ASIL Insights, Volume 19, Issue 18, July 2015
https://www.asil.org/insights/volume/19/issue/18/first-case-cyberwar-non-international-armed-conflict-matrix-iraq

The First Case of Cyberwar in Non-International Armed Conflict? The Matrix in Iraq

By: David Turns

The multi-faction insurgency that has been tearing Iraq apart ever since the fall of Saddam Hussein's regime in 2003 has often involved the use of such crude and indiscriminate methods and means of warfare as the suicide bomb and the improvised explosive device. But in mid-2014 there were reports that some aspects of the armed conflict had risen to unexpected heights of contemporary sophistication, with the apparent use of cyberspace as a domain for hostilities. These manifestations included reports of computer hacking to gather intelligence, malware attack programmes to subvert and exercise remote control over hostile computer networks, the use of booby-trapped messages on email, and the use of social media to spread fear in specifically-targeted sectors of the population.[1] Whereas the only previous recorded use of cyberwar within the context of an actual armed conflict occurred in a situation that was clearly international in nature (the South Ossetia War of 2008 between Russia and Georgia),[2] the conflict in Iraq is at present equally undoubtedly a non-international one. The moment is therefore opportune to consider the application of international humanitarian law (IHL) to cyber hostilities in non-international armed conflicts (NIAC) generally, as well as the legality of certain specific acts allegedly occurring in the present situation in Iraq.

Cyberwar in NIAC: Some Generalities

There is no treaty of IHL that specifically regulates the conduct of hostilities or the protection of victims of armed conflict in the cyber context; nor is there clear evidence of normative customary international law on point in the form of state practice and *opinio juris*. States are wary, for a variety of reasons, of making express pronouncements on their views of the existence or content of any specific customary law of cyber operations; nor is there any appetite on the part of states for the kind of multilateral law-making exercise that would be necessary for the adoption of a new treaty on the topic. The International Committee of the Red Cross (ICRC) has expressed the view that "means and methods of warfare which resort to cyber technology are subject to IHL just as any new weapon or delivery system has been so far when used in an armed conflict by or on behalf of a party to such conflict,"[3] although this does not necessarily represent the settled view of a plurality of the international community. In the absence of primary sources of law, the commentaries of scholars have become paramount as evidence of *lex lata*—the widely agreed default position being that the existing corpus of IHL applies, *mutatis mutandis*, to hostilities in the cyber domain.[4] Academic writings on the topic have recently been boosted, albeit still in the

form of non-binding "soft law," by the publication of the Tallin Manual, an extensive non-official manual drafted by an International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence.[5] Part B of the Tallinn Manual surveys the traditional corpus of IHL and discusses its application in cyber armed conflict, and unequivocally accepts that doctrinally the rules of IHL applicable in NIAC are capable of application also in the event of non-international cyber hostilities, provided they meet the relevant threshold for scope of application.[6] However, in view of the nature of these authorities and the well-known difficulties in securing application of the rules even in conventional NIAC in many situations, it must surely remain a matter of some conjecture as to whether, and if so to what extent, any states engaged in NIAC might accept their applicability either *de jure* or *de facto*.

The substantive rules of IHL applicable in situations of NIAC are to be found primarily in Common Article 3 of the 1949 Geneva Conventions[7] and the 1977 Additional Protocol II (AP II).[8] Common Article 3 lays down basic minimum standards for the treatment of persons taking no active part in hostilities, whilst AP II contains much more extensive and detailed provisions for the humane treatment of such persons;[9] for the protection of the wounded, sick, and shipwrecked;[10] and for the protection of the civilian population.[11] Neither instrument says anything about the conduct of hostilities or the methods and means of warfare, including the use of certain types of weapons. These topics are, however, extensively dealt with in the law relating to international armed conflicts (IAC), and the ICRC has—not without controversy—suggested that very many of the same rules are equally applicable in NIAC.[12] The Tallinn Manual specifically includes many of those rules in the context of NIAC within the cyber domain.[13]

IHL, Cyber Activities, and the NIAC in Iraq

There can be no doubt that the situation in Iraq amounts to a NIAC, since there is occurring within the territory of the state protracted armed violence meeting the requisite minimum levels of intensity and organisation of the parties.[14] The applicable law, however, is limited to Common Article 3 and customary international law,[15] since Iraq has never become a party to AP II. By the same token, enforcement will present a serious problem: Iraq has never become a state party to the International Criminal Court, either. Whilst a United Nations Security Council referral under Chapter VII of the UN Charter would bring the situation in Iraq within the Court's jurisdiction,[16] the currently fractious relationship between certain of the permanent members of the Council would surely make it all but impossible to secure the necessary diplomatic and political agreement.

Specific cyber activities reported recently in Iraq that might raise questions under IHL involve the use of social media to rally supporters and spread propaganda, the use of hackers to gather intelligence, the subversion of routers in order to obtain remote control of networks by the malware programme Njrat, and the deception of users with the result that they open booby-trapped attachments or access web pages that exploit vulnerabilities in their Internet browsers.[17] Some of these activities are unproblematic in terms of IHL in the sense that they do not disclose violations of the law—although they are interesting enough to elicit some comment. The use of social media such as Facebook and YouTube would not seem to violate any rules of IHL as long as it is only for the purposes of rallying supporters, spreading propaganda or obtaining intelligence, or alternatively as a permitted ruse: Rule 61 of the Tallinn Manual specifically provides that, "Cyber operations that qualify as ruses of war are permitted."[18] Included within the scope of such permissible ruses are "psychological warfare activities;"[19] this would certainly encompass the dissemination of propaganda, which is not as such prohibited by any rule of IHL. By the same token, information-gathering (by whatever means) is not prohibited in situations of armed conflict,[20] and may indeed constitute only computer network exploitation (CNE), rather than rising to the level of cyber espionage.[21]

Cyber operations will not qualify as "attacks" within the meaning of IHL unless they can be "reasonably expected to cause injury or death to persons or damage or destruction to objects;"[22] once they have crossed that threshold, however, they must not be targeted deliberately at civilians or civilian objects,[23] nor have the primary purpose of spreading terror among the civilian population.[24] Some of the activities reported in Iraq have apparently violated these rules and have been very selectively targeted, down to specific families or even just personal friends of people involved in the armed conflict in particular cities—principally Baghdad, Basra, Mosul, and Erbil. The effect of these activities, if it is to intimidate people into not supporting or helping others in connection with the conflict, would amount to a violation of Rule 36, but only if they rose to the level of "attacks." The same qualification would apply in the case of cyber booby traps; the information available does not specify whether deaths, injuries, destruction, or damage has actually occurred in any instances as a result of cyber booby traps, but if that were to be the case, it would disclose a violation of Rule 44.

A final point of interest here concerns the legal status of persons engaged in cyber hostilities in connection with the armed conflict in Iraq. Although the formal category of combatant does not as such exist in NIAC, the concept of civilians who directly participate in hostilities does, and has the same effect as in international armed conflicts: namely, that civilians who do so lose their entitlement to protection from attack.[25] However, it would be necessary to show that the civilians in question are not members of an organised armed group and have been directly participating in hostilities on an individual, unaffiliated basis; furthermore, the acts in question would have to meet the three cumulative criteria stipulated to constitute direct participation in hostilities – those of adversely affecting the enemy's military

capabilities, having a direct causal link to the resulting harm, and having the requisite belligerent nexus.[26] The information currently available in respect of the armed conflict in Iraq is not sufficiently detailed to permit such assessments to be made as yet.

About the Author: David Turns is Senior Lecturer in International Law at the Centre for International Security and Resilience (Cranfield University), Defence Academy of the United Kingdom. Opinions are stated in a private capacity and do not represent any official position of the Armed Forces, Ministry of Defence or Government of the United Kingdom.

---

[1] Mark Ward, *Iraq Conflict Breeds Cyber-War Among Rival Factions*, BBC NEWS, Jul. 22, 2014, *available at* http://www.bbc.co.uk/news/technology-28418951.

[2] *See* AFCEA INTERNATIONAL, THE RUSSO-GEORGIAN WAR 2008: THE ROLE OF THE CYBER ATTACKS IN THE CONFLICT, (2012), *available at* http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf.

[3] *See* 31st International Conference of the Red Cross and Red Crescent, Nov. 28–Dec. 1, 2011, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, 36–38, ICRC Doc. 31IC/11/5.1.2.

[4] *See* Michael N. Schmitt, *Wired warfare: Computer Network Attack and Jus in Bello*, 84 INT. REV. RED CROSS 365, 368–375 (2002).

[5] *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Michael N. Schmitt ed., 2013) [hereinafter Tallinn Manual]. An updated and revised version, *Tallinn Manual 2.0*, is currently in preparation and due for publication in 2016.

[6] *Id.* r. 23.

[7] Geneva Conventions 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; Geneva 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; Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 287; Geneva 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.

[8] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), *opened for signature* Dec. 12, 1977, 1125 U.N.T.S. 609, 16 I.L.M. 1442 [hereinafter AP II].

[9] *Id.* arts. 4-6.

[10] *Id.* arts. 7-12.

[11] *Id.* arts. 13-18.

[12] *See* JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW – VOLUME I: RULES (2005).

[13] *E.g.*, Tallinn Manual, *supra* note 5, r. 31 (rule of distinction), 32 (prohibition on attacking civilians), 35 (civilians directly participating in hostilities), 36 (prohibition of terror attacks), 37 (prohibition on attacking civilian objects), 42 (prohibitions of causing superfluous injury or unnecessary suffering), 43 (prohibition of indiscriminate means or methods of warfare), 44 (prohibition of cyber booby traps), 49 (prohibition of indiscriminate attacks), 51 (rule of proportionality), 52-57 (precautions in attack), 60 (prohibition of perfidy), 61 (ruses), 66(a) (cyber espionage).

[14] The legal criteria are taken from the wording of Common Article 3 and *Prosecutor v. Tadić*, Case No. IT-94-1-I, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995) as subsequently developed by the jurisprudence of the International Criminal Tribunal for the Former Yugoslavia.

[15] For Iraqi state practice as to customary IHL, see Customary IHL, ICRC, http://www.icrc.org/customary-ihl/eng/docs/v2_cou_iq (last visited July 15, 2015).

[16] Final Act of the U.N. Diplomatic Conference of Plenipotentiaries on the Establishment of an International Criminal Court, July 17, 1998, art. 13(b), 37 I.L.M. 999.

[17] Ward, *supra* note 1.

[18] *See* William Boothby, *Cyber Deception and Autonomous Attack – Is There a Legal Problem?*, *in* 5th International Conference on Cyber Conflict – Proceedings 245–262 (K. Podins, J. Stinissen & M. Maybaum eds. 2013).

[19] Tallinn Manual, *supra* note 5, r. 61, ¶ 2(f).
[20] *Id.* Rule 66(a).
[21] *See id.* R. 61, ¶ 3.
[22] *Id.* r. 30. *See* David Turns, *Cyber War and the Concept of 'Attack' in International Humanitarian Law, in* INTERNATIONAL HUMANITARIAN LAW AND THE CHANGING CHARACTER OF WAR 209-227 (DAN SAXON ed., 2013).
[23] Tallinn Manual, *supra* note 5, r. 32 (civilians), 37 (civilian objects).
[24] *Id.* r. 36.
[25] *Id.* r. 35.
[26] *See* ICRC, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (2008) 90 INT. REV. RED CROSS 991.