INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Cyber Warfare: Implications for Non-international Armed Conflicts

Robin Geiss

89 INT'L L. STUD. 627(2013)

Volume 89 2013

Cyber Warfare: Implications for Non-international Armed Conflicts

Robin Geiss[*]

I. INTRODUCTION

Cyberspace is considered by many to be a new warfighting domain.[1] Legal discussions concerning warfare in this domain have primarily focused on the level of the *ius ad bellum*[2] and international armed conflicts.[3] With the exception of action on cybercrime, especially the 2001 European Convention on Cybercrime and tentative attempts to design a similar instrument

* Professor at the Faculty of Law, University of Potsdam, Potsdam, Germany.

1. U.S. DEPARTMENT OF DEFENSE, QUADRENNIAL DEFENSE REVIEW REPORT 37 (2010) [hereinafter QUADRENNIAL DEFENSE REVIEW REPORT].

2. Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE JOURNAL OF INTERNATIONAL LAW 421 (2011); HEATHER H. DINNISS, CYBER WARFARE AND THE LAWS OF WAR 37 (2012); Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARVARD INTERNATIONAL LAW JOURNAL 373 (2011); Marco Roscini, *World Wide Warfare:* Jus ad Bellum *and the Use of Cyber Force*, 14 MAX PLANCK UNITED NATIONS YEARBOOK 85 (2010).

3. Michael N. Schmitt, *Wired Warfare: Computer Network Attack and* Jus in Bello, 84 INTERNATIONAL REVIEW OF THE RED CROSS 365 (2002); Sean Watts, *Combatant Status and Computer Network Attack*, 50 VIRGINIA JOURNAL OF INTERNATIONAL LAW 392 (2010).

on the global level,[4] the focus of contemporary discussions has primarily been on inter-State issues and State-sponsored cyber operations. Conversely, the relevance of cyber warfare in non-international armed conflicts and the corresponding legal challenges arising under the laws of armed conflict have only rarely been addressed.[5]

One reason is certainly the notion that non-international armed conflict today encompasses such a wide range of rather different scenarios,[6] ranging from low-intensity armed conflicts between organized armed groups in failed-State scenarios like Somalia[7] to traditional types of civil war like the ongoing armed conflict in Syria to "internationalized" scenarios like the armed conflict in Afghanistan,[8] that the relevance of cyber warfare in a particular conflict varies widely. Quite clearly, in many non-international armed conflict scenarios sophisticated cyber weaponry is without significant military relevance. Nevertheless, when parties to a non-international armed conflict rely on cyber infrastructure and cyber operations to further their strategic aims, cyber operations will also become increasingly relevant. The Syrian government, for example, has repeatedly shut off the Internet

4. Marco Gercke, *Ten Years [after the] Convention on Cybercrime: Achievements and Failures of the Council of Europe's Instrument in the Fight against Internet-Related Crimes*, 12 COMPUTER LAW REVIEW INTERNATIONAL 142 (2011); UNITED NATIONS OFFICE ON DRUGS AND CRIME, THE GLOBALIZATION OF CRIME 218 (2010) [hereinafter GLOBALIZATION OF CRIME]; Susan W. Brenner, *Cybercrime, Cyberterrorism and Cyberwarfare*, 77 REVUE INTERNATIONALE DE DROIT PENALE 454 (2006).

5. Rather the focus has been on potential terrorist attacks by non-State actors. *See, e.g.*, Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent,* 43 VANDERBILT JOURNAL OF TRANSNATIONAL LAW 59 (2010).

6. Sylvain Vité, *Typology of Armed Conflicts in International Humanitarian Law: Legal Concepts and Actual Situations*, 91 INTERNATIONAL REVIEW OF THE RED CROSS 75 (2009); Marko Milanovic & Vidan Hadzi-Vidanovic, *A Taxonomy of Armed Conflict*, *in* RESEARCH HANDBOOK ON INTERNATIONAL CONFLICT AND SECURITY LAW (Nigel D. White & Christian Henderson eds., forthcoming 2013**)**; SANDESH SIVAKUMARAN, THE LAW OF NON-INTERNATIONAL ARMED CONFLICT (2012).

7. Robin Geiss, *Armed Violence in Fragile States: Low-intensity Conflicts, Spillover Conflicts, and Sporadic Law Enforcement Operations by Third Parties,* 91 INTERNATIONAL REVIEW OF THE RED CROSS 134 (2009).

8. Robin Geiss & Michael Siegrist, *Has the Armed Conflict in Afghanistan Affected the Rules on the Conduct of Hostilities?*, 93 INTERNATIONAL REVIEW OF THE RED CROSS 11, 13–14 (2011).

to block opposition groups' channels of communication,[9] U.S. drones have reportedly been hacked by Iraqi insurgents,[10] and websites used by Al-Qaida have repeatedly been hacked and manipulated by the U.S. Department of State,[11] although it remains, of course, controversial as to whether the latter activities have occurred in the context of a non-international armed conflict.[12] Moreover, as Stuxnet and other malware tools proliferate, it may be only a question of time before non-State actors will be able to carry out more sophisticated cyber operations. Against this backdrop, this article seeks to discuss particular legal issues arising under the laws of armed conflict with regard to the use of military cyber operations in non-international armed conflicts. The analysis proceeds in three steps and will analyze three general questions.

The first question that arises when considering the issue of cyber warfare in non-international armed conflicts is whether cyber operations in and of themselves, without accompanying kinetic military operations, could ever trigger a non-international armed conflict.[13] In view of the relatively high threshold required for a non-international armed conflict, it appears this could happen only in the most exceptional cases. Nevertheless, States

---

9. *See Syria Internet Services Shut Down as Protesters Fill Streets*, WASHINGTON POST (June 3, 2011, 9:58 AM), http://www.washingtonpost.com/blogs/blogpost/post/syria-internet-services-shut-down-as-protesters-fill-streets/2011/06/03/AGtLwxHH_blog.html.

10. *See US Drones Hacked by Iraqi Insurgents*, GUARDIAN (Dec. 17, 2009, 3:02 PM), http://www.guardian.co.uk/world/2009/dec/17/skygrabber-american-drones-hacked.

11. *See* David P. Fidler, *Recent Developments and Revelations Concerning Cybersecurity and Cyberspace: Implications for International Law*, AMERICAN SOCIETY OF INTERNATIONAL LAW INSIGHTS (June 20, 2012), http://www.asil.org/pdfs/insights/insight120620.pdf; Hillary Clinton, U.S. Secretary of State, Remarks at the Special Operations Command Gala Dinner (May 23, 2012), http://www.state.gov/secretary/rm/2012/05/190805.htm; Benjamin Wittes, *State Department Hackers?*, LAWFARE (May 24, 2012, 7:08 AM), http://www.lawfareblog.com/2012/05/state-department-hackers/. *See, e.g.*, *Hillary Clinton Boasts of US Cyberwar against Al-Qaeda*, TELEGRAPH (May 24, 2012, 6:00 AM), http://www.telegraph.co.uk/news/worldnews/al-qaeda/9286546/Hillary-Clinton-boasts-of-US-cyberwar-against-al-Qaeda.html; *Hacking Terrorist Websites Commonplace*, THE INVESTIGATIVE PROJECT ON TERRORISM (June 3, 2011, 1:32 PM), http://www.investigativeproject.org/2937/hacking-terrorist-websitescommonplace; Adam Rawnsley, *Stop the Presses! Spooks Hacked al-Qaida Online Mag*, WIRED (June 1, 2011, 1:56 PM), http://www.wired.com/dangerroom/2011/06/stop-the-presses-spooks-hacked-al-qaida-online-mag/.

12. *See* Claus Kress, *Some Reflections on the International Legal Framework Governing Transnational Armed Conflicts,* 15 JOURNAL OF CONFLICT AND SECURITY LAW 245, 261, 266 (2010).

13. *See* Schmitt, *supra* note 3, at 368.

are concerned that sophisticated non-State actors could launch severe attacks against modern States in which civil society, the economy and financial markets are increasingly reliant on a functioning, unimpeded cyber infrastructure.[14] Indeed, while States have become much more aware of their cyber vulnerabilities—the Clinton administration issued a presidential directive on critical infrastructure protection as early as in 1998[15]—some technical experts maintain that significant vulnerabilities remain and that ultimately only disconnecting critical systems from networks could bring about a satisfactory degree of protection.[16]

At this time, it is difficult to determine the significance of the cyber threat presented by non-State actors. Non-State actors committing cyber crime[17] and economic cyber espionage[18] do pose serious threats, but to date there have been no public reports of significant and highly devastating cyber attacks launched by non-State actors against a State. There is widespread agreement among experts that cyber operations like Stuxnet and Flame, in view of their complexity and sophistication, could only have been carried out by a State, by a coalition of States or at least with significant State support.[19] Therefore, on the yet-to-be-proven assumption that non-State actors could wage highly destructive cyber operations upon States,

---

14. *See* Gable, *supra* note 5, at 73; *Intelligence Community Annual Threat Assessment: Hearing Before the S. Select Comm. on Intelligence*, 111th Cong. 39 (2009) (statement of Dennis C. Blair, Director of National Intelligence), *available at* http://intelligence.senate.gov/090212/blair.pdf ("Terrorist groups, including al-Qai'da, HAMAS, and Hizballah, have expressed the desire to use cyber means to target the United States.").

15. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 22, 1998, *available at* http://www.fas.org/irp/offdocs/pdd/ pdd-63.htm.

16. SANDRO GAYCKEN, CYBERWAR—DAS WETTRÜSTEN HAT LÄNGST BEGONNEN 235–36 (2012).

17. COUNCIL OF EUROPE, CONVENTION ON CYBERCRIME: EXPLANATORY REPORT, *available at* http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm (last visited Sept. 13, 2012); Roderic Broadhurst, *Developments in the Global Law Enforcement of Cyber-crime*, 29 POLICING: AN INTERNATIONAL JOURNAL OF POLICE STRATEGIES AND MANAGEMENT 415 (2006), *available* at http://www.emeraldinsight.com/journals.htm?articleid=1571786& show=abstract.

18. *See, e.g.*, OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE, FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE (2011), *available at* http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

19. *See Cyberattacks on Iran—Stuxnet and Flame*, NEW YORK TIMES (Aug 9, 2012), http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html.

this article will assess whether and under what circumstances such operations in and of themselves could trigger the application of the laws of armed conflict.

The second question that arises when considering the issue of cyber warfare in non-international armed conflicts relates to the geographic scope of application of the laws of armed conflict. Cyberspace by definition transgresses all national boundaries. It defies any classic notion of a delimited battlefield and enables parties to an armed conflict to launch cyber operations from just about anywhere in the world, to target any network that is connected to cyberspace and to use components of the global cyber infrastructure (servers, cables, etc.) for military purposes. Therefore, it appears that the controversial debate over the geographic scope of application of the laws of armed conflict pertaining to non-international armed conflicts is of particular relevance in the cyber domain.

Finally, the third question relates to the use of cyber operations in the course of an already ongoing non-international armed conflict in which conventional kinetic military means and methods of warfare are being employed. It is now widely accepted that there is no legal vacuum in cyberspace[20] and that "[e]xisting principles of international law apply online, just as they do offline."[21] The critical question, however, is what particular legal challenges arise under the rules governing the conduct of hostilities in non-international armed conflicts when means and methods of cyber warfare are employed?[22] In order to answer these questions, it first needs to be determined what kind of cyber operations are likely to be employed in non-international armed conflicts before, in a second step, discussing the particular challenges arising under the laws of armed conflict.

---

20. *No Legal Vacuum in Cyber Space*, Interview with Cordula Droege, International Committee of the Red Cross (Aug. 16, 2011), http://www.icrc.org/eng/resources/ documents/interview/2011/cyber-warfare-interview -2011-08-16.htm.

21. Joe Biden, Vice President of the United States, Remarks at the London Conference on Cyberspace (Nov. 1, 2011), http://www.whitehouse.gov/photos-and-video/video/2011/11/01/vice-president-biden-delivers-remarks-london-conference-cyberspace#transcript .

22. Robin Geiss, *The Legal Regulation of Cyber-attacks in Times of Armed Conflict*, *in* BRUGES COLLOQUIUM, TECHNOLOGICAL CHALLENGES FOR THE HUMANITARIAN LEGAL FRAMEWORK 47 (College of Europe & International Committee of the Red Cross eds., 2011), *available at* http://www.coleurope.eu/sites/default/files/uploads/page/collegium_41_0.pdf.

II. CAN CYBER OPERATIONS BY THEMSELVES TRIGGER A NON-INTERNATIONAL ARMED CONFLICT?

In order to determine whether cyber operations alone could bring into existence a non-international armed conflict, it needs to be assessed whether, and, if so, under what circumstances, the requisite threshold of violence and the degree of organization required with regard to the armed group involved is reached.

A. The Intensity Requirement

As is well known, in the *Tadić* judgment the International Criminal Tribunal for the former Yugoslavia (ICTY) affirmed that a non-international armed conflict exists only when there is "protracted armed violence."[23] This formula has consistently been applied not only in the case law of the ICTY, but also by other tribunals, namely, the International Criminal Court (ICC), the International Court of Justice, the International Criminal Tribunal for Rwanda and the Special Court for Sierra Leone.[24] What is more, according to Article 1(2) of Additional Protocol II and Article 8(2)(d) and (f) of the ICC Statute, as well as customary international law, situations of internal disturbances and tensions, riots or sporadic acts of violence and other acts of a similar nature do not meet the required threshold of violence.[25] In order to facilitate the assessment of whether there is "protracted armed violence," the ICTY considers various indicative criteria such as the gravity of attacks and their recurrence,[26] the number of victims,[27] the temporal and

23. Prosecutor v. Tadić, Case No. IT-94-1-l, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the former Yugoslavia Oct. 2, 1995) [hereinafter *Prosecutor v. Tadić*]; Vité, *supra* note 6.

24. *See* ANTHONY CULLEN, THE CONCEPT OF NON-INTERNATIONAL ARMED CONFLICT IN INTERNATIONAL HUMANITARIAN LAW 121 nn.19–25 (2010).

25. *See* Prosecutor v. Jean-Pierre Bemba Gombo, Case No. ICC-01/05-01/08, Decision on the Confirmation of Charges, ¶ 225 (Pre-Trial Chamber II June 15, 2009; Anthony Cullen, *The Definition of Non-International Armed Conflict in the Rome Statute of the International Criminal Court: An Analysis of the Threshold Contained in Article 8(2)(f)*, 12 JOURNAL OF CONFLICT AND SECURITY LAW 419, 429 (2007).

26. Prosecutor v. Slobodan Milošević, Case No. IT-02-54-T, Trial Chamber Decision on Motion for Judgment of Acquittal (Rule 98bis Decision), ¶ 28 (Int'l. Crim. Trib. for the former Yugoslavia June 16, 2004) [hereinafter *Prosecutor v. Milošević*].

territorial expansion of violence[28] and the collective character of hostilities.[29]

Against this backdrop, it appears that no cyber attack has ever risen to the requisite threshold of violence. In terms of intensity, not even the Stuxnet operation, the only publicly known cyber operation (with the possible exception of the mysterious Siberian pipeline incident of 1982)[30] that has directly caused physical destruction in the "real world," approached the threshold of violence commonly required for a non-international armed conflict.[31] What is more, even though ICTY trial chambers have interpreted the criterion of "protracted armed violence" as referring more to the intensity of the armed violence than to its duration,[32] it follows from the explicit caveat contained in Article 1(2) of Additional Protocol II,[33] which is also considered reflective of customary international law with regard to Common Article 3 of the four 1949 Geneva Conventions,[34] that singular and merely sporadic cyber incidents, including those that directly cause physical damage or injury, would not amount to a non-international armed conflict. Clearly, mere network intrusions, cyber exploitation operations, data theft and data manipulation, as well as random denial-of-service attacks carried out by a non-State actor, while they would fall into the realm of domestic

---

27. *Id.*

28. *Id.*, ¶ 29.

29. Prosecutor v. Limaj, Case No. IT-03-66-T, Judgment (Trial Chamber), ¶¶ 94–134, 170 (Int'l Crim. Trib. for the former Yugoslavia Nov. 30, 2005); Prosecutor v. Haradinaj, Case No. IT-04-84-T, Judgment (Trial Chamber), ¶ 49 (Int'l Crim. Trib. for the former Yugoslavia Apr. 3, 2008); *see* EVE LA HAYE, WAR CRIMES IN INTERNAL ARMED CONFLICTS 9–13 (2010).

30. William Safire, *The Farewell Dossier*, NEW YORK TIMES, Feb. 2, 2004, at A21, *available at* http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html.

31. In fact, in the case of Stuxnet as far as can be seen no State—including Iran—has publicly qualified the incident as either an "armed attack" or an "armed conflict." *See, e.g.*, Gary Brown & Keira Poellet, *The Customary International Law of Cyberspace*, 6 STRATEGIC STUDIES QUARTERLY 132 (2012).

32. *Prosecutor v. Haradinaj, supra* note 29, ¶ 49.

33. "This Protocol shall not apply to 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." Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts art. 1(2), June 8, 1977, 1125 U.N.T.S. 609. *See also* COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶ 4471 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987).

34. CULLEN, *supra* note 24, at 108; *see* SIVAKUMARAN, *supra* note 6, at 105.

criminal law[35] and could arguably amount to "attacks" in the sense of Article 49 of Additional Protocol I if carried out in the context of an already ongoing armed conflict,[36] would not suffice to trigger a non-international armed conflict in view of the intensity threshold required for this particular armed conflict category. Therefore, while there may be some possibility that cyber operations by non-State actors in exceptional cases may reach the critical threshold of violence, it does not appear to be a likely scenario.

B. The Required Degree of Organization

In addition, for a non-international armed conflict to come into existence, a second criterion also needs to be fulfilled. As the ICTY has held, an armed conflict can exist only between parties that are sufficiently organized to confront each other with military means.[37] While it has rightly been pointed out that the required degree of organization should not be exaggerated,[38] in order to be sufficiently "organized" a non-State armed group must be under an established command structure and must have the capacity to sustain military operations.[39] In the *Lubanga* decision, the ICC Pre-Trial Chamber held that "the involvement of armed groups with *some degree of organization* and the ability to plan and carry out sustained military operations would allow for the conflict to be characterized as an armed conflict not of an international character."[40]

The explicit reference to "some degree of organization" is indicative of the uncertainty as to the exact degree of organization required. In part, this is due to the fact that, notwithstanding universal agreement about the requirement's existence, it has never fully been clarified nor is there full agreement about the criterion's precise function and purpose and why an armed group must be organized in the first place.[41] Is it because only an organized armed group can be expected to sustain military operations on a level that meets the required intensity threshold? Or must an armed group

35. *See* GLOBALIZATION OF CRIME, *supra* note 4, at 203.

36. *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE rule 30 (Michael N. Schmitt ed., 2013).

37. *See Prosecutor v. Tadić, supra* note 23, ¶ 70.

38. Claus Kress, *The 1999 Crisis in East Timor and the Threshold of the Law on War Crimes,* 13 CRIMINAL LAW FORUM 409, 416 (2002).

39. *See Prosecutor v. Limaj*, *supra* note 29, ¶ 129.

40. Prosecutor v. Lubanga, Case No. ICC-01/04-01/06, Decision on the Confirmation of Charges, ¶ 233 (Pre-Trial Chamber I Jan. 29, 2007) (emphasis added).

41. TALLINN MANUAL, *supra* note 36, cmt. to rule 23, ¶ 15.

be organized because only then can it be expected to ensure that its members abide by the laws of armed conflict?[42] The 2008 Report of the International Law Association's Use of Force Committee seems to support the former reading. It suggests that "[t]he criteria of organization and intensity are clearly related and should be considered together when assessing whether a particular situation amounts to an armed conflict. It seems that the higher the level of organization the less degree of intensity may be required and vice versa."[43] This assessment, of course, also leaves open the questions of the required minimum degree, if any, of organization and whether high intensity operations of only loosely organized or even unorganized actors could suffice.

Of course, it is beyond any doubt that armed groups like the Taliban and the Revolutionary Armed Forces of Colombia (the FARC) meet the requisite degree of organization. If distinct armed groups with a similarly high degree of organization launched cyber operations that reach the required intensity threshold, a non-international armed conflict would be triggered. At the same time, however, it is equally clear that cyber operations and computer network attacks by private individuals would not suffice. Such actions may invoke domestic criminal law, but not the laws of armed conflict. Even when a number of individual actors are acting collectively—for example in a spontaneous denial-of-service attack that finds more and more online followers or by sharing and spreading malware tools—they do not qualify as an organized armed group. Collective action—or even organized action—without more is neither sufficient nor decisive.

What matters is the existence of a distinct armed group and that that particular group has a visible and verifiable organizational structure.[44] Thus, the ICTY, when assessing the organizational structure of the Kosovo Liberation Army, referred, *inter alia*, to factors such as the existence of military headquarters,[45] the adoption of internal regulations,[46] the nomination of a

42. COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 33, ¶ 4470 (regarding Article 1(1) of Additional Protocol II); *see also* TALLINN MANUAL, *supra* note 36, cmt. to rule 23, ¶ 14 n.202.

43. Committee on the Use of Force, International Law Association, Initial Report on the Meaning of Armed Conflict in International Law 22 (2008) [hereinafter Meaning of Armed Conflict]; *see* Vité, *supra* note 6, at 76.

44. *See Prosecutor v. Limaj*, *supra* note 29, ¶¶ 89–90.

45. *Id.*, ¶ 90; *Prosecutor v. Milošević, supra* note 26, ¶¶ 23–24.

46. *See Prosecutor v. Limaj*, *supra* note 29, ¶¶ 98, 113–17.

spokesperson,[47] and the issuance of orders, political statements and communiqués,[48] as well as the establishment of military police and disciplinary rules.[49] Similarly, in the *Callixte Mbarushimana* decision the ICC Pre-Trial Chamber referred, *inter alia*, to the Democratic Forces for the Liberation of Rwanda's (FDLR's) hierarchical structure and high level of internal organization, the existence of a political and a military wing, and the FDLR's constitutive instruments, which included "a statute, a '*règlement d'ordre intérieur*' and a disciplinary code which provided the organization's internal disciplinary system."[50]

More recently, there have been discussions about whether so-called "virtual groups," i.e., groups that are organized exclusively on-line and consist of people dispersed over various locations, could be qualified as organized armed groups.[51] Setting aside the controversial question of international humanitarian law's geographic scope of application, it appears that merely virtual groupings that have no physical infrastructure, such as headquarters, physical meeting points, etc., would be too elusive to qualify as a reference point for the determination of the existence of a non-international armed conflict. What is more, due to the notorious human-machine gap in cyberspace, that is, the problem of identifying the natural person behind a given computer, it would be almost impossible to determine membership in a virtual group with any degree of certainty. Of course, over time using extensive forensic investigations and the means and methods of law enforcement such a determination may be possible, but within the narrow time frame that is typically available in a conduct of hostilities context it seems unrealistic.

Moreover, it appears that the different criteria referred to in the *Limaj* judgment and the *Callixte Mbarushimana* decision—albeit only non-exclusive and indicative—inherently presuppose a certain degree of effective control exercised through a chain of command of the group concerned. And, although it may be possible to issue orders online irrespective of geographic distance between the members of a virtual group, the means to enforce such orders are significantly limited when the connection between the

47. *Id.*, ¶¶ 99, 102.

48. *Id.*, ¶ 101.

49. *Id.*, ¶ 113.

50. Prosecutor v. Mbarushimana, Case No. ICC-01/04-01/10, Decision on the Confirmation of Charges, ¶ 104 (Pre-Trial Chamber I Dec. 16, 2011).

51. TALLINN MANUAL, *supra* note 36, cmt. to rule 23, ¶ 13 (a virtual organization is one "in which all activities that bear on the criterion [organization] occur on-line").

members of the group is only virtual. Therefore, the idea that a decentralized virtual group of persons in different locations—possibly dispersed all over the globe—could constitute an organized armed group in the sense of the laws of armed conflict should be dismissed. While it is undeniable that genuine and important security interests of States may be affected by the activities of such virtual groups, the laws of armed conflict hardly serve as a panacea to solve cyber security issues on a global level.

III. THE GEOGRAPHIC SCOPE OF APPLICATION OF THE LAWS OF ARMED CONFLICT IN THE CYBER CONTEXT

Cyberspace is a decentralized, global medium that transgresses national boundaries and defies any notion of a delimited battlefield.[52] The fact that cyber attacks can be launched from anywhere in the world with launch-to-impact times being reduced to milliseconds[53] certainly adds to the controversy regarding the geographic scope of application of the laws of armed conflict in non-international armed conflicts.[54] Is a Taliban fighter who launches a cyber attack from Islamabad, Pakistan against International Security Assistance Force (ISAF) member States still subject to the laws of armed conflict and thereby a legitimate military target? Is the individual hacker who operates out of Buenos Aires and launches cyber attacks against ISAF's communication infrastructure in Afghanistan thereby rendered a legitimate military target? Or is he only a criminal hacker subject to domestic law enforcement in Argentina?

It is not the purpose of this article to revisit or engage in a detailed review of this familiar debate that has been laid out extensively elsewhere.[55] In any case, as far as military operations against persons are concerned, the legal questions that arise in the cyber context are no different from those that arise with regard to the highly controversial practice of extraterritorial targeted killings. Suffice it to say, a number of authors agree that the notion of non-international armed conflict as set forth in Common Article 3 is not confined to single-State scenarios, but also comprises a certain cross-

52. *See* DINNISS, *supra* note 2.

53. Robin Geiss, *War and Law in Cyberspace: The Conduct of Hostilities in and via Cyberspace,* 104 AMERICAN SOCIETY OF INTERNATIONAL LAW PROCEEDINGS 371 (2011).

54. *See* SIVAKUMARAN, *supra* note 6, at 250–52 nn.102–20.

55. *See, e.g.*, Derek Jinks, *September 11 and the Laws of War,* 28 YALE JOURNAL OF INTERNATIONAL LAW 1 (2003); MARCO SASSÒLI, TRANSNATIONAL ARMED GROUPS AND INTERNATIONAL HUMANITARIAN LAW (2006); Kress, *supra* note 12.

border dimension.[56] Opinions vary, however, on whether this cross-border dimension is regionally confined to so-called "spill-over scenarios"[57] or whether it may warrant a wider, arguably even global, application of the laws of armed conflict.[58] The wording of Common Article 3 is sufficiently broad to accommodate a cross-border dimension, and in the case of spillover conflicts, where national boundaries are randomly and frequently crossed, pragmatic reasons and the geographic proximity to the original armed conflict may support such an interpretation.[59] Nevertheless, the various definitions of non-international armed conflict as they are laid out in treaty law, whether in Common Article 3, Article 1(1) of Additional Protocol II or Article 8(2)(f) of the ICC Statute, and the ICTY's ruling in *Tadić*, all contain a territorial link of some sort.[60] Against this background, and in light of the fact that the laws of non-international armed conflicts constitute a reaction to extreme levels of military violence (hence the high threshold requirements laid out above),[61] multi-State application that pays no heed to the geographical proximity to ongoing hostilities cannot, in the view of the present author, be sustained.[62]

Cyber warfare, by virtue of the technological nature of cyberspace, adds an additional aspect to the debate. Every cyber operation carried out via the Internet (except where malware is implanted directly into the target system as was the case with Stuxnet) typically uses cyber infrastructure components in different locations around the globe. Therefore, in the case of cyber warfare, the issue of geographic scope of application of the laws of

---

56. Milanovic & Hadzi-Vidanovic, *supra* note 6; NOAM LUBELL, EXTRATERRITORIAL USE OF FORCE AGAINST NON-STATE ACTORS 101–4 (2010); Dapo Akande, *Classification of Armed Conflicts: Relevant Legal Concepts, in* INTERNATIONAL LAW AND THE CLASSIFICATION OF CONFLICTS 32, 46–47 (Elizabeth Wilmshurst ed., 2012).

57. Jelena Pejic, *The Protective Scope of Common Article 3: More Than Meets the Eye*, 93 INTERNATIONAL REVIEW OF THE RED CROSS 189 (2011).

58. GEOFFREY S. CORN, VICTOR M. HANSEN, DICK JACKSON, ERIC TALBOT JENSEN & JAMES A. SCHOETTLER JR., THE WAR ON TERROR AND THE LAWS OF WAR: A MILITARY PERSPECTIVE 11 (2009)

59. Pejic*, supra* note 59, at 193.

60. The ICC Chamber in the *Bemba Gombo* decision therefore concluded that an armed conflict not of an international character "takes place within the confines of a State territory." *Prosecutor v. Bemba Gombo*, *supra* note 25, ¶ 231.

61. *See supra* notes 23–36 and accompanying text.

62. *See* YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 56 (2d ed. 2010) ("from the vantage point of international law . . . a non-international armed conflict cannot possibly assume global dimensions").

armed conflict is as relevant to the targeting of objects involved in cyber operations as it currently is with regard to persons.

Certainly, in an international armed conflict involving highly sophisticated military forces and large-scale cyber operations, a vast percentage of the worldwide civilian and dual-use cyber infrastructure will be used for military purposes, potentially posing a considerable challenge to the law of neutrality. But the trans-boundary nature of cyberspace and the dual-use character of the global cyber infrastructure may also play out in non-international armed conflicts. The following, admittedly rather simplistic, example may help to illustrate the point. Taliban fighters install a botnet—a worldwide network of remote-controlled civilian computers[63]—in order to generate computer power to launch a cyber operation against the communication infrastructure of States supporting the Afghan government in its fight against the Taliban. All the civilian systems unknowingly involved in the botnet are used to make an effective contribution—however individually minimal—to military action. Collectively they are the infrastructure used to carry out a cyber operation and thus would arguably qualify as legitimate military objects in accordance with the definition contained in Article 52 of Additional Protocol I, which is generally accepted as being reflective of customary international law in both international and non-international armed conflicts.[64]

Of course, it could be argued that even when certain components of the global cyber infrastructure are used for military purposes, this does not automatically render them a military objective because in the interconnected and largely resilient domain of cyberspace destroying or temporarily disrupting a server that is used for military purposes by non-State actors would not offer a definite military advantage since the cyber operation can be easily switched to other servers. Under these circumstances, destroying or disrupting individual components would not diminish the attacker's capacity to execute further cyber operations. After all, Article 52(2) and the corresponding customary law rule contain a two-pronged test. In order to qualify as a legitimate military objective, an object must not only be used to make an effective contribution to military action, but its destruction must

63. An example is the Mariposa botnet, which reportedly involved an estimated 13 million systems in over 190 countries. *See* Joseph Menn, *Investigators Shut Down Mariposa Hacking Network*, FINANCIAL TIMES, Mar. 4, 2010, World News, at 7.

64. 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW rule 8, at 29 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005).

also offer a definite military advantage in the circumstances ruling at the time.[65]

It appears doubtful, however, that Article 52(2)'s military advantage requirement will function as an effective constraint. Although the law clearly requires a two-pronged test when qualifying military objectives, the interplay of these two tests has remained ambiguous. In practice, the emphasis is usually placed only on the first. As the commentary in the *Air and Missile Warfare Manual* confirms, "[i]n practical terms, compliance with the first criterion [the requirement of nature, location, purpose or use] will generally result in the advantage required of the second."[66]

It must be noted that only if there is an assumption of a multi-State or global application of the laws of non-international armed conflicts can the use of the worldwide cyber infrastructure for military purposes by non-State actors potentially render its components military objectives. Article 52 and the customary law definition of legitimate military objectives are only of relevance when the laws of armed conflict apply in the first place. In traditional non-international armed conflicts, the use of State or civilian property by organized armed groups undisputedly rendered these objects legitimate military objectives. The problem is that cyberspace has enabled States and non-State actors to use State and civilian cyber infrastructure components located in countries around the world.

Yet it is far from clear that this justifies an automatic extension of the scope of application of the laws of armed conflict. In essence, this would allow non-State actors to turn components of the worldwide cyber infrastructure into legitimate military objectives basically by virtue of a few mouse clicks. Within milliseconds during a single cyber attack various data packages may randomly travel via different channels all over the world, thereby arguably using all of these channels to make an effective contribution to military action. A global application of the laws of armed conflict that encompasses any militarily useful cyber activity wherever it may occur would rapidly lead to a large-scale militarization of cyberspace and could obviously have far-reaching destabilizing effects on relations between States.

---

65. Robin Geiss & Henning Lahmann, *Cyber-Warfare: Applying the Principle of Distinction in an Interconnected Space,* 45 ISRAEL LAW REVIEW 1, 7 (2012).

66. PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, COMMENTARY ON THE HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE 49 (2010).

Absent a specific legal regime of neutrality relating to non-international armed conflicts,[67] *ius ad bellum* rules constrain military operations against cyber infrastructure in third States even if components of this infrastructure qualify as legitimate military objectives. However, if military operations are regarded as permissible in cases where States are unable due to lack of expertise or technology to stop physical cyber infrastructure located on their territory from being used to carry out cyber operations against other States,[68] *ius ad bellum* rules may not impose a significant constraint in the cyber context. Currently, even States with the most advanced cyber technology are often unable to detect and immediately end malicious cyber activity that occurs on, or originates from, their territory, let alone attribute such operations to individual persons.

IV. CYBER OPERATIONS AS A METHOD OF WARFARE IN NON-INTERNATIONAL ARMED CONFLICTS IN WHICH THERE ARE TRADITIONAL KINETIC MILITARY OPERATIONS

While there is little doubt that military cyber operations will become increasingly relevant in future non-international armed conflicts, currently the focus of military strategists is principally on inter-State scenarios and international armed conflicts.[69] This is reflected in contemporary legal literature on cyber warfare, which has largely focused on the laws of armed conflict as they apply in international armed conflicts.[70] In future inter-State armed conflicts that involve high-tech belligerents with sophisticated cyber capabilities and corresponding vulnerabilities, gaining information dominance—i.e., control over cyberspace and outer space—will become as important a strategic goal as obtaining control over territory, airspace or the

67. The law of neutrality applies only during international armed conflicts. *See* TALLINN MANUAL, *supra* note 36, ch. VII, ¶ 1.

68. *Id.*, cmt. to rule 13, ¶ 22. The "unable and unwilling" standard, however, remains controversial. *See* TOM RUYS, ARMED ATTACK AND ARTICLE 51 OF THE UN CHARTER—EVOLUTIONS IN CUSTOMARY LAW AND PRACTICE (2010).

69. *See, e.g.*, Secretary of Defense, Sustaining U.S. Global Leadership: Priorities for 21st Century Defense (2012), *available at* http://www.defense.gov/news/Defense_Strategic _Guidance.pdf.

70. *See, e.g.*, Schmitt, *supra* note 3; Watts, *supra* note 3; Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks,* 88 TEXAS LAW REVIEW 1533, 1542 (2010); KNUT DÖRMANN, APPLICABILITY OF THE ADDITIONAL PROTOCOLS TO COMPUTER NETWORK ATTACKS (2004), *available at* http://www.icrc.org/eng/assets/files/other/ applicability ofihltocna.pdf; Geiss, *supra* note 55.

sea has been in traditional conflicts.[71] As the U.S. Quadrennial Defense Review Report emphasizes, "in the 21st century, modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communication networks and assured access to cyberspace."[72]

Military cyber operations in future inter-State armed conflicts will aim to degrade the enemy's capacity to use cyberspace for military operations, to manipulate the enemy's data and the functioning of its cyber-connected systems, and to block the enemy's ability to communicate via cyberspace. It is well known that sophisticated military forces of major States are already preparing for potential future cyber battlefields by preimplanting concealed codes and software tools in various strategically relevant "places," as well as by manipulating hardware components along the supply chain.[73] This type of cyber warfare will not only use cyberspace as a medium to deliver attacks against "real world" military targets (e.g., launching a cyber attack against an electrical power plant that is used for military purposes), but will also include large-scale kinetic military operations against strategically relevant cyber infrastructure components, including software and hardware, all over the globe.

Cyber warfare in non-international armed conflicts will likely feature only some of these aspects of cyber war between States. While fears have been expressed that non-State actors could use cyber operations to enhance their military capabilities and to attack critical infrastructure of States, it is not clear that non-State actors currently have that capacity. Yet, the cyber vulnerabilities of organized armed groups against which cyber attacks could be conducted also remain limited. Even though some of the States currently involved in the non-international armed conflict in Afghanistan are heavily reliant on cyber capabilities for their military operations in Afghanistan,[74] the Taliban do not appear to have the technological ability to attack these capabilities or even interfere with them to any significant

71. QUADRENNIAL DEFENSE REVIEW REPORT, *supra* note 1, at 37.

72. *Id.*

73. *See* BRYAN KREKEL, PATTON ADAMS & GEORGE BAKOS, NORTHRUP GRUMMAN CORPORATION, OCCUPYING THE INFORMATION HIGH GROUND: CHINESE CAPABILITIES FOR COMPUTER NETWORK OPERATIONS AND CYBER ESPIONAGE 11–12 (2012) ("By providing counterfeit hardware that already contains the Trojanized access built into the firmware or software, a foreign intelligence service or similarly sophisticated attacker has a greater chance of successfully penetrating these downstream supply chains." *Id.* at 11).

74. Wayne W. Grigsby Jr., Garrett Howard, Tony McNeill & Gregg Buehler, *CEMA: A Key Success in Unified Land Operations,* 62 ARMY MAGAZINE 44 (2012).

degree. Conversely, the reliance of the Taliban on cyber assets or systems connected to cyberspace to carry out military operations or attacks—apart perhaps from the use of mobile telephones for military communications and the remote detonation of improvised explosive devices (IEDs)[75]—also appears to be limited.

Of course, the situation may be different if third States become involved in a non-international armed conflict. Thus, in the currently hypothetical scenario of an intervention by third States in the ongoing non-international armed conflict in Syria, it is certainly conceivable that cyber operations would be used to disable Syrian air defense systems. Needless to say, however, that intervention of external States would lead to an international armed conflict between the intervening States and Syria, in addition to the already ongoing non-international armed conflict.

In traditional non-international armed conflicts, i.e., those in which other States do not intervene, it seems that cyber warfare in the strict sense of the actual conduct of hostilities is today of only rather limited relevance. Rather, cyberspace is used for vastly different purposes, namely, using social media and media reporting for public information purposes and political mobilization. Even though it is likely that with the rapidly growing worldwide dependence on cyberspace, further technological evolution and the proliferation of malware tools, the relevance of cyberspace will increase in non-international armed conflicts, the legal questions that arise in relation to the conduct of hostilities in such conflicts are generally similar to those arising in international armed conflicts.

Thus, when cyberspace is used as a medium to deliver attacks against "real world" targets, as opposed to "virtual targets," typically no particular legal challenges will arise. Whether a legitimate military objective, such as a military communications center, is attacked via cyberspace or by an airstrike, the same legal principles apply.[76] Clearly, any attacker planning to carry out such an attack would be bound, *inter alia*, by the principle of pro-

75. Mobile telephones are often a vital military instrument for organized armed groups in various parts of the world; they are used to detonate bombs and to coordinate military movements and operations.

76. *See* Geiss & Lahmann, *supra* note 67. The precautions in attack norm is codified in Article 57 of Additional Protocol I for international armed conflict, whereas the rule of proportionality is codified in Articles 51 and 57.

portionality and would be required to take precautions in accordance with customary international law.[77]

Moreover, as in international armed conflicts, it may be questionable whether a particular operation qualifies as an "attack" in the legal sense of Article 49 of Additional Protocol I, which, by virtue of customary international law, also applies to non-international armed conflicts.[78] It appears, however, that various aspects of this debate have now been settled by the definition in the *Tallinn Manual*, according to which "[a] cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects," which by and large appears to reflect widespread consensus.[79]

Controversy persists only with regard to the question of whether damage and destruction also encompass the temporary loss of functionality in cases where no direct physical damage results.[80] For example, computerized systems may be manipulated via cyberspace in order to shut down connected systems. Thus, the distribution of electrical energy could be stopped by virtue of data manipulation in the control systems of power grids and power plants with no direct physical destruction. Such operations may be strategically appealing, particularly in non-international armed conflicts where States will aim to deprive their non-State enemies of strategic assets such as electrical power, while leaving the underlying infrastructure intact. It is clear that not every military operation that causes inconvenience for the civilian population—for example, a roadblock—automatically qualifies as an attack in the legal sense.[81] It is also clear that collective punishments and the terrorization of the civilian population are strictly prohibited under all circumstances.[82] Nevertheless, there is nothing in the laws of armed conflict that would bar an interpretation that qualifies an operation leading to the loss of functionality—irrespective of how this loss is caused and whether this involved physical destruction—as an attack. In fact, the overall object and purpose of the rules governing the conduct of hostilities—"to ensure respect for and protection of the civilian population and civilian

77. 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 64, rules 15–21, at 51–67.

78. Schmitt, *supra* note 3, at 368–75; TALLINN MANUAL, *supra* note 36, cmt. to rule 30, ¶¶ 1–19.

79. TALLINN MANUAL, *supra* note 36, rule 30.

80. *Id.*, cmt. to rule 30, ¶ 10.

81. Geiss, *supra* note 55.

82. 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 64, rule 103, at 374 and rule 8, at 29.

objects"[83]—would generally seem to militate in favor of a broader, rather than a more limited, understanding of the notion of attack, given that only attacks in the legal sense are subject to the principle of distinction and proportionality.

V. CONCLUSION

At present, many of the issues pertaining to non-international armed conflicts and cyber warfare remain the subject of some speculation. In particular, the military cyber capabilities that non-State actors currently have, or may develop, is unclear. Though it appears highly unlikely that cyber attacks by a non-State actor could alone trigger a non-international armed conflict, specific cyber attacks in the course of an ongoing conflict in which traditional kinetic forms of attack are occurring are certainly conceivable. As far as legal issues pertaining to the actual conduct of hostilities are concerned, the legal questions raised are generally the same as those that are currently being discussed with regard to international armed conflicts. There is widespread agreement that cyberspace is not a legal vacuum and that international law, including the laws of armed conflict, applies in cyberspace. But in view of the dual-use nature of the entire cyber infrastructure and the fact that the artificial domain of cyberspace transgresses State boundaries, it seems that an unrestrained application of the laws of armed conflict, especially those relating to non-international armed conflicts, could lead to an unwarranted large-scale militarization of cyberspace. Quite clearly, therefore, the laws pertaining to non-international armed conflicts should be applied cautiously in the cyber domain and, in view of the unique and still insufficiently understood technical features of cyberspace and the possibilities for its military use, the precise parameters of their application need to be worked out more concretely than they have been to date.

83. *Id.*, rule 1, at 3; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 48, June 8, 1977, 1125 U.N.T.S. 3.