An interview with Prof. Alan Chong (RSIS – S. Rajaratnam School of International Studies - Singapore)

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

May 2013 – Article n°III.2

Alan Chong is Associate Professor at the S. Rajaratnam School of International Studies in Singapore. He has published widely on the notion of soft power and the role of ideas in constructing the international relations of Singapore and Asia. His publications have appeared in The Pacific Review; International Relations of the Asia-Pacific; Asian Survey; East Asia: an International Quarterly; Politics, Religion and Ideology; the Review of International Studies; Alternatives: Global, Local, Political; and the Cambridge Review of International Affairs. He is also the author of Foreign Policy in Global Information Space: Actualizing Soft Power (Palgrave, 2007). He is currently working on several projects exploring the notion of 'Asian international theory'. More information at: http://www.rsis.edu.sg/grad/faculty-members.htm

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"?

Alan Chong: Cyberspace refers to that communication space created between two or more connected digital sources. In political terms, it is a space parallel to terrestrial space. Unlike terrestrial space on earth, 'asymmetries' in cyberspace are less tangible and do not depend on the possession of natural resources, wide plains and rivers. What matters as strength in cyberspace is the possession and allocation of human talent. Cyberwar would logically refer to military-inspired attempts to disrupt, deny or destroy the electronic resources of the enemy through computer-based means with the aim of attaining military victory.
I would personally prefer the term 'information operations' to refer to that whole range of political interventions ranging from the theft of data, deception, disruption, to destruction enabled by electronic computer-based means. Information operations do not distinguish peacetime from wartime.

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?

AC: Definitely, a constructivist approach. The operational architecture of cyberspace requires the interaction between the 'structure' of electronic pathways and websites connected by multiple nodes, and numerous 'agents' in terms of terminals and operators. The design of malware and its corresponding 'anti-virus' software require agency-structure co-constitution of anticipated identities and lethalities.
On a conflict scenario level, waging cyberconflict requires the initiator to imagine the enemy's pre-existing vulnerabilities and planned reactions. The initiator must employ this knowledge in order to retain plausible deniability when challenged in the open media.

DV: How might be described the main conceptual differences between the 1990s' "information warfare" and today's "cyberwar"?

AC: The notion of 'information warfare' is more accurate, comprehensive, and more flexible than cyberwar, since information warfare includes psychological operations and simple deception strategies. The latter two can also be operated through computerised means. In any case, I would prefer the phrase 'information operations' to encompass the widest possible range of strategic operations within, or associated with, computer usage.

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?

AC: The War on Terror is more appropriate as a test case since it involves a whole array of non-state actors who act autonomously from sovereign states. Ideological considerations also factor in the cyber intentions of non-state actors. Using computer terminals, non-state actors can level the global playing field in relation to sovereign states. The Cold War was a largely sovereign state-to-state confrontation.

DV: How is the Singaporean approach of cybersecurity strategies differing from other nations?

AC: As far is it is revealed, the Singaporean cybersecurity approach is based on mostly civilian 'whole of government/society' principles. Secondly, the Singaporean approach is also based upon open information sharing at cyber conferences between civilian companies and government agencies. There is also a great deal of information learning between software firms at home and abroad.

DV: Your research expertise is focused on "soft power" concept. Could you please remind us the definition of this concept and its application in cybersecurity policies/strategies?

AC: Cybersecurity is connected to soft power in the sense that open information sharing on keeping the internet open, stable and dependable for global electronic commerce translates into a form of attracting a 'noble', 'good practices' community of experts and ordinary computer users into existence. This 'good practice' community is transnational and will hopefully transcend nationally-derived political obstacles.

Bibliography:

- Alan Chong, *Foreign Policy in Global Information Space: Actualizing Soft Power,* New York: Palgrave Macmillan, 2007
- Alan Chong, *Singapore's Encounter with Information Warfare: Filtering Electronic Globalization and Military Enhancements*, pp.223-250, in Daniel Ventre (Edit.), *Cyber Conflict. Competing National Perspectives*, Wiley-ISTE, 2012, 352 pages
- Alan Chong, Nah Liang Tuang, *Framing Cyber Warfare: Between Offence and Defence*, 28 juin 2011, RSIS Commentaries, n°95/2011 http://www.rsis.edu.sg/publications/Perspective/RSIS0952011.pdf

Webpage:

- http://www.rsis.edu.sg/about_rsis/staff_profiles/alan%20chong.htm