2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

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 Ziolkowsi'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*.[1] 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,[2] 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

1 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.

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

strategies,[3] formed cyber military units,[4] and established international centres dedicated to examining cyber conflict.[5]

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.[6]

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)[7]; it is universally recognized as

3 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).

4 E.g., United States Cyber Command.

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

6 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).

7 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.[8] The Charter's scheme is quite simple in the abstract – a State may *use force* when facing an armed *attack*.[9]

Note that the two articles employ different terminology – 'use of force' and 'armed attack'. The Charter's *travaux preparatoire* 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.[10]

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".[11] The Court later reaffirmed the existence of this 'gap' in the *Oil Platforms* case.[12]

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".[13] 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).[14] 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.[15] 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.

8 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.

9 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.

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

11 Nicaragua Case, *supra* note 8, paras. 191, 210.

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

13 UN Charter, preamble.

14 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).

15 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.[16] 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.[17] 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

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

17 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*.[18] 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 Ziolkowsk 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 confidant 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.[19] 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

18 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).

19 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".[20] 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.

20 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.