Towards the Development of a Rationalist Cyber Conflict Theory

Dr. Sergio Castro

ABSTRACT

We believe there is a lack of a coherent Cyber Conflict Theory with adequate descriptive, predictive, and prescriptive capacities. We attribute this shortfall to the fact that the study of Cyber Conflict falls into two largely separate camps: International Relations and Information Security. International Relations experts study the phenomenon mostly using traditional conflict analysis models derived from the theory of conflict. On the other hand, Information Security experts focus on the tactical details of how cyber-attacks are conducted, but they are usually not involved in International Relations studies. The objective of this paper is to bridge this gap by linking the types of cyber-attacks both to their military consequences and their broader strategic consequences. To achieve this, we use Fearon's Bargaining Model of War to analyze the impact that offensive cyber operations have on the probability of winning a war, the cost of war, and the risk of war. We identify three types of cyber operations: Extraction, Modification, and Denial of Service. Our model shows that these three types of cyber operations may have significant impacts on the risk of war and the outcomes of war at the strategic and tactical levels.

1. THE CURRENT STATE OF CYBER CONFLICT THEORY

It has been 20 years since the Joint Task Force - Computer Network Defense (JTF-CND) was created[1], and yet we still see a lack of a coherent Cyber Conflict Theory with adequate descriptive, predictive, and prescriptive capacities. We attribute this shortfall to the fact that the study of Cyber Conflict falls into two largely separate camps: International Relations and Information Security. International Relations experts study the phenomenon mostly using traditional conflict analysis models derived from the theory of conflict. On the

Dr. Sergio Castro is currently the president of the Instituto de Ciberdefensa, and has 11 years of experience in information security, having worked in Microsoft, Qualys, Varonis, Elastica, Blue Coat, and Symantec. He has conducted training events and conferences on information security and cyber defense across the Americas, Europe, and Israel. He holds an M.S. in Economics, an MBA, and a PhD in Education from Universidad Abierta de San Luis Potosí, Mexico. He can be contacted at scastro@ciberdefensa.org and https://www.linkedin.com/in/castrosergio/.

other hand, Information Security experts focus on the tactical details of how cyber-attacks are conducted, but are not involved in International Relations. There have been attempts to bridge this gap, but they have been inconclusive. Applegate and Stavrou[2] developed a detailed Cyber Conflict taxonomy capable of describing in detail a cyber-attack. However, their model does not extend to the International Relations level since it cannot describe or predict the strategic or even the narrower military consequences of a cyber-attack. And this is exactly the crux of the problem: linking cyber operations to their military and broader strategic consequences.

Kello explains that "It is superfluous to state that the field of international security studies is skeptical of the existence of a cyber danger: it has barely acknowledged the issue, as reflected in the scant relevant literature."[3] Kello also states that "The costs of scholarly neglect of the cyber issue to the advancement of theory are apparent: when the range of empirical topics that theory is able to elucidate narrows, the academic enterprise inevitably enters a process of internal corrosion, which reveals itself in one or both of two ways—a loss of conceptual fertility or a reduced capacity for explanatory analysis, each of which inhibits intellectual progress in the study of international relations."[4]

We attribute this large divergence of opinion to the lack of a formal mathematical theory of Cyber Conflict. Cyber Conflict is defined as "the use of computational technologies for malevolent and destructive purposes to impact, change, or modify diplomatic or military interactions."[5] The objective of this paper is to link mathematically the use of such computational technologies with their military and broader strategic effects.

2. THE RATIONALIST EXPLANATIONS FOR WAR MODEL

Fearon published in 1995 a paper titled "The Rationalist Explanations for War."[6] In this paper, Fearon developed a straightforward mathematical model to explain that war can be portrayed as a bargaining process. The main variables in this model are the probability of winning the war, the expected utility if the war is won, the cost it would entail for each participant, and how much we really know about these variables.

We will use this bargaining model of war as a basis to develop our Rationalist Cyber Conflict Theory, by adding information security variables that affect the model's outcomes.

2.1. THE BARGAINING MODEL OF WAR

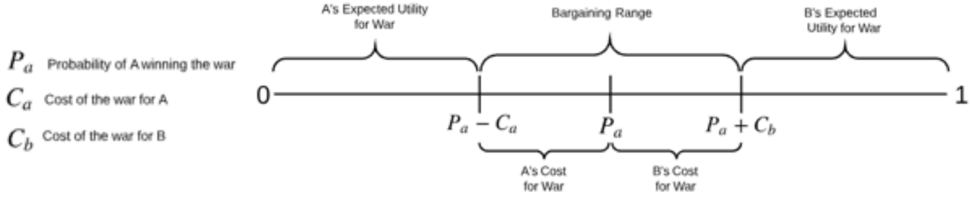

A's Expected Utility for War
Bargaining Range
B's Expected Utility for War
P_a Probability of A winning the war
C_a Cost of the war for A
C_b Cost of the war for B
0
1
$P_a - C_a$
P_a
$P_a + C_b$
A's Cost for War
B's Cost for War

Figure 1. Baseline Model, no Cyber Operations

This is the Bargaining Model of War. Country A and country B are in conflict. We draw a line that goes from 0 to 1 to represent the value to be gained in the war; it could be territory, access to oil or minerals, etc.[7] 1 represents winning 100% of the value.

P_a represents the probability of victory for country A. Since we have normalized the possible value gain to 1, it also represents the expected utility of war. To clarify, if the total value of winning the war were $500 billion, and the probability of winning the war was 50%, then the expected utility would be Ue=$500 billion x 0.5 = $250 billion. To simplify the model, instead of using $500 billion or any other money amount, we simply use 1. Therefore, the expected utility in the model is Ue=1 x P_a, which is the same as Ue=P_a. In other words, we will be calling Pa the probability of winning the war, but it is also the normalized expected utility of winning the war.

From the utility/probability of winning the war, we need to deduct the cost of the war. This gives us P_a-C_a, which is country A's true expected utility for the war. To calculate the expected utility for country B, we take 1-P_a, and add the cost of the war for country B, C_b. This gives us the point Pa+Cb in the line. We can then see that the bargaining range goes from Pa-Ca to Pa+Cb. In other words, as long as this bargaining range exists, it makes more economic sense for country A and country B to bargain, instead of going to war. This is because if they go to war, country A can only gain Pa-Ca worth of value, whereas if it negotiates, it can gain all the way up to P_a+C_b. Same thing goes for country B. If there is a war, country B can only gain 1-(P_a+C_b), but if they negotiate, country B can gain all the way up to 1- (P_a-C_a). The likely outcome of negotiation is of course somewhere between the two end points of the bargaining range; but any outcome in this range is better than the outcomes that could be gained through war.

Therefore, if there is an x such that:

$$P_a - C_a \leq x \leq P_a + C_b$$

Then we will have a bargaining range, and war will not make economic sense.

Our thesis is that different cyber operations can modify the probability P_a, and the costs C_a, and C_b, and therefore can alter the possible outcomes of a conflict.

2.2. INFORMATION SECURITY OBJECTIVES: CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

Information Security as a discipline has three main objectives: to ensure the confidentiality, integrity, and availability of data in the organization.

Confidentiality consists in allowing only authorized users to access data. Integrity consists in allowing only authorized users to modify data. Availability consists in ensuring that data are available to authorized users when required.

2.3. CYBER ATTACK OBJECTIVES: EXTRACTION, MODIFICATION, AND DENIAL OF SERVICE

There are three cyber offensive actions that can be taken: extraction, modification, and denial of service.

Extraction is the opposite of confidentiality: a hacker accesses confidential information and extracts it.

Modification is the opposite of integrity: the hacker modifies data without authorization, causing a disruption in the workflow supported by the IT system attacked.

Denial of Service is the opposite of availability: the hacker overwhelms an IT resource to deny its use to legitimate users.

We will call these variables the EMD variables (Extraction, Modification, and Denial of Service).

2.4. VULNERABILITIES

These actions of Extraction, Modification, and Denial of Service can be performed by hackers due to vulnerabilities in information technology systems. These vulnerabilities can be classified in three broad categories: configuration errors, technical errors, and human errors.

Configuration errors occur when IT administrators or users do not properly configure or manage IT resources. An example would be leaving a default password in a system. Since default passwords are well known, a hacker could easily access the IT resource.

Technical errors are the result of programming or hardware design mistakes. A common mistake in software programming is to mismanage memory access, giving hackers the opportunity to take over a CPU remotely by injecting malware into available memory.

Human errors occur when administrators or users do not follow proper procedures.

2.5. CYBER OPERATIONS

We propose the following taxonomy for cyber operations:

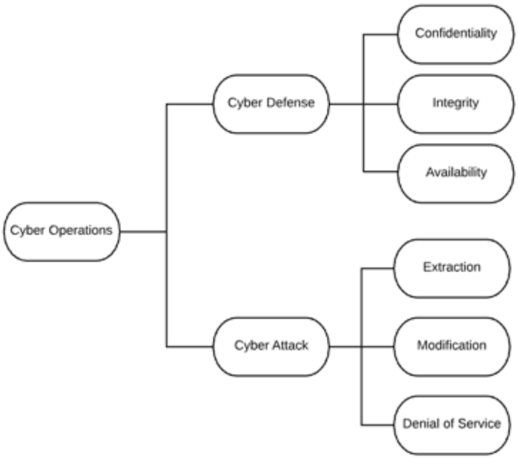


Figure 2. Cyber Operations Taxonomy

Cyber Operations are divided into action types: Cyber Defense Operations and Cyber Attack Operations. In turn, Cyber Defense, as above, is divided into three possible objectives: maintaining Confidentiality, maintaining Integrity, and maintaining Availability. Any information security software or procedure in place has to help achieve at least one of these objectives.

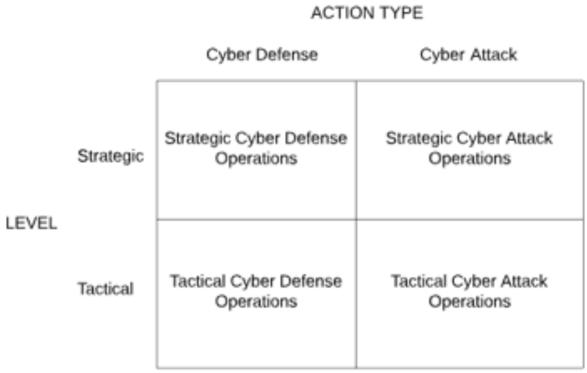
Cyber Attack is divided into three objectives: Extraction of data (E), Modification of data (M), and Denial of Service (D).

Cyber Operations can also be classified on their implementation level: Strategic Cyber Operations and Tactical Cyber Operations.

Strategic Cyber Operations are conducted at the nation-state level. Strategic Cyber Defense consists of the policies and plans in place to defend the infrastructure of companies and organizations within the nation-state in order to prevent strategic cyber-attacks. A Strategic cyber-attack may consist of the Extraction or Modification of valuable business, technological, or military information, or a Denial-of-Service attack that cripples vital infrastructure.

Tactical Cyber Operations are conducted during a kinetic war. Tactical Cyber Defense consists of the implementation of technical controls to prevent cyber-attacks on the command and control, communications, computer, intelligence, surveillance and reconnaissance (C4ISR) systems of a fighting force. A Tactical cyber-attack consists of the disruption of the enemy's corresponding systems through Extraction, Modification, or Denial of Service of tactical information that may affect the results of a battle.

We can combine the action types with the implementation levels into a Cyber Operations Matrix:



		ACTION TYPE	
		Cyber Defense	Cyber Attack
LEVEL	Strategic	Strategic Cyber Defense Operations	Strategic Cyber Attack Operations
	Tactical	Tactical Cyber Defense Operations	Tactical Cyber Attack Operations

Figure 3. Cyber Operations Matrix

A nation-state must have plans in place for each of the four combinations.

The objective of Strategic Cyber Attack Operations is to disrupt the critical infrastructure of a nation-state, which can be:

- Government
- Electricity grid
- Oil and gas production and distribution
- Logistic networks
- Telecommunications
- Financial sector
- Manufacturing sector
- Services

The objective of Tactical Cyber Attack Operations is to disrupt a military unit's C4ISR systems, as well as the networks of government and civilian entities supporting a military operation. An example would be the disruption of logistical networks that feed military operations.

Both Strategic and Tactical Cyber Operations should be used as force multipliers during a kinetic war.

2.6. EFFECTS OF STRATEGIC CYBER OPERATIONS ON THE RISK OF WAR

Based on their effects on the Bargaining Model of War, we can divide cyber-attacks in the following manner:

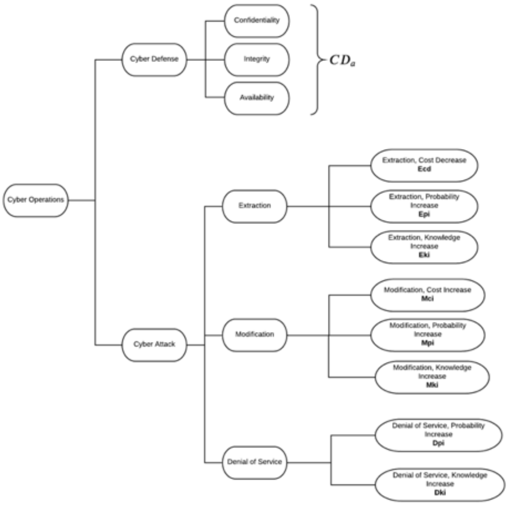

Confidentiality
Integrity
Availability
CD_a
Cyber Defense
Cyber Operations
Extraction
Extraction, Cost Decrease Ecd
Extraction, Probability Increase Epi
Extraction, Knowledge Increase Eki
Modification, Cost Increase Mci
Modification, Probability Increase Mpi
Modification, Knowledge Increase Mki
Cyber Attack
Modification
Denial of Service
Denial of Service, Probability Increase Dpi
Denial of Service, Knowledge Increase Dki

Figure 4. Cyber-attacks Taxonomy

We have divided Extraction into three types: Extraction, Cost Decrease (Ecd); Extraction, Probability Increase (Epi); and Extraction, Knowledge Increase (Eki). We are assigning them variable names because we will use them to analyze their effects in the Bargaining Model of War equation.

Modification is divided into Modification, Cost Increase (Mci); Modification, Probability Increase (Mpi); and Modification, Knowledge Increase (Mki).

Denial of Service is divided into Denial of Service, Probability Increase (Dpi), and Denial of Service, Knowledge Increase (Dki).

We saw in the Bargaining Model of War the following inequality:

$$P_a - C_a \leq x \leq P_a + C_b$$

Where P_a is the probability of country A winning the war, C_a is country A's cost of war, and C_b is country B's cost of war. Our Rationalist Cyber Conflict Theory is based on the thesis that the cyber-attack variables we listed above, Ecd, Epi, Eki, Mci, Mpi, Mki, Dpi, and Dki, have the capacity of altering P_a, C_a, and C_b, and therefore can modify the possible outcomes of a war.

Cost Decrease or Increase variables (Ecd, Mcd) can increase or decrease C_a and C_b. An Extraction, Cost Decrease (Ecd) can occur, for example, when a nation-state uses an Extraction cyber-attack to steal military technology from a rival nation-state, reducing its own research and development and production costs, part of C_a. A Modification, Cost Increase (Mci) could happen when a nation-state implements a Modification cyber-attack and sabotages the R&D or production of military technology, increasing the rival's costs, part of C_b.

Probability Increase variables (Epi, Mpi, Dpi) increase the nation-state's probability of winning the war, P_a. The nation-state can steal military technology via Extraction or can sabotage the rival's military capacity through Modification or Denial of Service, increasing its own probability of winning.

Knowledge Increase variables (Eki, Mki, Dki) increase the nation-states' knowledge about each other's military capabilities, changing the perception of the probability of winning, P_a. In a situation in which a nation-state does not fully understand its rival's military capabilities, an Extraction cyber-attack can obtain such information, making P_a clearer. Also, a nation-state can launch a limited Denial of Service attack as a signal of its strength, increasing the knowledge of P_a for its rival. Another strategy is to do a Modification, Knowledge Increase (Mki) attack, which has been called a "flag planting attack." This consists of penetrating the rival's network and leaving evidence of the intrusion in the form of a "flag," which is a document stating that the network was penetrated, but without causing any damage. This is a clear signal of the nation-state's cyber operations capabilities and can act as a deterrent.

Regarding Cyber Defense Operations, we are adding the cost of Confidentiality, Integrity, and Availability into a single variable: CD_a.

2.7 THE RATIONALIST CYBER CONFLICT THEORY

We will now cover how the EMD variables affect the Bargaining Model of War's three variants: The Baseline Model, the Uncertainty Model, and the Preventive War Model. We will also see an example of the application of the EMD variables in game theory, used in the Preemptive War Model. We will use William Spaniel's models described in his book "Game Theory 101: The Rationality of War,"[8] and add the Extraction, Modification, and Denial of Service (EMD) variables to them, to analyze their effects on their respective bargaining ranges and probabilities of war. We will then analyze the impact of the cost of cyber defense, and finally we will examine the complete inequality of the Rationalist Cyber Conflict Theory.

2.8. BASELINE MODEL

The Baseline Model shows the simplest version of the Bargaining Model of War: country A's probability of victory is well known by both rivals, and there are no future considerations, only the present.

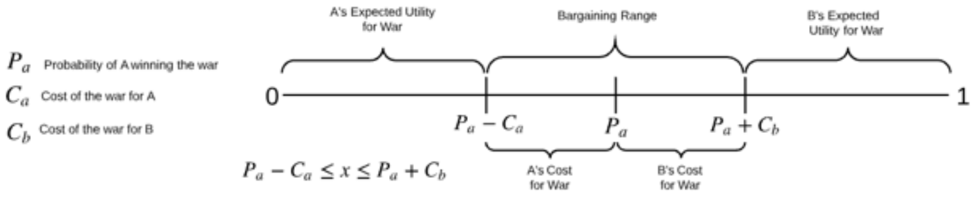

A's Expected Utility for War
Bargaining Range
B's Expected Utility for War
P_a Probability of A winning the war
C_a Cost of the war for A
C_b Cost of the war for B
0
1
$P_a - C_a$
P_a
$P_a + C_b$
$P_a - C_a \leq x \leq P_a + C_b$
A's Cost for War
B's Cost for War

Figure 5. Baseline Model, no Cyber Operations

Above we can see the Baseline Model with no Cyber Operations. The result is that there is, theoretically, no risk of war, since there is a clear bargaining range available. This means that the rational course of action is for both rivals to negotiate, because winning the war brings less utility (due to its cost) than any possible negotiation outcome. However, we must take into consideration that this is a model. In real life, bargaining ranges are not clearly visible, and there are emotional factors not taken into consideration by the model. But as a rule, we can say that the bigger the theoretical bargaining range and the smaller the expected utilities of war, the less probability that war will break out. A large bargaining range gives both parties more space for perception and interpretation errors, without those errors necessarily resulting in war.

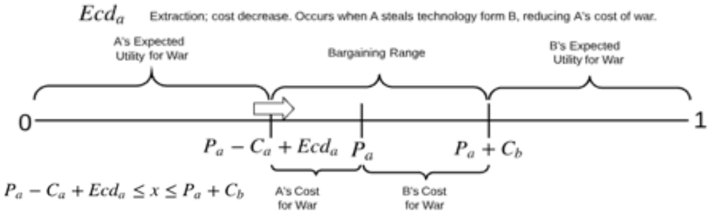

Ecd_a Extraction; cost decrease. Occurs when A steals technology form B, reducing A's cost of war.
A's Expected Utility for War
Bargaining Range
B's Expected Utility for War
0
1
$P_a - C_a + Ecd_a$
P_a
$P_a + C_b$
$P_a - C_a + Ecd_a \leq x \leq P_a + C_b$
A's Cost for War
B's Cost for War

Figure 6. Baseline Model, Extraction, Cost Decrease

In this scenario, country A launches an Extraction, Cost Decrease (Ecd) cyber operation against country B. This means that country A manages to hack into country B’s networks, and steals technology from country B that allows country A to conduct war in a less costly manner. This knowledge could be, for example, how to build weapons more efficiently, or knowledge on country B’s military doctrine, allowing country A to plan a more efficient doctrine that requires less expensive weapons systems or troop dispositions. The end result is that country A's cost of war goes down, increasing country A's Expected Utility for War, and reducing the bargaining range. This in turn increases the risk of war; any reduction in the bargaining range has such effect because as mentioned, in real life the boundaries of the bargaining range are not clearly visible, and the smaller it is, the smaller the margin for errors in perception that could lead to war.

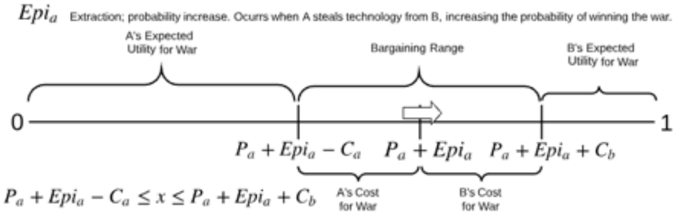

Epi_a Extraction; probability increase. Ocurrs when A steals technology from B, increasing the probability of winning the war.
A's Expected Utility for War
Bargaining Range
B's Expected Utility for War
0
1
$P_a + Epi_a - C_a$
$P_a + Epi_a$
$P_a + Epi_a + C_b$
$P_a + Epi_a - C_a \leq x \leq P_a + Epi_a + C_b$
A's Cost for War
B's Cost for War

Figure 7. Baseline Model, Extraction, Probability Increase

In this scenario, country A launches an Extraction, Probability Increase (Epi) cyber operation against country B. This could be, for example, stealing technology on how to build better weapon systems, which increases the probability of winning the war. Notice that the cost does not change, only the capabilities of the weapon system. In a real-life scenario, CD_a could also increase. The result is that country A's probability of winning increases. The bargaining range shifts in favor of country A. Also, country A’s Expected Utility for War increases and country B’s decreases, which in turn increases the risk that A will choose war.

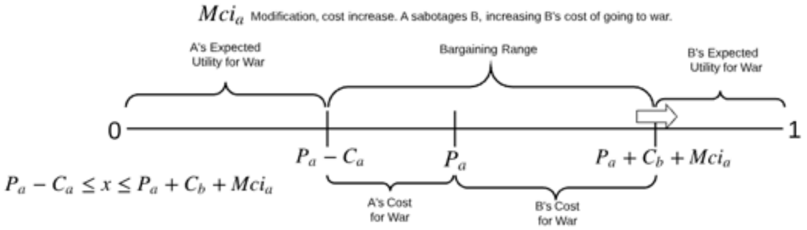

Mci_a Modification, cost increase. A sabotages B, increasing B's cost of going to war.
A's Expected Utility for War
Bargaining Range
B's Expected Utility for War
0
1
$P_a - C_a$
P_a
$P_a + C_b + Mci_a$
$P_a - C_a \leq x \leq P_a + C_b + Mci_a$
A's Cost for War
B's Cost for War

Figure 8: Baseline Model, Modification, Cost Increase

In this scenario, Country A launches a Modification, Cost Increase (Mci) against country B. This could consist of an act of sabotage that increases country B’s cost of developing, manufacturing, or fielding weapons or troops. Notice that country B’s probability of winning the war does not change; rather, winning becomes much costlier. Such sabotage can be intense, or it can be slow and insidious. The end result is that country B's cost of war increases. This increases the bargaining range to the advantage of A, and also reduces country B’s Expected Utility for War. This reduces the overall risk of war, but significantly benefits A in the negotiations.

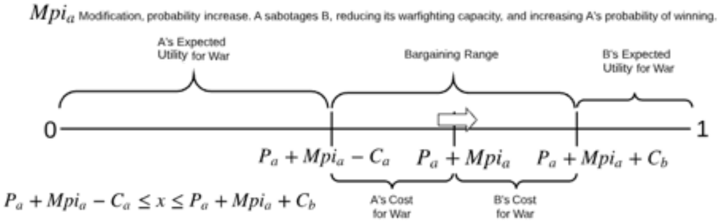

Mpi_a Modification, probability increase. A sabotages B, reducing its warfighting capacity, and increasing A's probability of winning.
A's Expected Utility for War
Bargaining Range
B's Expected Utility for War
0
1
$P_a + Mpi_a - C_a$
$P_a + Mpi_a$
$P_a + Mpi_a + C_b$
$P_a + Mpi_a - C_a \leq x \leq P_a + Mpi_a + C_b$
A's Cost for War
B's Cost for War

Figure 9. Baseline Model, Modification, Probability Increase

In this scenario, country A launches a Modification, Probability Increase (Mpi) cyber operation against country B. This cyber operation could consist of sabotaging country B’s capacity to develop new weapons systems, thus reducing country B’s probability of winning a war. The result is that country A's probability of winning the war increases. The bargaining range remains the same, but it benefits country A. At the same time, country A’s Expected Utility of War increases and country B’s decreases, thus increasing the overall risk of country A initiating a war if the bargaining range is not properly perceived.

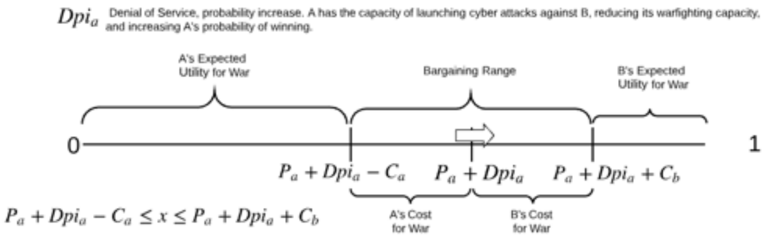

Dpi_a Denial of Service, probability increase. A has the capacity of launching cyber attacks against B, reducing its warfighting capacity, and increasing A's probability of winning.
A's Expected Utility for War
Bargaining Range
B's Expected Utility for War
0
1
$P_a + Dpi_a - C_a$
$P_a + Dpi_a$
$P_a + Dpi_a + C_b$
$P_a + Dpi_a - C_a \leq x \leq P_a + Dpi_a + C_b$
A's Cost for War
B's Cost for War

Figure 10. Baseline Model, Denial of Service, Probability Increase

In this scenario, country A launches a Denial of Service, Probability Increase (Dpi) against country B. This is a more overt version of the previous scenario, Mpi, but the end results are the same: A's probability of winning the war increases, and the bargaining range shifts in favor of country A. At the same time, country A’s Expected Utility for War increases, thus increasing the risk of war.

2.9. UNCERTAINTY MODEL

The Uncertainty Model includes a more realistic complication: the disparity of perception of the probability of winning.

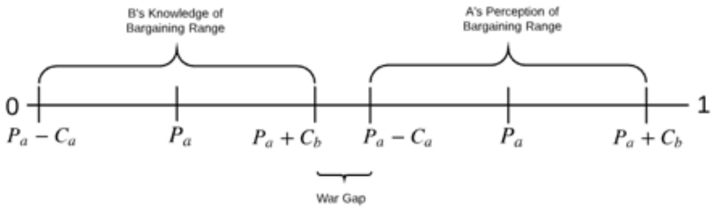

B's Knowledge of Bargaining Range
A's Perception of Bargaining Range
0
1
$P_a - C_a$
P_a
$P_a + C_b$
$P_a - C_a$
P_a
$P_a + C_b$
War Gap

Figure 11. Uncertainty Model, no Cyber Operations

This is the Uncertainty Model, without Cyber Operations introduced yet. In this model, we assume that country B has a precise knowledge of the probability of winning, P_a, whereas country A has an erroneous perception of the probability of winning. Under this scenario, country A thinks it can win, while country B knows that the probability of country A winning is very low. We can see in the graph that there is no bargaining range, only a War Gap; therefore, it is very likely that war will occur.

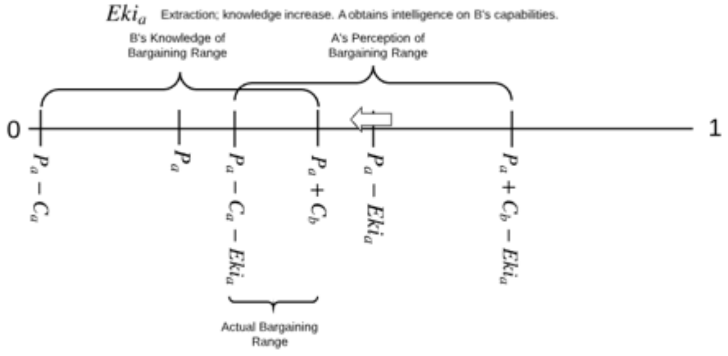

Eki_a Extraction; knowledge increase. A obtains intelligence on B's capabilities.
B's Knowledge of Bargaining Range
A's Perception of Bargaining Range
0
1
$P_a - C_a$
P_a
$P_a - C_a - Eki_a$
$P_a + C_b$
$P_a - Eki_a$
$P_a + C_b - Eki_a$
Actual Bargaining Range

Figure 12. Uncertainty Model, Extraction, Knowledge Increase

In this scenario, country A launches an Extraction, Knowledge Increase (Eki) cyber operation against country B. This could consist of stealing information on country B’s technology and troop dispositions. The result is that country A increases its knowledge on country B's capabilities, shifting country A's Perception of its probability of winning, creating an Actual bargaining range, and reducing the risk of war. In the diagram we can see that country A’s perception is still not the same as country B’s; however, the bargaining ranges overlap enough to make it possible for both to choose negotiation.

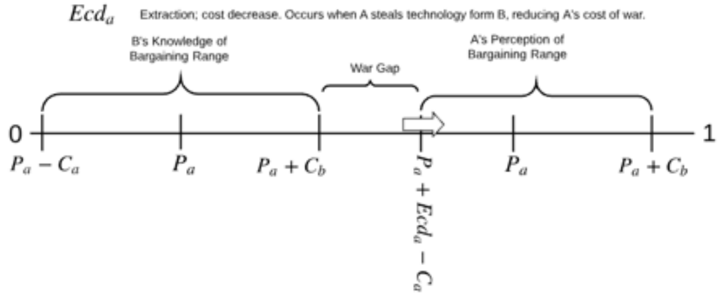

Ecd_a
Extraction; cost decrease. Occurs when A steals technology form B, reducing A's cost of war.
B's Knowledge of Bargaining Range
War Gap
A's Perception of Bargaining Range
0
1
$P_a - C_a$
P_a
$P_a + C_b$
$P_a + Ecd_a - C_a$
P_a
$P_a + C_b$

Figure 13. Uncertainty Model, Extraction, Cost Increase

In this scenario country A launches an Extraction, Cost Decrease (Ecd) cyber operation against country B. This reduces country A's cost of war, which, together with country A's wrong perception of Pa, increases the War Gap, and therefore the probability of war.

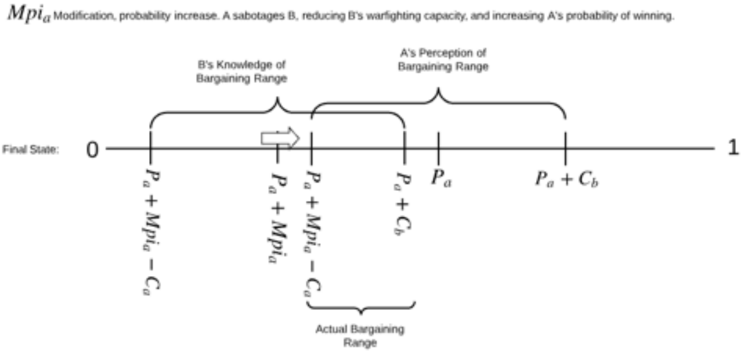

Mpi_a Modification, probability increase. A sabotages B, reducing B's warfighting capacity, and increasing A's probability of winning.
B's Knowledge of Bargaining Range
A's Perception of Bargaining Range
Final State:
0
1
$P_a + Mpi_a - C_a$
$P_a + Mpi_a$
$P_a + Mpi_a - C_a$
$P_a + C_b$
P_a
$P_a + C_b$
Actual Bargaining Range

Figure 14. Cyber Operation: Modification, Probability Increase

In this scenario, country A launches a Modification, Probability Increase (Mpi) against country B, resulting in an increase in country A's probability of winning the war. If country A's perception remains the same, the actual bargaining range increases, reducing the risk of war. However, if country A's perception shifts also (not shown in the diagram), the whole equation just shifts to the right, and the chance of war does not vary.

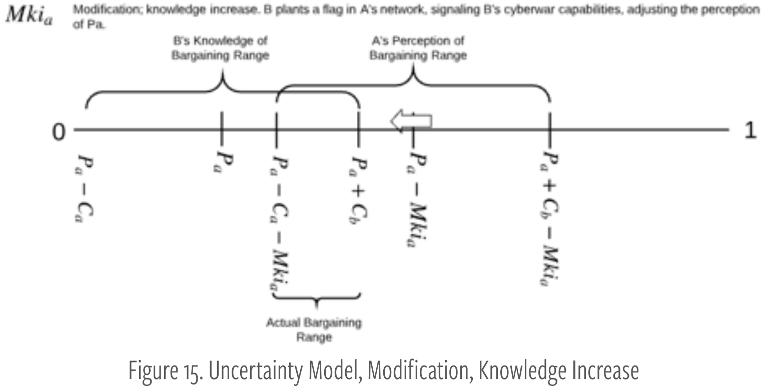

Mki_a
Modification; knowledge increase. B plants a flag in A's network, signaling B's cyberwar capabilities, adjusting the perception of Pa.
B's Knowledge of Bargaining Range
A's Perception of Bargaining Range
0
1
$P_a - C_a$
P_a
$P_a - C_a - Mki_a$
$P_a + C_b$
$P_a - Mki_a$
$P_a + C_b - Mki_a$
Actual Bargaining Range

Figure 15. Uncertainty Model, Modification, Knowledge Increase

In this scenario, country B launches a Modification, Knowledge Increase (Mki) cyber operation against country A. This could consist of planting a “flag” in country A’s network. A flag is an innocuous document that signals country B’s capabilities of compromising country A’s networks and causing damage if it so chooses. The result is that country A increases its knowledge of country B's capabilities, shifting country A's Perception of bargaining range, creating an Actual bargaining range, and reducing the risk of war.

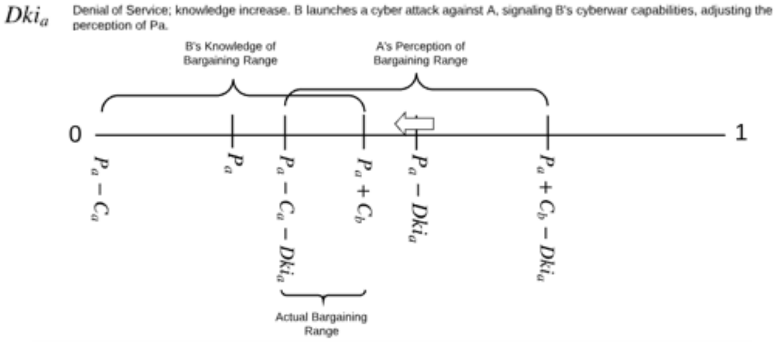

Dki_a
Denial of Service; knowledge increase. B launches a cyber attack against A, signaling B's cyberwar capabilities, adjusting the perception of Pa.
B's Knowledge of Bargaining Range
A's Perception of Bargaining Range
0
1
$P_a - C_a$
P_a
$P_a - C_a - Dki_a$
$P_a + C_b$
$P_a - Dki_a$
$P_a + C_b - Dki_a$
Actual Bargaining Range

Figure 16. Uncertainty Model, Denial-of-Service, Knowledge Increase

In this scenario, country B launches a Denial-of-Service, Knowledge Increase cyber operation against country A. This is a more severe version of the previous model; country B signals its capacity and willingness to engage in cyberwar, increasing country A’s knowledge of the real probability of winning, Pa. As a result, an Actual bargaining range is generated, reducing the risk of war.

2.10. PREVENTIVE WAR MODEL

We will now cover the Preventive War Model. Preventive war occurs when we have a declining state, country A, vs. a rising state, country B. Seeing the increase of power of country B, country A decides to attack before country B becomes too powerful.

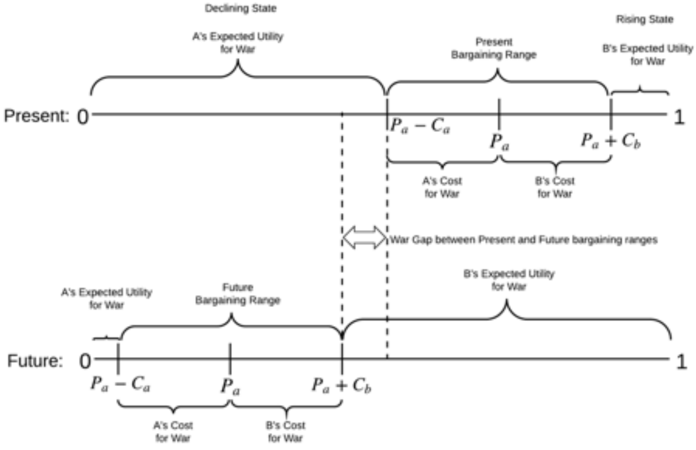


Figure 17. Preventive War Model, no Cyber Operations

This is the Preventive War Model without cyber operations. We now have two diagrams: one for the present and one for the future. In the present diagram, country A has a higher probability of winning a war, P_a, and we can see a Present bargaining range that favors country A. We can also see that in the future, since B is a rising state, country A's probability of winning a war is greatly reduced. We can see that there is a Future bargaining range, but notice how there is a War Gap between the Present and Future bargaining range. This means that country A may decide to attack country B now, before country B becomes too powerful and the probability of winning the war, P_a slides to the favor of B.

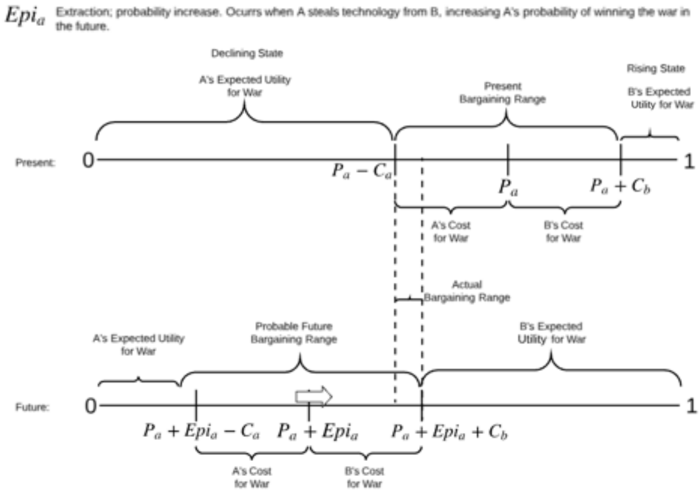

Epi_a
Extraction; probability increase. Ocurrs when A steals technology from B, increasing A's probability of winning the war in the future.
Declining State
A's Expected Utility for War
Present Bargaining Range
Rising State
B's Expected Utility for War
Present:
0
1
$P_a - C_a$
P_a
$P_a + C_b$
A's Cost for War
B's Cost for War
Actual Bargaining Range
A's Expected Utility for War
Probable Future Bargaining Range
B's Expected Utility for War
Future:
0
1
$P_a + Epi_a - C_a$
$P_a + Epi_a$
$P_a + Epi_a + C_b$
A's Cost for War
B's Cost for War

Figure 18. Cyber Operation: Extraction, Probability Increase, Declining State Steals Technology

In this scenario, country A, the declining state, launches an Extraction, Probability Increase (Epi) cyber operation, and steals technology from country B, the rising state. This increases country A's probability of winning a future war, sliding the Probable Future bargaining range to the right, in favor of country A. This creates an Actual bargaining range, reducing the risk of war.

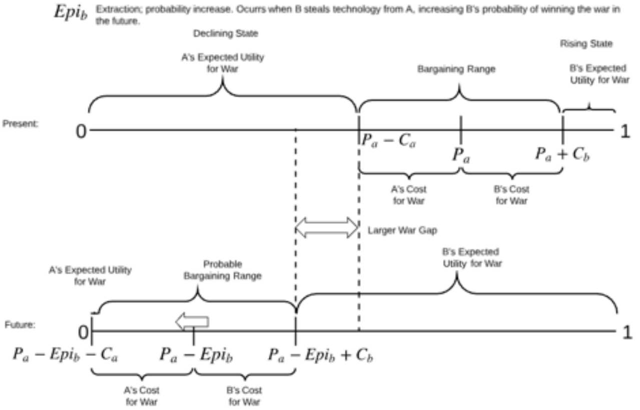

Epi_b
Extraction; probability increase. Ocurrs when B steals technology from A, increasing B's probability of winning the war in the future.
Declining State
A's Expected Utility for War
Bargaining Range
Rising State
B's Expected Utility for War
Present:
0
1
$P_a - C_a$
P_a
$P_a + C_b$
A's Cost for War
B's Cost for War
Larger War Gap
A's Expected Utility for War
Probable Bargaining Range
B's Expected Utility for War
Future:
0
1
$P_a - Epi_b - C_a$
$P_a - Epi_b$
$P_a - Epi_b + C_b$
A's Cost for War
B's Cost for War

Figure 19. Cyber Operation: Extraction, Probability Increase, Rising State Steals Technology

In this scenario, country B, the rising state, launches an Extraction, Probability Increase (Epi) cyber operation and steals technology from country A, the declining state. This increases country B’s probability of winning the future war, sliding the Probable bargaining range to the left, widening the War Gap, and increasing the risk of war.

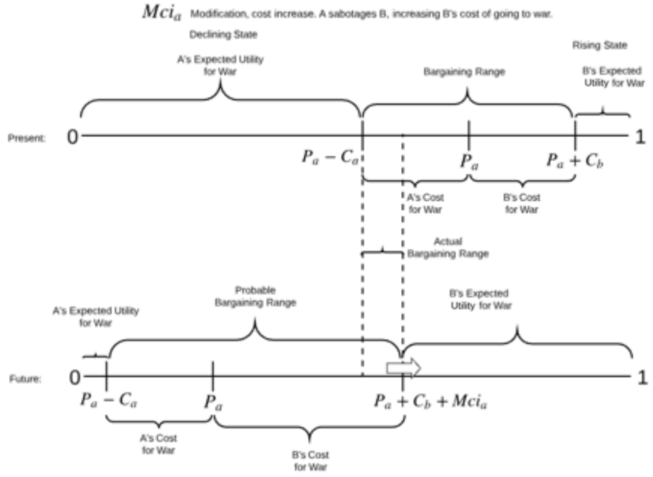
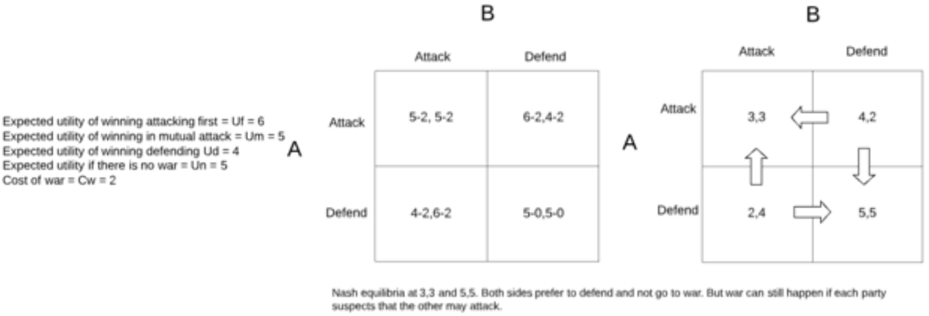

Mci_a Modification, cost increase. A sabotages B, increasing B's cost of going to war.
Declining State
A's Expected Utility for War
Bargaining Range
Rising State
B's Expected Utility for War
Present:
0
1
$P_a - C_a$
P_a
$P_a + C_b$
A's Cost for War
B's Cost for War
Actual Bargaining Range
Probable Bargaining Range
A's Expected Utility for War
B's Expected Utility for War
Future:
0
1
$P_a - C_a$
P_a
$P_a + C_b + Mci_a$
A's Cost for War
B's Cost for War

Figure 20. Cyber Operation: Modification, Cost Increase

In this scenario, country A launches a Modification, Cost Increase (Mci) cyber operation against country B, sabotaging country B’s warfighting capabilities, and increasing country B’s cost of war, C_b. This will increase the Probable bargaining range, creating an Actual bargaining range, and therefore reducing the risk of war.

2.11. PREEMPTIVE WAR MODEL

We will now cover the Preemptive War Model. A preemptive war occurs when country A decides to attack country B before country B attacks first, taking into consideration that the country that attacks first has a first strike advantage. For this model we will not use the Bargaining Model of War, but game theory, specifically the concept of Nash equilibrium. A Nash equilibrium occurs when the optimal outcome of a strategic interaction is one where no participant has an incentive to deviate from its chosen strategy after considering an opponent’s choice.



Expected utility of winning attacking first = Uf = 6
Expected utility of winning in mutual attack = Um = 5
Expected utility of winning defending Ud = 4
Expected utility if there is no war = Un = 5
Cost of war = Cw = 2

		B	
		Attack	Defend
A	Attack	5-2, 5-2	6-2,4-2
	Defend	4-2,6-2	5-0,5-0

		B	
		Attack	Defend
A	Attack	3,3	4,2
	Defend	2,4	5,5

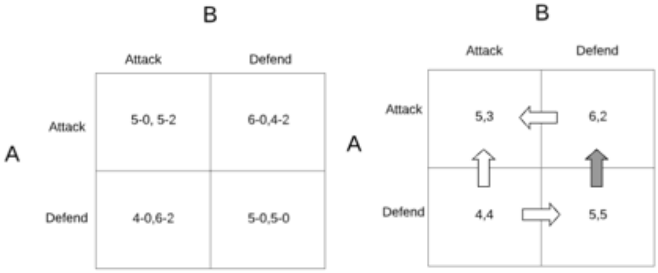
Nash equilibria at 3,3 and 5,5. Both sides prefer to defend and not go to war. But war can still happen if each party suspects that the other may attack.

Figure 21. Preemptive War Model – No Cyber Operations

This is the Preemptive War Model without cyber operations. We will add some representative numbers to make the model work. The expected utility of winning the war when attacking first while the other side defends is 6. The expected utility of winning the war if both attack at the same time is 5. The expected utility of winning when defending is 4. The expected utility of no war, that is, both defending, is 5. And the cost of war is 2. In the first matrix of the diagram above we can use the arithmetic calculation of the total utility for each combination. For example, the total utility for both country A and country B, if they both attack, would be the expected utility of winning if both attack, 5, minus the cost of war, 2, which gives us a total utility of 3. We can see the results in the second matrix.

We can see that there are Nash equilibria at 3,3 and 5,5. Both sides prefer to defend and not go to war. The arrows show the likely movement between possible combinations. But in real life, war can still happen if there is an error of perception.

Ecd_a Extraction; cost decrease. Occurs when A steals technology form B, reducing A's cost of war to 0.



A \ B	Attack	Defend
Attack	5-0, 5-2	6-0,4-2
Defend	4-0,6-2	5-0,5-0

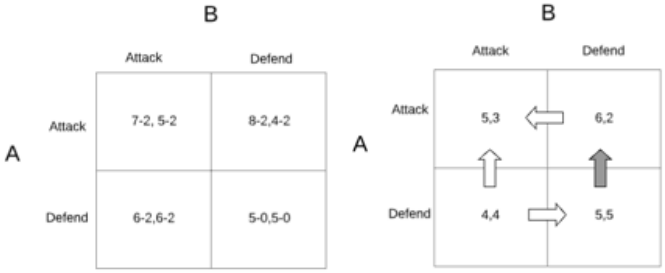
A \ B	Attack	Defend
Attack	5,3	6,2
Defend	4,4	5,5

Consequence: Nash equilibria at 5,5 dissapears. A is motvated to attack due to the low cost of war, and B has no option but to attack too.

Figure 22. Cyber Operation Extraction, Cost Decrease

In this scenario, country A launches an Extraction, Cost Decrease (Ecd) cyber operation against country B, stealing technology, and reducing country A's cost of war to 0. We can see this reflected in the first matrix; instead of subtracting a cost of war of 2 to country A, we subtract 0. The result can be seen in the second matrix. The consequence is that the Nash equilibrium at 5,5 disappears, because the 6,2 combination brings more utility. At this point, country A is now motivated to attack, and country B has no option but to attack, too, to optimize its utility, leading to war. The gray arrow shows the changed flow.

Mpi_a Modification, probability increase. A sabotages B, reducing B's warfighting capacity, and increasing A's probability of winning by 2 points.

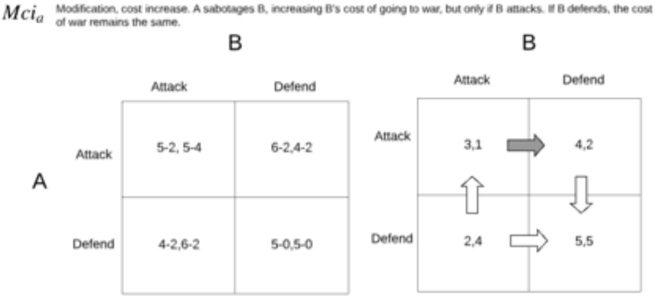


A \ B	Attack	Defend
Attack	7-2, 5-2	8-2,4-2
Defend	6-2,6-2	5-0,5-0

A \ B	Attack	Defend
Attack	5,3	6,2
Defend	4,4	5,5

Figure 23. Cyber Operation: Modification, Probability Increase

In this scenario, country A launches a Modification, Probability Increase cyber operation against country B, reducing country B's war fighting capacity, and increasing country A's probability of winning by 2 points. The consequence is that the Nash equilibrium at 5,5 disappears, pushing the flow to 6,2, and then to 5,3, causing war.



Mci_a Modification, cost increase. A sabotages B, increasing B's cost of going to war, but only if B attacks. If B defends, the cost of war remains the same.

A \ B	Attack	Defend
Attack	5-2, 5-4	6-2,4-2
Defend	4-2,6-2	5-0,5-0

A \ B	Attack	Defend
Attack	3,1	4,2
Defend	2,4	5,5

Figure 24. Cyber Operation: Modification, Cost Increase

In this scenario, country A launches a Modification, Cost Increase (Mci) cyber operation against country B, increasing country B's cost of going to war (5-4), but only if country B attacks. If country B defends, the cost of war remains the same. The consequence is that country B is not motivated to move from defend to attack, due to the reduction in utility resulting from an increase of the cost of war if it attacks. Because of this, country A is not motivated either, so they both go to defend-defend. In other words, we get a Nash equilibrium at 5,5, eliminating the risk of war.

2.12. CYBER DEFENSE IMPACT MODEL

We will now analyze the relationship between the cost of cyber defense and the probability of a cyber-attack being successful, and how this impacts the Bargaining Model of War.

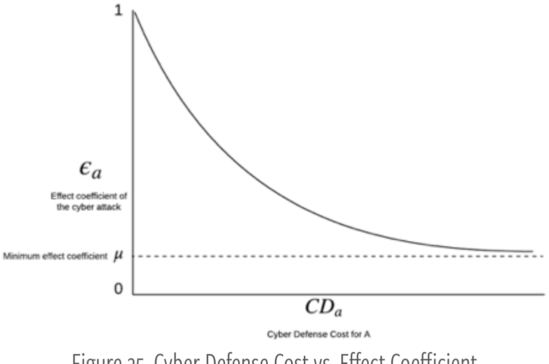


Figure 25. Cyber Defense Cost vs. Effect Coefficient

In the diagram above we can see the relationship between country A's cyber defense cost, CD_a, and ε_a (epsilon a), the effect coefficient of a cyber-attack. As we increase cyber defense spending, logically the probability of a cyber-attack being successful goes down, approaching asymptotically a line which we call the minimum effect coefficient, μ (miu). If we invest zero in cyber defense, then the probability of being hacked is 1. As we increase our investment, the probability of being hacked approaches μ.

We now need to relate ε_a to the probability of winning the war, P_a. To do so, we multiply 1-ε_a times P_a, (1-ε_a)P_a. 1-εa describes how much the cyber-attack affects the probability of winning. For example, if we do not invest anything in cyber defense and therefore ε_a=1, then 1-ε_a = 1-1 = 0, which multiplied by P_a, gives country A a zero probability of winning the war, because country B would have launched devastating cyber-attacks that render country A's military totally ineffective.

The relationship between ε_a and CD_a is expressed by the following equation:

$$\epsilon_a = \frac{1-\mu}{1+kCD_a} + \mu$$

Where k is a constant that shapes the curve. If the investment in cyber defense, CD_a, is equal to zero, then ε_a=1, meaning that the probability of getting hacked is 100%.

If we substitute this equation into (1-ε_a)P_a, we get the following:

$$\left(1 - \frac{1-\mu}{1+kCD_a} + \mu\right) P_a$$

This part of the equation is telling us that as we increase our cyber defense expenditure, CD_a, the probability of a cyber-attack being successful goes down to a minimum of μ, and therefore the probability of winning the war, P_a, goes up from 0 (when ε_a = 1) and approaches P_a (1- μ) (when CD_a is very large).

When we insert this into the overall equation, and also subtract CD_a since it's also part of the cost of war, we get the following inequality:

$$\left(1 - \frac{1-\mu}{1+kCD_a} + \mu\right) P_a - C_a - CD_a \leq x \leq \left(1 - \frac{1-\mu}{1+kCD_a} + \mu\right) P_a + C_b$$

Let us see how this equation affects the Bargaining Model of War.

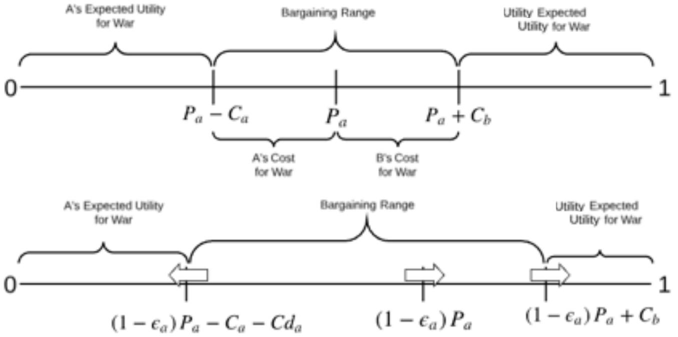
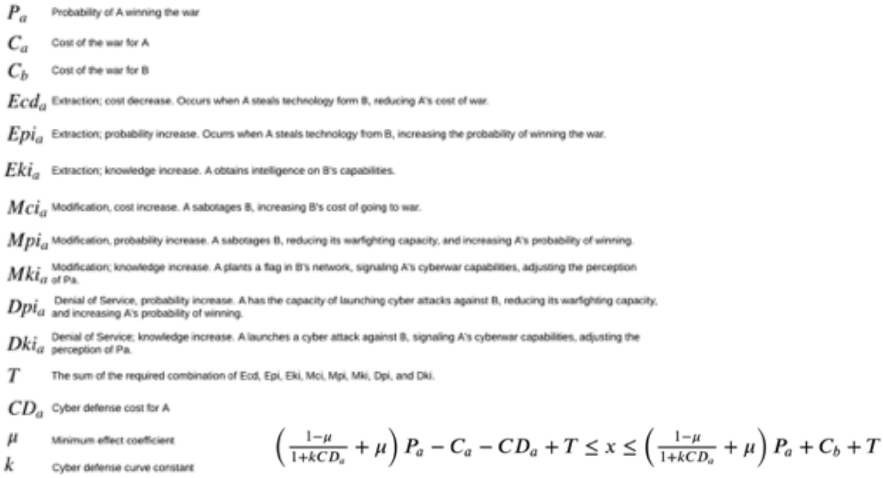

A's Expected Utility for War
Bargaining Range
Utility Expected Utility for War
0
1
$P_a - C_a$
P_a
$P_a + C_b$
A's Cost for War
B's Cost for War
A's Expected Utility for War
Bargaining Range
Utility Expected Utility for War
0
1
$(1-\epsilon_a)P_a - C_a - Cd_a$
$(1-\epsilon_a)P_a$
$(1-\epsilon_a)P_a + C_b$

Figure 26. Baseline Model, No Cyber Operations & Implement Cyber Defense

On the previous page we can see the Baseline Model with no cyber operations, and the Baseline Model with cyber defense implemented. We can see that as CD_a increases, the probability of winning for country A, P_a, increases. This happens because, as we saw, as CD_a increases, the effect coefficient of a cyber-attack, ε_a, decreases, and therefore P_a increases. This increase in Pa shifts the bargaining range to the right, favoring country A. At the same time, the increase in CD_a expands the bargaining range to the left, reducing country A's Expected Utility for War. So, in general, increasing CD_a reduces the risk of war, shifting the bargaining range to country A's benefit.

2.13. COMPLETE INEQUALITY

Here we can see the complete inequality for the Rationalist Cyber Conflict Theory.



P_a	Probability of A winning the war
C_a	Cost of the war for A
C_b	Cost of the war for B
Ecd_a	Extraction; cost decrease. Occurs when A steals technology form B, reducing A's cost of war.
Epi_a	Extraction; probability increase. Ocurrs when A steals technology from B, increasing the probability of winning the war.
Eki_a	Extraction; knowledge increase. A obtains intelligence on B's capabilities.
Mci_a	Modification, cost increase. A sabotages B, increasing B's cost of going to war.
Mpi_a	Modification, probability increase. A sabotages B, reducing its warfighting capacity, and increasing A's probability of winning.
Mki_a	Modification; knowledge increase. A plants a flag in B's network, signaling A's cyberwar capabilities, adjusting the perception of Pa.
Dpi_a	Denial of Service, probability increase. A has the capacity of launching cyber attacks against B, reducing its warfighting capacity, and increasing A's probability of winning.
Dki_a	Denial of Service; knowledge increase. A launches a cyber attack against B, signaling A's cyberwar capabilities, adjusting the perception of Pa.
T	The sum of the required combination of Ecd, Epi, Eki, Mci, Mpi, Mki, Dpi, and Dki.
CD_a	Cyber defense cost for A
μ	Minimum effect coefficient
k	Cyber defense curve constant

$$\left(\frac{1-\mu}{1+kCD_a}+\mu\right)P_a - C_a - CD_a + T \leq x \leq \left(\frac{1-\mu}{1+kCD_a}+\mu\right)P_a + C_b + T$$

3. MODEL PREDICTIONS

The Rationalist Cyber Conflict Theory is a theoretical model, not an empirical one. This means that it is not designed to make precise predictions, but rather to aid in understanding of possible cause-and-effect dynamics.

1. Strategic Cyber Operations in the form of Extraction, Modification, and Denial of Service, have the capacity of modifying the probability of winning a war, and the cost of a war.
2. In the Bargaining Model for War, the larger the bargaining range is, the less likely it is that there will be a war.
3. A cyber operation that increases the cost of war (Mci) increases the bargaining range, and therefore reduces the risk of war. In other words, the costlier the war, the less likely it will happen.
4. A cyber operation that decreases the cost of war (Ecd) reduces the bargaining range, and therefore increases the risk of war.

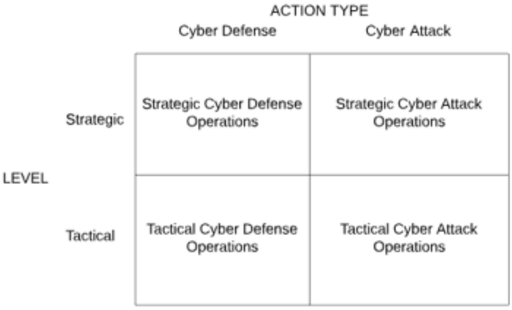
5. A cyber operation that increases the probability of winning a war (Epi, Mpi, Dpi) does not modify the magnitude of the bargaining range, but it does shift it in favor of country A. This also means that country A's Expected Utility for War increases. If the bargaining range is small and country A's Expected Utility for War is large, there is a greater probability that country A may misjudge the situation and cause a war.
6. A cyber operation that increases knowledge (Eki, Mki, Dki) causes the convergence between country A's and country B's perception of the probability of winning the war, making the bargaining range more visible, and reducing the risk of war.
7. In a preventive war scenario, if a rising state launches cyber operations that increase its future probability of winning the war (Epi, Mpi, Dpi), it will increase the War Gap between the present and future bargaining ranges, increasing the risk of war. The faster a rising state steals technology from the declining state, the higher the risk for war.
8. If a declining state launches cyber operations that increase its future probability of winning the war (Epi, Mpi, Dpi) by stealing technology from the rising state, it will create an actual bargaining range, reducing the risk of war.
9. In a Preemptive War Model, modeled with game theory, any cyber operation that increases the probability of winning the war, will increase the probability of war; any cyber operation that increases the cost of war reduces the risk of war; and any cyber operation that decreases the cost of war increases the risk of war.
10. An increase of cyber defense spending will increase the probability of winning a war but will also increase the cost of war. This will cause a shift of the bargaining range in the favor of country A, and increase the size of the bargaining range, reducing the risk of war.
11. Every cyber operation, when discovered, becomes a Knowledge Increase operation in a sense, because country B learns about country A's cyber operations capabilities.

It is important to note that the model focuses on cyber operations undertaken by nation-states with clear geopolitical goals in mind. The model does not cover cybercrime activities, hacktivism, cyber terrorism, or emotion-driven attacks from cyber militias outside the control of the nation-state.

4. CONCLUSION: IMPLICATIONS OF THE MODEL FOR CYBER WARFARE DOCTRINE

The objective of a national cyber doctrine is to describe the procedures that will be put into place to achieve specific objectives against rivals in the cyber domain. We offer here some strategy and policy implications drawn from the modeling; these ideas need also to be considered in their broader strategic and security contexts.

Cyber doctrine should be organized according to this Cyber Operations Matrix:



		ACTION TYPE	
		Cyber Defense	Cyber Attack
LEVEL	Strategic	Strategic Cyber Defense Operations	Strategic Cyber Attack Operations
	Tactical	Tactical Cyber Defense Operations	Tactical Cyber Attack Operations

Figure 27. Cyber Operations Matrix

The first consideration is that the entities that implement each of the four quadrants should be independent from one another, albeit with close coordination.

All Cyber Attack Operations should be conducted by the armed forces or other governmental entities explicitly operating under the authority of the nation's defense leadership, given the possible political and military implications of such attacks. Allowing independent civilian organizations to participate in such cyber operations, such as hack-backs, could easily get out of hand. Likewise, Tactical Cyber Defense Operations should logically be conducted by the armed forces, given the fact that the networks being defended are military.

On the other hand, Strategic Cyber Defense Operations should be a coordinated effort of civilian entities and the armed forces. The logic behind this is that many of these types of cyber operations happen mainly in civilian networks.

We will now cover in detail the implications of the model for Strategic Cyber Defense Operations, Strategic Cyber Attack Operations, and Tactical Cyber Operations.

4.1. IMPLICATIONS FOR STRATEGIC CYBER DEFENSE OPERATIONS

Companies tend to invest in information security no more than the expected loss that could result from a hack, expressed by the probability of being hacked times the loss of a breach. This is an optimum behavior for a single company, but very much suboptimal for the entire nation-state. For example, if a telecom gets hacked as a prelude to a kinetic war, the telecom loses money, but also the entire nation-state becomes vulnerable due to the lack of telecommunications when the war starts.

We can describe this investment dynamic with the following graph:

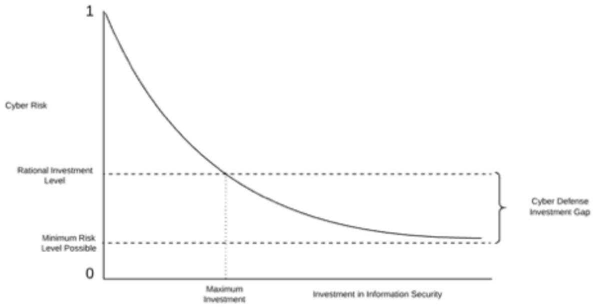


Figure 28. Rational Investment Level

As we increase investment in information security, cyber risk goes down. In theory, if we were to invest enough, we would approach asymptotically the Minimum Risk Level Possible line. However, companies will stop at the Rational Investment Level, which is equal to or less than the expected loss of a hack. This will generate a Cyber Defense Investment Gap like that shown on the graph, which represents a danger for the nation-state. The only way of reducing this gap is through government action that would reduce the cost of information security for companies. For example, the government could subsidize software, equipment, and training in information security for strategic infrastructure companies, or it could give special tax breaks on their purchase. This economic support would shift the Rational Investment Level down, reducing the Cyber Defense Investment Gap.

A related problem is the jobs gap for information security professionals. According to the 2017 Global Information Workforce Study,[9] the worldwide information security workforce gap will reach 1.8 million by 2022. We put forth that the reason behind this shortage is rooted in the Rational Investment Level. The jobs market is ruled by the forces of supply and demand, and the price that responds to differences between supply and demand for a job type is its salary. Given the large supply-demand gap in information security jobs, the salaries for such positions should be extremely high. If they were, this salary signal would eventually attract enough information security professionals to fulfill those jobs. But there is an economic restriction: The Rational Investment Level. Infosec salaries are a large component of a company's annual information security expenses, and a company will not invest above its Rational Investment Level, which is equal to or lower than the expected loss of being hacked, calculated by multiplying the risk of being hacked in a given year times the cost of a breach. So, no matter how large the information security gap is, salaries are not going high enough to close the gap thanks to this investment limit. We believe that the only possible solution is for governments to subsidize the training and salaries of information security professionals, remembering that this not only benefits the companies, but increases the national security of the country.

On the other hand, as a response to the lack of enough qualified cybersecurity professionals, information security vendors are developing automated solutions driven by AI. We can expect this trend to grow, and eventually reach a point in which most cyber defense and cyber-attack processes will be largely executed by AI.

4.2. IMPLICATIONS FOR STRATEGIC CYBER ATTACK OPERATIONS

A nation-state may choose as part of its cyber doctrine not to engage in Cyber Attack Operations and focus only on cyber defense; that is a rational option if the nation-state does not have other nation-states as natural enemies.

For those nation-states that do have rivals and wish to engage them in the cyber domain, the main implication of this model starts with the concept that they only have three general types of strategic Cyber Attack Operations they can engage in (Extraction, Modification, and Denial-of-Service), and that these cyber operations should be used to achieve strategic shifts in relations with geopolitical rivals. Therefore, the nation's cyber security community should develop a catalog of possible Extraction, Modification, and Denial-of-Service actions it could implement against each rival's economic, political, and military programs, to achieve specific strategic or military objectives. These plans should include an analysis indicating how each operation may increase or decrease the probability of winning a war, how it may increase or decrease the costs, and how it may modify the bargaining ranges. Logically, the cyber security community should also analyze the possible Extraction, Modification, and Denial-of-Service cyber operations that rivals could launch against their nation-state, what would be the strategic motivations and consequences, and which Cyber Defense Operations should be in place to neutralize these strategic cyber-attacks.

It is important to note that Extraction and Modification can be conducted equally during peacetime and wartime, whereas Denial-of-Service should be used almost exclusively during wartime. This is because Denial of Service attacks can be temporarily devastating, but countries have the capacity to recover quickly from them. Therefore, it makes little sense to launch a Denial-of-Service attack if it is not going to be followed by a kinetic war, since such an attack would achieve nothing. The only exception to this is a Denial-of-Service, Knowledge Increase (Dki) attack, used to signal the nation-state's cyber-attack capabilities. But one must take into consideration that after each attack, the rival will learn from it and harden its defenses. The best use of a Denial-of-Service attack is to launch it as a prelude to a kinetic war, to throw into disarray the enemy's electrical grid, telecom services, logistics, and financial services, and use that as a force multiplier for the kinetic war that would follow immediately. Using a street fight as an analogy, the Denial-of-Service attack is the equivalent of knocking your opponent to the ground, while the kinetic war attack is the equivalent of pounding on him once he's on the floor. If you just knock him to the ground and stop at that, he will just get up.

4.3. IMPLICATIONS FOR TACTICAL CYBER OPERATIONS

In their paper "Understanding Centers of Gravity and Critical Vulnerabilities,"[10] Strange and Iron postulate that a center of gravity has three characteristics: critical capabilities, critical requirements, and critical vulnerabilities. Within the context of a military unit, its critical capabilities are the means it has to fulfill its operational mission. Its critical requirements are the conditions and resources essential for the military unit to exercise its critical capabilities. And its critical vulnerabilities are those critical requirements that can be neutralized by the enemy, significantly reducing the military unit's critical capabilities. As an example, a critical capability of a battalion is the firepower it can bring to bear against enemy forces. Its critical requirements are personnel, equipment, fuel, ammunition, supplies, etc. Its critical vulnerabilities are the core requirements that can be attacked by the enemy under its current operational scenario; these could be, for example, supply lines, or telecommunication capabilities through an electronic warfare attack.

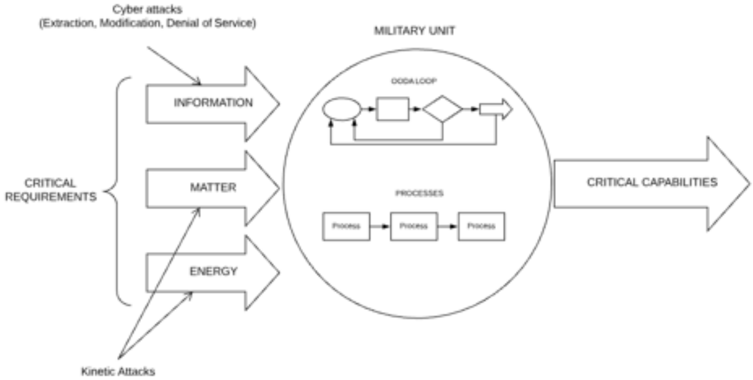


Figure 29. Center of Gravity

In this Critical Requirements and Critical Capabilities diagram we see that we can further deliver critical requirements into three categories: information, matter, and energy. Matter critical requirements can be equipment and ammo, for example. Energy critical requirements are fundamentally fuel and electricity. And information critical requirements are the capabilities provided by C4ISR systems (command, control, communications, computer, intelligence, surveillance and reconnaissance). Within the military unit, we can see the OODA Loop (observe–orient–decide–act), which is the method used to process all information coming into the unit and decide how to respond. We can also see that there are other processes running that are not related to decision making but are important for the unit. When all the critical requirements are met, and the OODA Loop and support processes are running correctly, then the military unit can deliver its critical capabilities. On the other hand, an attack on its critical requirements will degrade its critical capabilities.

Matter and energy requirements are affected through kinetic attacks, such as attacking supply lines and bombarding supply depots. And germane to the model, information requirements are affected through tactical cyber-attacks, in the form of Extraction, Modification, and Denial of Service (EMD) operations launched against C4ISR systems. Military planners should focus on identifying the information security vulnerabilities that, when attacked, would cause the most degradation to the OODA Loop of the enemy military unit. Likewise, they should identify the vulnerabilities within the information critical requirements of their own military units, and how to protect them.

It is important to note that the EMD cyber operations can be either intensive and close to the battlefield, or insidious and far removed from the battlefield. An intensive attack could be a Denial of Service of a system controlling military telecommunications. While effective, such an attack is immediately obvious, and the enemy will likely be able to mitigate it in some way. On the other hand, an insidious attack could be, for example, the modification of a database in an equipment maintenance warehouse that causes the system to order the wrong parts for critical equipment. By the time the enemy discovers the attack, its critical capabilities may be significantly diminished, and it will take a long time to recover. So, both intensive and insidious EMD tactical cyber operations should be combined for maximum effect. The critical point is that military planners should make the maximum effort to identify and understand the systems and procedures of the enemy's military units, develop a catalog of possible EMD attacks and their effects, and plan for the syncing of cyber-attacks with kinetic attacks to achieve a force multiplier effect. Likewise, they should map to the maximum detail possible the systems and procedures of their own military units, identify their information critical requirements, pinpoint their vulnerabilities, and implement the required tactical cyber defense systems.

NOTES

1. US Cyber Command History, (n.d.), Retrieved from https://www.cybercom.mil/About/History/.
2. S. D. Applegate & A. Stavrou, (2013, July 25), Towards a Cyber Conflict Taxonomy. In *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, https://ieeexplore.ieee.org/document/6568391.
3. L. Kello, (2013), The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*,38(2), 7-40. doi:10.1162/isec_a_00138.
4. Ibidem.
5. B. Valeriano and R. C. Maness, (2015), *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (New York: Oxford University Press).
6. J. D. Fearon, (1995), Rationalist explanations for war. *International Organization*,49(03), 379. doi:10.1017/s0020818300033324.
7. W. Spaniel, (2012), *Game theory 101: The rationality of war*. Createspace.
8. Ibidem.
9. The 2017 Global Information Security Workforce Study, (2017). Retrieved from https://iamcybersafe.org/wp-content/uploads/2017/06/europe-gisws-report.pdf.
10. Dr. J. Strange & Colonel R. Iron (n.d.), Understanding Centers of Gravity and Critical Vulnerabilities. Retrieved from http://www.au.af.mil/au/awc/awcgate/usmc/cog2.pdf.