Helsinki
Center
of
Economic
Research

Discussion Papers

Cyber Technology and the Arms Race

Vesa Kanniainen
University of Helsinki and HECER

Discussion Paper No. 424
February 2018

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. 424

Cyber Technology and the Arms Race*

Abstract

Cyber technology represents digital military capability with the purpose of causing damage to the military strength of a potential enemy. War using conventional weapons may be preceded by or combined with a strike using cyber technology. This paper introduces such technology into the theory of conflicts. The cost of war relative to the payoff from victory turns out to be crucial for the results on armament decisions. In the war game, two types of Nash equilibria both subject to warfare are possible depending on the perceived cost of war. In a symmetric war game with equal cyber capabilities and a low cost of war, hostile countries choose to invest an equal amount of resources in their militaries. A higher cost of war leads to increased armament. However, asymmetric access to cyber technology limits the international arms race with conventional weapons when the cost of war is small while it - again - intensifies the arms race when the cost of war is greater. In all cases, access to cyber technology makes wars with conventional weapons more likely. Heterogeneity in the success of cyber programs creates a first-mover advantage for a superior country in terms of a possibility for a pre-emptive strike.

JEL Classification: H12, H56

Keywords: military conflicts, cyber war, arms race

Vesa Kanniainen

Economics
P.O. Box 17 (Arkadiankatu 7)
FI-00014 University of Helsinki
FINLAND

e-mail: vesa.kanniainen@helsinki.fi

* The author is indebted to Anna-Maija Juuso and Tapio Palokangas for helpful comments. The responsibility of potential errors remains with the author. An earlier draft of the paper was published in the CESifo Working Paper series No. 6365, March 1, 2017.

1 Introduction

In June and July of 2010, the world learned about Stuxnet, a malicious computer worm believed to be jointly created by American and 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 computerised instruments like Stuxnet, the world has entered into a new age, the era of cyber war.[2]

Cyber issues are rapidly growing in importance to defence alliances. At the Wales Summit in 2014, allied heads of state and government affirmed that cyber defence is part of NATO's core task of collective defence. Ambassador Sorin Ducaru, NATO's assistant secretary general for emerging security challenges, gave a statement about NATO's efforts to improve its cyber defences against emerging threats.[3] The message is that by treating cyberspace as an operational domain, NATO aims to better protect its missions and operations. It will assist in the management of resources, skills, and capabilities, and will also ensure that cyber defence is better reflected in military planning, exercises, training, and how NATO responds to crises. One of the questions is whether Article 5 would be triggered in the case of a cyber attack on a member country. Until recently, the political impact of cyberspace was thought to be a matter of low politics—background conditions and routine processes and decisions. Now, however, experts have begun to recognise its effect on high politics—national security, core institutions, and critical decision processes. Choucri (2012) investigated the implications of this new cyberpolitical reality for international relations theory, policy, and practice, and the modes of cyber conflict and cyber cooperation in international relations.

---

[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 organisations 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 a cyber strike against the electric system in Ukraine in 2015, causing substantial trouble for a large number of people. On February 10, 2017, *Defense News* reported 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 committee, 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."

[3] Cf. *The Journal of International Affairs*, Winter 2016, Vol. 70, No1.

Contests are situations in which each participant expends resources to win a valuable prize. When resorting to warfare, values and lives are destroyed. The digital world has changed warfare not only in terms of the destructive power of the weapons and direct damage to the efficient use of the technology-dependent weapons of the opponent but also indirectly causing paralysing effects on the society at large. By its logic, a cyber attack represents a pre-emptive offensive, typically a remote action employing digital technologies to damage the social and/or military capabilities of an enemy. As cyber capability represents an instrument prior to a war with conventional weapons, modern warfare may consequently be viewed as a multi-stage game. A war with conventional weapons tends to be preceded by a cyber war. A static one-stage approach, therefore, does not appear appropriate.

There are a number of excellent surveys on economic theories of conflicts, including Jackson and Morelli (2009), Garfinkel and Skaperdas (2012), and Baliga and Sjöström (2013). The theoretical literature on cyber wars employing methods commonly used in economic research, however, appears non-existent. This paper develops a theory of conflict where countries invest in both cyber technology and conventional weapons as complementary military inputs. As far as the author is aware, the current paper is the first to use a formal economic approach in the analysis of cyber war. However, the model studied in this paper has links to the literature on contests and sabotage. Cyber strike can indeed be viewed as a special kind of sabotage, as it directly reduces the effectiveness of conventional arms. Papers on sabotage include Konrad (2000), Chen (2003), Beviá and Corchón (2006), Muenster (2007), Amegashie (2012), and Chang and Luo (2017), among others. Chowdhury and Guertler (2015) have provided a comprehensive review of the literature on contests and sabotage and a more extensive list of references. The contestants face a single prize for the winner and a prize of lesser value for losers. They are assumed to choose an action, an "effort" boosting the probability of winning, and an action of sabotage, reducing the probability of winning by the contestant, both determining the contest success function for each player and summing up to one.

Though our cyber war approach has a similar flavour with the economic literature on sabotage, there are differences. While the sabotage papers consider one-time decisions, our approach leads to sequential decision-making with a potential first-mover advantage in terms of a pre-emptive strike. The model therefore allows for asymmetries between the hostile countries to produce cyber capabilities. The return on cyber investment in terms of the probability of winning the war is strictly convex in its size. This is the remarkable property of the model. Convexity makes cyber technology a first-ranked military investment. In the conventional theory of conflict, the return on the investment effort in terms of the marginal increase in the probability of victory is concave and subject to diminishing returns. Moreover, while the papers on sabotage state that expectations of being sabotaged have a discouraging effect (causing the participants to reduce their effort), this is not the case in the current model.[4]

Access to a cyber attack raises new questions. First, how worthwhile is it to invest in conventional weapons if countries can resort to cyber instruments? Second, does the answer depend on the differences in cyber capability? Third, what are the implications for arms race and the probability of warfare? Fourth, is it always the case that a cyber war is followed by a war with conventional weapons? Fifth, does the threshold to a cyber war differ from that of a conventional war? Sixth, how much is it optimal to invest in the cyber capability if the expected success differs between the conflicting parties? These are the issues to be analysed in the current paper and some of the answers turn out to be unexpected.

[4] As Chowdhury and Guertler (2015) explicate, sabotage activities are common in various contexts of life and the economy. In the soccer world, one example is the case of Lionel Messi of F.C. Barcelona: whenever he obtains the ball, the dominating strategy of the opposing team appears to stop him physically kicking his feet, as he is faster than most the other players.

The roadmap of the model world of the paper is as follows. The cost of war is first introduced in the standard model of contests, but in a non-standard way. Then, an investment in cyber technology is introduced into this model in terms of the probability of being victorious in warfare. The investment in cyber capability is considered risky in terms of the outcome of the development effort. The outcome is private information for each country. The country that turns out to be more successful finds that it has the option of initiating a cyber attack against the enemy, but without knowing whether the enemy has been successful in its rival development effort, too. 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.

The cost of war turns out to be crucial for the results. The equilibrium analysis in the war game is conditional on the cost of war relative to the payoff of being victorious. The results of the paper can be summarised as follows. First, two types of Nash equilibria are possible depending on the cost of war relative to the payoff from a victory. Both are subject of warfare. With a "small" cost of war and in the absence of cyber technology, armament in conventional weapons is large; with a "large" cost of war, it is smaller. Second, if countries expect to have access to equally effective cyber capabilities, their cyber investments are neutral in respect to the optimal investment in conventional weapons, but only when the cost of war is small. Such a symmetric case is not necessarily typical if countries have access to different technological skills and competence to start with. The third result is therefore concerned with an asymmetric case. It is shown that hostile countries choose to invest an equal amount of resources in their militaries, even when their cyber capabilities differ, but with a low perceived cost of war, they invest less than in the absence of cyber war technology. Surprisingly, they invest more when the perceived cost of war is bigger. The fourth result is rather dramatic: *cyber technologies can make the world unsafe*. The intuitive reason is that technological advances in cyber capabilities lower the cost of war in conventional weapons. The fifth result adds to the concerns of the cyber war given that cyber technologies are difficult and costly. Namely, heterogeneity in the success of cyber programs creates the option of a pre-emptive strike. In is shown that a low success probability of the cyber program encourages exercising the cyber attack option by a successful country to be followed by warfare with conventional weapons. A successful cyber program means a new set of beliefs of the winning probability in the conventional war. The odds have thus been changed in favour of the attacking country.

2 Economic model of armament

2.1 Conflict theory without a cyber technolocy

In the model world of this paper, there are two countries (players), *A* and *B*. Potentially resorting to their military power, they compete for a resource with a value of $v > 0$ with imperfectly specified property rights. The "winner takes it all" principle applies. Section 2.1 examines a complete-information simultaneous-move game with two stages.

The timeline and action space in the current section are as follows. In stage 0, both players allocate their resources to a conventional military capacity to maximise their expected payoff. The investment

costs for conventional weapons are denoted by x and y for countries A and B, respectively.[5] In stage 1, both countries decide whether to resolve the conflict by war or not.[6] This section summarises the equilibrium in the baseline model of the contest theory and provides important qualifications for it in terms of the cost of war. It also shows that depending on the perceived cost of war relative to the payoff from victory, two types of equilibria in terms of armament can arise. Section 2.1 is followed by Section 2.2, which outlines a complete-information sequential game where both players are assumed to have access to a costly cyber program for the purpose of developing cyber weapons.

Let the probabilities of winning a war in the last stage of the war game be denoted by $P(A)$ and $P(B)$. The well-known 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, yielding the contest success functions

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

This model was suggested by Tullock (1967, 1980) and it has long been the standard approach in modelling the conflicts. Subsequently, it has been discussed and elaborated by a number of authors in particular by Hirshleifer (1989); Pérez-Castrillo and Verdier (1992); and further developed and evaluated by Nti (1997, 1999); Konrad (2009); and Chowdhury and Sheremeta (2011) and others.[7]

We notice 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 remarkable property of the contest success function is that the value of the marginal unit of arms for a country is 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!

[5] A linear cost is needed for technical reasons if only to solve the model analytically 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 in the later section.

[6] The possibility of a unilateral withdrawal is excluded.

[7] As discovered by Konrad (2009), an early solution of a structurally equivalent problem in the context of proportional competition was given by Mills (1961). We notice that the literature has recognised the asymmetry between an offensive war and a defensive one (Acre et al. 2012). In our model, the distinction becomes relevant if the costs of war differ. Slayton (2016/2017) has warned of overconfidence in the offensive advantage as it can create a "cult of the offensive" with potentially tragic results.

Another question is whether it is worthwhile to fight. Therefore, the model is adjusted for the costs of a mutual war if one takes place. [8] The cost functions are assumed to be identical and depend on *the military strength of the enemy*. They will be denoted by $C(y)$ and $C(x)$, respectively, with $C'(x) = C'(y) > 0$. [9] The expected *ex ante* payoffs of the war game to the countries involved are

$$E_0(\pi_A) = P(A)v - x - C(y) \quad (3)$$

$$E_0(\pi_B) = P(B)v - y - C(x). \quad (4)$$

In the two-stage war game, the solution of the last game must be found first in the spirit of backward induction. Suppose for a moment that the countries *A* and *B* can settle the issue peacefully, with both obtaining half of the resource, $\left(\pi_A = \frac{v}{2}, \pi_B = \frac{v}{2}\right)$ where (π_A, π_B) denote the *ex post* payoffs to each country, respectively. In such a naive trust game, neither side needs to invest in a military capacity in stage 0, $x = y = 0$. The outcome is Pareto-efficient.[10] However, it cannot be an equilibrium if peace is not contractible and the commitment to it is not credible.[11] Both countries would have an incentive to opportunistically make an investment in arms, attacking the non-investing country to gain exclusive access to the resource. If the defender has no military capacity, the cost of war for the offensive country is zero while it is positive for the defending country. In the absence of trust between the players, both thus end up making military investments in stage 0, regardless of whether the issue is settled by war or by negotiation subsequently in stage 1.

In order to highlight the effect of the cost of war on the results, assume first that the cost of war is zero. As commitment to zero-investment is not credible, both invest. In stage 1, the investments are sunk and as the cost of war is zero, the countries definitely fight. The *ex ante* and the *post investment* expected payoffs from investments and the subsequent warfare are

$$E_0(\pi_A) = E_1(\pi_A) = \frac{x}{x+y}v - x \quad (5)$$

[8] The cost of war was also introduced in the earlier work on conflicts, cf. Baliga and Sjöström (2013). However, the models with a cost of war have taken it to be constant and unrelated to the destructive power of the enemy. Once it is recognised that the cost of war results from the enemy's military capacity, it plays a more important role in the war games.

[9] The purpose of a cyber attack is to destroy part of the military capacity of the enemy. In the subsequent sections, the damage effect will be introduced in the expressions for the cost of war.

[10] The question has been raised in the literature as to why perfectly rational agents do not peacefully negotiate outcomes and why would they sometimes fight costly wars. The Coase theorem seems to rule out wars as free negotiation should lead to a surplus-maximising outcome. The question then is whether the conditions for the Coase outcome are valid. Such thought leads to analyses on imperfect commitment and incomplete information, starting with Brito and Intriligator (1985) and surveyed by Baliga and Sjöström (2013).

[11] Jackson and Morelli (2009) point out that commitment problems are probably the single most pervasive reason for bargaining failure.

$$E_0(\pi_B) = E_1(\pi_B) = \frac{y}{x+y}v - y. \quad (6)$$

Carrying out the maximisation of the expected returns (5) and (6) with respect to investments in stage 0, the reaction functions are

$$x = -y + \sqrt{yv},\ y = -x + \sqrt{xv}. \quad (7)$$

Then, the Nash equilibrium in investments in conventional weapons is given by a pair (x^0, y^0), satisfying[12]

$$x^0 = y^0 = \frac{v}{4}. \quad (8)$$

Natural as it is, the optimal investment is less than the available prize, $\frac{v}{4} < v$. A high prize *v* justifies a high investment. It follows that both countries have the same probability of winning the war, *P*(*A*) = *P*(*B*) = 1/2. In the absence of a cost of war, the countries fight, having access to an expected payoff which is solved to be $\frac{v}{4}$. As the winner takes it all, the *ex post* payoff to the winner, however, is $3v/4$ while it is $-v/4$ for the loser.

The existence of a Nash equilibrium in investments is no issue. By continuity, a Nash equilibrium also exists when a war is costly but the cost of war is "small", say $C_s(x) > 0, C_s(y) > 0$, when $x > 0, y > 0$. Introducing the cost of war into the model, the expected *ex ante* returns are

$$E_0(\pi_A) = \frac{x^N}{x^N+y^N}v - x^N - C_s(y^N) \quad (9)$$

$$E_0(\pi_B) = \frac{y^N}{x^N+y^N}v - y^N - C_s(x^N). \quad (10)$$

It is the cost of war that results in mutual externalities in the war game. As one is looking for a Nash equilibrium of the war game, we have denoted these investments by x^N and y^N. It turns out that the investments in the Nash equilibrium are independent of the cost of war, $x^N = y^N = \frac{v}{4}$ when the cost of war" is small". Given the investments, the expected *post-investment* payoffs from warfare are therefore

$$E_1(\pi_A) = \frac{v}{4} - C_s(x^N) = E_1(\pi_B) = \frac{v}{4} - C_s(y^N) < \frac{v}{4}, \quad (11)$$

while the realised *ex post* payoff for the winner, if *A*, is $3v/4 - C_s(y^N)$ and $-v/4 - C_s(x^N)$ for the loser, if *B*.

Notice that for any cost of war, the *ex post* payoffs would be greater under peaceful contracting than the expected payoffs from fighting,

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

$$\pi_A = \frac{v}{2} - x^0 = \frac{v}{4} > \frac{v}{4} - C_s(x^N). \quad (12)$$

$$\pi_B = \frac{v}{2} - y^0 = \frac{v}{4} > \frac{v}{4} - C_s(y^N). \quad (13)$$

The ultimate reason for not entering into a peaceful contract comes from outside the model. It is easiest to think that it is the imperfect commitment. Then, in the symmetric Nash equilibrium, both countries invest *v*/4 in their militaries in stage 0 and end up fighting in stage 1 if the expected *ex post* payoffs are positive, $E_1(\pi_A) > 0$ and $E_1(\pi_B) > 0$.The benefit/cost ratio has to be sufficiently high, to justify the warfare,

$$\frac{v}{C_s(x^N)} > 4, \qquad \frac{v}{C_s(y^N)} > 4. \quad (14)$$

When costly, wars are about externalities. When the conditions (14) hold, the externalities, however, are not sufficiently great to make the countries abstain from fighting.

Assume now instead that the cost of war is larger, $C_l(i) > C_s(i)$ for all $x^N > 0, y^N > 0$ violating conditions (14). Then, the no-fight solution appears attractive. With (x^N, y^N), the *post-investment* incentive conditions for a no-fight equilibrium, adjusted for the costs of war, are

$$E_1(\pi_A) = \frac{x^N}{x^N + y^N} v - x^N - C_l(y^N) \leq 0 \quad (15)$$

$$E_1(\pi_B) = \frac{y^N}{x^N + y^N} v - y^N - C_l(x^N) \leq 0. \quad (16)$$

What the conditions (15) and (16) dictate is that *the expected payoffs from fighting* in stage 1 have to be negative, or at most zero, for a no-fight equilibrium to arise. A greater cost of war relative to the available payoff then makes the players pay attention to the mutual externalities.

If the benefit/cost ratios from fighting do not satisfy the conditions (14), the no-fight conditions (15) and (16) suggest that a peaceful equilibrium may appear lucrative. War is too expensive. However, when the no-fight conditions are non-binding, the solution $x^N = y^N = \frac{v}{4}$ cannot represent an equilibrium. The two countries will obviously find it optimal to choose lower investments *ex ante*, say $x' < x^N, y' < y^N$, if only to save in investment costs. Under peaceful contracting, their payoffs are increased to $\frac{1}{2}v - x' > \frac{1}{2}v - x^N, \frac{1}{2}v - y' > \frac{1}{2}v - y^N$. This is not, however, the only mechanism involved. With lower investments in military, the perceived cost of war is reduced, too. As long as the no-fight conditions are not binding, it is optimal (even individually) for both countries to have a lower investment in armament. With a sufficient low cost of war, the no-fight conditions (15) and (16) become ultimately binding, say at some x', y'. Countries would be indifferent between *peace and war*. One plausible argument is that a country cannot pick up its share of the prize without fighting, even in the case of indifference. In such an equilibrium, the investment levels (x', y') are then determined from

$$\frac{1}{2}v - x' - C_l(y') = 0 \qquad (17)$$

$$\frac{1}{2}v - y' - C_l(x') = 0. \qquad (18)$$

We have included the costs of war in (17) and (18) to pinpoint the view that commitment to a no-fight equilibrium can be seen as non-credible. We have arrived at a remarkable conclusion that *disarmament can make warfare more attractive by reducing the cost of war*. Individually reducing the investment even below x', y' will not be an equilibrium strategy for either country. The probability of a war victory with such a strategy will be reduced to less than half while the cost of war would exceed the cost of war for the enemy. Therefore, neither country has an incentive to deviate from (x', y'), satisfying the two conditions (17) and (18). This establishes the existence of the second type of Nash equilibrium in the war game.

How much do the countries invest in the second type of Nash equilibrium? To illustrate, assume that the cost of war is given by $C_l(x') = \gamma x', C_l(y') = \gamma y', \gamma > 0$. Solving for x', y' from (17) - (18), one obtains $x' = y' = \frac{v}{2(1+\gamma)}$. The conditions $x' < x^N, y' < y^N$ are satisfied if the cost of war is sufficiently high, $\gamma > 1$.

We summarize the findings as follows,

Proposition 1. *In the war game, there can be two Nash equilibria in terms of armament investment. If the no-fight conditions (15) and (16) do not hold at $x^N = y^N$, the solution $x^N = y^N = \frac{v}{4}$ qualifies as a Nash equilibrium in armaments. There is fighting in equilibrium. If the conditions (15) and (16) hold at the solution (x^N, y^N), another Nash equilibrium exists with $x' < x^N, y' < y^N$, and in the absence of commitment, the countries fight in this equilibrium, too.*

To state the above results intuitively, under a low cost of war relative to the prize available, the players abstract from the mutual externalities resulting from a war when *deciding* on armament and the peace and war. However, war is ultimately about mutual externalities. Under a greater cost of war relative to the prize available, the players settle in a game equilibrium where the cost of war is effectively internalised.

2.2 Investment in arms with access to a cyber technology[13]

2.2.1 Action space and assumptions

The paper now introduces cyber capability as a new warfare instrument. The action space in stage 0 is two-dimensional: both countries expecting a military confrontation invest in both the conventional military capacity and in the cyber capability. Those investments are denoted by (*x*,*a*) for country *A* and by (*y*,*b*) for country *B*. When the model is extended to a two-instrument framework, the armament expenditures are given by $M^A = x + c(a), M^B = y + c(b)$.

The success of the cyber program is subject of uncertainty. In stage 1, the investment probabilistically yields a cyber capability. The outcome of the cyber program is private knowledge: the success or

[13] Only pure strategies are examined. The resulting equilibria are of the Bayesian Nash type.

failure of the enemy is not observable. In stage 2, a successful country decides on whether to launch a cyber attack against the enemy. The decision is conditional on the expectations concerning the success of the enemy. In stage 3, the cyber war is followed by a war with conventional weapons, provided that the expected payoff to at least one of the countries is positive.

The model to be developed is an extension of the Tullock-model to the case of multiple investments and sequential decision-making in choosing between peace and war. Several assumptions are introduced as follows.

Assumption 1. *The costs of a cyber program,* $c(a), c(b)$ *are strictly convex with* $c'(0) = 0, c'(a) > 0, c''(a) > 0, c'(b) > 0, c''(b) > 0.$ [14]

To make the analysis tractable, simplifying assumptions in the model world are introduced. As the confrontation in the model world is of a one-shot type, it is assumed that:

Assumption 2. *The beliefs concerning the success of the cyber programs are exogenous.*

Beliefs concerning the enemy's access to cyber weapons are formed in stage 0. In the current section, two scenarios on belief formation are examined. In the first, both countries are assumed to have *confident expectations*, not only of their own success but also of the success of the enemy in the development of cyber weapons. In the second scenario, one country expects to have *a superior ability* in the development of the cyber instrument. Based on such beliefs, two fundamental results will be reported.

Assumption 3. *The success probability of a cyber program is given by* $0 < p < 1$.[15]

When successful, the damage caused in a cyber attack by country *A*, say, on the military strength of country *B*, is assumed to be proportional to the scale of the cyber cyber program, and given by λa where $\lambda > 0$ is a parameter. Similarly, if country *B* is successful in the cyber program, it can cause damage $\lambda b > 0$ to country *A*. The damage of a cyber attack thus depends on the scale of cyber investments (*a*,*b*).[16]

Assumption 4. *With a successful cyber program, the damage effects on the military capacity of the enemy on countries A and B are proportional to cyber investments and are given by*

[14] One can think that investments in conventional weapons employ existing technologies while the cyber capability necessitates the development of new technologies with increasing costs.

[15] Making the success probability dependent on the investment in the cyber program complicates the modelling task too much.

[16] In the model world of the current paper, the damage caused by a cyber attack concerns military targets as assets in the civil sector are not introduced.

$$d_A = \lambda a, \;\; d_B = \lambda b, \qquad \lambda > 0.$$

What is left of the armament capacity after a successful cyber attack is thus $x - \lambda bx = x(1 - \lambda b)$ for country *A*, and $y - \lambda ay = y(1 - \lambda a)$ for country *B*, respectively.

2.2.2 Interaction between cyber and conventional armament

The following research agenda is developed. We 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*, $\lambda a = \lambda b$. Then, we examine the Nash equilibrium under different costs of cost of war relative to the potential prize.

With the stated effects of a cyber attack on the quality of the conventional military, one of the Nash equilibria has to satisfy the following conditions:

$$max_{x,a}\, E_0(\pi_A) = \frac{x(1-\lambda b)}{x(1-\lambda b)+y(1-\lambda a)} v - x - c(a) - C(y(1 - \lambda a)) \qquad (19)$$

$$max_{y,b}\, E_0(\pi_B) = \frac{y(1-\lambda a)}{y(1-\lambda a)+ x(1-\lambda b)} v - y - c(b) - C(x(1 - \lambda b)). \qquad (20)$$

There are four first-order conditions to determine such a Nash equilibrium, to be called (x^c, y^c, a^c, b^c).[17] Evaluating the partial derivatives the equilibrium conditions are given by

$$MP_x = \frac{y(1 - \lambda a)(1 - \lambda b)}{m^2} v - 1 = 0 \qquad (21)$$

$$MP_y = \frac{x(1 - \lambda a)(1 - \lambda b)}{m^2} v - 1 = 0 \qquad (22)$$

$$MP_a = \frac{\lambda xy(1 - \lambda b)}{m^2} v + \lambda y C'\big(y(1 - \lambda a)\big) = c'(a) \qquad (23)$$

$$MP_b = \frac{\lambda xy(1 - \lambda a)}{m^2} v + \lambda x C'\big(x(1 - \lambda b)\big) = c'(b). \qquad (24)$$

We have denoted $m = x(1 - \lambda b) + y(1 - \lambda a)$. By imposing symmetry, $x^c = y^c, a^c = b^c$, one obtains

$$x^c = y^c = \frac{v}{4} \qquad (25)$$

[17] The approach is built to satisfy the subgame perfectness.

$$\frac{\lambda v}{4(1-\lambda a^c)} + \lambda x^c (C'\big(x^c(1-\lambda a^c)\big) = c'(a^c), \quad a^c = b^c. \tag{26}$$

To qualify for a Nash equilibrium, this solution must satisfy the conditions

$$\frac{x^c(1-\lambda b^c)}{x^c(1-\lambda b^c)+y^c(1-\lambda a^c)} v - x^c - c(a^c) - C\big(y^c(1-\lambda a^c)\big) > 0$$
$$\frac{y(1-\lambda a^c)}{y^c(1-\lambda a^c)+\ x^c(1-\lambda b^c)} v - y^c - c(b^c) - C\big(x^c(1-\lambda b^c)\big) > 0$$

In a symmetric equilibrium, the conditions are reduced

$$\frac{v}{c(a^c)+C\big(y^c(1-\lambda a^c)\big)} > 4, \qquad \frac{v}{c(b^c)+C\big(x^c(1-\lambda b^c)\big)} > 4. \tag{27}$$

These conditions dictate that the sum of the costs of a cyber program and the cost of war cannot be too large relative to the potential prize available. These conditions are extensions to what was found in Section 2.1 above without cyber investment. The first observation is that in such a symmetric Nash equilibrium, the investment in conventional armament is unrelated to the cyber capability, as $x^c = y^c = v/4$,

Proposition 1. *(Neutrality of cyber in an equilibrium with war). When the cost of war is sufficiently small and 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. From above.

For an intuition of this case, one should notice that the contest success functions are homogeneous of degree zero in $(1-\lambda a)$ and $(1-\lambda b)$. We notice that although the cyber capabilities are neutral in respect to the optimal conventional armament, the cost of war in the last stage of the game is reduced, intensifying the fighting incentive.

To illustrate the optimal cyber investment in such a Nash equilibrium, we first consider a case where the cost of war is zero and we introduce a quadratic cost function, say $c(a) = \frac{1}{2}\tau a^2, \tau > 0$. Then, the first-order condition for the cyber investment of country *A* after imposing symmetry, $b^c = a^c$, is reduced to $\frac{\lambda v}{4} = (1-\lambda a^c)\tau a^c$. The solution for the cyber investments is

$$a^c = b^c = \frac{1 \pm \sqrt{1-\lambda v/\tau}}{2\lambda}. \tag{28}$$

Conditional on $1-\frac{\lambda v}{\tau}>0$, both roots are real and positive. Because $\partial E_0(\pi_A(x^c,y^c,a,b^c))/\partial a>0$ at $a=0$, only the smaller root qualifies as the maximising value. It thus represents the solution $a^c=b^c$ in the Nash equilibrium in the absence of the cost of war. The natural comparative statistics include $\frac{\partial a^c}{\partial v}>0, \frac{\partial a^c}{\partial \tau}<0$ while the sign of $\frac{\partial a^c}{\partial \lambda}$ remains uncertain.

When the cost of war is zero, only one type of equilibrium exists. By continuity, a Nash equilibrium must also exist when the joint costs of war and the cyber program are "small" relative to the payoff from victory. Both countries, if successful in their cyber programs, therefore expect to launch a cyber attack against each other, subsequently anticipating a mutual war with conventional weapons. The equilibrium to be considered is analogous to the first type of Nash equilibrium in Section 2.1. The perceived joint costs are sufficiently limited so that fighting is expected to take place. The existence of such an equilibrium is guaranteed when the value of the prize, v is sufficiently high relative to the joint costs.

However, in the symmetric case with a greater cost of war, we again suggest that the equilibrium is of another type. Suppose thus that the perceived costs relative to the prize are sufficiently large at the above solution $(x=x^c, y=y^c, a=a^c, a=b^c)$ so as to make it not worthwhile to launch a cyber attack in stage 2 and fight in stage 3, $E_0(\pi_A)\leq 0, E_0(\pi_B)\leq 0$. This means that (x^c,y^c,a^c,b^c) cannot represent an equilibrium when the cost of war is high. However, another type of Nash equilibrium is available. As it is expected that no war takes place, it is optimal even individually to cut armament. The effects of cyber capability can be evaluated as follows. With positive cyber investment, the no-fight condition becomes binding at a higher level of investments (x,y) than in Section 2.1, say at (x'',y'') with $x'<x''<x^c,\ y'<y''<y^c$. The conclusion holds for a cyber program of *any (positive) size* in equilibrium $(a>0, b>0)$.[18] This means that under cyber technology, the *post-investment* incentive conditions for a no-fight equilibrium, analogous to conditions (15) and (16), become binding at a higher level of armament than in the absence of cyber abilities. The result follows from the impact of cyber ability on the cost of conventional warfare and the cost of the cyber program. *A successful cyber program makes wars more likely by lowering the cost of war when conventional weapons are used.* In the symmetric Nash equilibrium of the first type, the countries fight in any case. In the second type, the condition for fighting is met at the higher level of armament. Thus,

Proposition 2. *(Armament effect of cyber when the cost of war is large). When the sum of the perceived costs of war and a cyber program is large relative to the potential prize and countries expect to have access to equally effective cyber capabilities, their cyber capabilities increase the incentive to enhance the investment in conventional weapons compared to when no cyber technology is available.*

The purpose of the rest of the paper is to explore what other results are attainable in such a two-instrument framework. The symmetric case studied above is destroyed *if one of the countries expects to be superior in creating the cyber capability while the other country expects to be inferior*.[19] With homogenous beliefs in the cyber capability, it is implied that the access to a mutual cyber attack is neutral in respect to the action space concerning the investment in conventional weapons with a low

[18] We consider the cyber investment in equilibrium later in the paper.

[19] Such asymmetry may arise if country *A*, say, has better resources in terms of inherited technological competence to be allocated to the cyber program.

cost of war while an incentive to enhance investment was created by a higher cost of war. With non-homogenous beliefs, however, such a strong result, is not available. In the case of asymmetric beliefs, an unexpected result is reported.

Proposition 3. *In a Nash equilibrium of both types, countries with superior and inferior cyber abilities 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. Suppose that country *A* expects to be superior in its cyber program, while both expect that country *B* will not be able to create such a capability. It holds that

$$E_0(\pi_A) = \frac{x}{x+y(1-\lambda a)}v - x - c(a) - C(y(1-\lambda a)) \tag{29}$$

$$E_0(\pi_B) = \frac{y(1-\lambda a)}{y(1-\lambda a)+x}v - y - C(x). \tag{30}$$

Solving for the Nash equilibrium (of the first type), the optimal investments in the conventional weapons are

$$x^c = y^c = \frac{(1-\lambda a)v}{(2-\lambda a)^2} < \frac{v}{4} \tag{31}$$

The inequality follows from that when $\lambda = 0$, $x^c = y^c = \frac{v}{4}$. Moreover, for $\lambda > 0$,

$$\frac{\partial\left[\frac{(1-\lambda a)v}{(2-\lambda a)^2}\right]}{\partial\lambda} = -\frac{a^2\lambda v}{(2-\lambda a)^3} < 0.$$

QED

Notice the reduced cost of war in (29) only for country *A*, $C(y(1-\lambda a)) < C(y)$, as a result of the successful cyber strike. The result holds for both types of Nash equilibria, though they differ in terms of the scale of the investment in conventional armament.

Proposition 3 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). Once the enemy invests less, so does the other country. Intuition is readily available. The country with the superior cyber capability can economise in its arms investment because it knows that part of the military capacity of its enemy can be destroyed. Furthermore, even with this knowledge, 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, it is the superior country that has the greater probability of winning the war

$$P(A) = \frac{1}{2-\lambda a} > \frac{1-\lambda a}{2-\lambda a} = P(B).$$

According to Proposition 3, country *B* ends up investing the same amount as the superior 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 equalised in the Nash equilibrium with the marginal costs,

$$\frac{\partial P(A)}{\partial x} v = 1, \frac{\partial P(B)}{\partial y} v = 1.$$

Notice that country *B* saves resources by not investing in the cyber program. Is the cyber program reasonable for country *A* from the cost/benefit point of view? Not necessarily: the condition is that the cost of the program shall not be too high. Evaluating the expected payoff for country *A* with and without the cyber program, the condition can be stated as

$$c(a^c) < \left[\frac{x^c}{x^c + y^c(1-\lambda a^c)} - \frac{x^N}{x^N + y^N}\right] v - (x^c - x^N) + C(y^N) - C(y^c(1 - \lambda a^c). \qquad (32)$$

In the next sections, the case is considered where condition (32) is assumed to hold. There, questions are raised about how much to optimally invest in the cyber program and whether it is worthwhile to initiate a cyber attack.

From the above analysis under asymmetric cyber abilities, a dramatic conclusion arises. Whether there is a mutual cutback in the armament in conventional weapons or not, a war with conventional weapons is not eliminated. Unexpectedly and in contrast, it follows that cyber warfare makes the wars in conventional weapons less costly and less destructive and therefore *more likely*. To emphasize this result, we summarize

Corollary 1. *A successful cyber program makes wars more likely by lowering the cost of war in conventional weapons when the cyber capabilities differ among the countries involved in the hostilities.*

3 Cyber attack as a first-mover pre-emptive strike

3.1 Uncertainty of the success of the enemy

This section considers a cyber attack as an option to a pre-emptive strike arising from asymmetry in the development success of the cyber program. The action space in stage 0 is again two-dimensional: both countries expecting a military confrontation invest in both the conventional military capacity and in the cyber capability. Moreover, the beliefs concerning the enemy's access to cyber weapons are formed in stage 0. We let $p > 0$ denote the success probability of a cyber program, assumed to be common knowledge. Following the cyber investments, there are four possible outcomes from the *ex ante* perspective to be revealed in stage 1: 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. The case of information asymmetry arises. In stage 1, the game analyzed is therefore turned into one in incomplete information as the success in the program is private information. The successful player does not know the type of

enemy in this round. Moreover, and as a consequence, it expects either a high or low cost of war. In stage 2, a successful country decides on whether to launch a cyber attack against the enemy. The decision is conditional on the expectations of the enemy's success. In stage 3, a war based on conventional weapons takes place if the cyber attack has taken place.

Intuitively, a first-mover strike in stage 2 can be particularly attractive when the success probability p is low because if A has succeeded, it expects that B has been successful at most with a low probability. This suggests that the probability of a first-mover attack may be high when the *ex ante* success probability is small.

Consider therefore, the action space of the successful country in stage 2. If this is country A, for example, it knows that it has successfully completed its cyber program, but it faces uncertainty concerning the success of its enemy. It has to decide in stage 2, whether to launch a cyber attack against country B knowing that country B with cyber capability will (say immediately) retaliate with a cyber counterattack followed by warfare with conventional weapons in stage 3. By stage 2, all investments (x,y,a,b) have been undertaken (optimized in stage 0) and are bygone. Denote their values by (x^*, y^*, a^*, b^*).

Let $E_2(\pi_{A1})$ denote the expected payoff on a cyber attack by country A in stage 2 based on the perceived first-mover advantage, and let $E_2(\pi_{A0})$ denote the expected payoff on a cyber attack on the condition that country B has been successful in its cyber program, too. With the investments (x^*, a^*) as bygone, the incentive condition for country A to exercise its option to initiate a cyber attack in stage 2 to be followed by the warfare in conventional weapons is given by

$$pE_s(\pi_{A0}) + (1-p)E_2(\pi_{A1}) \geq 0 \tag{33}$$

where

$$E_2(\pi_{A0}) = \frac{x^*(1-\lambda b)}{x^*(1-\lambda b^*)+y^*(1-\lambda a^*)} v - C(y^*(1-\lambda a^*)) \tag{34}$$

captures the effect of a mutually successful cyber program and

$$E_2(\pi_{A1}) = \frac{x^*}{x^*+y^*(1-\lambda a^*)} v - C(y^*(1-\lambda a^*)) \tag{35}$$

captures the case where only country A was successful. Clearly, $E(\pi_{A1}) > E(\pi_{A0})$.

Denote the probabilities of the victory of war by

$$P^*(A) = \frac{x^*}{x^* + y^*(1-\lambda a^*)}, P^*(B) = \frac{y^*(1-\lambda a^*)}{y^*(1-\lambda a^*) + x^*(1-\lambda b^*)}.$$

Inserting into (30), the condition for exercising the attack option under uncertainty can be stated in terms of the success probability,

$$p \leq p^* = \left(\frac{1}{\lambda b^*}\right)\left[1 - \frac{C(y(1-\lambda a^*)}{P^*(A)}\right]\frac{1}{P^*(B)}, \tag{36}$$

The condition (36) determines the threshold for exercising the attack option for country *A* based on the understanding of the potential cyber power of country *B* and the probability of its victory in war (stage 3).

If the probability of success of the enemy is greater, $p > p^*$, the best move is not to exercise the attack option. The best response of the enemy, country *B*, is to fight back, as no option of surrendering is assumed. Its expected payoff depends on whether it was successful, too, in its cyber program and whether it is able to cause damage to the attacker with its counterattack.

We report:

Proposition 4. *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.*

The result is logical: a country that has been able to acquire the cyber capability knows that the enemy may have a similar capability but with a *small* probability.

A convenient interpretation a successful cyber program is available in the current model: it means a new set of beliefs of the winning probability in the Tullock model of the conventional war. The odds have been changed in favour of the attacking country. [20]

3.2 Optimal investment in cyber: the superior country

Within the context of our model world, we now turn to look at a country expecting to be superior in the cyber capability and analyse the question how much it will invest in a cyber program. Suppose it is the country *A*. We first notice the implication of the ability of a cyber strike to create a proportionate damage to the military of the enemy,

Lemma 1. *The probability of winning the war is strictly convex in the size of the investment in cyber.*

Proof. Taking the partial derivatives of the winning probability in (19), it holds for country *A* that

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

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

[20] The superior country may threaten the inferior country with a cyber attack, which may lead to bargaining. This possibility is not considered in the current paper, however. The bargaining protocol should include negotiations on the restrictions of conventional weapons imposed on the weaker country, which would take the analysis to a side track for the purposes of the current paper.

. QED

It follows that the superior country has a strong incentive to acquire the destructive cyber capability, hoping it will enhance the probability of winning the war with conventional weapons in the final stage of a conflict.

With one country being expected to be superior in its cyber program while the other is not, a Nash equilibrium has to satisfy the conditions

$$max_{x,a}\, E_0[\pi_A(x,y,a)] = \frac{x}{x+y(1-\lambda a)}v - x - c(a) - C(y(1-\lambda a))$$

$$max_y\, E_0[\pi_B(y)] = \frac{y(1-\lambda a)}{y(1-\lambda a)+\ x}v - y - C(x).$$

Country *A* therefore faces a cost/benefit analysis of how to allocate its military resources between conventional weapons and the cyber capability. Intuitively, conventional investment can be cut when part of the military budget is allocated to cyber weapons. Moreover, as part of the enemy's military is destroyed, the cost of war for the superior country is reduced. The optimal investment in cyber is, however, controlled by its cost. One can distinguish two cases. One possibility is a corner solution where the cost of the cyber program, though increasing with the scale of the cost, yet allows the advanced country to invest to the extent that the whole military capacity of its enemy can be destroyed. This is the case where the optimal cyber satisfies

$$a^* = \frac{1}{\lambda}.$$

The necessary and sufficient condition for such a case is that $MP_a\left(\frac{1}{\lambda}\right) > c'\left(\frac{1}{\lambda}\right)$. Its implications for armament investments are strong. The probability of victory in war for country *A* becomes 1 and is obtained with a small army size, $x^* = \varepsilon > 0$. The expected *ex ante* payoff for country *A*, then, is $E_0[\pi_A(x,y,a)] = v - \ \varepsilon - c\left(\frac{1}{\lambda}\right)$. Cyber weapons are used as substitutes for conventional weapons. Such a world is characterized by a ruling superpower. A monopoly on cyber weapons shows up as a frightening view.

With higher costs of a cyber problem, only an interior solution appears feasible with $MP_a(a^*) = c'(a^*)$, thus $a^* < \frac{1}{\lambda}$.[21] The solution satisfying $\lambda a * < 1$ is indeed is more interesting. Notice first that at the origin with $a = 0$, $MP_a > 0$ while $MC_a = 0$. At a low level of a, MP_a is therefore exceeds MC_a. With a higher level of a, the MC_a-function reaches the MP_a-function from below. The internal equilibrium is obtained if the MC_a-function cuts the MP_a-function from below at a point where $a^* < \frac{1}{\lambda}$. Therefore, *when a country expects to acquire a superior cyber capability, there is a unique solution for its optimal cyber investment. The cost of the cyber program determines whether the solution is an interior one or whether it is at a corner. The incentive to have great cyber capability is strong.*

[21] Even the plan for the "star war" during the Reagan administration in the USA turned out to be too expensive.

Such results based on the convexity of the payoff to modern weapons point to strong incentives to develop new instruments in an unsafe world with increasingly effective destruction power.

4. Final remarks

The current paper has established some regularities concerning modern warfare. The key results can be summarised follows. The role of the cost of war relative to the payoff from victory appears decisive for the characterisation of armament in equilibrium. When extended to the case of access to cyber technology, the distinction between symmetric and asymmetric cases is important.

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 when the benefit/cost ratio of warfare is high. In a symmetric Nash equilibrium, countries with superior and inferior cyber abilities have incentives to invest an equal amount in conventional weapons, but this is less relative to the case when cyber technology is not expected to be available for either of them. This is good news. Unfortunately, a successful cyber program appears to increase the likelihood of war by lowering the cost of war with conventional weapons. Moreover, a low success probability of the cyber R&D program encourages the successful country to exercise its cyber attack option to be followed by warfare in conventional weapons. When a country expects to acquire a superior cyber capability, there is a unique solution for the optimal cyber program in the model world studied in the paper. A dramatic corner solution is not excluded.

In the Georgian war, both cyber attack and conventional weapons were involved. Stuxnet made cyber war a reality in modern warfare. A cyber attack may have its limits for several reasons. The success of Stuxnet was conditional on several flaws in the cyber security of Iran. Moreover, once a cyber attack is accomplished, the operation reveals information to the target country, which may benefit from reverse engineering of the cyber instrument used in the operation. Finally, the attempts to hit North-Korea have apparently not been that successful. Yet, the cyber technology has huge potential in modern warfare.

In the Stuxnet attack, conventional weapons were not employed. Many observers believe that 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? To explain why the Stuxnet attack did not lead to a war with conventional weapons requires a reinterpretation of the prize available. If the cyber attack is effective enough in its destruction power, that may represent a sufficient prize itself.

References

Amegashie, J.A. (2012). "Productive versus Destructive Efforts in Contests", *European Journal of Political Economy* 28(4), 461-468.

Arce, D.G., Kovenock, D., and Roberson, B. (2012). "Weakest-Link Attacker-Defender Games With Multiple Attack Technologies." *Naval Research Logistics* (NRL), *59*(6): 457–469.

Baliga, S., and Sjöström, T., (2013). "Bargaining and War: A Review of Some Formal Models", *Korean Economic Review* 29, 235-266.

Beviá, C., and Corchón, L.C. (2006). "Rational Sabotage in Cooperative Production with Heterogenous Agents." *The B.E. Journal of Theoretical Economics*, *6*(1): 1–27.

Brito, D., and Intriligator, M., (1985). "Conflict, War and Redistribution", *American Political Science Review*, 79, 943-957.

Chang, Y.-M., and Luo, Z. (2017). Endogenous Destruction in Conflict: Theory and Extensions", *Economic Inquiry* 55(1), 479-500.

Chen, K.-P. (2003). "Sabotage in Promotion of Tournaments." *Journal of Law, Economics and Organization, 19*(1): 119–140.

Choucri, N. (2012). *Cyperpolitics in International Relations.* MIT Press.

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

Chowdhury, S.M., and Gurtler, O. (2015). "Sabotage in Contests: a Survey." *Public Choice, 164*: 135–155.

Defense News. "Cyber Integral to US Kill/Capture Missions in 2016." Accessed 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.

Garfinkel, M.R., and Skaperdas, S., (2012). "Economic Perspectives on Peace and Conflict", in Garfinkel, M.R., and Skaperdas, S., (eds.), *The Oxford Handbook of the Economics of Peace and Conflict*, New York: Oxford University Press.

Jackson, M., O., and Morelli,M., (2009). "The Reasons for Wars. An Updated Survey", in C.Coyne (ed.), *Handbook on the Political Economy of War*, Elgar.

The Journal of International Affairs, Winter 2016, 70, No1.

Konrad, K.A. (2000). "Sabotage in Rent-Seeking Contests." *Journal of Law, Economics and Organization*, *16*(1): 155–165.

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

Mills, H.D. (1961). "A Study in Promotional Competition." In Frank M. Bass et al. (Eds.), *Mathematical Models and Methods in Marketing* (pp. 245–301). R.D. Irwin: Homewood. (Reprinted from *Research Paper No. 1-1-103*, December 1959, Mathematica: Princeton)

Muenster, J. (2007). "Selection Tournaments, Sabotage, and Participation." *Journal of Economics and Management Strategy*. *16*(4): 943–970.

Nti, K.O. (1997). "Comparative Statics of Contests and Rent-Seeking Games." *International Economic Review*, *38*(1): 43–59.

Nti, K.O. (1999). "Rent-Seeking with Asymmetric Valuations." *Public Choice*, *98*(3): 415–30.

Slayton, R. (2016/2017). "What Is the Cyber Offence-Defence Balance?", *International Security*, 41(3), 72-109.

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

Tullock, G. (1980). “Efficient Rent-Seeking.” In J.M. Buchanan, R.D. Tollison, & G. Tullock (Eds.), *Toward a Theory of the Rent-Seeking Society*, 97–112. College Station: Texas A&M University Press.

Peréz-Castrillo, J.D., and Verdier, T. (1992). “A General Analysis of Rent-Seeking Games.” *Public Choice, 73*: 335–350.

Sutherland, B. (2012). (ed.),. *Economist. Modern Warfare, Intelligence and Deterrence. The Technology That is Transforming Them*, London: Profile Books LTD.