An interview with Dr. Martin C. Libicki (*RAND Corporation*)

by Daniel Ventre[1] (*CNRS; Chair in Cyberdefense and Cybersecurity - Ecoles de Saint-Cyr Coëtquidan / Sogeti / Thales*)

February 20, 2013 – Article n°III.1

Daniel Ventre: Although several definitions of "cyberspace" and "cyberwar" have been proposed (among militaries, governments, researchers…), there is no consensus on the definition of this object/concept. What is your own definition of "cyberspace" and "cyberwar"?

Martin Libicki: Cyberwar should be the use of cyberwarfare (that is, techniques used to usurp the control of computers from their authorized users), in pursuit of politico-military aims (i.e., something that Clausewitz would recognize). Cyberspace is something that I define like this: it's the Internet and everything connected to the Internet that is like the Internet. That's more than a little fuzzy, to be sure. More to the point, I don't believe there's much point to defining cyberspace, in large part because it's just a conduit to what is more interesting: the systems being hacked. The emphasis on cyberspace as such is like saying that traffic accidents happen in road-space, or that poison-pen campaigns happen in mail-space.

DV: If we agree that cyberspace is a new domain, what is a « frontier » / « borderline » in it ? Is it really necessary for nation-states to set up virtual frontiers? Is such a project feasible?

ML: The frontier of cyberspace is basically the first router that inbound traffic hits in the country (or the last router that outbound traffic hits); where the wires go is irrelevant. That formulation does not work if the Internet goes directly from an external source (satellite, RF transmissions) to end-consumers, but that's a very small share of Internet traffic. States can apply border controls there (it's feasible, China does it), but the first question in a democratic state is what a state gains by doing so (given that interference with the Internet is unpopular in some quarters and not costless).

DV: According to you, what is the most appropriate approach to analyze/explain/understand cyberconflict (ie. its impact on international relations, the origins of cyberwars, etc.): a constructivist approach, a (neo) realist or neoliberal perspective?

ML: This is probably as good a time as any to note that I was trained in economics, not international relations theory (and so I'm not so qualified to differentiate these terms). But maybe the place to start is with "cyberconflict," whose meaning I'm unsure of. We really haven't seen a true cyberwar. If cyberconflict means a difference of opinion among states, we have seen tussles about cyberspace in the latest ITU meeting in Dubai. The West told the ITU: hands off. The other big countries wanted the ITU to support a state's right to manipulate its citizens' access to the Internet. Was the West realist (Western media and the values it projects tend to be more popular with non-Western citizens than the reverse) or idealist (the West believes in its values and wants them propagated)? Hard to tell.

DV: What are the main conceptual differences between the 1990s' "information warfare" and today's "cyberwar"?

ML: Information warfare of the 1990s was a catch-all that included what we now call cyberwarfare but also psychological warfare, command-and-control warfare, and electronic warfare. It also could also include operational security (OPSEC) and military deception (MILDEP). The overall term evolved to "information operations" *circa* 1997, but that term is mostly used for psychological warfare and strategic communications today.

DV: Efforts to conceptualize cyberconflict refer to 'Cold war' and 'war on terror' strategies, policies, concepts (cyber Cold War; cyber deterrence; invisible threat; insider threat; …). What is the most appropriate analogy to analyse cyberconflict: Cold war or War on terror?

ML: Neither, really. The high-tech nature of cyber suggests the Cold War; the lone-wolf potential of cyber suggests the war on terrorism. But neither is a good fit, and, in both cases, for at least one common reason – cyberwar does not really inspire terror (as nuclear weapons do and terrorism aims to). So far cyberwar has been used for annoyance (Estonia, Georgia), as an aid to military operations (Operation Orchard), and for sabotage (Stuxnet). Note that nuclear weapons have been used for none of them; and terrorism is rarely used for sabotage, as such. I don't think we have much choice but to consider cyberwar on its own merits (although some of the questions from the Cold War such as escalation, signalling, confidence-building measures etc. are potentially interesting to place in a cyber context).