *The Jerusalem Post* online of 24 December 2010, available at <http://www.jpost.com/Defense/Article.aspx?id=200843> (last visited 16 April 2012).

<sup>30</sup> A denial of any physical damage by Iranian officials was reported by Reuters, “After Stuxnet: Iran says it's discovered 2nd cyber attack”, in *The Jerusalem Post* online of 25 April 2011, available at <http://www.jpost.com/IranianThreat/News/Article.aspx?id=217795> (last visited 16 April 2012).

the “directness” of the consequences of armed actions with the indirectness of e.g. economic coercion. This assessment is certainly true. However, the directness of the consequences of military actions can only apply to conventional kinetic operations – it is conceivable that the employment of BC-weapons in international relations, which will very likely always be considered “use of [armed] force”, can show already a much weaker “directness” between their employment and the effects caused. The picture can change dramatically, if the range of remote weapon systems at the disposal of highly developed military forces, and especially the development of offensive military cyber capabilities, is considered.

However, the criterion of “directness” between the initial act and the resulting consequences seems problematic. The criterion determines, as Professor Schmitt rightly states, the conditions of attribution of certain perceptible consequences to a certain action in terms of causation (and maybe also a direct nexus?) between an action and the effects of that action. According to the understanding of the author of the present survey, the causation and direct nexus between an action and the effects of an action cannot be part of the assessment of the legal nature of the action as such. Therefore, the criterion of “directness” cannot be used for the classification of the nature of a malevolent action as being or not being “use of [armed] force”. This opinion is certainly based on the different, rather dogmatic approach to the line of argumentation inherent to the civil law system.

### *Invasiveness*

Subject to further discussion, it could be beneficial to clarify how the criterion of “invasiveness” shows relevance beside the criterion of “severity”, the latter one describing the requirements of perceivable physical effects of malicious cyber-activities (not on the affected data only) in order to be likely to be categorised as “use of [armed] force”. Especially, espionage by the means of the Internet or other information and communication technologies, i.e. illegal copying of data, would clearly be excluded from such a categorisation by applying the criterion of “severity”.

Further, the same arguments and examples as demonstrated at the discussion of the criterion of “immediacy” are likely to apply to the criterion of “invasiveness”, i.e. “invasiveness” of malicious cyber-activities could be imperceptible for a long period of time – for different reasons – and thus the relevance of the criterion could be minimised in practice.

Finally, it shall be mentioned that the criterion of “invasiveness” could show a certain potential for misuse, if the invasiveness of malicious cyber-activities were applied in the context of “national interest” when assessing malicious cyber-activities in the context of *ius ad bellum*. The prohibition of the “use of [armed] force” in international relations in the meaning of Article 2(4) of the UN Charter (and the right to self-defence, given in most severe cases of “use of [armed] force”) does not protect national interests (see above).

### *Measurability*

The criterion of “measurability” of effects of malicious cyber-activities, or rather their “appearance”, is certainly an important one. It could be seen as complementing the criterion of “severity” of effects, although it might be beneficial for future discussions to further specify the relationship between these two criteria.

However, apparent effects of malicious cyber-activities will not always be measurable. For example, in the case of successful malicious cyber-activities against critical infrastructures of a State, apparent secondary, tertiary etc. effects, e.g. panic reactions within the population, disturbances of public order etc. (comparable to effects caused by e.g. a bombardment), will hardly be measurable. However, an aggressor who chooses a sophisticated way and modern means (i.e. malicious cyber-activities) for causing such effects of public disturbance, should not benefit from the fact that such effects are difficult to measure and, therefore, the classification of the actions as “use of [armed] force” could fail due to the requirement of the criterion of “measurability” of the effects. Therefore, indeed, the criterion should be used with caution.

Further, covering penetrations of computer systems and their negative effects by private companies, which own and operate the vast majority of critical infrastructure systems of a State (see above), could also minimise the relevance of the criterion in practice.

### *Presumptive legitimacy*

Again, due to the rather dogmatic approach inherent to the civil law system, the criterion of “presumptive legitimacy” seems – from this perspective – problematic for several reasons:

First of all, “legitimacy” (describing an ethically justifiable act) is rather a term of political and ethical discourse; law deals with legality and illegality of actions. The judgement of (il)legality of actions inherently involves questions of (il)legitimate behaviour, but only in the understanding of the nature of law as reflecting commonly agreed norms of morality and ethics, and as far as the (international) law explicitly foresees an ethical assessment by an individual or a group of individuals (e.g. in regard to the determination of the term “excessive” or of the notion of “proportionality”). Further, assuming that legitimacy of an action indicates its legality, the criterion seems to contain a circular reasoning: The presumption of legitimacy cannot be part of the assessment of the legality. In other words, it cannot be decided whether a particular act is indeed legal under the *ius ad bellum* by the simultaneous assertion or indication of its legality at the same time. Moreover, it seems problematic to assume that legitimacy would have an impact on the assessment of the legality of an act (in our case: under the *ius ad bellum*). For example, in 1999 the military campaign in Kosovo, which was conducted without the consent of the State in question and without authorisation from the UN Security Council, and aimed to rescue a certain ethnic group likely to suffer ethnic cleansing, was determined by the “Independent International Commission on Kosovo” in its respective report as “illegal but legitimate”.<sup>31</sup> This shows that (presumed or determined) legitimacy does not have an impact on the assessment of the legality. Last but not least, the “first sight” (or “jurisprudential intuition”?) of the legality of an action, indicated by the (subjective) perception of its legitimacy, cannot be part of a thorough legal assessment of a situation in question.

Even if the above considerations are ignored, the criterion shows potential for further discussion: The criterion of “presumptive legitimacy” shall help distinguish “use of [armed] force” from acts like propaganda, psychological warfare or espionage, which are not forbidden under the *ius ad bellum*. However, “psychological warfare”, according to the understanding of the author of the present survey, can be conducted only as the first step of or in the course of an already ongoing military operation, i.e. after the threshold of *ius ad bellum* has been crossed. Therefore,

<sup>31</sup> Independent International Commission on Kosovo, *Kosovo Report: Conflict, International Response, Lessons Learned* (Oxford, Oxford University Press, 2000), at p. 2.

the example of “psychological warfare” is not helpful in determining whether an activity would cross the abovementioned threshold. As for the examples of espionage and propaganda (the latter probably even if reaching the level of inciting insurgency against another State’s government), the criterion of “severity” could already rule out those activities as constituting “use of [armed] force”.

### *Responsibility*

The criterion of [State] “responsibility” addresses an especially complex issue, which has already initiated many debates within the legal and political sciences and which will surely be of most importance in the future. A thorough discussion of the topic would certainly exceed the scope of this paper. Therefore, in the following, a few thoughts will be sketched, hopefully initiating future discussions in more depth.

Cyberspace enables (skill and knowledge-wise) super-empowered individuals and groups of individuals to cause the most severe physical effects through manipulations of computer systems that the functioning of highly developed post-industrial countries depends on. Due to the possibility to act anonymously in cyberspace and to masquerade and hide the data streams, it will probably always be a major challenge to attribute malicious cyber-activities to a State. The technical attribution as well as the legal attribution (in the meaning of obtaining tangible evidence in form of Internet protocols from all the servers, nodes and switches the data stream was passing on its way around the world) are very limited in cases of highly sophisticated cyber-activities. The political attribution has – in a way – more freedom of action, as it can work with factors like the assessment of the overall political situation and can apply e.g. the *cui bono* test. However, taking into account the supposed indirect and quiet use of “proxies”, e.g. patriotic hackers (hacktivists), by certain States, invoking State responsibility for cyber-activities will very seldom meet the legal requirements as currently set by international jurisdiction and scholarly writings, i.e. the test of an “effective” or “overall” control of the State over the activities of the non-State actors.<sup>32</sup>

Considering the enormous difficulties in this context, it was proposed in diplomatic circles to introduce the principle of “due diligence” of States in regard to activities of non-State actors originating from the States’ territories. Indeed, a principle of “due diligence” can be identified in public international law, as States do have the obligation not to let their own sovereign territory be used for activities causing damage to another State. Such a principle can be derived from the principles of sovereign equality of States and of good neighbourship (see also Articles 2(1) and 1(2) of the UN Charter), and can be supported by several resolutions of the UN General Assembly (see e.g. Friendly Relations Resolution<sup>33</sup> and Definition of Aggression<sup>34</sup>). The obligations and rights deriving from such a “due diligence” principle are already expressed

32 The discussion of the control levels for actions of non-State actors in the context of State responsibility would certainly exceed the scope of the present paper. For further information see e.g. A. Cassese, “The Nicaragua and Tadic Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia”, Vol. 18 *European Journal of International Law* 2007, pp. 649 *et seq.*

33 Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, A/RES/2625 (XXV) of 24 October 1970, Annex.

34 Definition of Aggression, A/RES/3314 (XXIX) of 14 December 1974, Annex.

in numerous international treaty provisions<sup>35</sup>, in various States' declarations<sup>36</sup>, and are endorsed by the jurisdiction of the ICJ<sup>37</sup> in regard to international environmental law. A "due diligence" in regard to cyberspace would surely involve the implementation of precautionary measures, including political, organisational, administrative, legal and technical measures in order to prevent the misuse of the possibilities that cyberspace offers for malicious activities by non-State actors harming other States. However, it is rather doubtful that violating the "due diligence" obligations would automatically lead to the responsibility of a State for all malicious cyber-activities originating in its territory without considering requirements that the current law of State responsibility sets.

It was also proposed during a conference to use the concept of "reverse of proof" as is known in many national legal systems. However, such a reverse of proof would establish a *prima facie* responsibility of a State for all malicious cyber-activities which seem to originate from the State's territory. This could lead to undesirable results. For example, despite the greatest efforts, the data stream between the worm *Stuxnet* and its creators could be traced the farthest to command and control servers located<sup>38</sup> in Denmark and Malaysia – States clearly not suspected to be responsible for the creation, implementation, control of and effects supposedly caused by *Stuxnet* in either legal or political terms.

The "safe haven" theory<sup>39</sup>, developed in the context of Article 51 of the UN Charter in regard to terrorists acting from the territory of so-called "failed States" or States unwilling or unable to impede activities of non-State actors harmful to other States, would be a valuable thought also in regard to the State responsibility for malicious cyber-activities of non-State actors otherwise qualifying as "use of [armed] force" and enabling the victim State to legally conduct a range of possible retorsions and counter-measures. However, this approach would also not conform to the current law of State responsibility, thus further discussions within the international community will be necessary.

The question of whether individuals can trigger the right to self defence<sup>40</sup> could be relevant – in parallel – also in regard to the question of whether non-State actors could undertake activities otherwise judged as "use of [armed] force" and triggering the right of States to undertake retorsions and counter-measures. There are considerable pros and cons – their demonstration would, unfortunately, clearly exceed the scope of this paper.<sup>41</sup> Considering the power the

35 See an overview of treaties on international environment protection deposited with the UN at the UN Treaty Collection Website, available at <http://treaties.un.org/Pages/Treaties.aspx?id=27&subid=A&lang=en> (last visited 17 April 2012). It shall be mentioned that the overview does not contain (numerous) regional treaties, especially the ones on international regimes for the use of rivers, lakes and other territorial waters.

36 L. Gründling, "Environment, International Protection", in R. Bernhardt (ed.), *Encyclopedia of Public International Law* (Vol. II., 1995), p. 96 *et seq.*, at p. 101.

37 See ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, ICJ Rep. 1996, p. 226 *et seq.*, at p. 241 *et seq.* para. 29; ICJ, *Gabikovo-Nagymaros Project (Hungary v. Slovakia)*, ICJ Rep. 1997, p. 7 *et seq.*, at p. 41 para. 53. See also *Trail Smelter Case (United States, Canada)*, 16 April 1938 and 11 March 1941, in *United Nations, Reports of International Arbitral Awards*, (Vol. III, United Nations Publication, 2006), pp. 1905-1982, available at [http://untreaty.un.org/cod/riaa/cases/vol\\_III/1905-1982.pdf](http://untreaty.un.org/cod/riaa/cases/vol_III/1905-1982.pdf) (last visited 16 April 2012).

38 Falliere, Murchu & Chien, *supra* note 27, at p. 21.

39 For an overview on the major lines of argumentation see Schmitt, *supra* note 23, at p. 602 *et seq.*

40 *Id.*, at pp. 600-602.

41 See e.g. Ziolkowski, *supra* note 26, at pp. 221-229, demonstrating the lines of interpretation of Article 51 of the UN Charter, of the respective international customary law, as well as of international jurisdiction, State practice and resolution practice of UN organs after the events of 9 September 2001.

Internet gives, especially to skilled and knowledgeable individuals, a respective discourse can very probably not be avoided in the future.

## 5. CONCLUDING REMARKS

“Use of [armed] force” is given in the case of malicious cyber-activities which (indirectly) cause (1) deaths or (2) physical injuries of living beings, (3) destruction of property or (4) medium to long-term disruption of critical infrastructure systems of a State, if the effects are equal to the physical destruction of the respective systems. When additionally showing a considerable scope and intensity of effects, such malevolent cyber-activities can be considered an “armed attack”, triggering the right of a State to self-defence. The criteria thus stay – deliberately – vague.

Given the highly political nature of the question of whether “use of [armed] force” in international relations or an “armed attack” occurred and, subsequently, a State considers itself in the right to undertake either a range of unfriendly acts and counter-measures or self-defence measures, more meticulous criteria for such an assessment seem inappropriate. Even if States would develop internal guidance on such questions, it is likely that they would display a considerable grade of abstraction. Only such general criteria will leave enough room for political manoeuvring in a process of decision-making, which potentially can lead to political tensions, disturbance of international peace and security and – as *ultima ratio* – to the possible rigorous result of resorting to use of force.

Additionally, the effects-based approach to the question of whether particular malicious cyber-activities are to be considered “use of [armed] force” or an “armed attack” should lead to the conclusion that the criteria for a respective decision taken by a State will perfectly resemble those used to identify whether conventional military actions causing similar effects would be considered as comprising such situations. Therefore, there is no need for the development of special criteria for malicious cyber-activities going beyond those focusing on the effects (indirectly) caused.

The assessment of malicious or damaging activities, reaching the level of political concern, cannot make a difference according to the – rather conventional or rather modern – means used in order to cause the effects raising political concern. Therefore, only criteria referring to the effects caused should be considered appropriate.

The author of the present survey acknowledges that the proposed general criteria will not be useful in situations “[...] in which the necessity of self-defence is instant, overwhelming, leaving no choice of means, and no moment for deliberation.”<sup>42</sup>, i.e. in the situation of an immediate “armed attack” triggering the so-called preventive self-defence. This is based on the fact that – despite additional intelligence – the intended effect of malevolent cyber-activities will not be visible beforehand. Very likely, cases of (legal) preventive self-defence will stay theoretical. Moreover, judged from today’s perspective, even in the case of discovery of malicious codes in e.g. governmental computer networks there still would be a “choice

<sup>42</sup> Quoted in I. Brownlie, *International Law and the Use of Force by States* (Oxford, Clarendon Press, 1963), at p. 43.

of means” and a “moment for deliberation”. Malware can be isolated, penetrated networks disconnected and IT-security measures directed at the targeted networks – instead of more drastic, including forceful, measures directed against the malevolent aggressor. At the end of the day, the prohibition of the use of force in international relations and the right to self-defence do not protect the interest in modernity and comfort of life, economic returns or other national interests as such. The threshold of endangering the (physical) security of a State is a high one and should not be diluted.

Finally, it shall be mentioned that in regard to the academic discussions, whether a certain category of a malicious cyber-activity can be considered “use of [armed] force” or “armed attack”, the – otherwise very commendable – distinction between *lex lata* and *lex ferenda*, as stated by many scholars, might be not always be appropriate. A line of argumentation can only be presented *de lege ferenda* if it differs from the already existing law. The discussions, however, mostly examine how the already existing law applies to cyberspace. Indeed, the development of a common understanding of the interpretation of the *ius ad bellum* in regard to cyberspace is very much needed, in terms of both the scientific research and the use for political practice; academia and Professor Schmitt, especially, is to be congratulated for pioneering with benefit for both areas.

# The 'Use of Force' in Cyberspace: A Reply to Dr Ziolkowski

**Michael N. Schmitt**

International Law Department  
United States Naval War College  
Newport, U.S.A.  
schmitt@aya.yale.edu

**Abstract:** This article responds to Dr Ziolkowski's article *Ius ad bellum in Cyberspace – Some Thoughts on the 'Schmitt-Criteria' for Use of Force*. It discusses the distinction between the terms 'use of force' and 'armed attack' in an effort to situate the former as a legal term of art. The article concludes that as the meaning of use of force is uncertain, it is useful to identify those factors that States are likely to take into consider when faced with the need to characterize an action. Such factors may be legal in nature, but will also often reflect national security interests.

**Keywords:** *use of force, Article 2(4) UN Charter, Schmitt Criteria*

Over a decade ago, I had the occasion to consider the *jus ad bellum* implications of 'computer network attack' in an article published in the *Columbia Journal of Transnational Law*.<sup>1</sup> At the time, such operations were emerging as a new method of warfare, but international legal assessments thereof lagged far behind. Although the piece drew a degree of attention,<sup>2</sup> interest in cyber matters rapidly faded as transnational terrorism captured the international legal community's attention following the horrific '9/11' attacks.

The cyber operations mounted by hacktivists against Estonia in 2007, as well as employment of cyber operations during the international armed conflict between Georgia and Russia the next year, refocused attention on the subject. Since then, cyber issues have dominated discussions among international lawyers and international security specialists. In reaction to these and other cyber incidents, most notably the 2010 Stuxnet attack, States have formulated national cyber

<sup>1</sup> Michael N. Schmitt, *Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework*, 37 *Columbia Journal of Transnational Law* 885 (1999). The *jus ad bellum* is that aspect of international law that addresses when it is that States may lawfully resort to use force as an instrument of their national policy. It must be distinguished from the *jus in bello*, which concerns how hostilities may be conducted once an armed conflict is underway. The latter body of law is also labeled international humanitarian law.

<sup>2</sup> The term was coined in Thomas C. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace* (2000).

strategies,<sup>3</sup> formed cyber military units,<sup>4</sup> and established international centres dedicated to examining cyber conflict.<sup>5</sup>

Of particular note in this regard is a Cooperative Cyber Defence Centre of Excellence (CCD COE) funded project to draft *The Tallinn Manual on the International Law of Cyber Warfare*. As director of the project, I have benefitted from the knowledge and insights of the group of 25 world-class international legal and technical experts who have been participating in the effort, which will conclude this summer. Among the topics they have explored is the legal notion of ‘use of force’. In the process, the group submitted the so-called ‘Schmitt Criteria’ for the use of force that I had originally set forth in the *Columbia Journal* article to a rigorous peer review. I remain convinced that they are sound, at least when applied as I originally intended.<sup>6</sup>

My friend and colleague Dr Katharina Ziolkowski has graciously asked me to pen a reply to her impressive and insightful contribution to this volume in which she offers thoughts on my criteria. I am delighted to engage in this ‘dialogue’ with her and hopefully clarify my approach somewhat. It is comforting to know that our overall conclusions part ways only at the margins.

The question at hand is when does a cyber operation amount to a use of force in the *jus ad bellum* sense? The prohibition on the use of force is codified in Article 2(4) of the United Nations Charter. That article, which applies only to the actions by or attributable to States, provides:

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.

Article 2(4) must be juxtaposed to Article 51:

Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.

Self-defence as provided for in Article 51 constitutes one of the two universally recognised exceptions to Article 2(4)’s prohibition on the use of force by States (the other being an authorization or mandate to use force pursuant to Article 42)<sup>7</sup>; it is universally recognized as

<sup>3</sup> See, e.g., Department of Defense, *Strategy for Operating in Cyberspace* (July 2011); White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (May 2011).

<sup>4</sup> E.g., United States Cyber Command.

<sup>5</sup> E.g., The Cooperative Cyber Defence Centre of Excellence, a NATO centre of excellence.

<sup>6</sup> For my most recent discussion of the criteria, see Michael N. Schmitt, *Cyber Operations and the Jus ad Bellum Revisited*, 56 Villanova Law Review 569 (2011).

<sup>7</sup> Although Article 2(4) refers to a prohibition on “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”, it is clear that the prohibition extends to any use of force not authorized by the Charter. Originally, the draft Charter contained no reference to territorial integrity or political independence. Their subsequent inclusion was controversial; the “other manner” language was inserted to make clear that their inclusion was not meant to limit the article’s reach.

reflective of customary international law.<sup>8</sup> The Charter's scheme is quite simple in the abstract – a State may *use force* when facing an armed *attack*.<sup>9</sup>

Note that the two articles employ different terminology – ‘use of force’ and ‘armed attack’. The Charter's *travaux préparatoire* suggest that the difference was intentional. Negotiators at the 1945 San Francisco Conference, where the Charter was drafted and adopted, rejected the premises that ‘force’ was limited to ‘armed’ force and that actions qualifying as a use of force also necessarily qualified as an armed attack.<sup>10</sup>

In the *Nicaragua* case, the International Court of Justice addressed this carefully crafted distinction. It held that the terms embodied different legal thresholds. According to the Court, there are “measures which do not constitute an armed attack but may nevertheless involve a use of force”. In other words, it is necessary to differentiate “the most grave forms of the use of force from other less grave forms”.<sup>11</sup> The Court later reaffirmed the existence of this ‘gap’ in the *Oil Platforms* case.<sup>12</sup>

The distinction between the terms epitomizes the Charter's conceptual architecture. A horrendous conflagration initiated by States acting forcefully had just occurred, one resolved only through the collective action of other States. Accordingly, the Preamble identifies the key purpose of the United Nations as “sav[ing] succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind”. This purpose was to be accomplished by “unit[ing] our strength to maintain international peace and security”.<sup>13</sup> In light of these aims, it made sense to set a low threshold for qualification as acts that seriously endangered international security (use of force), but a high one for qualification as acts that rendered unilateral forceful actions permissible (armed attack).<sup>14</sup> A Security Council empowered to authorize forceful actions by a United Nations military force would presumably police the gap between the two, that is, act in response to actions that amounted to a use of force, but not an armed attack.<sup>15</sup> Thus, while Article 2(4) establishes when a State has violated international law by using force, Article 51 permits the use of force as a remedy for States victimized by certain egregious uses of force known as armed attacks.

<sup>8</sup> Military and Paramilitary Activities in and Against Nicaragua (*Nicaragua v. U.S.*), 1986 I.C.J. 14, paras. 185-190 (June 27). Note that some scholars dispute whether the treaty and customary norms are identical. For the purpose of this article, any possible differences are irrelevant. The author takes the position that they are in fact identical.

<sup>9</sup> States may also employ force in the face of an imminent armed attack under certain circumstances. Those circumstances do not bear on the points made in this article or Dr Ziolkowski's.

<sup>10</sup> See U.N. GAOR Special Comm. on Friendly Relations, U.N. Doc. A/ AC.125/SR.114 (1970).

<sup>11</sup> *Nicaragua Case*, *supra* note 8, paras. 191, 210.

<sup>12</sup> *Oil Platforms (Iran v. U.S.)*, 2003 I.C.J. 161, para. 51 (Nov. 6).

<sup>13</sup> UN Charter, preamble.

<sup>14</sup> The right of self-defence is interpreted by many States today as extending to acts conducted by non-State actors that meet the armed attack threshold. However, this premise is somewhat controversial. See Michael N. Schmitt, *Responding to Transnational Terrorism under the Jus ad Bellum: A Normative Framework*, in *International Law and Armed Conflict: Exploring the Faultlines* 157 (Michael N. Schmitt & Jelena Pejic eds., 2007).

<sup>15</sup> UN Charter, arts. 43-49. The Charter also envisioned actions “by some of the members” that were to be authorized by the Council. This has proven to be the prevailing response. Article 51's right of individual or collective self-defence was but a fail-safe mechanism in the event the system could not respond quickly enough, a point illustrated by Article 51's authorization to act defensively only “until the Security Council has taken measures necessary to maintain international peace and security.”

In light of this gap, it can be concluded that actions that do not qualify as an armed attack may nevertheless comprise a use of force. But what do the two terms mean? I have contended elsewhere that an armed attack is an action with consequences that involve death or injury of individuals or damage to objects.<sup>16</sup> Unfortunately, the meaning of the term use of force is more problematic. The Charter's text provides no guidance beyond structurally indicating that any armed attack is equally a use of force. Charter *travaux preparatoire* and subsequent events are of some assistance in that they demonstrate that the notion generally excludes economic or political coercion.<sup>17</sup> The *Nicaragua* case also provided examples of actions that qualify uses of force (arming and training guerrillas fighting against another State), and that do not (merely funding them).

What seems clear is that while all coercive actions are not uses of force, a use of force need not be armed (or necessarily even directly related to armed actions). Beyond this broad deduction, the criteria for qualification as a use of force remain abstruse. This uncertainty led to my proposal of the 'Schmitt Criteria'.

The criteria – severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility – are replicated in the article by Dr Ziolkowski and need not be described in detail here. However, before turning to my reflections on her comments, it is essential to grasp how the criteria were intended to be used ... and how they were not.

Despite the absence of a consensus understanding of the term use of force in either judicial pronouncements or State practice, States will sometimes be compelled to assess cyber operations against the prohibition set forth in Article 2(4) and contained in customary international law. At times, they will have to do so with respect to cyber operations conducted against them in order to decide whether to characterize the initiating State's actions as a violation of the norm. Sometimes, they will need to resolve whether other States will characterize cyber operations they are contemplating as a use of force. And in still other cases, they will have to assess cyber operations targeting other States. In light of the definitional lacuna described above, perhaps the best States can do is to engage in educated conjecture as to how the international community is likely to view the cyber operations in question as a matter of law.

The criteria were meant to assist in that effort. What is often misunderstood is that they are not legal criteria against which to perform such evaluations. For instance, the criteria do not have the legal status that the necessity, proportionality, and imminency/immediacy requirements associated with taking action in self-defence enjoy. Rather, they are merely factors that can be expected to influence States when making use of force appraisals. After all, what matters in international relations is not whether the actions in question are lawful in the abstract, but instead whether the international community considers them as such. Lest this assertion seem extreme, recall that customary international law is formed through the confluence of State

<sup>16</sup> See my other article in this volume, '*Attack as a Term of Art in International Law: The Cyber Operations Context*'.

<sup>17</sup> U.N. Doc. 2, G/7(e)(4), 3 U.N.C.I.O. Doc. 251, 253-54 (1945); Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), U.N. Doc. A/RES/8082 (Oct. 24, 1970); U.N. GAOR Special Comm. on Friendly Relations, U.N. Doc. A/AC.125/ SR.114 (1970); Report of the Special Committee on Principles of International Law Concerning Friendly Relations and Co-operation Among States, U.N. Doc. A/7619 (1969); Schmitt, *supra* note 6, at 574.

practice and *opinio juris*.<sup>18</sup> Consequently, an action that may have been unlawful in the past, but which is not viewed as such in the present, contributes to the eventual emergence of new customary norms.

Both the absence of meaningful State practice as to cyber operations (and the reaction thereto) and the definitional vagueness regarding the prohibition of the use of force signal that the law regarding the use of force in the cyber context is ripe for this evolutionary process. Therefore, for the immediate future, we can expect a period of relative flexibility in the application to cyber operations of the prohibition. As State practice accompanied by expressions of *opinio juris* develops, the law will slowly crystallize. Once this happens, prognostic criteria such as those I have proffered will be replaced by tangible legal requirements. In the meantime, States will continue to be influenced in their decisional process by factors like those I have suggested. They are, of course, non-exclusive, and their relative influence in matters of international security, including legal assessments as to State behaviour, is always contextual.

It should be evident that I am more cautious than Dr Ziolkowski with regard to characterizing the force contemplated in the prohibition as ‘armed’. Nevertheless, despite terminological divergence, we arrive a roughly the same conclusion as to force which causes physical harm to individuals or damages objects. They are uses of force as a matter of law, since I would equally assert that they meet the higher threshold of armed attack.

Interestingly, Dr Ziolkowski also characterizes cyber operations resulting in “massive, medium to long-term disruption of critical infrastructure systems of a State” as uses of force, at least to the extent that their effects are equal to the physical destruction of the system. I am somewhat less confident than she is in this respect, in part because I am unsure that States will readily equate non-kinetic effects with kinetic ones. In my view, only State practice can establish such a ‘bright line’ norm. While agreeing that States may well characterize such actions as uses of force based on the criteria I have set forth (and other contextual factors), I am uncomfortable offering the standard as *lex lata* at this time. It may mature into either customary law or a customary interpretation of Article 2(4) over time, but the uncertainty attendant to cyber operations leaves her proposed standard currently fixed in the realm of *lex ferenda*.

As to Dr Ziolkowski’s assessment of the criteria, I fear that she attributes rather more normative significance to them than I do. As noted, they are predictive tools, not normative standards. In this regard, I might suggest that the differences between our approaches derive less from our differing civil and common law backgrounds than from the different perspectives we have towards international law. Whereas she adopts an approach based primarily in positivism, mine reveals the influence of the policy-oriented New Haven School.<sup>19</sup> For me, law, contextually understood, often reflects policy choices that are shaped to achieve particular values. This explains my readiness to identify influences on legal assessments that are not strictly legal in nature. Thus, while both our approaches are consequence-based, she pays greater attention

<sup>18</sup> Statute of the International Court of Justice, art. 38(1)(b). See also *North Sea Continental Shelf* (Federal Republic of Germany v. Denmark; Federal Republic of Germany v. the Netherlands), 1969 I.C.J. 3, para. 77 (Feb. 20).

<sup>19</sup> The intellectual fathers of the New Haven School were Yale Professors Myres McDougal and Harold Lasswell. It was later championed by such scholars as Michael Reisman. The first piece setting forth the approach was Harold D. Lasswell and Myres S. McDougal, *Legal Education and Public Policy: Professional Training in the Public Interest*, 52 *Yale Law Journal* 203 (1943).

to the nature of the consequences caused by cyber operations, whereas I tend to focus on the policy perspectives States are likely to have vis-à-vis those consequences.

Our differing normative vectors are revealed in Dr Ziolkowski's comments on what we agree is the most important criterion, severity. She rejects my assertion that the more cyber operations impinge on critical national interests, the more likely States are to characterize them as uses of force. For her, international law protects the physical security of a State and its inhabitants, not the State's national interests. By my policy-oriented approach, however, national interest is the most determinative factor. The very reason States accede to (or reject) international legal regimes is to protect those interests and the various values they reflect.

Security interests may dominate in *jus ad bellum* matters, but they are not exclusive. For instance, Article 2 of the United Nations Charter expressly states that the instrument is intended to foster the purposes set forth in Article 1. Beyond the maintenance of international peace and security, these purposes include the development of "friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples" and the achievement of "international cooperation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion".<sup>20</sup> By the approach I have espoused, it is less the nature of the national interest than its intensity that matters.

An analogous thread runs through the immediacy criterion. Immediacy influences decision-makers because it heightens the need for a victim State to characterize the situation quickly lest the negative consequences of a cyber operation manifest themselves before the State can muster the domestic and international support necessary to validate any responsive action it might take. This will force the hand of other States, which in the majority of cases will be predisposed to a characterization benefitting the victim State. After all, because the cyber operation is likely to be unlawful irrespective of whether it amounts to an unlawful use of force, doubt is likely to be resolved in favour of the victim. Operations that only generate effects over the medium or long term, on the other hand, afford all parties a greater opportunity to rule out the possibility that the originator State has engaged in a use of force.

The other criteria will similarly influence assessments in ways that exceed their technical legal valence. For example, the more direct the casual connection between a cyber operation and its impact on national interests, the more comfortable States will be in describing the operation as a use of force. The law aside, portraying an originator State's actions as a violation of the *jus ad bellum* is a politically charged step, one that always presents political risks. Directness can serve to mitigate such risks by shifting the onus of responsibility for disrupting peace and security to the originator State. The same holds true with regard to invasiveness. The more invasive a cyber operation, the less politically risky the act of asserting that the originator State has used force in contravention of international law. In the case of cyber operations that are particularly direct and/or invasive, the victim State will also feel more aggrieved, thereby making it readier to style the operations as a use of force, a characterization with which other States are likely to sympathize.

<sup>20</sup> UN Charter, arts. 1(2) & (3).

Measurability and the lack of presumptive legitimacy will also make use of force characterizations easier to defend before both domestic audiences and the international community because the victim State and those States that support its characterization can offer hard facts to justify (as a matter of fact and law) their determination without having to rebut any presumption of legitimacy. Finally, although the legal issue is qualification as a use of force rather than State responsibility for the use of force, the victim State and its supporters will be more comfortable alleging that the originator State has engaged in a use of force when the latter is clearly responsible pursuant to the principles of State responsibility.

The point is that the factors set forth will, legal considerations aside, influence States when making determinations regarding an area of unsettled law. After all, States understandably tend to resolve uncertainty in favour of that position that best advances their interests. A State victimized by a cyber operation will usually deem it in its interest to assert that the delict has been severe, whether to engender sympathy or to generate support for any responsive measures it might wish to take. Uninvolved States are in a somewhat different position. In particular, a State that anticipates conducting similar cyber operations itself has an incentive to characterize analogous actions by other States as falling short of a use of force. Nevertheless, as a general rule, uninvolved States are more likely to accept the characterization of the victim State as reasonable the more the criteria set forth are met. This is especially so when they see themselves as potential victims of cyber operations.

Reduced to basics, the 'Schmitt criteria' represent an acknowledgement of the ambiguity resident in the use of force norm. Given the ambiguity, the decisional latitude of States is wide. They will inevitably leverage this decisional flexibility by adopting legal positions that optimize their national interests. The criteria are what I believe to be some of the key extra-legal influences on that complex process. Accordingly, they are meant to be predictive, not prescriptive.

I am grateful to Dr Ziolkowski for opening the dialogue about the 'Schmitt Criteria' to a wider audience, especially those concerned with the technical and policy aspects of uses of cyber force. She is to be applauded for offering a sophisticated assessment of them and I am sincerely appreciative to her for the opportunity to clarify my thoughts.