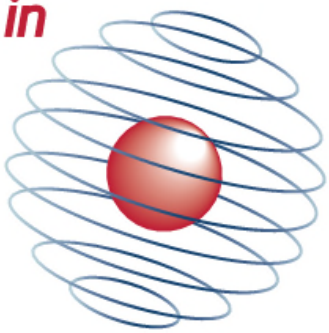
CENTRE *for* DOCTORAL TRAINING *in*
CYBER SECURITY



CDT Technical Paper

02/17

Unfair competition in the information environment. DDoS attacks

Oleh Stupak

Unfair competition in the information environment. DDoS attacks

Oleh Stupak

September 10, 2017

1 Introduction

The purpose of this paper is the investigation of issues related to modern competition. It focuses on the situation in which two firms (players) are competing on the market for higher profits using unfair methods of competition. Particularly, the paper focuses on a specific type of cyber-attack that is being adopted on the multiple markets: distributed denial-of-service attack (McDowell, 2009). The particular attack has been chosen due to its simplicity, effectiveness (including cost effectiveness) and prevalence around the world (as a consequence)(IBM Security, 2015). Technical details of the attack will not be discussed in the paper; the attack itself will be mostly referred as 'cyber-attack'.

The presented framework has a game theoretic nature and could be considered as a good starting point for an economic analysis of the issue.

Aggression in the information environment is proven to be an effective method of obtaining a competitive advantage. Cyber-attacks influence on market price, firms profits, consumer benefits and overall aggressive market performance is discussed and compared to identical peaceful market indicators. Methods of aggressive market regulations are also discussed in the paper.

The structure of the paper is as follows: Section 2 presents background and setting information. Section 3 provides equilibrium estimations. Deviation tests results provided in Section 4. Section 5 presents the comparative analysis of different market environments. Method of aggressive market regulation presented in Section 6. Finally, Section 7 concludes.

2 Setting and background

2.1 Basic information and definitions

The paper assumes that there are only two identical firms (players) in the industry that are competing for profits by independently choosing the amount of output they will produce and sell. It is assumed that major share of sales in the industry have been done online (using e-commerce technologies). Consequently, the possible amount of output that could be chosen by the player depends on the information environment of the industry. The maximum output that could be sold by the enterprise is restricted by server capacity.

Definition 1. Server capacity quantity of sales that could be processed by the server.

Players do not hesitate using instruments of unfair competition. Each player chooses the amount of investment that she is ready to devote to the DDoS-type cyber attack.

Definition 2. Cyber-attack offensive instrument that enterprises use to reduce the capacity of the opponent. This paper implies DDoS-type attacks.

The framework of the model is similar to classical Cournot model with a few modifications done [ref]. The models share the following assumptions[ref]:

- There is more than one firm on the market;
- The number of players is fixed. The presented model has only two players: Player 1 and Player 2;
- All firms (players) produce and sell a homogeneous product, i.e. there is no product differentiation;
- Firms do not cooperate;
- Firms have market power, i.e. their decisions influence the market price;
- Firms compete in quantities (output quantity, cyber-attack investment, server capacity investment), and choose respected quantities simultaneously;
- Firms are economically rational and act strategically, always maximising their profit given competitors' decisions.

2.2 Time frame

Period 0 initial period; enterprises choose the optimal server capacity by choosing k_i;

Period 1 intermediate period; enterprises choose the optimal Cyber-attack power by choosing a_i;

Period 2 final period; enterprises choose the optimal output level based on the knowledge from previous periods.

The model is solved using the backward induction method. The model is considered from the end to determine the sequence of optimal actions for each player (Adda Cooper, 2003).

For the sake of simplicity, this paper discusses only two latter periods: *Period 1* and *Period 2*. The initial *Period 0* will be discussed in the future research.

2.3 Costs

The model assumes that marginal costs in the final period are equal to zero. Production costs are not of the interest for the paper. The assumption that online sales costs are also equal to zero reasonably realistic (ignoring, of course, marketing costs).

$$MC = 0$$

However, firms bear costs of purchasing the capacity and cyber-attack costs. However, server capacity costs will not be discussed in this paper.

For the sake of simplicity, the paper proposes quadratic cost function of the cyber-attack:

$$c(a_i) = a_i^2 c_a$$

Where:
a_i - cyber-attack strength chosen by the firm; the amount on which opponent's capacity will be reduced;
c_a - marginal DDoS-type cyber-attack costs.

2.4 Inverse demand function

In order to construct players' profit functions, model introduces classical inverse demand function. The function maps the quantity of the demanded output (independent variable in this case) to the market price (dependent variable). The inverse demand function could be represented as follows:

$$P = d - bQ$$

Where:
P - price of the good;
d - intercept where price is 0; it represents all other (than price) factors affecting the price (e.g. policy restrictions, households income);
b - slope of the demand curve;
Q - overall demand quantity. The paper assumes that whole demand is satisfied by the firms, i.e. $Q = q_i + q_j$, where q_i and q_j - quantities chosen by *Firm 1* and *Firm 2* respectively.

For the sake of simplicity, the paper assumes that model external coefficients d and b are equal to 1. Their properties will be studied further in the paper.

2.5 Constructing profit functions

The paper considers three separate cases:

2.5.1 Case 1

Symmetric case in which constraints created by the cyber-attacks are not binding. It means that cyber-attacks are not powerful enough to reduce server capacities below the quantity demand. It could be represented by the following expressions:

$$k_i - a_j > q_i$$

$$k_j - a_i > q_j$$

These conditions bring us to the normal Cournot duopoly case, where optimal quantities can be estimated. It is sufficient to estimate quantities only in the final period. The estimation will be presented further in the paper.

2.5.2 Case 2

Symmetric case in which constraints created by the cyber-attacks are binding. It means that cyber-attacks performed by enterprises are powerful enough to cause server capacities to drop below the quantity demand level. The case conditions could be represented by the following expressions:

$$k_i - a_j < q_i$$

$$k_j - a_i < q_j$$

This case relies on decisions that firm makes through the entire game. Estimations for the *Period 2* and *Period 1* of the case will be presented in the next section.

2.5.3 Case 3

The paper suggests that considering only symmetric cases is not enough. The asymmetric case in which only one of the firm does not hesitate to use unfair methods of competition, whereas the second firm remains within the legal field. This suggests that only one firm has binding constraint. It could be represented as follows:

$$k_i - a_j < q_i$$

$$k_j - a_i > q_j$$

These conditions allow the second player to choose the optimal output in the final period. Estimations for the constrained player will also be presented later in the paper. It is also interesting to discuss the case from the perspective of non-constrained foe-player.

3 Equilibrium derivations

In this section, every case will be solved for equilibrium and discussed separately.

3.1 Case 1

As described above, the first case assumes that cyber-attacks performed by firms are not strong enough to restrict opponents server capacity. Therefore, it becomes irrational to invest any resources in the cyber-offensive actions, therefore: $a_i = 0$ and $a_j = 0$. It is rational for companies to purchase the server capacity that exactly matches the quantity demand. The case could be considered and solved as a classic Cournot case with zero marginal costs. It is sufficient to solve the case only in the final (second) final period to derive and estimate optimal quantities. Inverse demand function for the case is presented below:

$$P^1 = d - b(q_i^1 + q_j^1)$$

Assuming that $MC^1 = 0$, *Firm's 1* profit function could be represented by the equation:

$$\Pi_i^1 = P^1 q_i^1 = (d - bq_i^1 - bq_j^1)q_i^1$$

As the case is symmetric, *Firm's 2* function will be similar.

Corresponding *Firm's 1* profit maximization problem:

$$\max_{q_i^1} \Pi_i^1 = (d - bq_i^1 - bq_j^1)q_i^1$$

Derivation of first order condition (FOC):

$$\frac{\partial \Pi_i^1}{\partial q_i^1} = 1 - 2q_i^1 - q_j^1 = 0$$

Solving FOC for q_i gives reaction function[1] of *Firm 1*:

$$q_i^1 = \frac{1 - q_j^1}{2}$$

Solving similar profit maximisation problem for the second player gives a system of reaction functions of two firms:

$$q_i^1 = \frac{1 - q_j^1}{2}$$

$$q_j^1 = \frac{1 - q_i^1}{2}$$

It is now possible to present the solution of the symmetric equilibrium:

$$q_i^{1*} = q_j^{1*} = \frac{1}{3}$$

Optimal market price for the case:

$$P^1 = \frac{1}{3}$$

Equilibrium profits:

$$\Pi_i^1 = \Pi_j^1 = \frac{1}{9}$$

3.2 Case 2

Assuming cyber-attacks are now powerful enough to reduce competitiors' servers capacity below the optimal quantity demand, it is rational to suggest that companies will produce (sell online) as many goods as it is possible within constraints. The suggestion yields the following quantities for the case:

[1]Reaction function - the function specifying the choice of a strategic variable by one economic agent as a function of the choice of another agent (Giocoli, 2011)

$$q_i^2 = k_i^2 - a_j^2$$

$$q_j^2 = k_j^2 - a_i^2$$

Therefore, the inverse demand function in the second case takes the following form:

$$P^2 = d - b(k_i^2 - a_j^2 + k_j^2 - a_i^2)$$

Firm's 1 equilibrium profit function in the final period:

$$\Pi_i^1 = (d - b(k_i^2 - a_j^2 + k_j^2 - a_i^2))(k_i^2 - a_j^2)$$

To obtain a proper solution for the case, equilibrium should also be estimated in periods 1 (to evaluate the optimal cyber-attack function) and period 0 (to evaluate server capacity). For the sake of simplicity as it is mentioned before, the paper considers only period 2 and period 1, leaving the initial period 0 for future research. In this case, server capacity is assumed to be an external variable.

To evaluate optimal cyber-attack functions, it is necessary to derive a specific profit function for the intermediate period. It could be done by subtracting presented above quadratic cyber-attack price function from the final period equilibrium price functions:

$$\Pi_i^1 = (d - b(k_i^2 - a_j^2 + k_j^2 - a_i^2))(k_i^2 - a_j^2) - (a_i^2)^2 c_a$$

Corresponding profit maximisation problem for the intermediate period:

$$\max_{a_i^2} \Pi_i^2 = (d - b(k_i^2 - a_j^2 + k_j^2 - a_i^2))(k_i^2 - a_j^2) - (a_i^2)^2 c_a$$

FOC:

$$\frac{\partial \Pi_i^2}{\partial a_i^2} = -2a_i^2 - a_j^2 + k_i^2 = 0$$

Solving for a_i provides a cyber-attack reaction curve for Firm 1:

$$a_i^2 = \frac{1}{2}(-a_j^2 + k_i^2)$$

As the second case is also symmetric, *Firm's 2* cyber-attack reaction function is similar. Combining reaction function yields the system:

$$a_i^2 = \frac{1}{2}(-a_j^2 + k_i^2)$$

$$a_j^2 = \frac{1}{2}(-a_i^2 + k_j^2)$$

The solution of symmetric equilibrium for intermediate period of the second case now could be derived:

$$a_i^{2*} = \frac{1}{3}(2k_i^2 - k_j^2)$$

$$a_j^{2*} = \frac{1}{3}(-k_i^2 + 2k_j^2)$$

Substituting cyber-attack functions for its equilibrium values yields the following market price function:

$$P^2 = \frac{1}{3}(3 - 2k_i^2 - 2k_j^2)$$

Equilibrium profit functions for the second case could be represented as follows:

$$\Pi_i^2 = -\frac{2}{9}(2k_i^2 - k_j^2)(-3 + 2k_i^2 + 2k_j^2)$$

$$\Pi_j^2 = -\frac{2}{9}(2k_j^2 - k_i^2)(-3 + 2k_j^2 + 2k_i^2)$$

3.3 Case 3

The paper now assumes that only one of the firms is capable of powerful enough cyber-attack. The situation could be considered from two perspectives:

- One firm respects law and stays in the legal field, while its competitor is a foe and does not hesitate to use cyber-offensive tools;
- Both firms do not hesitate to use cyber-offensive tools, but only one of them poses an appropriate resource to perform strong enough cyber-attack. In this situation, it is rational for the backward company not to perform a cyber-attack at all.

Situations described are considered equal, and there will be no difference between them in the mathematical representation.

In this case, the non-constrained player will just choose the optimal quantity of the output to produce and sell in the last period.

We assume that *Firm 1* is constrained, and *Firm 2* is not. It yields the following optimal quantity of *Firm 1* in the final period:

$$q_i^3 = k_i^3 - a_j^3$$

Inverse demand function in Case 3 takes the following form:

$$P^3 = d - b(k_i^3 - a_j^3 + q_j^3)$$

It yields the following profit functions in the final period:

$$\Pi_i^3 = (d - b(k_i^3 - a_j^3 + q_j^3))(k_i^3 - a_j^3)$$

$$\Pi_j^3 = (d - b(k_i^3 - a_j^3 + q_j^3))q_j^3$$

The optimal value of foe-player's quantity could be estimated by solving the following maximisation problem:

$$\max_{q_j^3} \Pi_j^3 = (d - b(k_i^3 - a_j^3 + q_j^3))q_j^3$$

FOC:

$$\frac{\partial \Pi_j^3}{\partial q_j^3} = 1 + a_j^3 - k_i^3 - 2q_j^3 = 0$$

Solution for q_j^3 yields:

$$q_j^{3*} = \frac{1}{2}(1 + a_j^3 - k_i^3)$$

Inverse demand function becomes:

$$P^3 = 1 + a_j^3 - k_i^3 + \frac{1}{2}(-1 - a_j^3 + k_i^3)$$

Firm's 1 optimal profit function in the final period becomes:

$$\Pi_i^3 = (-a_j^3 + k_i^3)(1 + a_j^3 - k_i^3 + \frac{1}{2}(-1 - a_j^3 + k_i^3))$$

It is now possible to move backwards to the first period and derive intermediate profit functions for both players:

$$\Pi_i^3 = (-a_j^3 + k_i^3)(1 + a_j^3 - k_i^3 + \frac{1}{2}(-1 - a_j^3 + k_i^3)) - (a_i^3)^2 c_a$$

$$\Pi_j^3 = \frac{1}{2}(1 + a_j^3 - k_i^3)(1 + a_j^3 - k_i^3 + \frac{1}{2}(-1 - a_j^3 + k_i^3)) - (a_j^3)^2 c_a$$

Similarly to the previous cases, corresponding profit maximisation problems should be presented. However, for the third case maximisation problems are not symmetric and should be solved separately.

Maximisation problem of constrained firm:

$$\max_{a_i^3} \Pi_i^3 = (-a_j^3 + k_i^3)(1 + a_j^3 - k_i^3 + \frac{1}{2}(-1 - a_j^3 + k_i^3)) - (a_i^3)^2 c_a$$

Constrained firm's FOC:

$$\frac{\partial \Pi_i^3}{\partial a_i^3} = -2a_i^3 = 0$$

Maximisation problem of non-constrained firm:

$$\max_{a_j^3} \Pi_j^3 = \frac{1}{2}(1 + a_j^3 - k_i^3)(1 + a_j^3 - k_i^3 + \frac{1}{2}(-1 - a_j^3 + k_i^3)) - (a_j^3)^2 c_a$$

Non-constrained firm's FOC:

$$\frac{\partial \Pi_j^3}{\partial a_j^3} = -2a_j^3 + \frac{1}{4}(1 + a_j^3 - k_i^3) + \frac{1}{2}(1 + a_j^3 - k_i^3 + \frac{1}{2}(-1 - a_j^3 + k_i^3)) = 0$$

Solving FOCs yields the following system of cyber-attack reaction functions:

$$a_i^3 = 0$$

$$a_j^3 = \frac{1 - k_i^3}{3}$$

Substituting cyber-attack functions for its equilibrium values yields the following market price function:

$$P^3 = -\frac{2}{3}(-1 + k_i^3)$$

Consequently, equilibrium profit functions become:

$$\Pi_i^3 = -\frac{2}{9}(-1 + k_i^3)(-1 + 4k_i^3)$$

$$\Pi_j^3 = \frac{4}{9}(-1 + k_i^3)^2$$

4 Deviations

In this section, the paper presents results of the deviation tests. Having profit functions derived for every particular case, it is now necessary to check for conditions, which keep players in certain equilibrium (in certain case). Deviation check procedure itself will not be presented in the paper.

Another necessary assumption done in the paper is that it considers only equilibriums in pure strategies. The assumption has been made for the sake of simplicity. It means that both players will choose equal server capacities: $k_i = k_j$ Mixed strategies will be discussed in the future research.

Deviation tests yield the following results:

$k_{i/j} < \frac{1}{2} \rightarrow$ **Case 2**

$\frac{1}{2} < k_{i/j} < \frac{3}{2} \rightarrow$ **Case 1**

$\frac{3}{2} < k_{i/j} \rightarrow$ **Case 3**

To conclude, case allocation directly depends on server capacities decisions.

5 Comparative analysis

In this section, the paper presents a comparative analysis of the cases. Inverse demand (price) functions, profit functions, consumer surplus and total surplus, will be compared assuming all conditions being equal.

For now, the paper sticks to the assumption that all external model coefficients are equal to 1: $d = b = c_a = 1$

The Nash equilibrium solution for the Case 1 (classical Cournot case) presented above - firms will choose server capacities equal to the optimal quantity:

$$k_i = k_j = q_i = q_j$$

Assuming all things being equal, the paper uses presented equilibrium server capacity of the first case for a numerical comparison.

5.1 Price

As presented above, the equilibrium price value for the case with peaceful information environment is:

$$P^1 = \frac{1}{3}$$

Inserting server quantities to the price functions of the case 2 and case 3, we obtain:

$$P^2 = \frac{5}{9}$$

$$P^3 = \frac{4}{9}$$

Obviously, the presence of restricting cyber-attacks on the market drives the price up:

$$P^1 < P^3 < P^2$$

This could be explained by the fact that constraining cyber-attacks have a direct influence on the available to sell quantities of the firms. It is capable of creating a deficit, which, in turn, drives price upwards.

5.2 Profits

Case 1 profit functions have been presented previously in the paper. It takes the following equilibrium value:

$$\Pi_i^1 = \Pi_j^1 = \frac{1}{9}$$

By inserting $k_i = k_j = \frac{1}{3}$ to Case 2 profit functions we get:

$$\Pi_i^2 = \Pi_j^2 = \frac{10}{81}$$

As Case 3 is asymmetric in the cyber-attack decision making, obviously, it produces two different profit functions:

- Peaceful firm profit function: $\Pi_i^3 = \frac{4}{81}$
- Aggressive firm profit function: $\Pi_j^3 = \frac{16}{81}$

It is now possible to compare equilibrium profits of the players assuming all thing being equal:

$$\Pi_i^3 < \Pi_i^1 < \Pi_i^2 < \Pi_j^3$$

We observe that the smallest profit will be obtained by the peaceful company in the aggressive environment. Contrary, foe-company from the same Case (Case 3) will obtain the highest profits in all cases. Cyber-attack gives an uncontested competitive advantage to a foe player. Playing peaceful in

the aggressive cyber environment seems unreasonable (at least, while some regulations have not been presented to the market); the peaceful player is not competitive in Case 3 setting.

Interestingly, Case 2 profit functions achieve higher values than functions of the Classical Cournot case. To conclude, cyber-aggressive environment is capable of triggering competitive dynamics and drive players profits up. Presence of offensive instruments on the market could have a positive effect on companies' profits. However, it is also obvious that asymmetric usage of the attacks brings strong disbalance to the market, which is, potentially, could lead to market monopolisation.

5.3 Consumer surplus

To measure consumer benefits for each case, consumer surplus (CS) should be presented. Consumer surplus could be described as a difference between the maximum price a consumer is willing to pay and the market price (actual price) they do pay.

It is estimated as an area of a triangle under the quantity demand which is above the market price. See graph below.

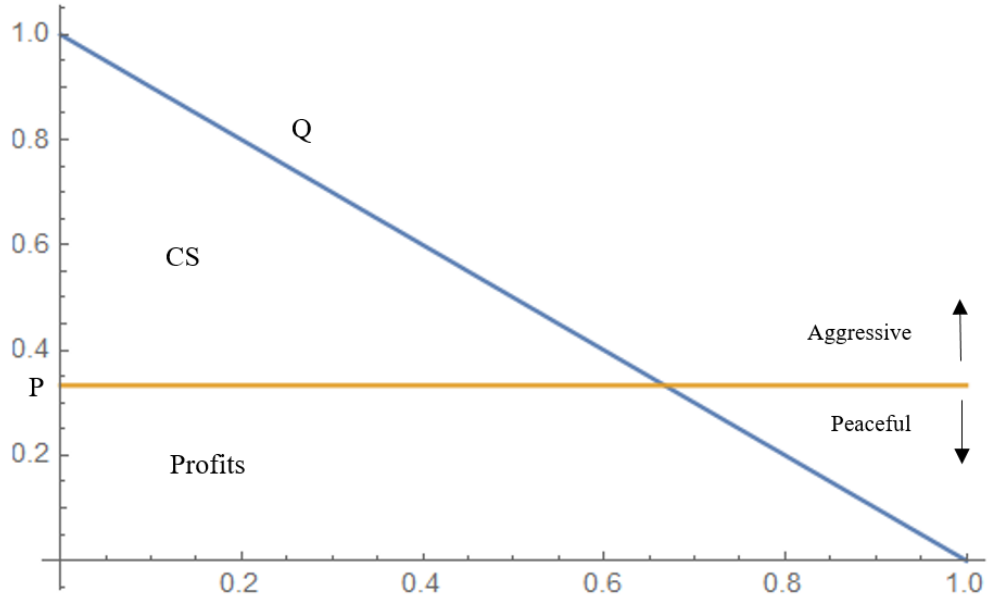


Figure 1. Inverse demand and overall quantity

Estimated values for CS shown below:

$$CS^1 = \frac{2}{9}$$

$$CS^2 = \frac{8}{81}$$

$$CS^3 = \frac{25}{162}$$

Comparing values:

$$CS^2 < CS^3 < CS^1$$

Clearly, a peaceful environment provides better conditions for the consumers. Price would be the main factor explaining this phenomenon. Under the peaceful conditions, market achieves the lowest price, which, in turn, increases the area of CS triangle. Consequently, the case with the highest price achieves the smallest CS in the equilibrium (Case 2). Asymmetric Case 3 shows slightly better results.

To conclude, cyber-attacks are no good for the consumers.

5.4 Total Surplus

Total surplus is calculated to evaluate overall market performance. It is a sum of total profits earned by players plus consumer surplus. Estimations can be found below:

$$TS^1 = \frac{4}{9}$$

$$TS^2 = \frac{28}{81}$$

$$TS^3 = \frac{65}{162}$$

Results are similar to the consumer surplus comparison. Again, the cyber-attack free market achieves better results than the aggressive environment.

$$TS^2 < TS^3 < TS^1$$

6 Cyber-attack regulations

The effect of marginal cyber-attack costs on price, profit functions, consumer surplus and total surplus is also of interests of the paper. The paper suggests that cyber-attack costs could be influenced by policy makers. It could be key to an aggressive market control.

Case 2 is used as a reference case for this section.

To simplify the analysis of the effect of the increase of cyber-attack costs, the paper assumes all other coefficients to be equal to 1 (including server capacities $d = b = k_i = k_j = 1$).

To investigate the influence of an increase in cyber-attack costs on the price, the following partial derivative should be calculated:

$$\frac{P^2}{\partial c_a} = -\frac{4}{(1+2c_a)^2}$$

An increase in cyber-attack costs will always have a negative influence on the price. The higher cyber-attack costs are, the lower price will be achieved by the market.

Obviously, cyber-attack costs will also influence aggressive companies' profits:

$$\frac{\partial \Pi^2}{\partial c_a} = -\frac{2(-1+6c_a)}{(1+2c_a)^2}$$

The sign of the derivative depends on the marginal cyber-attack costs value. In this case, cyber-attack costs will drive profit upward IFF:

$$c_a < \frac{1}{6}$$

Only reasonably cheap cyber-attacks could be interesting to the firms. Influencing the price of cyber-attacks could be a good method of market regulations. Restricting the access to the offensive tools sellers, imposing penalties for cyber-attack usage, and other could drive marginal cyber-attack costs high enough to make it obsolete.

Of course, the entirely opposite effect is expected on the consumer surplus:

$$\frac{\partial CS}{\partial c_a} = \frac{16c_a}{(1+2c_a)^3}$$

Every possible (assuming non-zero cyber-attack costs) value of the cyber-attack marginal cost will have a positive influence on the consumer benefits. Overall, an increase in cyber-attack costs have an ambiguous effect: it has a negative impact on firms' profits and positive impact on consumer' benefits.

Its' ambiguity could be observed in the following derivative:

$$\frac{\partial TS}{\partial c_a} = -\frac{4(-1+2c_a)}{(1+2c_a)^3}$$

The presented above derivative will have a positive sign IFF:

$$c_a < \frac{1}{2}$$

In all other cases, cyber-attack costs will have a negative impact on the total surplus of the market. It could be explained by the assumption that overall negative effect of the increase of cyber-costs on overall profits earned by firms dominates overall positive effect on the consumer surplus. Keeping cyber-attack costs reasonably low (or even unregulated) could have a positive effect on the market.

7 Conclusion

This paper made an attempt to develop a model of a competitive market with aggressive information environment (environment, where competitors do not hesitate to use DDoS-type attacks to obtain a competitive advantage). The model could be considered as a modified Cournot duopoly and inherited major assumptions. However, companies now make three decisions in three sequential time periods, instead of choosing quantity directly. Firms choose server capacity in the initial zero period, cyber-attack power in the intermediate first period and actual quantity in the final second period.

For the sake of simplicity, only last two periods were analysed in the paper. The initial period should be analysed in the future research. Server capacity that firm chooses at the start is considered as an external variable. Another simplicity assumption implied the analyses of pure strategies equilibriums only. In this case, it also means, that companies choose symmetric capacities regardless of the case they are situating. Mixed strategies will also be analysed in the future research.

Three different equilibriums were calculated for three different cases:

Case 1: a peaceful market with no cyber-attacks. It simplified to a classical Cournot case and used as a reference point the further comparison;

Case 2: aggressive market, all companies use cyber-attacks;

Case 3: an asymmetric case with only one foe-firm, the second firm is peaceful.

The allocation in the certain equilibrium entirely depends on the server capacity values.

Comparing key performance indices (price, profits, consumer surplus, total surplus), the paper discovered that the presence of cyber-offensive tools on the market has have a negative impact.

Indeed, equilibrium in peaceful Case 1 achieves the smallest price among the cases and highest values for consumer and total surpluses, which represent the overall market performance. However, the statement is not true if it comes to profits. DDoS-type cyber-attacks are proved to be an efficient method of unfair competition. The usage of cyber-attacks drives companies profits up by creating a deficit on the market (driving the price upwards).

Companies, which allocated within an aggressive market will generate more profits by sacrificing consumer surplus.

Asymmetric case 3 illustrates a situation of the dominance of the aggressive player. Foe-player in the peaceful environment is capable of significant balance shift. The usage of cyber-attacks against peaceful firms leads to a market monopolisation and negative market performance issues.

Aggressive competitive markets is possible to regulate by influencing marginal cyber-attack costs. The logic is simple, high enough cyber-attack costs make the offensive behaviour obsolete by driving profits to negative values. It could be done by introducing law enforcement, penalties or restricting the access to offensive services. Consumers benefit more in the environment with higher attack costs. However, there also exists a situation in which reasonably low cyber-attack costs could have an overall positive impact on the total surplus. It could be achieved by balancing between the strong negative effect on the firms' profits and positive effect on the consumer surplus. Obviously, the deeper analysis should be performed in order to achieve an adequate result and propose efficient regulative measures.

References

1. Adda, J., Cooper, R. (2003). Dynamic Economics - Quantitative methods + applications. October, 187 Suppl, 293. Retrieved from http://discovery.ucl.ac.uk/12691/

2. Giocoli, N. (2011). Reaction curves, (33809).

3. IBM Security. (2015). IBM 2015 Cyber Security Intelligence Index. IBM Security Managing Security Services, 24. https://doi.org/SEW03039-USEN-02

4. McDowell, M. (2009). Understanding Denial-of-Service Attacks. Retrieved from http://www.us-cert.gov/ncas/tips/st04-015

5. Varian, H. R. (2006). Intermediate microeconomics: a modern approach (7th ed.). W.W. Norton Co. Retrieved from https://books.google.com/books?id=4X