Conjuntura Austral

RESENHA

Bookreview

CYBER CONFLICT: COMPETING NATIONAL PERSPECTIVES[1]

Thiago Correa Malafaia[2]

How cybernetic constraints and considerations may potentially re-shape modern conflict is a pressing issue nowadays in many countries political agendas. If on the one hand more technology is being inserted in military forces, on the other this increased reliance on electronic interfaces only makes so that these forces be even more exposed to outside tempering in the form of actions specially targeting neuralgic systems to a country's civil/security apparatus.

There is extensive record of occurrences, some highly publicized, others not so much. Anyhow, this electronic "realm" of activity is bound to have lasting and stark effects on how war and conflict is going to be conducted in the near future. That is exactly the theme of Ventre's edited book. He and the various authors therein draw a reasonable picture about the state of readiness some countries have as to cyber matters. They assess nine case studies (Canada, Cuba, France, Greece, Italy, Japan, Singapore, Slovenia and South Africa) to show that each country responds to cyber menaces differently and that regional environments exert powerful influence, orienting, thusly, individual security postures when it comes to cyber issues.

The purpose of the book is to show how mostly non-centric countries, in terms of global security matters, behave as to the topic. It is evident, however, that one cannot comprehend the full picture without referring back to American, Chinese and Russian

[1] VENTRE, Daniel (eds.). Cyber Conflict: Competing National Perspectives; ISTE Ltd. and John Wiley & Sons, Inc.; UK & USA; 2012. ISBN: 978-1-84821-350-0.

[2] Mestre em Relações Internacionais (PUC-Minas); Doutorando em Relações Internacionais (PUC-Minas); Bolsista CAPES. (thiagomalafaia@hotmail.com).

actions and policies basically for these are the most active countries when it comes to this issue.

Countries' actions aside, the book also advances definitions for cyberspace and cyber-attacks, which are useful for their non-ambiguity. A cyberspace is a dimension encompassing the total of human activity, including combat. It is transversal to all other four dimensions: air, land, sea and space. However, it also has three layers to it: 1) that of physical infrastructure/hardware; 2) that of software/applications; and 3) that of cognition, affecting more directly the interface man-machine, or rather and bluntly put, the way man reacts to "inputs" delivered by machine (mal)functioning. Each of these layers is associated to a different type of action: the first, to netwar; the second, to cyberwar; and the third, to electronic warfare. Thus, cyberspace becomes a (virtual) medium through which attacks coming from one end of the "real" world can reach another of its "ends". This is exactly the definition of cyber-attack put forth by the authors — to use a virtual means to produce deleterious effects elsewhere in the "real" world.

Even though the authors disregard the main actors as to this particular global security issue, China, Russia, and the United States, which they agree, would complicate the analysis, the book brings powerful insights as to where global security matters are likely to be heading in the years to come. The book might be of interest to students and practioners of IR and Political Science alike.

Recebida dia 06 de janeiro de 2015. Aprovada em 23 de abril de 2015.