

Business and social evaluation of denial of service attacks in view of scaling economic counter-measures

L-F Pau, Prof. Mobile business Copenhagen business school, and Rotterdam school of management lfp.inf@cbs.dk

ABSTRACT

This work in progress aims at addressing two strategic aspects of cyber-warfare via communications networks and IT applications: a) first to take a total economic and social view in the assessment of evaluating damages of a cyber-warfare attacks on a society or business target; b) scaling a trade, economic, or legal retaliation or dissuasion for decision makers. It is assumed that the target of the attack does not have itself any or sufficient defence or attack means, so that a corporate or national level may decide ex-ante (dissuasion) or ex-post (retaliation, compensation) to scale a business defence affecting the economic sphere of the attacker. Such an approach is also relevant sometimes when attacker cannot be identified and localized precisely, so that the economic sphere of the attacker is restricted to business networks to which the attacker belongs.

Traditionally the damage assessment has been considered “binary” and limited in time, in that the target was considered to be rendered totally dysfunctional until full restoration only of its information and communication capabilities. Lessons learnt tell us that other organizational, physical, human and social capabilities are to be counted as often larger collateral damage of the attacks and their restoration eventually takes quite some time, especially if the surrounding society does not have enough civil defence means in place. Vice-versa, sometimes, the replacements made to infrastructure damaged by the attack will be less obsolete leading to better future robustness. To address this issue, the approach is capitalize on the ability of cost-benefit analysis to bundle into the internal rate of return both tangible and some intangible effects. The internal rate of return expresses the time preference on tangible and intangible assets, old and new, which gives a break even net present value over the long term. It is then proposed to treat short term dynamics of this internal rate of return, when exposed to a Brownian shock linked to an attack affecting the command and control node for the society or business target which have their normal long term equilibrium return rates.

Knowing the dynamic time preference resulting from a cyber-attack, it becomes possible to estimate all of the following :a) the incremental monetary mass needed short term for restoration of equilibrium business and social capabilities; b) long term investment over a given pay-back horizon needed long term to restore and improve capabilities to get back to the equilibrium rate c) the value of the assets degraded by the cyber-attack as short term and long term restoration measures impact the target.

Apart from relevance in a national or corporate budgeting process, such a three-dimensional scaling of compensation, retaliation or dissuasion gives decision makers a way to communicate efficiently around them and to implement such counter measures against the attacker’s economic sphere while referring eventually to a game theoretical equilibrium required by legal/treaty provisions.

As a conclusion, the proposed methodology empowers decision makers to scale eventual economic counter-measures or threats against attackers, the efficiency of which cannot be guaranteed as economic-social effects may not always impact attackers but surely their surroundings, and as the resolution of decision makers may also vary. It will be up to the reader to assess relevance in her/his own context, while this project has assessed some concrete cases. This project has also been motivated by specific concerns and abilities of wireless communications operators.