
INTERNATIONAL LAW STUDIES

PUBLISHED SINCE 1895

U.S. NAVAL WAR COLLEGE



Classification of Cyber Conflict

Michael N. Schmitt

89 INT'L L. STUD. 233 (2013)

Volume 89

2013

Classification of Cyber Conflict

*Michael N. Schmitt**

I. INTRODUCTION

Few international humanitarian law topics are proving as problematic in modern warfare as “classification of conflict,” that is, the identification of the type of conflict to which particular hostilities amount as a matter of law.¹ Classifying the conflict in question is always the first step in any international humanitarian law analysis, for the nature of the conflict determines the applicable legal regime. Accordingly, classification is a subject of seminal importance.

The current difficulties derive from the advent of hostilities over the past two decades that do not neatly fit the traditional bifurcation of conflict

* Chairman, International Law Department, U.S. Naval War College. A previous version of this paper was published in 17 *JOURNAL OF CONFLICT AND SECURITY LAW* 245 (2012). The opinions shared in this paper are those of the author and do not necessarily reflect the views and opinions of the U.S. Naval War College, the Dept. of the Navy or Dept. of Defense.

1. For a comprehensive survey of the subject, including case studies, see *INTERNATIONAL LAW AND THE CLASSIFICATION OF CONFLICT* (Elizabeth Wilmschurst ed., 2011). The work is the culmination of a two-year Chatham House-sponsored project involving a group of international experts. This article has benefitted from participation in that process and the author is grateful to his colleagues for their insights.

into either State-on-State or purely internal. For instance, the International Criminal Tribunal for the former Yugoslavia (ICTY) struggled with criteria for internationalization of non-international conflict in its first case, *Tadić*.² Less than a decade later, transnational terrorism refocused attention on classification issues. Was such terrorism international in character because it transcended borders or non-international because it did not involve the forces of one State engaging in hostilities against those of another (or was it even armed conflict at all)?³ More recently, external recognition of the National Transitional Council as the legitimate government of Libya raised the question of whether such recognition “de-internationalized” the conflict between the States that were fighting on the side of the rebels and Qaddafi’s forces.⁴

In the future, cyber warfare will further complicate classification. Cyber operations have the potential for producing vast societal and economic disruption without causing the physical damage typically associated with armed conflict. They are also inherently transborder, thereby frustrating any approach to classification based on geographical factors. Moreover, massive attacks can be launched by a single individual or by a group that is organized entirely on-line. This is in sharp contrast to traditional warfare, which depends on either the involvement of a State’s armed forces or that of a group capable of mounting typical military operations.

2. Prosecutor v. Tadić; Case No. IT-94-1-I, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 76 (Int’l Crim. Trib. for the former Yugoslavia Oct. 2, 1995) [hereinafter Tadić Decision on Defence Motion]. The seminal article on internationalization is Hans-Peter Gasser, *Internationalized Non-International Armed Conflicts: Case Studies of Afghanistan, Kampuchea, and Lebanon*, 33 AMERICAN UNIVERSITY LAW REVIEW 145 (1983). See also Christopher Greenwood, *International Humanitarian Law and the Tadić Case*, 7 EUROPEAN JOURNAL OF INTERNATIONAL LAW 265 (1996); Theodor Meron, *Classification of Armed Conflict in the Former Yugoslavia: Nicaragua’s Fallout*, 92 AMERICAN JOURNAL OF INTERNATIONAL LAW 236 (1998).

3. For conflicting views on this subject, see HCJ 769/02 Public Committee against Torture in Israel v. Government of Israel 2006(2) PD 459 [2006] (Isr.), reprinted in 46 INTERNATIONAL LEGAL MATERIALS 373 (2007), available at http://elyon1.court.gov.il/files_eng/02/690/007/a34/02007690.a34.pdf; Hamdan v. Rumsfeld, 548 U.S. 557 (2006).

4. Clearly, the conflict between NATO (and other) forces and the Libyan security apparatus was international in character. The question is whether the recognition of the rebels (National Transitional Council) meant that NATO forces were now fighting on the side of the government against dissident armed forces (the remnants of the Libyan armed forces still loyal to Qaddafi) such that the conflict became non-international. On the recognition of the National transitional Council, see Stefan Talmon, *Recognition of the Libyan National Transitional Council*, AMERICAN SOCIETY OF INTERNATIONAL LAW INSIGHTS (June 16, 2011), <http://www.asil.org/insights110616.cfm>.

This article explores these and other classification of cyber conflict issues.⁵ Two caveats are in order. First, the occurrence of cyber operations in no way alters the classification of an ongoing kinetic conflict. The paradigmatic example is the cyber operations conducted by “patriotic hackers” during the 2008 international armed conflict between Georgia and Russia.⁶ Second, this article will not consider the possible emergence of new categories of armed conflict, such as “transnational armed conflict.”⁷ Rather it adopts a conventional approach, one acknowledging two basic genre of conflict—international and non-international. To the extent cyber operations bear of classification, they do so within this generally accepted framework.

II. THE BASIC TYPOLOGY

The modern era of conflict classification began in 1949 with adoption of the four Geneva Conventions.⁸ Earlier treaties governing hostilities had

5. On classification more generally, see Sylvain Vité, *Typology of Armed Conflicts in International Humanitarian Law: Legal Concepts and Actual Situations*, 91 INTERNATIONAL REVIEW OF THE RED CROSS 69 (2009); Jelena Pejic, *Status of Armed Conflicts*, in PERSPECTIVES ON THE ICRC STUDY ON CUSTOMARY INTERNATIONAL LAW 77 (Elizabeth Wilmschurst & Susan Breau eds., 2007).

6. On the Estonian and Georgian cases, see generally ENEKEN TIKK, KADRI KASKA & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS (2010).

7. See, e.g., Geoffrey Corn, *Hamdan, Lebanon, and the Regulation of Armed Conflict: The Need to Recognize a Hybrid Category of Armed Conflict*, 40 VANDERBILT TRANSNATIONAL LAW JOURNAL 295 (2006); Geoffrey S. Corn & Eric Talbot Jensen, *Untying the Gordian Knot: A Proposal for Determining Applicability of the Laws of War to the War on Terror*, 81 TEMPLE LAW REVIEW 787 (2008); Geoffrey S. Corn, *Making the Case for Conflict Bifurcation in Afghanistan*, in THE WAR IN AFGHANISTAN: A LEGAL ANALYSIS 181 (Michael N. Schmitt ed., 2009) (Vol. 85, U.S. Naval War College International Law Studies). For a well-reasoned piece suggesting a category of “extra-State” armed conflict, see Roy Schondorf, *Extra-State Armed Conflict: Is There a Need for a New Legal Regime?*, 37 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 1 (2004). The International Committee of the Red Cross has correctly rejected the notion of armed conflicts that are other than international and non-international. International Committee of the Red Cross, *How is the Term “Armed Conflict” Defined in International Humanitarian Law?* (Mar. 2008), <http://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf>.

8. Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135;

been silent as to the conditions under which they applied. They merely assumed the existence of a “war.”

Lassa Oppenheim set forth the classic definition of war in his 1906 treatise *International Law*: “War is a contention between two or more States through their armed forces, for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases.”⁹ The critical element in the definition was that war must be between States. Intra-State conflict was principally a matter of domestic concern unless it rose to the level of a “belligerency.”¹⁰ Only then, and only because the conflict now resembled inter-State hostilities, did the law of war attach.

Oppenheim’s definition implied that the existence of a war was a question of fact. The undeclared 1905 war between Japan and Russia brought this approach into question. In response to the conflict, the 1907 Second Hague Peace Conference adopted Hague Convention III relative to the Opening of Hostilities. In that instrument, State parties agreed that “hostilities between themselves must not commence without previous and explicit warning, in the form either of a declaration of war, giving reasons, or of an ultimatum with conditional declaration of war.”¹¹ Consequently, a failure to declare war or the non-recognition of a state of war by a party to the conflict precluded application of treaties governing the conduct of hostilities.

Subsequent events discredited this formalistic approach. The Spanish Civil War illustrated the extent to which fratricidal violence could match that which occurred during inter-State conflict,¹² while the carnage of the Second World War highlighted the risk of leaving humanitarian law to the mercy of political decisions as to whether to declare war. Sensitive to these realities, the international community took a different tack in the 1949 Geneva Conventions. The approach taken in those instruments, which recog-

Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter GC I–IV respectively].

9. LASSA OPPENHEIM, II INTERNATIONAL LAW: A TREATISE 56 (1906).

10. UNITED KINGDOM MINISTRY OF DEFENCE, THE MANUAL OF THE LAW OF ARMED CONFLICT ¶ 15.1.2 (2004). On belligerency, see Yair M. Lootsteen, *The Concept of Belligerency in International Law*, 166 MILITARY LAW REVIEW 109 (2000).

11. Convention No. III Relative to the Opening of Hostilities art. 1, Oct. 18, 1907, 36 Stat. 2259, T.S. No. 538, 1 Bevans 619.

12. Interestingly, parties to that conflict occasionally agreed to apply the norms set forth in the 1929 Geneva Convention on Prisoners of War. See Frédéric Siordet, *The Geneva Conventions and Civil War*, in III INTERNATIONAL REVIEW OF THE RED CROSS (Supp. to Nos. 8, 9 & 11) (Aug., Sept. & Nov. 1950).

nizes war in both the technical and material sense, has since matured into customary international law.¹³

The Geneva Conventions adopt a bifurcated scheme in Articles 2 and 3, which are “Common” to all four conventions. Common Article 2 sets forth the standard for international armed conflict. It provides that “the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them.”¹⁴ Reduced to basics, there are two key factual criteria for international armed conflict—a confrontation between States and hostilities that amount to “armed” conflict.

In 1949, Common Article 3 signaled a sea change in the international community’s attitude towards internal conflagrations, for it represented the first *lex scripta* expressly applicable to non-international armed conflicts. By its terms, the article applies to an “armed conflict not of an international character occurring in the territory of one of the High Contracting Parties.” As with Article 2, an armed conflict is a condition precedent to applicability, although the article does not address the nature of such a conflict in the non-international context. One point is clear, though. Given Common Article 2, a non-international armed conflict cannot involve hostilities between two or more States. Its applicability is resultantly limited to conflicts between a State and an armed group or those in which multiple armed groups are fighting each other.

In light of the many post-1949 conflicts, the International Committee of the Red Cross (ICRC) convened a Diplomatic Conference between 1973 and 1977 to “update” international humanitarian law. The Conference adopted two Protocols to the 1949 Geneva Conventions. Additional Protocol I addresses international armed conflict by reference to Article 2 of the 1949 Conventions.¹⁵ Controversially, it also reaches “armed conflicts in which peoples are fighting against colonial domination and alien occupa-

13. For instance, guidance issued by States to their armed forces typically adopts this approach. *See, e.g.*, U.S. Navy, U.S. Marine Corps & U.S. Coast Guard, NWP 1-14M/MCWP 5-12/COMDTPUB P5800.7A, The Commander's Handbook on the Law of Naval Operations ¶¶ 5.1.2.1 & 5.1.2.2 (2007). On the notion of “war,” see YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 3–15 (4th ed. 2005).

14. GC I-IV, *supra* note 8, Common art. 2. The article also extends applicability of the Conventions to occupation, even when uncontested.

15. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 1(3), June 8, 1977, 1125 U.N.T.S. 3.

tion and against racist regimes in the exercise of their right of self-determination.”¹⁶ Numerous States, most notably the United States, refused to become party to the instrument, in part due to this latter provision.¹⁷

Additional Protocol II applies to non-international armed conflicts. However, it sets a higher threshold of applicability than Common Article 3’s naked reference to armed conflict that is not international. By Article 1, Protocol II applies

to all armed conflicts which are not covered by Article 1 of [Additional Protocol I] and which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol.¹⁸

The provision differs from Common Article 3 in its requirement that dissident or other armed forces control territory and its limitation to conflicts involving a State, thereby excluding non-international armed conflicts between organized armed groups. Importantly, Article 1 specifically excludes “situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature, as not being armed conflicts” from the ambit of non-international armed conflict.¹⁹ This exclusion has been broadly accepted as reflective of customary international law in all non-international armed conflicts, a fact evidenced by its adoption in the Statute of the International Criminal Court.²⁰

Taken together, this collage of provisions envisions four categories of conflict: 1) international armed conflict between States; 2) international

16. *Id.*, art. 1(4).

17. INTERNATIONAL AND OPERATIONAL LAW DEPARTMENT, UNITED STATES ARMY JUDGE ADVOCATE GENERAL’S LEGAL CENTER AND SCHOOL, LAW OF WAR DOCUMENTARY SUPPLEMENT 232 (2011). *See also* Michael J. Matheson, *The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AMERICAN UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLICY 419 (1987).

18. Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts art. 1(1), June 8, 1977, 1125 U.N.T.S. 609 [hereinafter AP II].

19. *Id.*, art. 1(2).

20. Rome Statute of the International Criminal Court art. 8.2(d), July 17, 1998, 2187 U.N.T.S. 90. The statute is not limited to conflicts that meet the Additional Protocol II threshold.

armed conflict involving national liberation movements; 3) non-international armed conflict between a State and an organized armed group or between organized armed groups; and 4) non-international armed conflict at the Additional Protocol II level. The second and fourth categories are relevant only to application of Additional Protocols I and II respectively for Parties thereto. The first and third are acknowledged as customary categories of conflict.

III. INTERNATIONAL ARMED CYBER CONFLICT

As noted, international armed conflicts must be both “armed” and “international.” The first criterion presents the quandary that cyber operations are not kinetic in nature and do not employ what would in common usage be considered as “weapons.” At first glance, a conflict consisting of only cyber operations would, therefore, appear not to be “armed.” Such a conclusion would be incongruous for cyber operations can have highly destructive, even deadly, results. A State involved in an exchange of cyber attacks at this level would be very likely to characterize the situation as international armed conflict, much as it would if it fell victim of another State’s non-kinetic bacteriological attack.

The official ICRC *Commentary* to Article 2 provides that

any difference arising between two States and leading to the intervention of members of the armed forces is an armed conflict within the meaning of Article 2, even if one of the Parties denies the existence of a state of war. It makes no difference how long the conflict lasts, how much slaughter takes place, or how numerous are the participating forces.²¹

The ICRC *Commentary* to Additional Protocol I is in accord:

[H]umanitarian law . . . covers any dispute between two States involving the use of their armed forces. Neither the duration of the conflict, nor its

21. COMMENTARY TO GENEVA CONVENTION III RELATIVE TO THE TREATMENT OF PRISONERS OF WAR 23 (Jean Pictet ed., 1960) [hereinafter GC III COMMENTARY]. See also Dietrich Schindler, *The Different Types of Armed Conflicts According to the Geneva Conventions and Protocols*, 163 RECUEIL DES COURS DE L'ACADEMIE DE DROIT INTERNATIONAL 131 (1979). But see Christopher Greenwood, *Scope of Application of Humanitarian Law*, in THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 37, 48 (Dieter Fleck ed., 2d ed. 2009).

intensity, play a role: the law must be applied to the fullest extent required by the situation of the persons and the objects protected by it.²²

Adopting the same approach, the ICTY has defined armed conflict as the “resort to armed force between States” without recognizing any threshold for the duration or intensity of hostilities.²³

By these standards, the concept of armed conflict implies forceful acts at whatever level.²⁴ *A fortiori*, any cyber operation that amounts to an “attack” in international humanitarian law terms would qualify as armed. Article 49(1) of Additional Protocol I defines attacks as “acts of violence against the adversary, whether in offence or defence.” Although cyber operations are not violent in themselves, they can nonetheless generate violent consequences. To the extent that they result in injury or death of persons or damage or destruction of property, they are attacks satisfying the armed criterion of armed conflict.²⁵ For instance, if a State was behind the 2010 “Stuxnet” attack against supervisory control and data acquisition systems upon which the power centrifuges at an Iranian nuclear power plant depended, it would meet this threshold because physical damage resulted.²⁶

22. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶ 62 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1988) [hereinafter AP COMMENTARY].

23. Tadić Decision on Defence Motion, *supra* note 2, ¶ 70.

24. It should be noted that an armed conflict can exist even in the absence of uses of force. For instance, Common Article 2 of the four 1949 Geneva Conventions extends to “all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance.”

25. *See, e.g.*, Michael N. Schmitt, *Cyber Operations and the Jus in Bello*, in INTERNATIONAL LAW AND THE CHANGING CHARACTER OF WAR 89, 92–94 (Raul A. “Pete” Pedrozo & Daria P. Wollschlaeger eds., 2011) (Vol. 87, U.S. Naval War College International Law Studies). It has been suggested that operations falling below the threshold may also qualify. INTERNATIONAL COMMITTEE OF THE RED CROSS, REPORT 31IC/11/5.1.2, INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICTS 37 (2011) [hereinafter ICRC REPORT]; Knut Dörmann, *Applicability of the Additional Protocols to Computer Network Attacks* 6 (Nov. 19, 2004), <http://www.icrc.org/eng/assets/files/other/applicabilityofihltozna.pdf> (paper delivered at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm). The issue is addressed at length in the TALLINN MANUAL ON THE INTERNATIONAL LAW OF CYBER WARFARE (Michael N. Schmitt ed., 2013). The author is grateful to his colleagues on the project leading to the *Manual* for their insights, many of which find reflection in this article.

26. The question remains as to whether a State was behind the operation.

But might a cyber operation by one State against another that does not cause physical injury or damage nevertheless initiate an armed conflict? The ICRC has taken the position that a cyber operation that “disables” an object is also an attack even when it does not cause physical damage.²⁷ This is a reasonable extension of the notion of damage, at least to the extent repair (as distinct from merely reloading software) of the cyber infrastructure concerned is necessitated. Since the operation is an attack, it is also armed in terms of qualification for armed conflict. That said, a *de minimis* standard should attach. In much the same way that a soldier throwing a rock across the border does not propel the States concerned into international armed conflict, it would not suffice, for instance, to merely disable a single computer that performs non-essential functions.

Beyond these cases, it is unclear where State practice will lead. Consider a situation in which a State takes control of critical infrastructure in another State, conducts denial-of-service attacks against essential societal services, or begins deleting or changing data in a manner that severely disrupts another State’s economy. As perceptively noted by the ICRC, “[i]t would appear that the answer to these questions will probably be determined in a definite manner only through future state practice.”²⁸

In addition to being armed, cyber attacks must be of an “international” nature to qualify as international armed conflict. The term international denotes actions conducted by, or attributable to, a State. By the plain text of the provisions cited above, those conducted by a State’s armed forces qualify. Although not mentioned in those provisions, it is beyond dispute that cyber attacks conducted by other organs of a State, such as intelligence or law enforcement agencies, also qualify.²⁹

As noted by the ICTY in *Tadić*, “private individuals acting within the framework of, or in connection with, armed forces, or in collusion with

27. ICRC REPORT, *supra* note 25, at 37.

28. *Id.*

29. Draft Articles on Responsibility of States for Internationally Wrongful Acts, Rep. of the Int'l L. Comm'n, 53d Sess., GAOR 56th Sess., Supp. No. 10, U.N. DOC. A/56/10 (2001), *reprinted in* [2001] 2 YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 32, U.N. DOC. A/CN.4/SER.A/2001/Add.1 (Part 2) [hereinafter Articles of State Responsibility]. Article 4(2) of the Articles of State Responsibility provides that an “organ includes any person or entity which has that status in accordance with the internal law of the State.”

State authorities may be regarded as *de facto* State organs.”³⁰ Any cyber attacks they launch would be treated as if launched by *de jure* State organs. Cyber attacks carried out by a person or entity that, although not an organ of the State, is “empowered by the law of that State to exercise elements of the governmental authority . . . provided the person or entity is acting in that capacity in the particular instance” would likewise suffice.³¹ An example would be a private corporation that a State authorizes by law to conduct cyber operations on its behalf, so long as the operations in question are of the sort for which said authorization was granted.

More problematic in terms of qualifying as international are activities engaged in by individuals or groups that are neither organs of a State nor authorized to act on its behalf. It appears clear that cyber attacks by individuals or groups acting *sua sponte* are generally not attributable to a State for the purpose of finding an international armed conflict. The classic example is the “hactivist” cyber campaign against Estonia in 2007 (moreover, they were not “armed”).³² However, if a State endorses and encourages the perpetuation of the cyber operations, the individuals or groups involved will be deemed “*de facto* organs” of the State, such that the activity meets the international criterion. This principle was enunciated (albeit, in the State responsibility context) by the International Court of Justice in the *Hostages* case and cited with approval by the ICTY in *Tadić* when dealing with attribution for the purposes of conflict classification.³³

Consider, for example, a case in which a group of one State’s nationals conduct cyber attacks against another State. If the government of the first State announces its approval of the attacks and takes steps to perpetuate the attacks, as in the case of establishing cyber defense mechanisms that preserve the group’s ability to continue its attacks, the group becomes a *de facto* State organ even if that State did not originally provide direction to the group.

A scenario in which some relationship exists between a State and the individuals or group conducting the cyber attacks is more likely. The ICTY

30. Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment, ¶ 144 (Int’l Crim. Trib. for the former Yugoslavia July 15, 1999) [hereinafter Tadić Appeals Chamber Judgment].

31. Articles of State Responsibility, *supra* note 29, art. 5.

32. See generally the discussion of these incidents in TIKK, KASKA & VIHUL, *supra* note 6.

33. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 3, ¶ 74 (May 24); Tadić Appeals Chamber Judgment, *supra* note 30, ¶¶ 133–37.

addressed this situation head on in *Tadić* when assessing whether the conflict in Bosnia-Herzegovina was international by virtue of the relationship between the Bosnian Serb armed groups and the Serb-dominated Federal Republic of Yugoslavia. In an often-overlooked distinction, the Tribunal took different approaches to the actions of organized armed groups (defined below) and individuals.

As to the former, the ICTY held that the correct threshold was one of “overall control going beyond the mere financing and equipping of such forces and involving also participation in the planning and supervision of military operations.”³⁴ The issuance of specific orders or instructions relating to a single operation is not required. To illustrate, a State that exercises control over a group sufficient to allow it to direct the group to mount (or to desist from mounting) a broad campaign of cyber attacks exercises overall control. Similarly, if a State instructs the group to attack, or refrain from attacking, a particular category of cyber targets (as distinct from specific targets), it enjoys overall control of the group. But note the Tribunal’s mention of equipping the group. Merely providing software or hardware with which attacks are conducted does not suffice to attribute a group’s actions to the State for the purpose of finding an international armed conflict (although such assistance may violate certain norms of international law).

The requisite degree of control over the actions of individuals who conduct cyber attacks without being members of an organized armed group is much higher. In such cases, the State must issue “specific instructions or directives aimed at the commission of specific acts” before attribution of the acts to the State for the purpose of classifying the conflict as international occurs.³⁵ Absent such instructions, the attacks cannot be attributed to the State for that purpose. Neither would the conflict be non-international since, as will be discussed, the individuals do not comprise an organized armed group.

34. *Tadić Appeals Chamber Judgment*, *supra* note 30, ¶ 145. See also *Lubanga*, where the International Criminal Court described overall control as “a role in organising, coordinating, or planning the military actions of the military group.” *Prosecutor v. Lubanga*, Case No. ICC-01/04-01/06, Decision on Confirmation of Charges, ¶ 211 (ICC Jan. 29, 2007) [hereinafter *Lubanga*]. In the *Genocide* case, the International Court of Justice observed that the overall control test “may well be . . . applicable and suitable.” *Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. and Montenegro)*, 2007 I.C.J. 43, ¶ 404 (Feb. 26).

35. *Tadić Appeals Chamber Judgment*, *supra* note 30, ¶ 132.

Should a State permit cyber attacks to take place from its territory, it may be in breach of its international legal obligation to “police” its territory in order to ensure it is not used for purposes harming other States.³⁶ Yet, its tolerance of the attacks does not satisfy the international criterion unless, as mentioned, the State goes further. It is irrelevant whether the attacks in question are mounted by a single individual or, as in the Estonian case, hundreds of persons.

Finally, it is sometimes questioned whether attribution to a State is required at all for qualification as an international armed conflict. In the *Targeted Killing* case, the Israeli Supreme Court argued that attribution is not necessary so long as the group in question operates transnationally, that is, the conflict “crosses the borders of the state.”³⁷ In the cyber context, this situation is highly probable, for organized armed groups might well launch cyber attacks from relative safety abroad. The U.S. Supreme Court took a contrary approach in *Hamdan*, where it found that the conflict with the Al-Qaeda terrorist organization was “not of an international character” because it was not between States.³⁸ In light of the earlier discussion, the U.S. position on this particular point is better reasoned.

IV. NON-INTERNATIONAL ARMED CYBER CONFLICT

Common Article 3 to the Geneva Conventions defines non-international armed conflicts in the negative as those that are “not of an international character.”³⁹ The ICTY has further developed the notion of non-international conflict. In *Tadić*, the Tribunal described such conflicts as “protracted armed violence between governmental authorities and orga-

36. The International Court of Justice affirmed this principle in its first case, *Corfu Channel*. The Court held that every State has an “obligation to not allow knowingly its territory to be used for acts contrary to the rights of other States.” *Corfu Channel* (U.K. v. Alb.), 1949 I.C.J. 4, 22 (Apr. 9).

37. Public Committee against Torture in Israel, *supra* note 3, ¶ 18.

38. *Hamdan*, *supra* note 3, 628–32 (2006).

39. GC I–IV, *supra* note 8, Common art. 3 (“In the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties, each Party to the conflict shall be bound to apply, as a minimum, the following provisions. . . .”). Only States can be High Contracting Parties. On non-international armed conflict generally, see ANTHONY CULLEN, *THE CONCEPT OF NON-INTERNATIONAL ARMED CONFLICT IN INTERNATIONAL HUMANITARIAN LAW* (2010); EVE LA HAYE, *WAR CRIMES IN INTERNAL ARMED CONFLICTS* (2008); LINDSAY MOIR, *THE LAW OF INTERNAL ARMED CONFLICT* (2002).

nized armed groups or between such groups within a State.”⁴⁰ The equivalent definition has been adopted by international tribunals and in the Statute of the International Criminal Court.⁴¹ Additional Protocol II also refers to a conflict between a State’s armed forces “and dissident armed forces or other organized armed groups.” Accordingly, two essential criteria apply for all non-international armed conflicts—participation by an organized armed group and a particular level of intensity.

Organized armed groups must be both “organized” and “armed.” Common Article 3 refers to “parties to a conflict,” a reference that serves as the source of the organization requirement. In considering this requirement, the ICTY has noted

some degree of organisation by the parties will suffice to establish the existence of an armed conflict. This degree need not be the same as that required for establishing the responsibility of superiors for the acts of their subordinates within the organization, as no determination of individual criminal responsibility is intended under this provision of the Statute.⁴²

But the group must nevertheless be organized. Organization allows for acting in a coordinated manner, thereby generally heightening the capability to engage in violence. In military operations, such coordination typically involves mission planning, sharing intelligence, and exercising command and control. In other words, the organization criterion implies that the actions are best understood as those of a group and not its individual members. This structural requirement is fundamental, for absent structure there is no identifiable enemy to treat as the other party to the conflict.⁴³

Whether a group is organized is always a fact and context specific determination. In *Limaj*, the ICTY looked to such factors as, *inter alia*, the existence of a formal command structure, the creation of unit zones of opera-

40. Tadić Decision on Defence Motion, *supra* note 2, ¶ 70.

41. Prosecutor v. Akayesu, Case No. ICTR-96-4-T, Judgment, ¶ 619 (Sept. 2, 1998); Prosecutor v. Rutaganda, Case No. ICTR-96-3-T, Judgment, ¶ 92 (Dec. 6, 1999); Prosecutor v. Fofana, Case No. SCSL-2004-14-AR73, Decision on Appeal Against “Decision on Prosecution’s Motion for Judicial Notice and Admission of Evidence,” ¶ 32 (May 16, 2005) (Robertson, J., separate opinion); *Lubanga*, *supra* note 34, ¶ 233; Prosecutor v. Bemba Gombo, Case No. ICC-01/05-01/08, Decision on Confirmation of Charges, ¶ 229 (June 15, 2006); Rome Statute, *supra* note 20, art. 8(2)(f).

42. Prosecutor v. Limaj, Case No. IT-03-66-T, Judgment, ¶ 89 (Int’l Crim. Trib. for the former Yugoslavia Nov. 30, 2005) [hereinafter *Limaj*].

43. For instance, in order to open termination of conflict negotiations.

tion, the issuance of orders, the establishment of a headquarters and the promulgation of disciplinary orders to find that the Kosovo Liberation Army qualified as an organized armed group in its conflict with the Federal Republic of Yugoslavia.⁴⁴

What is clear is that individuals acting alone that conduct cyber attacks against a State (or a particular armed group) cannot meet the organized criterion. For example, despite the number of hacktivists involved in the cyber operations against Estonia, they lacked the requisite degree of organization and therefore the operations did not amount to non-international armed conflict. Similarly, consider a case in which a website containing malware and listing potential cyber targets is accessed by large numbers of individuals who are unaffiliated with the creator of the website. Those individuals who do so do not qualify as an organized armed group; they lack the requisite structure. When cyber attacks are merely collective in the sense of occurring in parallel, they are not organized.

Cyber attacks conducted by a group that organizes entirely on-line are more difficult to classify. The members of virtual organizations may never meet nor even know each other's actual identity. Nevertheless, such groups can act in a coordinated manner against the government (or an organized armed group), take orders from a virtual leadership and be highly organized. For example, one element of the group might be tasked to identify vulnerabilities in target systems, a second might develop malware to exploit those vulnerabilities, a third might conduct the operations and a fourth might maintain cyber defenses against counter-attacks.

The primary obstacle to characterization of the group as organized would be its inability to enforce compliance with international humanitarian law. Additional Protocol II imposes a requirement that a group be "under responsible command" before a non-international armed conflict covered by the instrument exists.⁴⁵ This requirement should not be interpreted too strictly. As noted in the ICRC *Commentary* to the article, the term

implies some degree of organization of the insurgent armed group or dissident armed forces, but this does not necessarily mean that there is a hierarchical system of military organization similar to that of regular armed forces. It means an organization capable, on the one hand, of planning

44. *Limaj*, *supra* note 42, ¶¶ 94–129.

45. AP II, *supra* note 18, art. 1(1).

and carrying out sustained and concerted military operations, and on the other, of imposing discipline in the name of a de facto authority.⁴⁶

In a virtually organized group, the requirement of an ability to carry out sustained and concerted military operations could be met to the extent that cyber operations are equated with military operations, which, as discussed, is the case. However, imposing discipline would be difficult since the group lacks physical control over its members.

Complicating matters is Additional Protocol II's requirement that the group be able "to implement this Protocol."⁴⁷ The phrase is generally understood as an ability to comply with and enforce international humanitarian law. Before violence can qualify as a Protocol II conflict, "the parties may reasonably be expected to apply the rules developed in the Protocol, since they have the minimum infrastructure required therefor."⁴⁸ While there is no requirement that the law actually be enforced, the group must be organized so as to enable enforcement. In a virtually organized group, such organization is lacking since there is no physical connection between the members.

It must be cautioned that since this treaty law requirement derives from Additional Protocol II, it is only applicable in and of itself to conflicts in which that instrument applies. Common Article 3 contains no equivalent condition, thereby raising the question of whether an analogous customary law norm applies to conflicts other than Additional Protocol II non-international armed conflicts. In this regard, the commentary to Article 3 notes that the Diplomatic Conference that drafted the 1949 Geneva Conventions considered setting express preconditions for such conflicts. Although the proposal was rejected, the *Commentary* asserts that they "constitute convenient criteria."⁴⁹ The first condition was that the "Party in revolt against the *de jure* Government possesses an organized military force, an authority responsible for its acts, acting within a determinate territory and having the means of respecting and ensuring respect for the Convention."⁵⁰ It would appear reasonable, therefore, to extend the Additional Protocol II requirements regarding responsible command (*vis-à-vis* enforcing disci-

46. AP COMMENTARY, *supra* note 22, ¶ 4663.

47. AP II, *supra* note 18, art. 1(1).

48. AP COMMENTARY, *supra* note 22, ¶ 4470.

49. COMMENTARY ON GENEVA CONVENTION I FOR THE AMELIORATION OF THE CONDITION OF THE WOUNDED AND SICK IN THE ARMED FORCES IN THE FIELD 49 (Jean Pictet ed., 1952).

50. *Id.*

pline) and an ability to implement international humanitarian law to all non-international armed conflicts. The ICTY adopted this approach in *Boskoski*⁵¹ and it is consistent with the principle of command responsibility in non-international armed conflicts.⁵² If valid, the extension to all non-international armed conflicts would preclude virtually organized groups from qualifying as organized armed groups for the purpose of classifying a conflict as non-international.

In addition to being organized, the group in question must be armed. The meaning of armed in the non-international armed conflict context parallels that attending international armed conflict. As discussed, it generally presumes the conduct of “attacks.” Yet, since non-international armed conflict is premised on the activities of a group, as distinct from a State, the question of attribution of an individual member’s conduct to the group as a whole arises. Since it is the group that must be armed, the group itself must have a purpose of carrying out armed activities. If individual members of an organized group carry out cyber attacks on their own accord, that is, not on behalf of the group, the group does not meet the armed criterion.

In contradistinction to international armed conflict, non-international armed conflict entails a certain degree of intensity. Recall that riots, civil disturbances, or isolated and sporadic acts of violence do not suffice; the hostilities must also be protracted. Decisions of the ICTY have cited such factors as the gravity of the attacks, the collective character of the hostilities, the need to increase forces to deal with the situation, the time over which the hostilities have taken place, and whether the United Nations Security Council has addressed the matter as bearing on whether the intensity threshold is satisfied.⁵³ However, no bright-line intensity test exists, nor is there any clear standard for “protracted” conflict.⁵⁴ In light of the manner

51. Prosecutor v. Boskoski, Case No. IT-04-82-T, Judgment, ¶ 205 (Int’l Crim. Trib. for the former Yugoslavia July 10, 2008).

52. Although responsible command and command responsibility are separate legal concepts, it would be illogical to impose command responsibility on an individual for the actions of individuals who are members of a group that are not under responsible command; the concepts are therefore different, but related. On the issue, see Prosecutor v. Hadzihasanovic, Case No. IT-01-47-AR72, Appeals Chamber Decision on Interlocutory Appeal Challenging Jurisdiction in Relation to Command Responsibility, ¶¶ 16–22 (Int’l Crim. Trib. for the former Yugoslavia July 16, 2003).

53. Prosecutor v. Haradinaj, Case No. IT-04-84-T, Judgment, ¶ 49 (Int’l Crim. Trib. for the former Yugoslavia Apr. 3, 2008) (summarizing various indicative factors).

54. In *Abella*, the Inter-American Commission on Human Rights characterized a thirty-hour clash between dissident armed forces and the Argentinian military as non-

in which cyber campaigns are mounted, it must be noted that although cyber attacks have to be frequent enough to be considered related, they clearly do not have to be continuous.

This is a high threshold that would preclude many cyber operations from sufficing for the purpose of finding a non-international armed conflict. Even highly destructive cyber attacks would fail to qualify unless they occurred on a regular basis over time. They would instead be addressed within the criminal law paradigm and be governed internationally by human rights, not humanitarian, law.

One issue that is somewhat murky is the classification status of cyber attacks conducted by an organized armed group during an international armed conflict between two States. It is clear that if a group “belongs to” a party to the conflict, the conflict remains wholly international in character. The concept of belonging to, which stems from Article 4 of Geneva Convention III, implies at least some de facto relationship between the group and a State that is a party.⁵⁵ The article’s commentary suggests that even tacit agreement is sufficient so long as it is clear for which side the group is fighting.⁵⁶

Much more complicated is the situation in which a group engages in cyber attacks without doing so on behalf of one of the parties to an international armed conflict. This is not a remote hypothetical. For instance, when the conflict in Iraq was still international in character, organized armed groups lacking any connection with the Baathist regime attacked coalition forces. The groups, such as the Shia militia, were opposed to both sides during that conflict. An analogous situation could easily arise in which a group mounts cyber attacks against a party *sua sponte*.

The ICRC’s *Interpretive Guidance on the Notion of Direct Participation in Hostilities* addresses such situations. It contends that “organized armed groups operating within the broader context of an international armed conflict without belonging to a party to that conflict could still be regarded as parties to a separate non-international armed conflict.”⁵⁷ Some participants in the expert process that resulted in the *Guidance* rejected the ICRC’s position

international armed conflict. *Abella v. Argentina*, Case 11.137, Inter-Am. Comm’n H.R., Report No. 55/97, OEA/Ser.L/V/II.98, doc. 6 rev. ¶¶ 148, 327 (1998).

55. GC III, *supra* note 8, art. 4A(2).

56. GC III COMMENTARY, *supra* note 21, at 57.

57. NILS MELZER, INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION UNDER INTERNATIONAL HUMANITARIAN LAW 24 (2009).

on the basis that it would prove problematic in practice because it requires application of the law of both international and of non-international armed conflict in the same battlespace.⁵⁸ In their view, it was more appropriate to ask whether an unambiguous nexus existed between the actions of the group in question and the international armed conflict, rather than any party thereto. For instance, an organized armed group might conduct cyber attacks against an occupying force because of religious or political opposition to the occupants, not to expel them on behalf of the government. The requisite nexus between the group and the conflict would be their opposition to the occupation. In such a case, the conflict would remain entirely international irrespective of the lack of a relationship between the group and the occupied State.

Finally, recall that Additional Protocol II only applies when organized armed groups control territory. Since a group cannot control territory without physical presence, the instrument is generally thought to be inapplicable to cyber-only conflicts. It would accordingly only apply to cyber operations in those Additional Protocol II conflicts involving an organized armed group that controls territory and conducts such operations.

V. CONCLUSION

To date, States have refrained from characterizing any cyber operations conducted outside the context of an on-going armed conflict as either international or non-international armed conflict. Be that as it may, cyber operations will in the future inevitably present difficult conflict classification challenges for States. With regard to international armed conflict, attribution of cyber operations conducted by non-State actors will likely prove even more problematic than the attribution to States of kinetic actions has been in the past. In the context of non-international armed conflict, qualification as an organized armed group will prove increasingly complex as the structures, means and prevalence of virtual organization grow and evolve. Perhaps most importantly, the approach taken in this article to the interpretation of the term “armed” is, although presently reflecting *lex lata*, unlikely to survive. With States and non-State actors engaging in ever more destructive and disruptive cyber operations and societies becoming deeply dependent on the cyber infrastructure, State practice accompanied by *opinio juris* can be expected to result in a lowering of the current threshold. The

58. Based on author’s participation.

law of cyber armed conflict is a work in progress and will remain so for the immediate future.