Helsinki Center of Economic Research

Discussion Papers

Cyber Technology and Arms Race

Vesa Kanniainen
University of Helsinki, HECER and CESifo

Discussion Paper No. 409
February 2017

ISSN 1795-0562

HECER – Helsinki Center of Economic Research, P.O. Box 17 (Arkadiankatu 7), FI-00014
University of Helsinki, FINLAND,
Tel +358-2941-28780, E-mail info-hecer@helsinki.fi, Internet www.hecer.fi

HECER
Discussion Paper No. 409

Cyber Technology and Arms Race*

Abstract

Cyber technology represents digital military capability with the purpose of causing damage to the military strength and the social infrastructure of a potential enemy. War using conventional weapons may be preceded by or combined with a war using cyber technology. This paper introduces such technology into the theory of conflicts, suggesting the striking proposal that the expected return on cyber investment is convex. It is shown that an asymmetric successful cyber program results in an option for a pre-emptive cyber attack. These features of the model make the cyber technology a first-ranked military investment. The optimal scale of a cyber program of a country expected to have access to a superior cyber capability is derived. It is shown that the asymmetric cyber capability reduces the international arms race but nevertheless raises the likelihood of a war reducing the deterrence.

JEL Classification: H12, H56

Keywords: military conflicts, cyber war, arms race

Vesa Kanniainen

Department of Political and Economic Studies
University of Helsinki
P.O. Box 17 (Arkadiankatu 7)
FI-00014 University of Helsinki
FINLAND

e-mail: vesa.kanniainen@helsinki.fi

* The author is indebted to Tapio Palokangas for helpful comments.

1 Introduction

In June and July of 2010, the world learned about Stuxnet, a malicious computer worm believed to be jointly created by American-Israeli cyber weapon specialists.[1] Experts have been convinced that Stuxnet was meant to sabotage the uranium enrichment facility at Natanz in Iran and its centrifuge operational capacity but the damage spread to other units, too. It is believed that most of the infected computers worldwide by Stuxnet have been in Iran. Judging from such a cyber operation, Israel apparently preferred to mount a cyber attack rather than a military strike on the nuclear facilities of Iran. There is little downside to such an attack because it would be virtually impossible to prove who did it. Though the attack against Iran was a success the same is not true of the corresponding attempts to cause damage to the nuclear program of North Korea. It is conceivable that such strikes have been planned and even attempted. With computerized instruments like Stuxnet, the world has moved to a new area in warfare, the era of cyber war.[2]

Wars represent an exploitation of resources by destructive measures in an inefficient non-Paretian way: they destroy value and lives. The digital world has changed warfare not only in terms of the destructive power of the weapons, but also by causing damage either directly to the efficient use of the technology-dependent weapons of the opponent or by indirectly causing

[1] For details, see Sutherland (2012), for example.

[2] Cyber measures were also employed in the Georgian war in 2008 by the Russian military though success was apparently rather limited. Recently, successful invasions in several servers in military organizations abroad have taken place. Civilian targets have been subject to attacks over the years, including the Warshaw Stock Exchange and a German steel -mill, both in 2014. Russians also launched in 2015 a cyber strike against the electric system in Ukraine, causing substantial trouble for a large number of people. Defense News reported in February 10, 2017 that the US Air Force has conducted a multitude of cyber missions over the last year that have contributed to captured or killed terrorists. According to written testimony provided to the House and Senate Armed Services committees this week, Air Force Vice Chief of Staff Gen. Stephen Wilson said, "The Air Force conducted 4,000 cyber missions against more than 100,000 targets, disrupting adversaries and enabling over 200 High Value Individual kill/capture missions."

paralyzing effects on the society at large. By its logic, a cyber attack represents a pre-emptive offensive action. Cyber measures often mean a remote attack by digital technology with the purpose of causing damage to the social and/or military capability of an enemy. The cyber capability represents an instrument prior to the war with conventional weapons. Modern warfare may consequently be viewed as a multi-stage process in a new way.

In the development of military capabilities, enemies typically hide their development plans. Once the success is confirmed, they may have an incentive to signal their success to create deterrence. Though such signals may result in counter actions by the enemy and may accelerate investment in the military, they also serve as an information communication device of the strength of the enemy![3]

Viewed as a game, modern warfare appears to have several consecutive stages. A war with conventional weapons tends to be preceded by a cyber war. The potential of a cyber capability is unlimited. How strong is the incentive to exploit the innovative success from the first-mover basis? Several thoughts support the following propositions: (i) the cyber and the conventional military capability of the defender is deteriorated if its cyber capability suffers from the attack, (ii) a cyber attack need not result in civilian casualties, and (iii) the target cannot easily identify the attacking country. Therefore, it is not trivial to initiate a counter-attack. For these reasons, the threshold for a cyber attack may be low.

This paper develops a theory of conflict where countries invest both in cyber technology and conventional weapons as complementary military inputs. This leads to a sequential decision-making approach employing methods commonly used in economic research. As far as the author is aware, the current paper is the first one using a formal economic approach in the analysis of

[3]The Soviet Union apparently wanted to hide the development of its nuclear weapons in the 1950s until it obtained them. Saddam Hussein's regime in Iraq wanted to confuse the enemy (i.e., Iran), suggesting that it had built up mass destruction programs, though it actually had not. The signals were misleading on purpose.

cyber war.

Several questions will be addressed. What is the optimal investment in cyber war technology in contrast to the conventional technology? Does the incentive for a premature attack arise? Given that a cyber attack can be directed to destroy the enemy's ability to efficiently employ its conventional weapons, what is the value of the first-mover advantage created by the cyber capability?

The roadmap of the paper is as follows. Investment in cyber technology is introduced into a standard model of conflicts in terms of the probability of being victorious in warfare.[4] Investment in cyber capability is considered risky in terms of the outcome of the development effort. Moreover, the outcome is private information for each country. The country that turns out to be more successful finds that it has access to an option of initiating a cyber attack against the enemy, but without knowing whether the enemy has been successful in its rival development effort. In the latter case, a counterattack by cyber measures is expected. After the cyber war stage, the countries enter warfare with conventional weapons. It is a fundamental notion in the model world of this paper that the war cannot be won by a cyber attack only: conventional weapons are needed to capture the prize. A first-mover advantage appears highly valuable. Expectations of the capability of the enemy become crucial.

In the conventional theory of conflict, the return on the investment effort in terms of the marginal increase in the probability of a victory is concave and subject to diminishing returns. This will not hold true in the case of a cyber investment. The remarkable property of the model shown here is that the return on a cyber investment is convex. Convexity makes cyber technology a first-ranked military investment. It is shown that countries choose

[4]When referring to the standard approach, we resort to the approach suggested by Tullock (1967, 1980) and subsequently elaborated by many, including Pérez-Castrillo and Verdier (1992), Hirshleifer (1989), Chowdhury and Sheremeta (2011) and developed and evaluated by Konrad (2009).

to invest an equal amount of resources in their militaries even when their cyber capabilities differ but less than in the absence of cyber war technology. One of the key claims of the paper is that access to cyber technology limits the international arms race with conventional weapons. Asymmetries in the success of cyber programs create the option of a pre-emptive strike, reducing the deterrence of war between countries by lowering the cost of war with conventional weapons, though it invites less investment in an arms race.

2 Model of armament

2.1 Time line and stages: equilibrium with and without deterrence

In the model world of this paper, there are two symmetric countries (players) A and B which compete for a resource with value $v > 0$ using their military power.[5] The time line is as follows. In stage 0, both countries expecting a military confrontation invest both in the conventional military capacity and in the cyber capability. Those investments are denoted by (x, a) for the country A and by (y, b) for the country B. In stage 1, the investment probabilistically yields a cyber capability. When successful, the damage caused by the cyber attack of, say country A, on the military strength of country B is given by az with $z > 0$. Similarly, if country B is successful in the cyber program, it can cause damage bz on country A. The damage thus depends on the scale of investments (a,b).

The cost of the military program is given by the social cost of public funds. It is assumed that the cost of investment in conventional weapons equals the investments x and y.[6] This section examines first the equilibrium in the base

[5] Access to a peaceful negotiation is exhausted. It is possible to think that the resource is an outside one with badly defined property rights, but it can also be in the possession of one of the countries encountering the conflict.

[6] A linear cost is needed for technical reasons if only to solve the model analytically

line model of the conflict theory, the well-known Tullock (1967, 1980) model. In the absence of a cyber technology, the Tullock-model predicts that the probabilities of winning a (conventional) war between two countries $P(A)$ and $P(B)$ are dictated by their relative military investments x and y,

$$P(A) = \frac{x}{x+y};\ P(B) = \frac{y}{x+y}. \tag{1}$$

The fundamental property of this formulation is that the marginal returns on investment are strictly concave. For example, for country A (similarly for country B),

$$\frac{\partial P(A)}{\partial x} = \frac{y}{(x+y)^2} > 0,\ \frac{\partial^2 P(A)}{\partial x^2} = -\frac{2y}{(x+y)^3} < 0. \tag{2}$$

The value of the marginal unit of arms to a country is therefore related to the amount of arms *acquired by the enemy*. We are thereby at the source of explanation as to why the arms races arise! In the absence of cyber weapons and abstracting from the cost of war, the expected returns from a warfare are

$$E(\pi_A) = P(A)v - x,\ E(\pi_B) = P(B)v - y. \tag{3}$$

Carrying out the maximization of the expected returns, the reaction functions are

$$x = -y + \sqrt{yv},\ y = -x + \sqrt{xv}. \tag{4}$$

Then, the unique Nash equilibrium in investments in conventional weapons

for the optimal conventional investment. Access to such an explicit solution is helpful to illustrate the mechanisms of the model. The cost of a cyber program is introduced below.

is given by a pair (x^N, y^N) satisfying[7]

$$x^N = y^N = \frac{v}{4}. \tag{5}$$

A high prize v justifies a high investment. Yet, it follows that both enemies have the same probability of winning the war, $P(A) = P(B) = 1/2$. The expected return from warfare is positive in the absence of a cost of war,

$$E(\pi_A) = P(A)v - x = P(B)v - y = v/4 > 0.$$

Whether it is worthwhile to fight, the model should be adjusted for the costs of a mutual war if it takes place. These costs apparently depend on the military strength of the enemy. They will be denoted by $C(y)$ and $C(x)$ with $C'(x) = C'(y) > 0$, $C''(x) = C''(y) > 0$. Therefore, the incentive conditions for deterrence, adjusted for the costs of war, are

$$E(\pi_A) = P(A)v - x - C(y) \leq 0$$

$$E(\pi_B) = P(B)v - y - C(x) \leq 0.$$

It is a fascinating observation that deterrence is not only conditional on the magnitude of the cost of war but also depends on the type of cost. Suppose that the cost of war is quadratic, $C(y) = \frac{1}{2}cy^2$. The deterrence condition is $v/4 - \frac{1}{2}cv^2/16$, or $c > 8/v$. Unexpectedly, a high prize discourages the outbreak of war. The reason is that a high prize creates an incentive to have a large equilibrium investment in the conventional equilibrium not to give lead to the enemy, which leads to a high mutual destruction power and a high cost of war. The prize of war will not have such an impact if the cost is linear in the destruction power of the enemy, $C(y) = cy$. In this case, the

[7]The second-order conditions are satisfied as $P(A)$ is strictly concave in x and $P(B)$ in y.

deterrence condition is simply $c > 1$.

Access to a cyber attack raises new questions. First, how much is it worthwhile to invest in conventional weapons if countries can resort to cyber instruments? Second, does the answer depend on the differences in cyber capability? Third, is it always the case that a cyber war is followed by a war with conventional weapons? Does the threshold to a cyber war differ from that of a conventional war? These are the issues to be analyzed next and some of the answers turn out to be unexpected.

2.2 Investment in arms with expected success in a cyber program

We now introduce cyber capability as a new warfare instrument. Suppose first that both countries are planning their investment programs in conventional weapons, x and y, *expecting to be equally successful in creating the cyber destructive power*, $z > 0$. Suppose that the deterrence condition will not be satisfied in stage 1 and that both expect to launch a cyber attack against each other. Subsequently, in stage 2, they expect to be engaged in a mutual war with conventional weapons. The *ex ante* expected returns from warfare then are

$$E(\pi_A) = \frac{x(1-bz)}{x(1-bz)+y(1-az)}v - x - c(a) - C(y) \tag{6}$$

$$E(\pi_B) = \frac{y(1-az)}{y(1-az)+x(1-bz)}v - y - c(b) - C(x). \tag{7}$$

The social costs of the cyber investments have been denoted by $c(a)$ and $c(b)$. The following strong result is available:

Proposition 1. (*Neutrality of cyber*). *If countries expect to have access to equally effective cyber capabilities, their cyber capabilities are neutral in respect to the optimal investment in conventional weapons.*

Proof. Solving for the Nash equilibrium from equations (6) and (7) under condition $az = bz$, one can see immediately that the cyber capability does not interfere with the optimal investments x and y. QED

The outcome of such a symmetric game was given above by (5). The symmetric case, however, is destroyed *if one of the countries expects to be superior in creating the cyber capability.* Suppose that it is country A while both expect that country B will not be able to create such a capability. It holds

$$E(\pi_A) = \frac{x}{x + y(1 - az)}v - x - c(a) - C(y), \tag{8}$$

$$E(\pi_B) = \frac{y(1 - az)}{y(1 - az) + x}v - y - c(b) - C(x). \tag{9}$$

An unexpected result follows,

Lemma 1. *In a Nash equilibrium, countries with a superior and inferior cyber ability have incentives to invest an equal amount in conventional weapons, but less relative to the case when cyber technology is not expected to be available for either of them.*

Proof. Solving for the Nash equilibrium, the optimal investments in the conventional weapons are

$$x^C = y^C = \frac{(1 - az)v}{(2 - az)^2} < \frac{v}{4}. \tag{10}$$

The inequality follows from that when $z = 0,\ x^C = y^C = v/4$. Moreover, for $z > 0$,

$$\partial \left[(1 - az)v/(2 - az)^2\right]/\partial z = -a^2 zv/(2 - az)^3 < 0. \tag{11}$$

QED

This result follows from the strategic interaction between the countries and from the fact that the marginal value of the armament for a country is positively related to the strength of its enemy, cf. (2). The country with

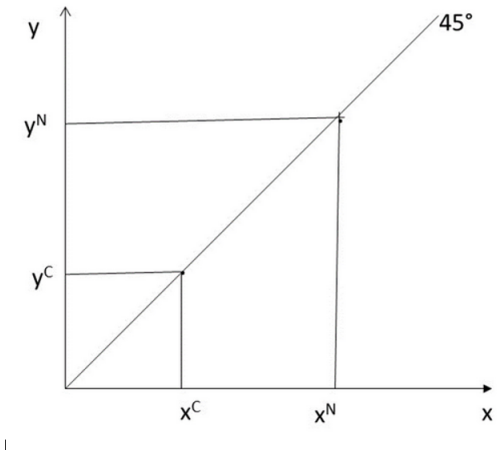

Figure 1: Nash equilibria in the absence of and under cyber capability

a superior cyber capability can economize in its investment in the arms as it knows that part of the military capacity of its enemy can be destroyed. Furthermore, even knowing that part of it is expected to be destroyed the best response of the enemy with the more limited cyber capability is to invest the same amount as the country with the superior cyber technology. However, the latter country has a greater probability of winning the war

$$P(A) = \frac{1}{2-az} > \frac{1-az}{2-az} = P(B) \tag{12}$$

and a greater expected return from a war

$$E(\pi_A) = \frac{1}{2-az}v - c(a) - C(y) > 0,\ E(\pi_B) = \frac{1-az}{2-az}v - c(b) - C(x). \tag{13}$$

Once the enemy invests less, so does the other country. There is a mutual cutback in the armament. This does not eliminate the wars nor is the deterrence more likely. Unexpectedly and in contrast, it makes the wars less costly and less destructive, but therefore more likely. Thus,

Proposition 2. *A succesful cyber program reduces deterrence by lowering*

the cost of war in conventional weapons.

Country B therefore ends up investing the same amount as country A even knowing that its probability of winning the war will be smaller. To make sure, the marginal values of the armaments for both countries are equalized in the Nash equilibrium with the marginal costs, $\partial P(A)v/\partial x = x$, $\partial P(B)v/\partial y = y$.

Next, we report a key implication of the model,

Lemma 2. *The return on cyber investment is strictly convex in a.*

Proof. Taking the partial derivatives of the winning probability in (6), it holds for country A,

$$\partial \left[\frac{x(1-bz)}{x(1-bz)+y(1-az)} \right] /\partial a = \frac{xyz(1-bz)}{\left[x(1-bz)+y(1-az)\right]^2} > 0$$

$$\partial^2 \left[\frac{x(1-bz)}{x(1-bz)+y(1-az)} \right] /\partial a^2 = \frac{2xy^2z^2(1-bz)}{\left[x(1-bz)+y(1-az)\right]^3} > 0$$

and similarly for country B. It follows that both countries have a strong incentive to acquire the destructive cyber capability, hoping to enhance the probability of winning the war with the conventional weapons in the final stage.

3 Cyber attack as an option

3.1 Uncertainty of the success of the enemy

Following the cyber investments, there are four possible outcomes from the *ex ante* perspective. With probability *pp,* both succeed in their cyber programs. With probability p(1-p), one succeeds while the other does not, and with probability (1-p)(1-p) neither succeeds. A success is private information and unobservable. A cyber attack leads to a counter attack if the other country has also succeeded. A first-mover strike is plausible when the success

probability p is low because if A has succeeded, it expects that B has been successful with only a low probability. This suggests that the probability of a first-mover attack may be high when the *ex ante* success probability is small. Yet, Proposition 2 above states that *success in cyber investment lowers the war threshold, increasing the risk of a war.* A question of interest is whether it is possible that the cyber capability facilitates a first-mover strike but whether there are conditions under which it can reduce the likelihood of a conventional war? Why did Israel limit action against Iran in cyber weapons instead of initiating a conventional war?[8]

Consider now the case where a country, say country A knows that it has been successful in completing the cyber program but faces uncertainty of the success of its enemy. In stage 1, it has launched a cyber attack, knowing that the enemy will retaliate with a cyber counter-attack followed (apparently) by warfare with conventional weapons. By this stage, all investments (x, y, a, b) were undertaken and bygone. The incentive condition for exercising the option of initiating a cyber attack in stage 1 to be followed by the warfare in conventional weapons is given by

$$E(\pi_A) = pE\left(\pi_{A0}\right)v + (1-p)E\left(\pi_{A1}\right)v - C(y(1-az)) \geq 0 \qquad (14)$$

where

$$E\left(\pi_{A0}\right) = \frac{x(1-bz)}{x(1-bz)+y(1-az)} = \frac{x}{x+y}$$

$$E\left(\pi_{A1}\right) = \frac{x}{x+y(1-az)}$$

What is the value of the option for a cyber strike and is it always worthwhile to exercise this option? How much is it optimal to invest *ex ante* in a cyber program by a country that *expects* to be superior in the cyber capabil-

[8]In the Stuxnet attack against Iran, no war with conventional weapons took place. Recall that Israel had, however, undertaken a pre-emptive strike on the nuclear facility of Iraq in Osirak in 1981.

ity? What are the conditions for a country with a superior cyber capability to abstain from warfare with conventional weapons given that it committed to a cyber strike in the first place?

The condition for exercising the attack option under uncertainty can then be stated in terms of the success probability of the enemy from (13),

$$p \leq \bar{p} = \frac{E\left(A_1\right) - C(y(1-az))}{E\left(A_1\right) - E\left(A_0\right)} \left(\frac{1}{v}\right). \tag{15}$$

Proposition 3. *A low success probability of the cyber R&D encourages exercising the cyber attack option by a successful country to be followed by warfare in conventional weapons,*

This result is logical: a country that has been able to acquire the cyber capability knows that the enemy has a similar capability but with a *small* probability. Moreover, while the cost of war reduces the critical probability and discourages exercising the option (and potentially unjustifying the attack), this cost is reduced by a successful cyber attack. A high value of the prize of winning the war, v, unexpectedly reduces the critical probability.

Consider next the case

$$C_A(y) > C_B(x).$$

Then,

Corollary 1. *It is sufficient for a country with a superior cyber capability launch a cyber strike against its enemy, but to abstain from warfare with conventional weapons that the cost of war for country A is sufficiently greater than the cost for country B.*

"Sufficiently greater" means here that $E\left(\pi_A\right) < 0$ while $E\left(\pi_B\right) > 0$.

It follows from the convexity property above: *a cyber capability can be viewed as representing an option of destroying the enemy's capacity* and an investment in cyber represents an investment in a call option. The view

of options therefore becomes helpful for the current analysis. The outcome of the risky R&D program represents the underlying risky asset analogous to a call option in the theory of finance. This option can be acquired by investing in the uncertain R&D project and may be worth exercising if the country has been successful in its risky R&D project and if the cost of war is tolerable. Ever since Black and Scholes, one of the basic messages of option pricing has been that a high risk makes the option valuable. The question is, how worthwhile it is to expand the cyber program given that it is subject to increasing costs? Moreover, if it turns out to be successful, what is the value of the attack option that a success creates?

The value of the option for country A created by its asymmetric success in its cyber program is given by the difference between the expected return from the war and the value of war in the absence of the cyber capability,

$$V = max\left[0, V(a) - V(0)\right] \tag{16}$$

where

$$V(a) = \frac{x}{x + y(1 - az)}v - C(y(1 - az)) - x$$

$$V(0) = \frac{x}{x + y}v - C(y) - x.$$

Notice that

$$\frac{x}{x + y(1 - az)} > \frac{x}{x + y}$$

and that

$$C(y(1 - az)) < C(y)$$

making the cyber attack option valuable. The option has no value when both countries or neither country has succeeded. We have both countries investing in the cyber program from the start - the technology frontier has made it feasible and there is no point in delaying. The return on cyber investment is convex; both countries prefer to have az and bz equal to 1, but this is a case

where the countries are capable of making the enemy completely helpless with no military strength. Such a highly unrealistic case is eliminated by an assumption which is now introduced,[9]

Assumption 1. $1 - az > 0$, $1 - bz > 0$.

3.2 Optimal investment in cyber: the superior country

Consider a case where one of the countries, say *A, ex ante* expects for sure to be superior in its cyber program.[10] Ask: how much will it optimally invest in the cyber technology? To analyze the optimal cyber investment of the superior country, introduce a convenient notation, $E[\pi_A(a)] = f(a)$. The function $f(a)$ is continuously differentiable everywhere, in particular on $[0, 1/z]$. The optimal investment in cyber of a country which expects to be superior then solves

$$a^* = arg\ max_a\ f(a) = \frac{x}{x + (1 - az)y} v - x - c(a) - C(y(1 - az)). \quad (17)$$

To have the solution for the optimal cyber as a finite interior investment choice, its cost of investment must be sufficiently convex in the relevant region of a.[11] With no loss generality, is is then convenient to let the cost be given by

$$c(a) = \frac{1}{3} ca^3,\ c > 0. \quad (18)$$

[9] Even the "star war" during the Reagan administration in the USA was too expensive to be accomplished.

[10] If both expect to become equally successful, the case was analyzed above.

[11] While there is a well-functioning international market for conventional weapons with publicly available information on the market prices, no such market exists for the specific human capital required to establish a cyber program. Training a new generation of electronic engineers is time-consuming and expensive.

To find the extreme values, evaluate the first-order condition $f'(a) = 0$ arriving at equality between the marginal revenue and the marginal cost,

$$MR_a = \frac{xyzv}{\left[x + (1 - az)y\right]^2},\ MC_a = ca^2.$$

The first-order condition can thus be stated as a fourth-order equation in a,

$$\frac{xyzv}{c} = \left[x + (1 - az)y\right]^2 a^2.$$

It must thus have four roots. Taking the square roots,

$$\sqrt{\frac{xyzv}{c}} = \left[x + (1 - az)y\right] a.$$

As the left-hand side is positive, only the plus sign qualifies on the right-hand side. The candidates for the optimal cyber investment therefore satisfy a second-order algebraic equation

$$yza^2 - (x + y)a + \sqrt{\frac{xyzv}{c}} = 0. \tag{19}$$

There are two solution candidates,

$$a^* = \frac{(x + y) \pm \sqrt{(x + y)^2 - 4yz\sqrt{\frac{xyzv}{c}}}}{2yz}.$$

It has to be assumed that the roots are real,

Assumption 2.

$$(x + y)^2 - 4yz\sqrt{\frac{xyzv}{c}} \geq 0.$$

This assumption can be defended when the cost c is sufficiently "large". Notice that the case $az \geq 1$ is excluded by Assumption 1. The roots satisfying $az < 1$ are more interesting.

As there are two roots, one has to choose. Of the candidates, only the

smaller one, $a_1^* < a_2^*$, qualifies as a maximum; the other solution has to be a minimum. A graphical illustration is illuminating.[12] Note that at the origin with $a = 0$, $MR_a > 0$ while $MC_a = 0$. At a low level of a, the MR_a-curve is therefore above the MC_a-curve. Thus, of the two extreme values it is the maximum that is located at $a = a_1^*$ while the minimum is located at $a = a_2^*$. There are two points of intersection of the MR_a- and the MC_a-curves given by the roots. [13]

Stating formally the second-order condition for the maximum,

$$f''(a) = \frac{xy^2z^2v}{[x + (1 - az)y]^3} - ca < 0. \tag{20}$$

The parameter space is rich enough to find combinations which satisfy such a requirement.

To summarize the key finding in the current section,

Proposition 4. *When a country expects to acquire a superior cyber capability there is a unique maximum solution for the optimal cyber investment.*

Proof. Above. □

The following comparative static effects

$$\frac{\partial a_i^*}{\partial v} > 0, \ \frac{\partial a_i^*}{\partial c} < 0$$

are as expected: the incentives to invest in the cyber technology are positively related to the prize of winning the war, and negatively to the cost of investment.

[12] Whether to initiate a war or not is a separate decision and is dictated by whether the expected total return $f(a)$ is positive or negative at the optimal choice of the military investments.

[13] It follows that the smaller solution, a_1^*, is stable while the greater one, a_2^*, is unstable. A small deviation from a_1^* leads to a process which induces the solution to move towards a_1^* while a small deviation from a_2^* induces the solution to move further away from a_2^*.

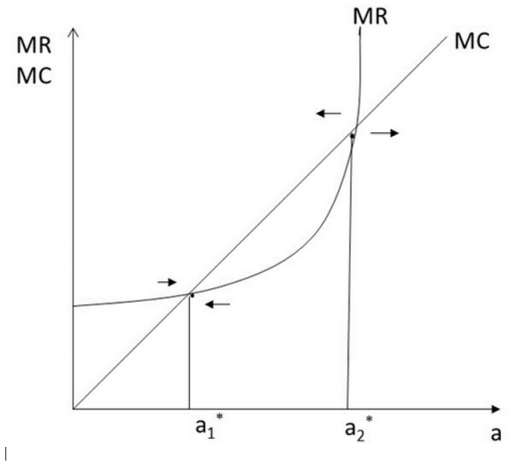

Figure 2: Optimal cyber program by a superior country

The comparative statics with respect to the damage z, however, has two opposite effects. The explanation goes as follows. The damage effect naturally raises the return on the cyber investment. However, there is a break to the scale of the cyber program as it is costly, and the more effective it is, the smaller the threat of the military capacity of the enemy.

We observe the additional result that a high investment in the conventional military both by a country and by its enemy (x,y) justify a high investment in the cyber capability of the technologically more advanced country. In this sense, the two military instruments are complements rather than substitutes.

4. Final remarks

The current paper has established some key regularities concerning modern warfare. It was shown that an asymmetric success in a cyber program creates an option for a first-mover attack, yet reduces international arms races in conventional weapons, but nevertheless increases the likelihood of a war, reducing deterrence.

As many believe, the attacks against the Iranian nuclear stations by the Stuxnet virus were undertaken by Israel. Why did the country abstain from an attack with conventional weapons? One reason might be that it was possible to carry out the attack secretly. This makes the cost of a cyber attack smaller than by resorting to conventional weapons where the cost should be viewed as including the international response. Another reason may be that resorting to a pre-emptive cyber attack provided extra time and potential access to new options in the long-lasting conflict. Anyway, Stuxnet has made cyber war a reality in modern warfare.

5. References

Black, F. and Scholes, M., (1973), "The Pricing of Options and Corporate Liabilities", *Journal of Political Economy*, 81 (3), 637-654.

Beviá, C., and Corchón, L.C., (2008), "Peace Agreements without Commitment", Departemento de Economia, Universidad Carlos III, Madrid.

Chowdhury, S., M., and Sheremeta, R.,M., (2011), "A Generalized Tullock Contest", *Public Choice*, 147: 413-420.

Defense New, "Cyber integral to US kill/capture missions in 2016", February 10, 2017, www.defensenews.com

Hishleifer, J., (1989), "Conflict and Rent-Seeking Success Functions: Ratio vs. Difference Models of Relative Success", Public Choice 63: 101-112.

Tullock, G., (1967), "The Welfare Costs of Tariffs, Monpolies, and Theft", *Western Economic Journal* 5: 224-232.

Tullock, G., (1980), "Efficient Rent-Seeking", in J.M.Buchanan, R.D. Tollison and G. Tullock (eds.), *Toward a Theory of the Rent-Seeking Society*, 97-112. College Station: Texas A&M University Press.

Konrad, K., (2009), *Strategy and Dynamics in Contests*, Oxfiord: Oxford University Press.

Peréz-Castrillo, J.D., and Verdier, T., (1992), "A General Analysis of

Rent-Seeking Games", *Public Choice* 73: 335-350.

Sutherland, B., (ed.), *Modern Warfare, Intelligence and Deterrence. The technology that is transforming them.* The Economist (2012).