Cyber warfare is taking place!

Ducheine, P.A.L.

Published in:
Internationale Spectator

ARTIKEL

Cyber warfare is taking place!

Paul Ducheine

In 2012, Thomas Rid concluded that "Cyberwar will not take place".[1] Besides the fact that his colleague John Stone argued otherwise,[2] it is now clear that cyber warfare has indeed become reality. Early 2016, the US Secretary of Defense Ashton Carter confirmed he had given US Cyber Command "its first wartime assignment" in the war with ISIS.[3] Likewise, in the UK Secretary of State for Defence Michael Fallon MP confirmed that UK's offensive cyber capabilities are also deployed in the campaign against Da'esh (also referred to as ISIS).[4] These two public statements, joined with NATO's announcement to "recognise cyberspace as a domain of operations",[5] have brought (the debate on) cyber warfare into the open.

Arguably, cyber capabilities had been used before. In 2007, Israel was believed to have employed cyber capabilities in *Operation Orchard* against an undeclared Syrian nuclear facility in Al Kibar.[6] In addition, Israel and the US are believed to have jointly launched *Operation Olympic Games* to delay Iran's nuclear programme in Natanz.[7] The latter operation became famous for the malicious software ('malware') used: Stuxnet. After these speculations, the UK and US official recognition of cyber operations is ground-breaking.

Stuxnet and the (legal) debate

Stuxnet triggered fierce academic debate and raised questions on various aspects of international relations. Firstly, whether Stuxnet should be considered sabotage (Rid's reasoning) or indeed warfare (conform Stone).

And secondly, in legal terms, whether or not states could resort or respond to cyber warfare. The issues at stake: did the operation qualify as a "use of force" or even an "armed attack" in the meaning of the UN Charter.[8] It is telling that the 'international group of experts' responsible for the Tallinn Manual on the International Law applicable to Cyber Warfare, although agreeing that Stuxnet amounted to the use of force,[9] thereby implicating a violation of the UN Charter by the attacking state(s), nevertheless disagreed on the issue of the armed attack.[10] Some of the experts were of the view that Olympic Games had "reached the threshold of an armed attack", meaning that Iran could have relied on self-defence in response (had Iran been aware of the attack at the time).

> Stuxnet triggered fierce academic debate and raised questions on various aspects of international relations

Thirdly, much of the legal discourse regarding cyber warfare also involved (the applicability of) the law of armed conflict (LOAC).[11] Positions ranged from not mentioning LOAC at all or that it ought to be supplemented at best,[12] to the acknowledgement that LOAC applies to all kinds of warfare, including cyberwar.[13]

These three debates will be covered briefly in this contribution. First, cyber warfare within the spectrum of military cyber operations will be defined. Second, the legal basis to commit cyber forces in military operations will be given. Thirdly, some remarks on the main legal regime applicable to the use of cyber capabilities in warfare, that is LOAC, will be presented.

Cyber warfare proper

As said, the first debate is on the meaning of cyber warfare. 'Cyber war' has become a common denominator for a variety of activities undertaken with the aim of achieving objectives in or through cyberspace. It is used in a variety of situations, referring to a diversity of actors and, quite obvious, for various motives ascribed to those actors.

© Flickr / Chris-Håvard Berge

'It is now clear that cyber warfare has become reality'.

Those actors, which may involve state and non-state entities – including the persons involved ('hackers') – will be inspired or driven by motives ranging from enhancing security on the one hand, to testing, training, boasting, activism, economic profit, sabotage, propaganda, subversion, theft, terrorism, espionage and (military) conflict on the other.[14]

It is evident that cyber warfare proper should be reserved for the paradigm of military conflict.[15] Cyber warfare involves 'warfare proper' and 'operations other than war', including peace support (and enforcement) operations related to conflict.[16]

Thus 'cyber warfare' can be defined as "employment of cyber capabilities with the primary purpose of achieving [military] objectives in or by the use of cyberspace".[17]

Legal basis for cyber warfare

The second debate addresses the question whether and when states may decide to engage in cyber warfare.[18] The basic rule is that States are prohibited to resort to force, cyberwar included, in their international relations, unless international law provides for an exemption. There are three exemptions: consent, a UN Security Council authorization, or self-defence.

International law, more specifically the *jus ad bellum,* prohibits offensive and defensive cross-border military operations in article 2(4) of the UN-Charter: 'All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.'

Use of force

This provision prohibits extraterritorial cyber operations insofar they can be conceived as 'use of force'.[19] Though lacking a definition,[20] 'use of force' operates as a threshold. It is generally accepted that it encompasses armed, i.e. military, physical force.[21] Actions are judged by the results or effects:[22] they are considered 'use of force' if they directly cause death, injury or physical damage to property.[23]

For cyber operations, this physically oriented reading may (and will) cause questions of interpretation, as some of the operations will only have non-physical effects.[24] The AIV&CAVV (Advisory Council on International Affairs and the Advisory Committee on Issues of International Law) concluded that a cyber operation qualifies as use of force "if the consequences are comparable to those caused by an attack with conventional or unconventional weapons".[25] The Tallinn Manual reaches a similar conclusion.[26]

Cross-border military cyber operations *below* the threshold of use of force are allowed, provided they respect,[27] most prominently, international law relating to sovereignty[28] and non-intervention.[29]

In the most likely scenario,[30] however, cyber warfare will only be one of many lines of action within a wider cross-border military campaign *above* the threshold of the use of force. They require a legal basis to be found in one of three exceptions to this prohibition on the use of force:[31]

- intervention with the consent of, or invitation by a (host) nation;
- authorization of the UN Security Council under Chapter VII of the UN Charter; and
- self-defence.

Self-defence

Whereas consent and a UN SC authorization cause little debate when used as a legal basis for cross-border military operations, self-defence may do so. Self-defence is only permitted under strict conditions, these conditions raise pressing questions in the cyber domain. Two of these will be addressed: armed attack and attribution.

> States and international organizations such as NATO are grasping to get attuned operationally and legally

First, without consent or UN SC authorization, a State may invoke its inherent right of self-defence only "if an armed attack occurs".[32] Thus, an 'armed attack' is required.[33] Generally, this includes a threat that is instant, overwhelming, leaving no choice of means, and no moment of deliberation.[34] Furthermore, a series of smaller and related attacks cumulatively can be considered an armed attack.[35] In its advisory report to the Dutch government,

AIV&CAVV reiterated the classic position that a cyber attack could certainly qualify as an 'armed attack' within the meaning of Article 51 of the UN Charter if it "leads to a significant number of fatalities or causes substantial physical damage or destruction to vital infrastructure, military platforms or installations or civil property".[36]

More importantly, however, AIV&CAVV concluded that an organized "cyber attack" on vital functions of the state could conceivably be qualified as such:

> *"if it could or did lead to serious disruption of the functioning of the state or serious and long-lasting consequences for the stability of the state".*[37]

For instance,

> *"a cyber attack that targets the entire financial system or prevents the government from carrying out essential tasks, […] could well be equated with an armed attack".*[38]

With this liberal view, the AIV&CAVV as well as the Netherlands' government take a liberal stance.

Secondly, once the effects of and the qualification as an armed attack are clear, attribution is required to determine the addressee of self-defence. Logically, that is against the attacker, provided it can be identified.[39]

To sum up, States may decide to engage in cyber warfare by launching – integrated or standalone – cross-border military operations, provided a legal basis in the *ius ad bellum* is available once it crosses the threshold of the use of force, or as long as it stays below the threshold and respects the principles of sovereignty and non-intervention.

Regimes applicable to cyber warfare

The final issue is how to conduct cyber warfare lawfully. In particular, issues related to the law of armed conflict (LOAC), such as targeting rules, protection of civilians, and civilian infrastructure will be covered here.[40]

Focusing on LOAC, this field of international law has developed well before cyber warfare came into existence, resulting in issues of interpretation and application. However, LOAC has effectively dealt with issues like these before. LOAC has always been adaptive in character. For instance, although aerial weapons came into use during World War I, a specific treaty dealing with warfare in the third dimension never saw light. Yet, it is beyond doubt that LOAC applies to aerial warfare. The same holds true for the applicability of LOAC to cyber warfare. That is, once (standalone or integrated) cyber operations cross the threshold of an "armed conflict" triggering the applicability of LOAC.[41] Once it does, numerous questions related to "how to conduct cyber warfare" in accordance with LOAC will have to be answered. Only two of those issues are addressed below: armed conflict and targeting rules.

Armed conflict

The first issue is of course the threshold itself. According to international jurisprudence, an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State.[42]

Two cumulative conditions must be met.[43] First, actual hostilities must take place.[44] Secondly, they must be carried out by opposing organized armed groups. When cyber warfare is part of a wider military campaign,[45] these integrated cyber operations will be assessed in relation to this campaign, which definitely eases the threshold question. The issue of a stand-alone cyber operation crossing the threshold thus triggering the applicability of LOAC is obviously more complicated given the nature of the effects generated.[46]

Targeting rules

Provided an armed conflict exists and thus LOAC applies, the second issue is whether cyber operations are constrained by the so-called targeting rules. First of all, for targeting rules to apply, cyber operations must be regarded as "hostilities" and "attacks".[47] Most rules relating to hostilities take the term "attack" as a starting point. Attacks are "acts of violence against the adversary, whether in offence or in defence".[48] The main problem is whether cyber operations can be regarded as "acts of violence".[49] The next problem is the often non-physical nature of the effects of cyber operations, and whether or not the consequences should be considered as "damage" in such a way that it affects collateral damage estimation prior to attacks.

© Flickr / 7th Army Training Command

'The main problem is whether cyber operations can be regarded as "acts of violence".'

And finally, there's the issue of the target of attacks. International lawyers still heavily rely on the tangibility of the target, the military objective. However, cyber operations most often 'target' software, applications, protocols, or data. Although these may be described as "cyber objects" by the present author, they remain non-tangible nevertheless, thereby complicating targeting decisions.

Conclusion

Cyber warfare proper is here to stay. States and international organizations such as NATO are grasping to get attuned operationally and legally. Legal efforts involve *ius ad bellum* issues on the legal basis for the decision to engage in cyber warfare, and *jus in bello* (LOAC) issues on the conduct of cyber warfare itself. Amongst other contributions, the Tallinn Manual may help States to answer some of these questions.

It is thus telling that shortly after its launch, the editor of the Tallinn Manual, Mike Schmitt, first of all raised the question "quo vadis?"[50] and immediately afterwards started on Tallinn Manual 2.0, a manual primarily dedicated to cyber operations below the thresholds of force, armed attack and armed conflict.[51] While these operations make up for the majority of activities in cyberspace, cyber warfare nevertheless is taking place.

Noten

[1]
Thomas Rid, 'Cyber War Will Not Take Place', (2012) 35 *Journal of Strategic Studies* 5.

[2]
John Stone, 'Cyber War Will Take Place!', (2012) 36 *Journal of Strategic Studies* 101.

[3]
Military.com, 'Cyber command gets first wartime assignment in fight isis (http://www.military.com/daily-news/2016/04/05/cyber-command-gets-first-wartime-assignment-in-fight-isis.html)', accessed 11 November 2016.

[4]
Michael Fallon, at The Second International Cyber Symposium (http://bit.ly/2fNxroM), RUSI, 20 October 2016, at 22'50". BBC News (http://bbc.in/2gFMcrk) (20 October 2016).

[5]
NATO, Warsaw Summit Communiqué (http://bit.ly/29wBtNW), 9 July 2016, para 70-71.

[6]
Der Spiegel Online, 'The Story of "Operation Orchard (http://bit.ly/2ggrUaW)". How Israel Destroyed Syria's Al Kibar Nuclear Reactor, 2 November 2009.

[7]
David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (Crown, 2012), pp. 188ff; and Ralph Langner, *To Kill a Centrifuge* (http://bit.ly/1dNShib) - *A Technical Analysis of What Stuxnet's Creators Tried to Achieve* (2013).

[8]

Article 2(4) of the UN Charter reads: "All Members shall refrain in their international relations from the threat or use of force […]"; and Article 51 UN Charter: "Nothing […] shall impair the inherent right of individual or collective self-defence if an armed attack occurs […]".

[9]
Michael N. Schmitt (ed.), *Tallinn manual* (https://ccdcoe.org/tallinn-manual.html) *on the international law applicable to cyber warfare : prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge University Press, 2013), p. 45, para 9.

[10]
Michael N. Schmitt (ed.), *Tallinn manual* (https://ccdcoe.org/tallinn-manual.html) *on the international law applicable to cyber warfare : prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge University Press, 2013), p. 59, para 13.

[11]
Also referred to as *ius in bello* or international humanitarian law (IHL).

[12]
Cordula Droege, 'Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians', (2012) 94 *International Review of the Red Cross* 533, p. 537, regarding the Chinese position. Also: Adam Segal, 'China, international law and cyber space', in: Council on Foreign Relations, 2 October 2012, available here (http://on.cfr.org/2gFRKlC).

[13]
Representing the position of the Tallinn Manual expert group, including the present author's view: Paul A.L. Ducheine, *'Je hoeft geen zwaard en schild te dragen om ridder te zijn' - Mythen over digitale oorlogsvoering en recht* (Oratie UvA ed, Amsterdam University Press 2016), pp. 21-22.

[14]
See: Paul A.L. Ducheine, 'The Notion of Cyber Operations in International Law', in: Nicholas Tsagourias & Russell Buchan (eds), *The Research Handbook on the International Law and Cyberspace* (Cheltenham: Edward Elgar Publishing, 2015).

[15]
On the other paradigms, see: Paul A.L. Ducheine, 'The Notion of Cyber Operations in International Law', in: Nicholas Tsagourias & Russell Buchan (eds), *The Research Handbook on the International Law and Cyberspace* (Cheltenham: Edward Elgar Publishing, 2015). Conform: Alexander Klimberg & Philipp Mirtl, 'Cyberspace and Governance—A Primer (http://bit.ly/2fltK0i)', Austrian Institute for International Affairs, accessed 11 November 2013, at p. 15, referring to these paradigms as 'mandates'.

[16]
For an illustrative summary of these operations, see: Terry D. Gill & Dieter Fleck, *The Handbook of the International Law of Military Operations* (2nd ed., Oxford University Press, 2015).

[17]
Michael N. Schmitt (ed.), *Tallinn manual on the international law applicable to cyber warfare : prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge University Press, 2013), p. 258, supplemented by the present author..

[18]
The constitutional and political procedures for this decision is not addressed here. See: Paul A.L. Ducheine & K.L. Arnold, 'Besluitvorming bij cyberoperaties', (2015) 184 *Militaire Spectator* 56 (in Dutch).

[19]
See: Paul A.L. Ducheine and others, 'Towards a Legal Framework for Military Cyber Operations', in: Paul A.L. Ducheine, Frans Osinga & J. Soeters (eds), *Cyber Warfare: Critical Perspectives* (TMC Asser Press, 2012), pp. 116ff.

[20]
For an overview of views on force within the meaning of art. 2(4) of the UN-Charter, see: Matthew Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)', (2011) 26 *Yale Journal of International Law* 421, pp. 426-430.

[21]
See *inter alia*: Paul A.L. Ducheine, *Krijgsmacht, Geweldgebruik & Terreurbestrijding; een onderzoek naar juridische aspecten van de rol van strijdkrachten bij de bestrijding van terrorisme* (Wolf Legal Publishers [diss. UvA], 2008), pp. 130-131; Jason Barkham, 'Information Warfare and International Law on the Use of Force', 34 *New York University School of Law Journal* 57, p. 71.

[22]
Davis Brown, 'A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict', (2006) 47 *Harvard International Law Journal* 187; furthermore, a criminal law approach was proposed that focuses on the genesis of a cyber attack; Graham H. Todd, 'Armed attack in cyberspace: deterring asymmetric warfare with an asymmetric definition', (2009) 64 *Air Force Law Review* 65, p. 70.

[23]
See: Paul A.L. Ducheine and others, 'Towards a Legal Framework for Military Cyber Operations', in: Paul A.L. Ducheine, Frans Osinga & J. Soeters (eds), *Cyber Warfare: Critical Perspectives* (TMC Asser Press, 2012), pp. 116ff.

[24]
Paul A.L. Ducheine & Jelle van Haaster, 'Fighting Power, Targeting and Cyber Operations', in: P. Brangetto, Markus Maybaum & Jan Stinissen (eds), *Proceedings of the 6th International Conference on Cyber Conflict (2014)* (CCDCOE, 2014).

[25]
AIV and CAVV, 'Cyber Warfare (report no. 77/22, 2011 (http://www.aiv-advice.nl))' Advisory Council on International Affairs (AIV) & Advisory Committee on Issues of Public International Law (CAVV), accessed 31 December 2012, p. 21.

[26]
Michael N. Schmitt (ed.), *Tallinn manual on the international law applicable to cyber warfare : prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge University Press, 2013), Rule 11.

[27]
Paul A.L. Ducheine, 'Military Cyber Operations', in: Terry D. Gill & Dieter Fleck (eds), *Handbook of the International Law of Military Operations* (2nd, pp. 456-475 edn, Oxford University Press, 2015), Rule 23.03, p. 465. See: Michael N. Schmitt (ed.), *Tallinn manual on the international law applicable to cyber warfare : prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge University Press, 2013), Rules 1 and 4.

[28]
On this principle in cyberspace, see: Terry D. Gill, 'Non-Intervention in the Cyber Context', in: Katharina Ziolkowski (ed.),, *Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy* (NATO CCD COE 2013).

[29]
Terry D. Gill & Paul A.L. Ducheine, 'Anticipatory Self-Defense in the Cyber Context', (2013) 89 *International Law Studies* 438.

[30]
Extensively: Terry D. Gill & Dieter Fleck (eds), *Handbook of the International Law of Military Operations* (2nd edn, Oxford University Press, 2015).

[31]
Art. 51 UN Charter. Furthermore, self-defence should be necessary, proportional, and should be reported to the UN Security Council.

[32]
See a more elaborated contribution: Paul A.L. Ducheine and others, 'Towards a Legal Framework for Military Cyber Operations', in: Paul A.L. Ducheine, Frans Osinga & J. Soeters (eds), *Cyber Warfare: Critical Perspectives* (TMC Asser Press, 2012), pp. 118ff; and: Michael N.

Schmitt (ed.), *Tallinn manual on the international law applicable to cyber warfare : prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge University Press, 2013), p. 54 ff.

[33]
Often referred to as 'pre-emptive self-defence'.

[34]
Paul A.L. Ducheine, *Krijgsmacht, Geweldgebruik & Terreurbestrijding; een onderzoek naar juridische aspecten van de rol van strijdkrachten bij de bestrijding van terrorisme* (Wolf Legal Publishers [diss. UvA], 2008), p. 221.

[35]
AIV and CAVV, 'Cyber Warfare (report no. 77/22, 2011)' Advisory Council on International Affairs (AIV) & Advisory Committee on Issues of Public International Law (CAVV), <www.aiv-advice.nl> accessed 31 December 2012, p. 21. A position that was endorsed by the Dutch Government: *Parliamentary Documents II* 2011/12, 33000 X, no. 79, reaction to AIV & CAVV's report on *Cyber Warfare*, dated 6-4-2012.

[36]
AIV and CAVV, 'Cyber Warfare (report no. 77/22, 2011)' Advisory Council on International Affairs (AIV) & Advisory Committee on Issues of Public International Law (CAVV), <www.aiv-advice.nl> accessed 31 December 2012, p. 21.

[37]
AIV and CAVV, 'Cyber Warfare (report no. 77/22, 2011)' Advisory Council on International Affairs (AIV) & Advisory Committee on Issues of Public International Law (CAVV), <www.aiv-advice.nl> accessed 31 December 2012, p. 21.

[38]
Paul A.L. Ducheine, *Krijgsmacht, Geweldgebruik & Terreurbestrijding; een onderzoek naar juridische aspecten van de rol van strijdkrachten bij de bestrijding van terrorisme* (Wolf Legal Publishers [diss. UvA], 2008), p. 570.

[39]
Apart from applicable legal regimes such as criminal law and human rights, authorities may wish to constrain the use of (cyber) force in the conduct of military operations for operational or policy reasons. They often do so through a variety of instructions described as rules of engagements (ROE), tactical directives, standard operation procedures (SOP), or via coordinating instruction in operation orders or plans.

[40]

Michael N. Schmitt (ed.), *Tallinn manual on the international law applicable to cyber warfare : prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge University Press, 2013), Rule 20, pp. 75 ff.; also: Paul A.L. Ducheine, 'Military Cyber Operations', in: Terry D. Gill & Dieter Fleck (eds), *Handbook of the International Law of Military Operations* (2nd, pp. 456-475 edn, Oxford University Press, 2015), p. 474, Rule 23.06.

[41]
Prosecutor v. Dusko Tadic a/k/a "Dule" (Decision on the defence motion for interlocutory appeal on jurisdiction) 35 (ICTY, Appeals Chamber), § 70.

[42]
Especially in the context of a non-international armed conflict. See: Paul A.L. Ducheine, *Krijgsmacht, Geweldgebruik & Terreurbestrijding; een onderzoek naar juridische aspecten van de rol van strijdkrachten bij de bestrijding van terrorisme* (Wolf Legal Publishers [diss. UvA], 2008), p. 474.

[43]
For an international armed conflict (between States): the force should exceed the threshold of minor or isolated armed incidents (AIV and CAVV, 'Cyber Warfare (report no. 77/22, 2011)' Advisory Council on International Affairs (AIV) & Advisory Committee on Issues of Public International Law (CAVV), <www.aiv-advice.nl> accessed 31 December 2012, p. 23); for non-international armed conflict this threshold is higher, see: Paul A.L. Ducheine & Eric H. Pouw, 'Controlling the Use of Force: Legal Regimes', in: Jan van der Meulen and others (eds), *Mission Uruzgan: Collaborating in multiple coalitions for Afghanistan* (Amsterdam University Press, 2012), pp. 72-73.

[44]
It is expected that cyber operations will not solely take place in cyberspace but will be part of military operations that include other dimensions as well; see: AIV and CAVV, 'Cyber Warfare (report no. 77/22, 2011)' Advisory Council on International Affairs (AIV) & Advisory Committee on Issues of Public International Law (CAVV), <www.aiv-advice.nl> accessed 31 December 2012, p. 12.

[45]
Michael N. Schmitt (ed.), *Tallinn manual on the international law applicable to cyber warfare : prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge University Press, 2013), Rule 20, pp. 75ff.

[46]
See Additional Protocol I to the Geneva Conventions, Part IV: Civilian Population - Section I General Protection against Effects of Hostilities.

[47]
Art. 49(1) Additional Protocol I to the Geneva Conventions.

[48]
Although this may appear to be the same question on the use of force (when to engage in cyber warfare) (see: the legal basis paragraph), this is a different issue on regimes applicable to warfare.

[49]
Michael N. Schmitt, 'The Law of Cyber Warfare: Quo Vadis?', (2014) 25 *Stanford Law and Policy Review* 269.

[50]
See this (http://bit.ly/1MlThp8) and this (http://bit.ly/2ggwqGb).

Auteurs

Paul Ducheine
Professor for Cyber Operations and Cyber Warfare at the NLDA and professor at the UvA ▸
(http://www.uva.nl/over-de-uva/organisatie/medewerkers/content/d/u/p.a.l.ducheine/p.a.l.ducheine.html)