publicaties/rapporten/2010/01/12/rapport-commissie-davids/rapport-commissie-irak.pdf. See also: Joost Oranje, "Acht vragen over onderzoek naar steun Irak-oorlog (Eight questions about inquiry into support for the Iraq war)", *NRC Handelsblad* (New Rotterdam Courier Trades' Paper, a Dutch quality newspaper), 3 February 2009.

NB: do you have any comments on Bas Wallage *et al.*'s article? Please send these to info@ethnogeopolitics.org, or through the contact form at http://www.ethnogeopolitics.org.

Criticism of the paper's definition and framework of 'digital weapons of mass destruction'

(Critical Response to Bas Wallage *et al.*'s "Non-proliferation of cyber weapons with a CBRN consequence")

My first and foremost concern is the use of the term "cyber weapons of mass destruction". It would be more logical to address cyber weapons as such; and in this specific case, to address the use of cyber weapons against CBRN weapons/systems/facilities/etcetera, rather than to address "cyber weapons of mass destruction". The latter term does not exist in international law and other international sources; and I believe it is the result of a confusion in the article about the various ways to categorise weapons.

The two main approaches to categorise weapons are: the intended use (purpose) of a weapon; and the effects of a weapon. The approaches are, however, not mutually exclusive. For certain weapons the differences between their intended use (purpose) and effects remain ambiguous and contextual—for example white phosphor, which can be used legally for the purpose of creating a smokescreen as an operational cover for combatants; but it can also be used illegally as an incendiary weapon against non-combatants and other persons.

Such dilemmas, however, do not yet arise with cyber weapons. Here the questions are much more basic, and thereby, also more fundamental. What characterises cyber weapons is that they operate within the cyber environment and they can produce effects in the (i) digital and (ii) physical world.

(i) With respect to effects in the digital world, there is a legal/philosophical discussion about what amounts to an attack, within the legal meaning, if this takes place entirely within the digital environment.

(ii) With respect to effects in the physical world, there are many discussions, and one of them concerns the use of such tools to disrupt our environment.

In the latter hypothetical situation, these cyber weapons are sometimes called weapons of mass *disruption* and it is in that situation that there is serious concern about the implications

of the use of these weapons against CBRN facilities, equipment, devices, materials, etcetera. This creates an entire new dimension of insecurity.

It is clear, however, that cyber weapons are not per definition CBRN weapons since they do not produce CBRN effects on their own (such a broad interpretation could lead to a similar logic that TNT, and practically any other explosive, is in essence a chemical weapon because of the use of chemicals to produce an explosion; such broad way of interpreting the nature and effects of a weapon would clearly not be supported by most States).

With respect to international law, the Article 36 of the Additional Protocol (I) to the Geneva Conventions does not per definition limit cyber weapons. It establishes an obligation for States Parties to review the legality of the weapons (and means and methods of warfare) that States Parties acquire or adopt. Since it leaves discretion to States Parties, and in the absence of any multilateral treaty restricting cyber weapons, it remains premature to state anything definitive on the legality of cyber weapons. Furthermore, the relevance of the Nuclear Non-Proliferation Treaty is not clear and in fact highly doubtful; especially when considering the problems, if not impossibility, of qualifying a cyber weapon as a nuclear weapon.

Finally the article describes, as in the media, the Stuxnet "attack" against Iran. While in the ordinary daily meaning this description may resonate with people's imagination, within the legal context there is serious doubt whether the Stuxnet event can be qualified as an "attack". This is for the reason that the term attack in international law has specific meanings, both within the context of collective security law (*jus ad bellum*) and the law of armed conflict (*jus in bello*); and that these meanings are definitely much more restrictive than the broad meaning used by media.

- Anonymous

Editorial Note

The current published version of the article in question has incorporated most of the practical suggestions and textual improvements offered by the anonymous peer review (these are not shown in the latter's published version, the Critical Response). However, the authors have decided to maintain their article's conceptual approach and framework.

The Editorial Board has decided to publish the article despite the reviewer's farreaching criticism, as we consider it of sufficient quality and interest to the reader. This decision was helped by the fact that the authors have consulted several senior scholars for their paper.

Naturally, we welcome additional reviews on this paper that can be published as Critical Responses in a future issue of our journal, with a Reply from the authors if they wish so.

- Caspar ten Dam, Executive Editor