Optimizing Deterrence Strategies in State-State Cyber Conflicts

Theoretical Models for Strategic Cyber Deterrence

Nasser S. Al-Azwani

Supervisor: Professor Tom Chen

School of Mathematics, Computer Science & Engineering
City, University of London

This Thesis is Submitted for the Degree of
Doctorate of Philosophy

January 2020

Dedication

I dedicate my thesis work to my loyal family and cooperative friends. A special feeling of gratitude to my Wife (Hidden Soldier), Children (Eman, Aflah, Sara, Fatima and Salma) and my loving parents, to the soul of my father whom I lost his influential prayers at the beginning of my journey and my Mom who still support my back and flourish my heart with her continuous precious prayers to achieve my dreams. Special thanks to my cheerful trustworthy brothers and sisters who have continuously encouraged me and lifted my spirit with their deep heartfelt laughter who have never left my side. I also dedicate this work to my companions at City, University of London who have been advising me during my tough days and sharing me their beneficial experiences throughout the journey. I will always appreciate all what they have done, words of encouragements and special thanks to my best friend at City, University of London Amir, Mohammed Ganem, Abdullah who stayed by my side , glaring at me with a pushing look and unforgettable inspiring wise words.

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This thesis is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and acknowledgements.

Nasser S. Al-Azwani
January 2020

Acknowledgements

I would like to express my deep sincere gratitude to my advisor whom I can proudly name as my teacher, Prof. Tom Chen for his support, patience, trust, and encouragement in addition to his immense knowledge that has always been advantageous to complete this piece of work. His tremendous inspiration and valuable advice led me to a deeper understanding of the topic and lightened my journey to grow as a researcher at the field of cyber security, cyber deterrence and strategic studies.

I would like to take this opportunity to thank the Erasmus Mundus program and Sultan Qaboos University for funding this research project and the support I have received over this research and without it this work would not achieve the goal. I am also using this opportunity to express my thanks to the City, University of London staff who supported me throughout the course of this research project.

Abstract

Deterrence has successfully prevented nuclear confrontation for more than five decades. The motive for conducting this research is to response to the problem of cyber threat growth and find out if deterrence is able to stop state cyber adversaries from utilizing cyber threats against its cyber space. A considerable effort of defensive cyber technologies and solutions have been developed, although massive cyber-attacks are still occurring and growing in terms of complexity, severity and quantity. For that, States need a new tactic to deal with cyber threats rather than relying only on cyber defense or offense. However, there is a satisfactory chance for cyber deterrence to work despite of challenges. Research approach is to examine cyber deterrence theory inspired by traditional deterrence theory combined with game theory models. This approach respond to the argument via three dimensions. First, it responds to analyze relevance of credibility to deterrence assumptions and the reasons beyond associating credibility of cyber threat with cyber deterrence strategy and its role either success or failure of deterrence strategy. The developed analytical model consists of two players involved in a cyber conflict. The selected case study assist in generating clear understanding of the pivotal role of credibility to support optimizing deterrence strategy from real life context. Second, cyber escalation model developed reflecting the failure of cyber threat credibility (as a threat of punishment) in deterring state cyber adversaries. The model has attempted to explore nature of cyber escalation ladder either it is going to be limited within cyber space or might exceed to involve nuclear or other domains of conflicts. Third, deterrence by entanglement model as a new approach could be the best approach for succeeding cyber deterrence strategy compared to other traditional deterrence model. Deterrence by entanglement model analysis has moved from general deterrence concepts to more narrowed investigation measuring effectiveness of deterrence by entanglement in reducing conflict heat. It explores the degree to which cyber deterrence by entanglement can assist state in deterring its cyber adversaries within more peacefully approach. Each chapter is concluded with a section that prescribes certain strategies which states can benefit from in real life practice. These strategies and learned lessons will assist states to understand the essential requirements for developing its credibility in cyber space and draw the lines for states optimizing its cyber deterrence.

Table of contents

List of figures

List of tables

Chapter 1

Introduction

The cyber domain consists of globally interconnected, integrated systems. The world is increasingly dependent on cyber technologies. Unfortunately, this domain has a weakness where a cyber attack can be launched against linked systems from anywhere by anyone. The past decade has seen a rapid increase in cyber threats targeting different sectors of information and communication infrastructures [1]. These threats showed a variety of attack types, methods, and technologies to deliver exploits to their targets.

Current growth in the Internet of Things (IoT) to support executing certain operations or exchanging goods has added to the challenges of securing state infrastructures [2]. In addition, the evolution of so-called smart cities where people benefit from smart social service systems such as smart meters, smart cars, and smart appliances is increasing concern for securing the infrastructure of these cities from cyber threats [3].

It has been widely noted that the cyber domain is not only a domain used for civil services but also one where political and military confrontations take place. Thousands of cyber attacks occur every day affecting the national infrastructures of different states. In the cyber domain, states threaten the national security of other states [4]. Moreover, the worst cyber attacks can be expected in the future despite development of better cyber defense (but also better offensive capabilities).

Documented cyber incidents during the last decade have revealed sophisticated cyber attacks and shown the challenge of predicting attacks, identifying the attacker, and the costs of dealing with post-attack consequences [5]. In the political context, cyber attacks are being used as weapons in conflicts between nations particularly to affect their critical infrastructure. Use of so-called cyber weapons are aimed to affect the national security of enemy countries.

Researchers have shown a growing interest in the idea of "cyber deterrence" evident from different publications trying to bridge the concept from the nuclear era to the cyber domain. Cyber deterrence is basically taken from traditional deterrence theory which was popularised during the Cold War to prevent any nuclear attack and to reduce the risk of distribution of nuclear weapons around the world [6]. The main idea of cyber deterrence is to prevent or reduce the likelihood of cyber attacks before they happen by threatening the opponent with retaliation in case the opponent decides to attack. The threat of retaliation is assumed to incite fear in the opponent and change the cost-benefit considerations.

Different countries have started reviewing the effectiveness of their cyber security strategies and questioning the effectiveness of these strategies in reacting against cyber threats. Numerous discussions have argued about how preemptive cyber threats can be avoided. A major player, the U.S. has started considering the development of cyber deterrence policy, and President Obama submitted a cyber deterrence policy to the Congress for a vote [7]. In Europe, Estonia suffered from massive cyber attacks, and the Estonian president asked NATO to cover cyber deterrence under the NATO deterrence umbrella [8]. As cyber deterrence has become a national security issue at the presidential level, it confirms the importance of moving to cyber deterrence. This movement should focus on answering the main cyber deterrence questions. States like Estonia, which has witnessed organised cyber attacks against its financial sector and other related critical sectors [9], would have benefited from successful deterrence.

This chapter explains the reasons and motivations for pursuing this research on cyber deterrence. It will also explain the proposed approach for conducting the research project. It will tie the research questions with aims and contribution expected by the end of this research. Finally, this chapter will clarify how this thesis is structured and what each chapter tries to accomplish.

1.1 Research Motivation

Cyber space has enabled the introduction of advanced threats to states, national security, and policy makers. States benefit from and depend on new cyber services, but at the same time, worry about threats against these cyber services.

Obviously, a great deal of cyber security defensive technologies and solutions have been developed, although massive cyber attacks are still occurring and growing in terms of complexity, severity and quantity. For example, the Iranian nuclear infrastructure was targeted for the purpose of physical destruction despite precautions taken by Iran [10]. Another case happened in the western part of Ukraine where the electricity grid was shut down for more than six hours on the 23rd of December 2015 [11]. The cause was malware called "Black Energy" which has a history of targeting control systems and wiping hard disks. When people rebooted their PCs, everything was gone because the drives were totally wiped.

Stuxnet, Black Energy, Sony attack, Lockheed Martin attack, Shamoon and Duqu are real examples around the world that has proved destructiveness of cyber attacks [12]. Typical consequences are financial and reputation damage. These days, attacks are capable of damaging the critical infrastructure and directly affecting national security which is obviously a top priority for states.

These cases indicate that cyber attacks have been used in political conflicts. Although efforts continue to develop cyber defense technologies for the purpose of detection, response, mitigation and recovery, it is often difficult to assure their efficacy in addition to the high costs of implementation. It is difficult to prevent states from massive cyber attacks by technology alone. It is necessary to look at other strategies to avoid cyber catastrophes.

Cyber threats need an effective response similar to traditional military response [13] but the main problem is no return address for the cyber attacker. An offensive cyber attack against a cyber attack could be a perfect retaliatory act [14]. However, retaliation could lead to unwanted escalation of a conflict.

States are responsible for protecting their citizens from threats coming via the sea, land and air. Cyber is another source of threats which requires sufficient protection [17]. At present, cyber defenses are not fully capable of protecting against a wide range of cyber attacks [15]. Kugler described cyber defenses as simply concentrating on protecting against known cyber attack [112]. States need to expand strategic initiatives to improve cyber security as well as prevention.

Going back to the nuclear arm race during the Cold War period, deterrence was the main factor to prevent nuclear war. The concept of cyber deterrence aims to take lessons from traditional deterrence and transfer them to the cyber domain [106]. The main motivation for this research is to help states with new response options that can support national cyber security. We next consider responses against new vulnerabilities and new threats in the cyber domain.

1. **New vulnerabilities:**

   Cyber vulnerability is a weakness or software bug within cyber systems or infrastructure which the attacker can utilize to exploit the attack or execute certain prohibited actions [18]. Actually, there are many definitions for the term of vulnerability. The U.S. National Institute of Standards and Technology (NIST) has defined vulnerability as “A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy” [23].

The complicated challenge facing states is that the cyber domain is free and open for everyone to participate. This means that other states can actively scan cyber infrastructure and systems looking for vulnerabilities. Cyber attacks can be initiated from anywhere around the world against the critical infrastructure, e.g., the malware attack against the Ukraine electric grid [24].

Vulnerabilities within critical infrastructure are a complicated problem to manage effectively. Vulnerability management should go through different phases from identification, to classification to remediation and mitigation [19].

2. **New threats:**

   Cyber threat is a possible danger that might exploit a vulnerability to breach security and thereby cause possible damage. ISO 27005 standard defines threat as “A potential cause of an incident, that may result in harm of systems and organization” [20]. The Federal Information Processing Standards (FIPS) has given a more comprehensive definition for the cyber threat according to its way of usage and its impact on the target: “Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability” [21].

   These threats can be an intentional mission for hacking or attacking, or an accidental result of malfunction or bugs or natural disaster (e.g., earthquake, fire). Exploitation of vulnerabilities can result in loss of information, loss of confidentiality, loss of integrity, or loss of availability. Some critical questions related to cyber threats include [22]:

   - Severity of the threat?
   - Is it possible is to replicate the same threat?
   - What is the effort needed for exploiting and delivering the threat?
   - What is the expected impact of the threat?
   - How challenging is to find out the threat?
   - What is the level of attribution for this particular cyber threat?

   These questions help to build a broad perception about the nature of cyber threats and how to deal with them.

3. **New responses:**

   Cyberspace is another domain for the challenges faced by states in addition to other domains such as air, sea and land. With the development of complex and interconnected technologies, systems and networks, many vulnerabilities have been created which have allowed attackers to overcome cyber defense systems.

   In many cases, cyber defense technologies have failed against cyber attacks [28]. Some have proposed the idea of responding by a cyber attack against the attacker. However, this is not currently practical due to the challenges of cyber attack attribution [141]. Initiating cyber offense against another state is not a trivial decision because it could lead to retaliatory action. Also, it is not clear under which circumstances cyber offensive action should be taken [80].

   The dilemma of proper response to cyber attacks has prompted a search for new preemptive strategies. Cyber deterrence is a strategy to maintain peace and availability of critical infrastructure.

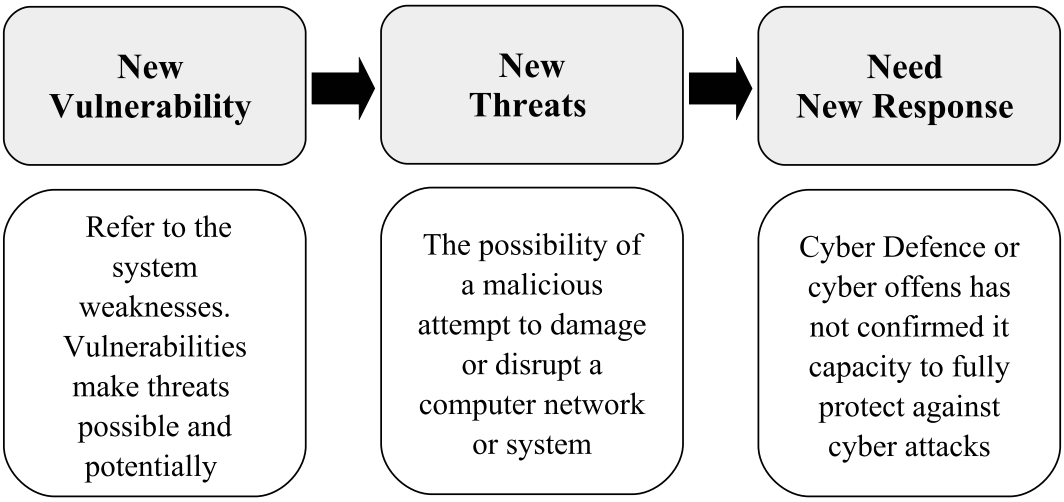

New Vulnerability
New Threats
Need New Response
Refer to the system weaknesses. Vulnerabilities make threats possible and potentially
The possibility of a malicious attempt to damage or disrupt a computer network or system
Cyber Defence or cyber offens has not confirmed it capacity to fully protect against cyber attacks

Fig. 1.1 Cyber Deterrence - Research Motivators

Figure 1.1 show the correlation between the new cyber space vulnerabilities and it consequence to develop new threat to the state national security then the need for new response to aligned with cyber defense as well as cyber offense. Cyber deterrence is expected to play a significant role to balance between cyber offense and cyber defense. If deterrence works, it would be a preventive strategy against cyber attacks. This is similar to what happened during the Cold War. Nuclear deterrence was the cornerstone to preventing nuclear war. Cyber deterrence has advantages that can be summarized as [31]:

- It is a preemptive strategy which is proactive more than reactive.
- It could be easier than cyber defense or cyber offense.
- The cost could be less than cyber defense or offense.
- It is a strategy for peace via showing strength.

1.2 Problem Statement

States need a new option to deal with cyber threats rather than rely on offense or defense. Cyber deterrence can be a better candidate if approached properly. On the other hand, cyber deterrence has its challenges which can be summarised as the following: attribution, retaliation, escalation and credibility [139]. However, there is a satisfactory chance of cyber deterrence to work despite these challenges [34]. These challenges will be discussed more in depth within the literature review chapter. The general questions reflecting this research problem will be:

1. What are the general principles for any effective national cyber deterrence strategy (based on game theory)?
2. How is deterrence theory different in the cyber domain from conventional (physical) deterrence, namely nuclear deterrence?
3. Are conventional principles such as MAD (mutual assured destruction) valid in cyber deterrence?
4. Are coalitions such as NATO effective for cyber deterrence (from a game theory viewpoint)?
5. How does cyber attack attribution support cyber deterrence strategies?
6. How to evaluate and measure the effectiveness of a national cyber deterrence strategy?

Specifically, the main research problem is to answer the general question, "How can a state develop a successful cyber deterrence policy?" Answering this question needs a deep analysis of the fundamental conditions for effective cyber deterrence. States need to look at each condition or challenge separately. This research attempts to split these challenges and tackle each individual challenge.

1.3 Proposed Approach

Our approach aims to develop a cyber deterrence theory inspired by traditional (nuclear) deterrence theory combined with game theory adapting to the uniqueness of the cyber domain. A mixed method (quantitative and qualitative) [35] has been followed due to the nature of cyber deterrence research which consists of two parts.

First, we observe the behavior of cyber adversaries under strict controlled conditions and context within developed models (game model), then observe how players will act. This approach applies more of the quantitative research method.

Second, we observe cyber deterrence in real life practice and how both adversaries (states) will behave. Real life case studies are different from controlled conditions (models). This approach applies more of the qualitative method.

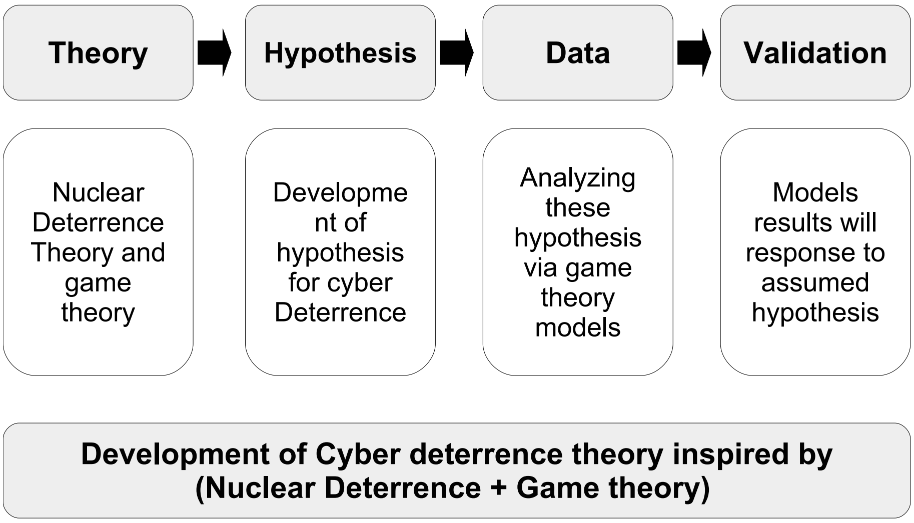

Theory
Hypothesis
Data
Validation
Nuclear Deterrence Theory and game theory
Developme nt of hypothesis for cyber Deterrence
Analyzing these hypothesis via game theory models
Models results will response to assumed hypothesis
Development of Cyber deterrence theory inspired by (Nuclear Deterrence + Game theory)

Fig. 1.2 Cyber Deterrence - Research Approach [37]

The reasoning approach followed is more of a deductive approach than inductive. Deductive reasoning approach reflects a hypothesis developed in cyber deterrence which is based on traditional (nuclear) deterrence theory toward developing cyber deterrence theory. Developing new theory from previous theory is the inductive reasoning approach, and it will complement the deductive approach in this research [36]. The analysis steps move from general deterrence concepts to more specific investigation to the effectiveness of specific strategies. Deductive reasoning approach is opposite to the inductive approach which begins with collecting data related to the research problem, then spends time on investigation and analysis. There are certain differences between deductive and inductive research approaches. Deductive main target is to test the theory while inductive approach aims to develop new theory. In some cases, both approaches complement each other and the researcher may need to join both to achieve the research goals. Figure 1.2 outlines the steps that are involved with a deductive research approach for optimizing cyber deterrence theory.

The approach will make assumptions about cyber deterrence followed by mathematical and logical analysis to explore the validity of the raised hypothesis. It will focus on effectiveness of newly developed cyber deterrence strategies and mechanisms that would lead to deter state cyber threats.

1.4 Contributions and Novelty

While an extensive academic literature exists on cyber deterrence, the literature is almost entirely qualitative. This research is among the first to approach the problem quantitatively through game theory. Specific contributions include:

1. Identifying research gaps by reviewing literature published on traditional deterrence, game theory and cyber deterrence.

2. Identifying general principles for an effective cyber deterrence strategy (based on game theory modeling).

3. Explaining the differences of deterrence theory in the cyber environment from conventional (nuclear) deterrence.

4. Explaining how conventional principles such as MAD (mutual assured destruction) could or could not be applied to cyber deterrence.

5. Developing cyber deterrence principles inferred from traditional deterrence literature.

6. Producing a set of relevant, logical hypotheses about cyber deterrence that could make deterrence function in the cyber domain.

7. Explaining the role of technologies to attribute cyber attacks sources and what extent attribution is practical.

8. Explaining how effectiveness of a national cyber deterrence strategy can be evaluated and measured.

9. Providing a mathematical model for cyber deterrence strategies based on game theory applications. The model will simulate gain, lose and best choices for both opponents.

10. Investigating how coalitions such as NATO can support cyber deterrence (from a game theory viewpoint).

11. Modelling escalation within deterrence games in the cyber domain.

1.5 Thesis Structure

This PhD thesis is organised in six chapters following this introductory chapter. A brief explanation about every chapter content is summarized below:

1. Chapter 2: Methodology

   Methodology chapter provides an outline of the research methodology used to identify the motivations, answer the research questions and problem, explaining research sampling and analysis methodology. In addition, the chapter will explain the limitation of the research method. It highlights the approach of research beginning by review of traditional deterrence (nuclear deterrence) strategies and tactics. It investigates the differences between cyber and nuclear domain for understanding the relationship aiming for producing a precise comparison presenting either similarity or differences. Furthermore, cyber deterrence theory section will be formed as result of joining together traditional and cyber deterrence supported by game theory models confirming the assumption and hypothesis raised within research. To tie this chapter, final section will explain expected strategies to be developed as result of mathematical analysis. Cyber deterrence strategies will be like a road-map for optimizing every state deterrence policy.

2. Chapter 3: Literature Review

   Literature review chapter provides an overview about main concepts of traditional deterrence and many other related essential concepts related to deterrence. Then, the chapter looks at feature selection game theory as a theory for analyzing cyber deterrence showing how game theory models can play a vital role in understanding how players act within cyber domain. The chapter will list cyber deterrence principles with explanation of each principle. Then, chapter will represent the challenges of achieving cyber deterrence followed by a section shed the light over the concern of what make cyber deterrence successfully working and limitations if not successfully working. Finally, the chapter will summarize and survey previous studies conducted in the field of traditional (nuclear) deterrence, cyber deterrence and game theory to focus how these literature will be employed in developing cyber deterrence models by researchers. Specifically, how the knowledge gap will get filled as a result obtained at the end of cyber deterrence research project.

3. Chapter 4: Credibility for Cyber Deterrence

   Chapter four will demonstrate the reason of associate credibility with cyber deterrence. It will analyze the relevance of credibility to cyber deterrence and assumptions for threat of retaliation strategies dealing with (rational and irrational) actors or state. On further thought, game theory working based on a presumption of rationality, then by having deep experimental analysis to a selected situation aiming for optimization current status. From this point, the need for more deep understanding and it will guide how to produce (rational and irrational) decision that help cyber deterrence working successfully. Furthermore, chapter will present a case study as motivational case study supported by mathematical model as experimental evidence supporting assumptions analyzed within chapter. The analysis within the model will aid to develop strategies considering certainty level as supportive factor. The chapter conclude with a section presenting the most successful strategies and lessons that could help optimizing cyber deterrence and helping states with ultimate strategies that lead cyber deterrence successfully working.

4. Chapter 5: Escalation for Cyber Deterrence

   This chapter discusses escalation ladder in cyber space. The approach will develop models for simulating cyber escalation and exploring how players mix their strategies, technology, people, regulations and treaties toward managing cyber escalation ladders or pursuing the conflict and aligning these efforts with national security policies. Escalation is not an easy strategy to followed after immediate calculation of state advancements or one own side advantage. Escalation without certain calculation of state opponent capacity and counter escalation is a total inaccurate strategy.

5. Chapter 6: Cyber Deterrence by Entanglement

   Chapter six demonstrates the need for trying another approach for cyber deterrence compared to traditional deterrence approaches. It is deterrence by entanglement. The chapter will define the concept of entanglement and then analyze the motivators for such like approach for the benefit of cyber deterrence. Chapter will discuss assumptions for developing strategies that lead to achieve progress in deterring state opponent via entanglement. On further thought, it will explore the role of entanglement between two states in supporting cyber deterrence. Follow that, chapter presents a case study as motivational case study followed by mathematical model supporting assumption. The chapter conclude with a section presenting strategies that help optimizing state approaches for the benefit of cyber deterrence and helping states with ultimate strategy that lead cyber deterrence successfully working.

6. Chapter 7: Conclusion

   This chapter summarizes research findings and shed lights mainly over the contribution. It focuses on present tasks accomplished during the research project aligned with the outcomes achieved. Conclusion chapter ties research questions, that has been listed at the beginning of the chapter with the results gained after analyses. In addition, the chapter discusses the limitation within cyber deterrence domain. Moreover, it points to the direction needed for future work.

Chapter 2

Methodology

This chapter provides an outline of the research methodology followed to identify the motivations for selecting cyber deterrence, procedure followed to answer research problem and questions, explaining research sampling methodology applied for analysis [38].

The methodology used in this research begins with reviewing traditional deterrence theory, principles, concepts and challenges in order to promote a theory that could be implemented in the cyber deterrence domain by analyzing research problem with the use of game theory models. The nominated methodology in this research can be summarized into five main prospects:

First, reviewing related nuclear deterrence literature as a main requirement to infer the principles, tactics and strategies that made nuclear deterrence efficient in convincing opponent to act the way it is preferred and assure sustain deterrence as best optimal strategy for the state adversary within the same conflict.

Second, highlight the uniqueness of cyber domain in term of players, vulnerabilities, threats and the nature of cyber attacks. This step will facilitate to compare and contrast between nuclear and cyber deterrence. This comparison will help to identify cyber deterrence principles, challenges and chances of success.

Third, cyber deterrence theory will be formed as outcome of previous two sections via joining together previous nuclear deterrence theory outcomes and cyber domain uniqueness that will leads to an initiation of cyber deterrence theory supported by game theory models for confirming assumed hypothesis.

Fourth, this phase will shed light on the utilisation of game theory for sake of validating cyber deterrence theory via mathematical model by analyzing cyber conflict. The developed model will analyze how opponents interact with each other within cyber domain and how one can strengthen his position for the purpose of deterring the other opponent.

This interaction within models will expand our understanding about cyber deterrence and it will clarify the tactics for maximizing cyber deterrence goals of any state aiming to deter its cyber threats.

Fifth, this section will explain expected strategies to be developed for the benefit of cyber deterrence resulted from mathematical analysis and these strategies will be like a road map for optimising cyber deterrence policy and make it efficient as expected by research hypothesis. Furthermore, methodology chapter attempts to explain the limitation of deterrence research methodology [39] within the cyber domain and how this methodology has tried to resolve this limitation for achieving better results.

In summary, this structured methodology is expected to be legitimate and sufficient to benefit from traditional deterrence experiences, explain the nature of cyber deterrence as well as it engenders cyber deterrence model from game theory point of view. Further more, it answer questions raised within research problem. Achieving all these is actually the essential target of the research.

2.1 Traditional Deterrence Theory

The tragic outcomes of World War II and the use of atomic bombs by the U.S. to blow up Hiroshima and Nagasaki on August 1945 has caused a dramatic change in the types of conflicts between states [40]. Since this holocaust, there has been no nuclear attack despite the undeniable nuclear race between U.S. and Soviet Union during the Cold War. Deterrence strategy was considered as the predominant factor for preventing any nuclear confrontation. As an overwhelming military trend between superpowers, a lot of noteworthy literature was written about nuclear deterrence.

The golden age of deterrence theory was during the Cold War especially in preventing the use of nuclear weapons. Regardless of the debate about the success or failure of traditional deterrence, our aim is to benefit from the literature and strategies that have prevented nuclear confrontation. From this perspective, research methodology attempt to provide an insight about nuclear deterrence confirming its importance to avert nuclear confrontation between superpowers [41]. Reviewing nuclear deterrence theory as part of research methodology is to understand the use of force in cyber similar to the nuclear threat to stimulate nuclear adversary to cooperate for the purpose of enforcing deterrence [42].

Our research methodology examines cyber deterrence theory and how it should work to solve the problem of deterring cyber threats inspired by nuclear deterrence theory. This methodology gives the research rigour through scientific analysis of cyber conflicts and cyber deterrence models. The target is to end with a focus on all related issues that are expected to shape cyber deterrence theory.

The structural process to develop cyber deterrence theory inspired by nuclear deterrence theory brings together different concepts related to nuclear deterrence. Moral lessons will be extracted and inferred from traditional deterrence and utilised while developing cyber deterrence policy for any state.

The methodology is to look at various types of nuclear deterrence strategies and investigate the literature to present what was beyond the success of these strategies. After that, this will help to facilitate modeling cyber deterrence and follow a robust analysis methodology via development of the game models. These models will reflect cyber uniqueness. Models will reveal the strength and weakness of each strategy either during nuclear and cyber deterrence.

Moreover, the concept of mutual assured destruction (MAD) was developed as a result of the nuclear race during the Cold War [43]. The idea is that both states will face mutual destruction in the case that both committed to retaliate in kind (nuclear attack). It was clear that neither state was capable to protect itself physically from its adversary and the probability for escalation and resulting nuclear holocaust to occur also was high. It is not an accepted end for both states due to the consequences. It was one of the supportive concepts to validate the effectiveness of threat between both adversaries despite the debate on whether it is working or not. The idea here is to review the validity of MAD in cyber deterrence.

In summary, the methodology of this research is to absorb the literature on nuclear deterrence theory with consideration of success factors and follow the same methodology. This approach will be like a road map for developing cyber deterrence theory based on game theory models. This approach will clarify the main principles and strategies that form the ground for cyber deterrence theory as an effective theory to deter cyber adversary.

2.2 Cyber Domain Uniqueness

The cyber domain has become a battleground for attacking critical infrastructure. The cyber domain is another avenue for attacks between superpowers in addition to the four traditional domains: land, sea, air and space [44]. These domains have a similarity in terms of military operations, and states need to have the control over each domain.

The research methodology aims to explore the uniqueness of the cyber domain benefiting from similarities between both nuclear and cyber domains in order to understand the validity to implement deterrence strategies in the cyber domain. Different elements include [45]:

- First, players within the cyber domain are different compared to the nuclear domain. In nuclear, the player was limited between state to state but cyber players can be classified as (State - State, State - Groups, State - Individuals).
- Second, technologies or weapons utilised for targeting or delivering the attacks are different. Moreover, cyber attacks vary and at the same time cyber vulnerabilities vary from state to state.
- Third, cyber attacks are generally more complex, stealthier, and unpredictable than traditional nuclear attacks.

In addition, this research methodology considers the vital role of cyber security technologies in supporting cyber deterrence to achieve its goals especially in the face of challenges like attribution and observability. Cyber security technologies have different capacity to support fundamental challenges of cyber deterrence and explore the correct approach to align cyber technologies for the benefit of cyber deterrence.

2.3 Cyber Deterrence Theory

The fundamental target of this research is to establish cyber deterrence theory benefiting from traditional deterrence and to be evaluated by game theory models. The theory is dedicated to deterring cyber threats and producing a peaceful cyber space. Any scientific theory begins as hypothesis that suggest certain solutions need to get approved. Accumulative evidences are needed to support success of any scientific theory. For that, developed theory does not mean it is the final optimal result but there is a possibility to get rejected or it can be improved in the case new data is observed [46].

Cyber deterrence theory aims to replace cyber confrontation with more cooperation for the sake of cyber space sustainability. Applying deterrence in cyber space is confusing compared to nuclear. Deterrence in nuclear depended on the assumption that the first state to attack will be destroyed by another retaliatory nuclear attack. This assumption is difficult to work in cyber as cyber attacks are occurring continuously in the background. This is one of the unique aspects of the cyber domain.

Differences between traditional and cyber deterrence are investigated in order to build up a proper hypothesis for cyber deterrence. Later the assumed hypothesis is examined by mathematical model based on game theory. The cyber conflict interactions are simulated while deterrence strategies are available. Cyber deterrence strategies are modified for each model to observe effectiveness of these strategies in the result of the model. This methodology of analysis provides a good understanding of principles of cyber deterrence, effectiveness of various cyber deterrence strategies, success of cyber deterrence, and the difficulties of deterrence in the cyber domain [47].

The uniqueness of this study exists in the fact that the hypotheses are mathematically tested and modeled in harmony with the strategy of each case that simply forms the cyber deterrence theory. The most difficulty in this part is developing a suitable model that reflects interaction of adversaries as well as the dynamism of state decisions within cyber domain. Cyber deterrence research methodology examine the strategies that help deter cyber threats. This examination been conducted via two dimensions. First, looking at the previous analysis of deterrence in cyber are generally attempting to shed the lights over possibility to benefit from deterrence in preventing cyber threat. Second, analyze cyber conflict by developing useful models that help to gain a deep understanding of cyber conflicts uniqueness. Following this methodology will answer the critical question raised within the research contribution and expected novelty to main issues that are forming cyber deterrence theory.

2.4 Game Theory and Conflicts Modeling

Game theory simply can be described as a mathematical tool that can be utilized to evaluate, describe and analyze particular problem. It is approach that helps to understand the problem by analyzing the interaction between two or more actors. The analysis investigate the strategies that has formed the problem and how each player move aligned with his opponent response [48]. International relations is interaction between specified actors for example between state to state or between multinational corporations. Game theory has contributed in modeling international relations issues related to the conflicts, cooperation, escalation, arm races, deterrence and crises stability [49].

Cyber space security is very complex domain and strengthening the security within the cyber space has become an important mission for the states and its national security team. Game theory has played a vital role in modeling different complex security issues. It provide a closer analysis about cyber conflicts and the interactions between attacker and defender [50]. Another developed model aim to explore player strategic interactions for the purpose of securing the networks [51] and these interactions are either opposing, challenging or cooperation [52]. Moreover, models are developed for the purpose of optimizing cyber security technologies like intrusion detection [53] and wireless network sensors [54] and its security. Game theory also has the applicability to contribute into modeling cyber attacks like DoS and DDoS attack [55]. Another model is based on game theory was developed for the purpose of forecasting cyber attacks [56]. Model methodology is to explain the interaction between attacker and defender during the DoS as single attack and during DDoS as multiply or distributed attacking nodes for the purpose to understand the nature of DDoS cyber attack.

The application to analyze the strategy of nuclear deterrence is not a new application but due to the increase of cyber threat against state critical infrastructure [57], the idea of the project is to benefit from traditional (nuclear) game theory and strategies by developing new models that is particularly working in analyzing the interactions between (Stat- Stat) cyber conflicts.

Methodology of this research is to utilize game theory as a tool for modeling cyber deterrence scenarios to understand how state can actively deter another state from conducting any cyber attack. The model is expected to provide a deeper understanding about the cyber conflict and strategies of cooperation among adversaries. Cyber deterrence model will begin from looking to the nuclear deterrence model that has been developed for the purpose of deterring nuclear adversary.

Cyber deterrence is a strategical situation with different players which may not be sufficient enough to analyze it with a simple game model compared to the nuclear deterrence game model and it might need to get expanded to a different models. Developed model will differentiate deterrence between different situation of cyber adversaries and their tactics within the cyber conflict for the purpose of all dimensions analysis for the same problem. First player should not act without considering his opponent response, and at the same time he cannot react to the opponent action without figuring out what strategy is going to follow for optimizing the payoff.

Strategic scholars has recommended game theory due to its capacity the analyses needed for such kind of strategic conflict and help to prescribe strategies that lead to progress current situation (statues quo) to a more peaceful domain. The main challenge of cyber deterrence game models is to deter state adversaries and keep cyber domain a peaceful domain for the benefit of all players as it is a share domain and at the same time all players need to keep it as domain of peace and cooperation.

The model is a tool that can be utilized for describing, evaluating and testing hypothesis for a certain selected problem and each game model consist of four main elements [58]:

1. Players: those involved in the same game whom could be human, devices, organization, animal or any other objects. So, players will interact with each other during the process of analysis.

2. Actions: Each move of every player within the game is considered as an action taken. For that, game theory helps the player to estimate/anticipate opponent next possible action.

3. Payoff: What each player gain within game interaction could be either positive or negative.

4. Strategies: It is the plan of players actions that he is going to take based on knowledge, background and expected consequences.

According to these elements within the game and for modeling any strategic problem, the game should get developed based on very strict criteria to assure problem alignment with model structure. Games can be classified according to criteria like: number of players within the game; players playing simultaneously or sequentially or random; players having perfect information when about to move or imperfect information; players having complete information or incomplete; zero-sum games or not; communication between players allowed or not; cooperative or non-cooperative [58]. When players negotiate, are the results of the negotiations enforced? Do they adhere to what they agreed upon or not? If not, a player can always move differently from what was promised in the negotiation (cheap talk).

In summary, deterrence policy is a strategy for cooperation rather than confrontation. Cooperative game is similar when the result of negotiation are to be enforced among the members of the coalition or players within the model [59].

2.5 Cyber Deterrence Strategies

The nature of cyber space is determined by many factors such as complexity, deception, players and threat severity. As we are investigating the methodology of optimizing cyber deterrence inspired by traditional deterrence, we need to consider the uniqueness of cyber space. Research approach aims to investigate the practicality of deterrence as well as producing practical strategies for cyber deterrence that states benefit for optimizing cyber deterrence. On the other hand, punishment like economical sanctions, military operations, or political negotiations may not be totally applicable in the cyber deterrence due to the unique nature of the cyber domain.

Lack of strategy in deterring cyber threats will give open invitation for foreign adversaries and malicious cyber opponents to continue targeting the state. This happens when state fails to develop, form, implement and declare its cyber deterrence doctrine and strategies.

The methodology of this research will help to explore cyber strategies that establish the ground for the cyber deterrence strategy (cyber defense and offense). Cyber deterrence model investigates practical strategies with corporation of security technologies or other strategic tools. Another example of strategy is the utilization of current available capacity for different deterrence mission like observability of cyber domain or threatening opponent who seek to send a a message regarding state credibility [60]. Developing offensive capability and holding the permission to initiate offensive operation in cyber is not yet a mature idea as it is leading to unwanted provocations.

Immediate and extended deterrence concepts are developed in alignment with the nature of threats being faced. These two concepts (immediate and extended) resulted from traditional deterrence literature and there is a need to adjust them for the benefit of cyber deterrence. Generally, any strategy consists of short term or long term objectives to be achieved. Likewise, the cyber deterrence domain needs to have immediate deterrence and extended deterrence strategies [89].

Strategy for immediate cyber deterrence listed in table 2.1 is responsible to deal against an immediate, known cyber threat whereas future (extended) cyber deterrence strategy determines how to deal with future highly expected cyber threats. But the most critical question here is how to develop effective cyber deterrence strategy and how to select the best strategy to respond against an immediate known cyber threat. The strategy of response against cyber attack hitting critical infrastructure for first time causing very limited damage is different from another highly severe, repeated attack. For that, both immediate and extended strategies for cyber deterrence are needed and made ready according to the conditions of the attack and attacker.

We assume three phases of practical cyber deterrence (Observability, Attribution and Retaliation) are relatively integrated in functionality. This assumption helps to make precise judgment regarding the strategy of response parameter in term of (WIN/LOSE) and assist national security staff to select the best optimal strategy. To remove the fog of the scene, the model will align strategies with a parameter weighing out both the strategy and its expected results according to the conditions of the conflict helps any state to evaluate current and future situation based on (WIN and LOSE). This parameter in table 2.1 is modified from traditional military strategies to serve the objective of cyber deterrence strategies [62]:

Immediate/Now	**Future/Extended**	**Strategy**
LOSE (weak deterrence/ defense)	LOSE	Retaliation
WIN (strong deterrence/ defense)	LOSE (opponent will escalate)	Retaliation
LOSE (weak deterrence/ defense)	WIN (strong deterrence)	NO Retaliation
WIN (strong deterrence/ defense)	WIN (strong deterrence)	NO Retaliation

Table 2.1 Cyber Deterrence Strategy Parameters

In conclusion, research methodology followed (represented in Fig (2.1)) will lead to develop strategies that help state in deterring cyber attacks. This strategies support states to discourage its cyber adversaries not to initiate any cyber attack and if they did so the consequence would result a lose for the attacker. Strategies could provide balance between promises of incentives or threat of punishment (carrot or stick) and guarantee the lost for discouraging by losing any expected gain. Cyber deterrence strategies will need to structure a sort of cooperation with other cyber defense or offense strategies [63]. As the deterrence is in the between offense and defense, it is very critical for cyber deterrence strategy to consider other strategies for the benefit of cyber deterrence strategies.

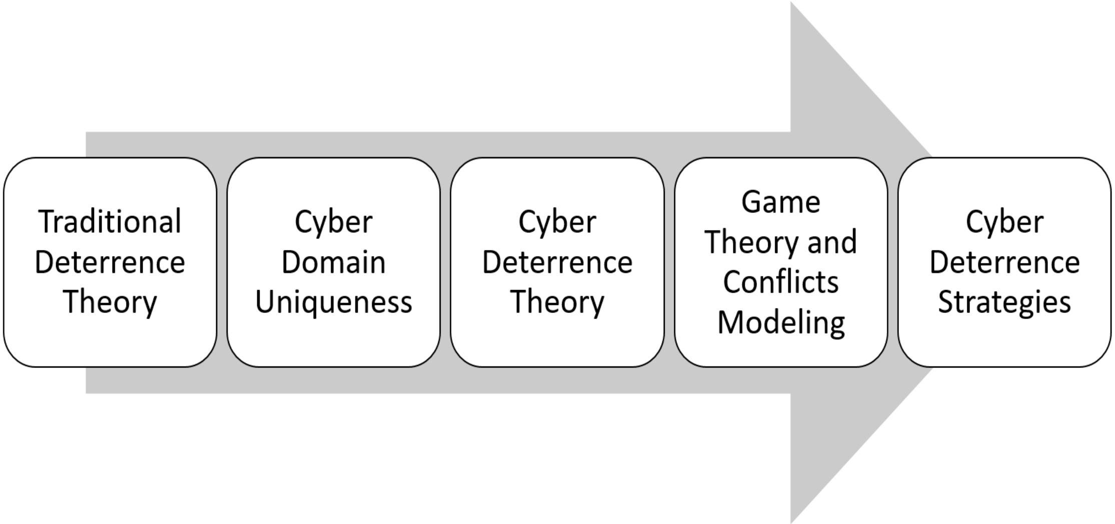

Traditional Deterrence Theory
Cyber Domain Uniqueness
Cyber Deterrence Theory
Game Theory and Conflicts Modeling
Cyber Deterrence Strategies

Fig. 2.1 Research Methodology

Chapter 3

Literature Review

3.1 Preface

The aim of this literature review chapter is to establish a theoretical framework for cyber deterrence. The research project aims to optimise cyber deterrence by developing certain strategies. Cyber deterrence strategies are inspired by nuclear deterrence strategies. Systematic literature review is the formal way for synthesizing the literature which has been written on nuclear deterrence, game theory and cyber deterrence.

The work begins by tracing the root of the deterrence concept, definitions given, history of its practice. Then, it sheds light on the role of deterrence in preventing or avoiding nuclear conflicts not to escalate. It enumerates advantages and shortcomings of deterrence in preventing nuclear conflict and maintaining peace between different states.

In addition, this literature review chapter justifies the choice of game theory for modeling cyber deterrence. It deeply investigates how game modeling can play a vital role in understanding how players (States) can act within cyber domain. The chapter goes through cyber deterrence principles that every state needs to consider when practicing deterrence policy. Also, the chapter reviews cyber deterrence challenges giving a quick overview to what makes cyber deterrence work successfully and what are the limitations. The chapter will conclude with a summary of the important aspects of the current literature, evaluation and attempt to identify the knowledge gaps.

Producing systematic literature review will give cyber deterrence research guarantee of finding most relevant literature aligned with many other advantages for the cyber deterrence research community. These advantages can be summarized as [64]:

- Mapping current cyber deterrence knowledge before researchers launch any repeated work.

- Identifying gaps of knowledge within the cyber deterrence domain and researchers will avoid any bias within the work.
- Publishing this systematic review and helping other cyber deterrence researchers avoiding any duplication.
- Highlights of cyber deterrence areas where additional future research is needed.

Towards the goal of the literature review, there is a need to align it with research requirements such as research problem, research questions, research methodology and approach followed. This alignment will achieve the expected advantages from following systematic literature review.

Literature Review Methodology

The approach followed in selecting and classifying the literature is focused on three parameters (traditional deterrence, game theory and cyber deterrence) and the work has been executed via three main phases can be simply explained as:

1. **Planning:** The Main objective of this phase is to specify the literature we are looking for and the parameters we should follow aligned with the research project problem and research questions. Focusing the literature over the research problem “Cyber Deterrence” will drive research project gain up to date understanding about this particular topic. Moreover, lead the current research methodology similar to the methods practiced with previous researches conducted in deterrence fields.

   Specifically, literature is carefully selected that that are linked to the main research question and utilized to bridge traditional deterrence studies to the benefit of cyber deterrence theory.

2. **Executing:** As the fundamental problem of this research project is “How state can Successfully Deter Cyber Attacks?” inspired by nuclear deterrence and what states should practice in this regards. Based on this mission the selection, filtration and prioritization of the literature was conducted. For that, *nuclear deterrence*, *game theory models* and *cyber deterrence* were parameters for selecting the literature. Other issues were considered like linkage to the research problem, quality of publications, credibility of publisher and specialty of the authors.

3. **Reporting:** Reporting is the final phase of reviewing the literature task. The structure of reporting begin by introducing main concepts of deterrence and traditional deterrence. Then explain different concepts related directly to the deterrence field. Then list

> related work been conducted based on the game theory and deterrence modeling as background for benefit cyber deterrence analysis and modeling. The chapter summarizes the knowledge that has been identified from literature review phase. Identifying the knowledge gap of this research and response to it can be assumed as the final contribution of the research project.

The literature review subjects are structured as per the research methodology. The framework build to serve research approach and to help to provide answers for the research questions. The chapter has been organized as follows: Section 2 introduces deterrence concept and historical background regarding benefits of deterrence in conflict prevention. Section 3 discusses various types of deterrence, the discussion includes details of methods and threats conditions used by each opponent. Section 4 reviews the nuclear deterrence theory and the development of the theory and its involvement in preventing nuclear confrontation and how to benefit from these strategies into cyber domain for the benefit of deterring cyber threats. Section 5 identifies the uniqueness of cyber domain compared to nuclear and what is the role of these uniqueness in supporting cyber deterrence success or failure compared to nuclear. Section 6 goes through cyber deterrence principles and challenges giving a quick overview then going through what make cyber deterrence successfully working and limitations of the failure. Section 7 reviews the literature that mainly discussing deterrence principles and attempt to transfer these principles to cyber era. Section 8 goes through what are the challenges of cyber deterrence. Finally, Section 9 summarises what could make cyber deterrence theory work successfully and limitations if expected not working. Finally, section 10 summarises the literature review chapter and specifies a research road map.

3.2 About Deterrence

History has given humanity enough lessons proving that conflicts are ultimately harmful for all opponents; which resulted into fetching for less harmful solutions. Strategies for manipulating opponent behavior has been implemented hoping for achieving the goal of averting any further escalation. The attempt here is to provides an adequate etymology to give definition for deterrence inferred from previous literature given by theorists, linguists and specialists of deterrence studies.

Thinking about simple concept of deterrence could happen when a mother tell her children to stop "eating sweet is permitted twice a week, and if you violate I will stop buying any sweet for two months", in such like case the mother is practicing deterrence. There is certain complication between threats and promise that forms the practice of deterrence. Due to conditions of threat, the behavior of children assumed to work. Deterrence could be approached with balance between threat of punish and promise of reward. success and failure of deterrence in different context are essential to have a deep absorption of the whole context.

States are having very strong motives to deter any conventional attack and in some cases to deter these attacks not to occur for their allies similar to what has happen during World War I, each superpower has tried to deter and interference with other superpower [65]. Of course, there is no mean to limit deterrence to nuclear domain or military missions. It is broader than that and it can be practiced in several field for the target of preventing a particular behavior.

Several studies have been developed toward deterring other violence like deterring biological terrorists [66], deterring social criminal and many other deterrence policies has been developed utilizing similar concepts but having different practices. within these studies a lot of debate happens regarding measuring success or failure of deterrence and how to confirm either this or that. Other debate about what is the perfect deterrence strategies could fit to this domain and could not fit with other deterrence domains. Another factor that has increased the attention to deterrence strategies and effectiveness, is deterring non-state terrorist. This problem is different from deterring drunk driver fatalities due to the differences between both situations. Both cases are under the general concept of deterrence theory but each context has its own uniqueness and need different practice to achieve its objectives [67].

The simple model about deterrence in international relation is when first actor tries to discourage the second actor from committing a particular task. The State "(A) deter (B)" statement reflects the situation or the normal implication of statement mentioned. This situation could be between two nations or two states in a conflict regarding one particular threat. It means that state (A) attempting to deter (B), and we need to look at from state (A) point of view. This can be titled as state (A) deterrence strategy [68].

Traditional deterrence theory began as a general theory then was developed in various waves because of the evolution in the recruitment mechanism of the concept of deterrence and the challenges that grow in international relations. Different concepts has developed to describe how deterrence get in practice as well as the complexities that have emerged in the threats that deterrence strategies attempts to deter. The development of theory has been categorized due to the continuous challenges that encountered deterrence to achieve its aims. Deterrence theory has been founded as strategic military theory for deterring opponent from initiating any surprise attack like nuclear. So, the theory has been established during the cold war [69].

Enormous interest was given to the nuclear deterrence theory because of its promising critical role in the conflicts and international relations affairs. Precisely, the studies about nuclear deterrence has grown especially after Hiroshima and Nagasaki atomic attack as many theorist consider this attack was like major deterrence action discouraging Japanese and many other nations not to go further in the conflict. But, another debate raised regarding sustainability or failure of deterrence in nuclear, also, capacity of deterrence policy in preventing the spread of nuclear weapons. As there are a different states working to develop their nuclear program, this has been considered as failure of nuclear deterrence [180].

Deterrence like many other subjects, has its dynamics held by a variety of factors. Most important among these factors is a divide between formal theories and the analysis of success and failure of particular deterrence strategy. In this research, we will try to distinguish between different deterrence types and justify which could work better in the benefit of cyber deterrence.

Linguistically, The root of the word Deterrence is "terror" [71]. In the Merriam Webster English dictionary "deter" is defined as to "discourage (someone) from doing something by instilling doubt or fear of the consequences". The dictionary has added another definition for the politics schools which is defined deterrence as: "the policy of developing a considerable of military power so that other countries will not attack main country."

One of the best studies that has been produced in the analysis of the term deterrence, as well as the semantics of each definition of the other definition was conducted by Morgan [72]. He has reviewed what each definition attempt to explain for example the first definition which is attempt to refer to two things within the same definition. The definition refer to the policy of deterrence and the situation of deterrence:

"A policy of deterrence is a calculated attempt to induce an adversary to do something, or refrain from doing something, by threatening a penalty for non-compliance. A deterrence situation, or system, is one where conflict is contained within a boundary of threats which are neither executed nor tested" [73].

The issue with this definition is separating between policy and situation, this could be broken down under careful examination. Deterrence situation is one and the one of the adversary within the conflict that should follow the deterrence policy and no chance to both adversary to be outside the situation of deterrence.

Another deterrence definition discussed from the dimension of national security prospective. The definition is more precise in term of defining the objectives from deterrence, it is:

"Simply put, deterrence means that State A seeks to prevent State B from Doing Z by threatening B with unacceptable costs if it does Z" [74].

This definition has several points that is important to shed light on. It has stated clearly that the adversaries are states were the deterrence can be applied. Another point, states involvement in deterrence is a valid due to the issue that states usually get influenced by outside world.

What is similar between these two definitions is the condition that if one adversary conduct unwanted action by the another adversary the condition after the action will not be similar as it was before. To deter an action is simply to frighten the doer from acting or behaving in a certain way. This term is widely used in military field and recently it is hesitantly used in the cyber domain.

Lebow has also studied the concept of deterrence and he showed how deterrence was used as tactics for over 2000 years [75]. To achieve the objectives of this definition will require an effort to convince the opponent that the cost of incur will outweigh any gains expected.

Another dimension for the linguistic meaning of deterrence concept important to discuss, is the definition developed by united state department of defense, they define deterrence as *"the prevention from action by fear of the consequences"* [76]. Considering the deterrence as a psychological than military problem is a valid point as the deterrence requires manipulating others behavior under given conditional threats. In other words, utilizing deterrence strategies make the attacker recalculate the cost of his action. which is going to overweight the bad consequences or the potential benefit of the attack? The psychological point of view to the both adversary is a valid point as the deterrence in total a behavioral manipulation and this lead to the point that the decision maker should be act rationally for both states.

Most of these definitions are generally defining the deterrence as concept with slight differences. This research is about implementing deterrence in cyber space and particularly between two states as adversary in cyber conflicts. For specifying the concept of deterrence we need to narrow the definition as per the strategy of deterring the particular threat. A detailed exploration the next section of this chapter is part of what the research attempt to accomplish.

3.3 Deterrence Types and Threat Conditions

A good amount of literature had been produced and need to be surveyed and to get organized in a scientific structured way that straightforward categorized literature review from traditional to the cyber deterrence. Also, it could be because of shifting the concept of deterrence from one domain to another, or change the utilization of deterrence from issues related to our daily life to the issues that are purely international relations. Referring to the nuclear deterrence theory, it is based on three core structures in order to succeed: (a) The deterrer should develop a sufficient capability, (b) The threat used for deterrence should be credible,

(c) Then, the deterrer should be able to communicate the threat to its opponent [77]. These elements should be activated in all deterrence classification. It is needed in narrow or general, and in immediate or extended, and either deterrence by denial or by punishment.

The attempt here is to satisfy the literature with discussion regarding the general concepts that has formed the strategy of deterrence and put it on the right direction for the benefit of cyber deterrence. The general understanding about deterrence is to prevent something might happen. It could be to prevent military attack, but it could also be to avert state from giving assistance to criminal groups or another state for exporting other types of threats. The target here is to study the nature of relation between the types of deterrence and threats that deterrence strategy aim to deter. Clarifying the relevance between the threat and deterrence is an essential step for matching the condition of deterrence strategy and threat conditions.

Threats should be defined before establishing the strategy and the team in charge of developing deterrence strategy should get a clear, defined and determine its function and the conditions of targeted threat. In other words, strategic deterrence include conditional threats and these threats are different according to what strategy aim to deter and how to achieve. Here there are four distinctions based on threats condition: Denial and Punishment, Narrow and Broad, Extended and Central, Immediate and General Deterrence [89].

- **Deterrence by Denial or Punishment [90]:**

  The value of deterrence for any particular type rely upon its effects on four essential factors in the opponent (gain- lose) calculation. Before taking any action opponents will assess the probability of retaliation or any military response, the cost of suffering if the probability of response is high, the value of gain if response probability is low and the probability of success in the mission. Differentiate between the deterrence by denial and deterrence by punishment is a reflection to these factors and the probability of retaliation or response the valuation of gain and loses. The assessment of each opponent intention is highly uncertain mission involve intangible and unknowable factors as value preferences. That is why this calculation is more tangible with deterrence by denial more than punishment. It is useful to distinguish between deterrence resulted from capacity to deny territorial gain to the opponent, and the deterrence by threat of punishment.

  Deterrence by denial is when someone develop the capacity such as surrounding wall, gigantic army or many other capacity to deny opponent or to make it very hard for succeed the attack. Which mean to control the situation in order to deny the opponent decision. So, if attacker decide to attack it will be very costly and very hard to success the attack. To achieve the potentials the opponent will calculate what to gain and the amount of lose and simply assumed to get deterred.

Deterrence by punishment is a pure coercion strategy, where the opponent did not denied the choice and attack by having a powerful incentives to choose to attack in a particular way. Even with deterrence by punishment there are some conditions for calculating the cost of (gain or lose). The practice deterrence by punishment during nuclear was via threatening opponent with a threat of nuclear retaliation if decide to attack by nuclear, the punishment by nuclear retaliation will guarantee destruction. So, between threat and promise, commitment of retaliation even after first strike deterrence by punishment are working. Punishment capability usually (nuclear power) working as massive or limited threat of retaliation, acting primarily after second factor of deterrence (denial). This distinction could not be absolute but estimation resulted from reviewing both definitions.

Fundamentally, deterrence by denial is more reliable strategy that deterrence by punishment. It is because if the threat to get implemented, it will give control rather than continue with the strategy of coercion and depend on the capacity to success the threat against opponent. With the punishment, the deterrent to decide how much need to decide what to do regards. Other issue is the capacity of B to deter A and what is the condition that B will exceed the value or not of the threat. These comparative will appear during the modeling of the conflict in the coming sections.

- **Immediate and General Deterrence:**

  Immediate deterrence as described by Patric Morgan [72] as a relationship between opposing states where at least one state is seriously considering an attack while other state still mounting the threat of retaliation in order to prevent it. Sometimes immediate deterrence is used in haste at a time of crises, emergent time without planing ahead for such an early aggression, This kind of deterrence is done in a short time with high level of anxiety.

  General deterrence when adversary who already maintain the armed forces adjust their relationship even though neither is anywhere near mounting an attack [89]. This occurs when opponents already make regulations and continuously strengthening the armed force in relax mood. The general deterrence strategies are almost routine and non-specific and deliberately not to be in need for further actions. However, when relationships with other states becomes unstable, then immediate deterrence is strongly urged. In general deterrence, state B might have consider to use the force against state A, but it decide not to press on when B receive a rather ambiguous threat from A. This situation could be sustain for long period and it could be forgotten after certain period of time if A not create another threat to B.

So, to differentiate between general and immediate deterrence we need to understand the degree of the strategic engagement between both states (A) and (B). Immediate deterrence involve the active and the urgent effort by (B) to deter (A) within the course of conflict and the effectiveness of threat of (B) to effect (A) decision. While general deterrence strategies are more relaxed and its more depend on the (A) assessment either to cooperate or not to cooperate with the source deterrent. There are a plenty of deterrence cases fall into the concept of general deterrence.

- **Extended and Central Deterrence:**

  The centralized and extended deterrence strategy concentrate to investigate whether state should extend its support to its alliances or limit the deterrence strategy only within its direct national security threats. Another dimension, does the state need to extend its deterrence if alliance is not capable and consider it as preventive deterrence strategy? The question raised highly concern regarding United state whether it should initiate nuclear war on behalf of third party if unable to protect US homeland against Soviet retaliation. The challenge is how to mix deterrence operation between political and nuclear attack for the purpose of deterring opponents. Kahn is considered to be one of the theorist during second wave of deterrence theory. He has distinguished three types of deterrence, first, the deterrence that involves superpowers and nuclear exchange, Second, the deterrence that involves conventional or tactical nuclear attack and involve allies, Third, most of general deterrence types like deterring criminal violations and its challenges [87].

  The scenario of central and extended deterrence is like when state (B) aim to deter (A) in cooperation with other alliance and both states (A) and (B) acquire nuclear arsenal. Not all stages of conflict will demand to threat by use nuclear and it could be in harmony with the political demand. So, to extend deterrence in cooperation with alliance based on political justification and whether state need to act centrally without relying to alliance. Central deterrence is believed to have higher efficiency than extended deterrence. The motivations of the state to threat its opponent is more understood compared to the extended, because it appears when US got the interest to cooperate with other powers to preventive deter Soviet Union via NATO. So, it was like USA interest to extend.

- **Narrow and Broad Deterrence:**

Narrow deterrence mainly involves deterring one particular selected type of military operation within a war, whereas Broad deterrence objectives to deter the whole war [89]. Referring to the history and traditional conflicts twenty centuries ago, there was no multi types of weapons similar to what has been produced during and after world war I and II. The expansion in developing different types of weapons and attacks has produced a real complexity in deterring these different weapons and producing anti-weapons for failing any attempts of attack or assure there is no success for any of these developed weapons against the anti weapons. Logically, Deterring limited one particular type of weapon/attack is easier than deterring multi type of weapons within the conflicts.

As example, after first world war the use of poisoned gas has been used and then there are serious actions to ban any use of it. In 1925 they initiated a protocol and they agreed to allow to hold but not to use and if any usage happen it will be followed by retaliation and guarantee all would be losing. So, narrow deterrence approach is promising more success than broad approach. Restrain the growth or disarmament can be achieved when approach it with specific mission and narrow tactics.

From my point of view *Narrow Deterrence* is more beneficial and more measurable and it has more leverage for cyber deterrence than broad deterrence. The cyber threats/weapons are various, hence a particular deterrence must be narrowly directed to each specific cyber threat. To clarify, what is benefit to deter DDoS attack might not work to deter manual attack from technical as well as strategical point of view. This specific strategy is more accurate and measurable.

Most of the literature look at cyber deterrence from the nuclear and broad deterrence approach. In terms of practise, it is incomparable to the cyber deterrence because the nature of cyber threats with all it varieties differ from nuclear threat. To be more specific, when state practise narrow deterrence it should select one particular cyber threat then implement deterrence by denial via hardening its cyber security controls. If this did not work, then it should go for deterrence by punishment approach and look if it works or not. So, for discouraging all forms of cyber aggression expect to be more beneficial to follow more narrowed approaches.

3.4 Nuclear Deterrence Theory

Traditional deterrence theory began by explaining how to prevent wide population from committing a broad range of different categories of offense. Deterrence as a concept is a general situation that is not limited to the military or conflicts. It can be practiced in different fields of human interaction either individually or collectively and this project is an example of implementing deterrence in cyber space. One of challenges with the traditional theory is that the scope of the theory was very wide but overall it was like a foundation for other deterrence theories to get established.

Nuclear deterrence theory is one of the best examples and it has played a vital role during the cold war to keep it cold between US and Soviet Union. It was the central and main focus in most of the international relations and strategic studies during the cold war and nuclear conflict between the superpowers [41].

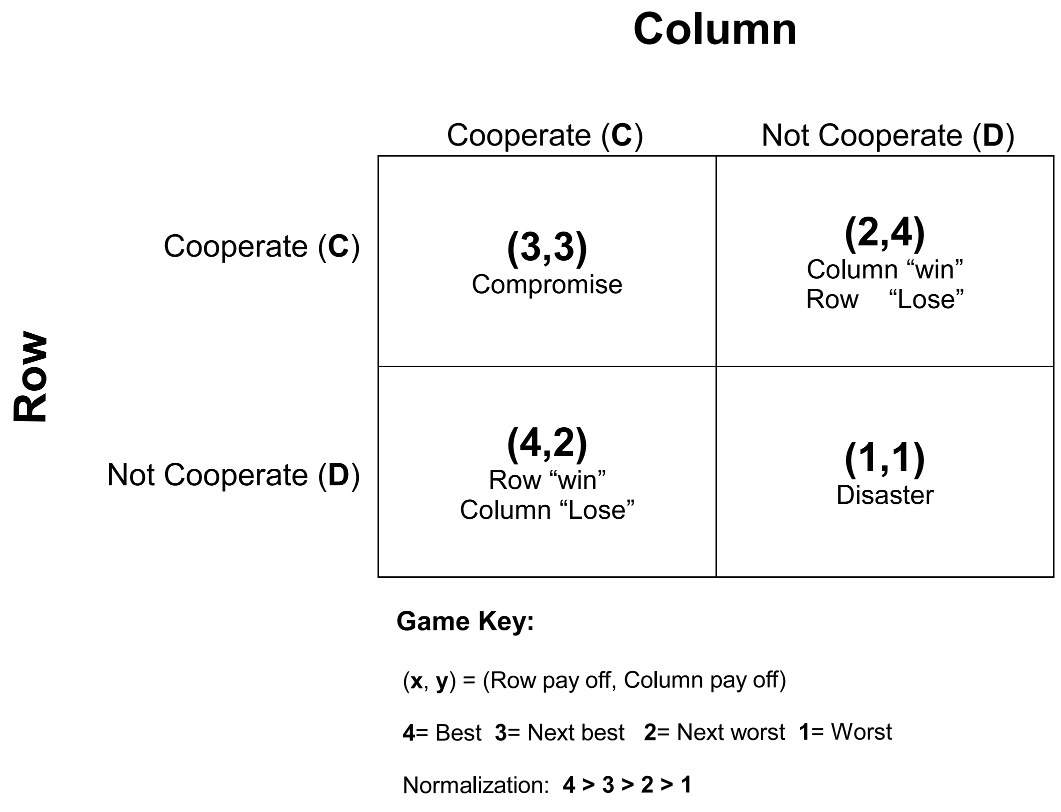
Nuclear arm race has encouraged scholars and strategist to produced a lot of literature explaining nuclear theory and its strategies in military and many other conflicts domains. But, as known nothing is perfect and this theory as many other theories became obsolete or get developed after a period of time. One of the best references that explained the deep meaning of the theory was written by Steff [88]. He described the root of the theory and what sort of development has been produced. The author divided the theory development to four main waves compared with Freedman [89] who has decided that there are only three waves of the deterrence theory. Each wave or each stage consist of certain principles and the differences between each wave will be explained in (section 3.2).

Traditional deterrence theory literature has discussed the need for defense, observability, attribution and readiness for retaliation as core for assuring successful deterrence [91]. Similarly, cyber deterrence follow the same by assuring availability of powerful defense controls in place to make it hard for the defender not to attack easily. Then, developing the optimum level of capacity for attributing cyber threats and identifying sources of attack. Also, attribution usually prepares the land for the decision of retaliation. Retaliation is based on the readiness, capacity and capability of the state. Moreover, retaliation could be initiated immediately or after period of time and the retaliation should be specific against the attacker or could be against random targets as retaliatory action for future deterrence.

There is a large amount of literature about the deterrence but there is not much about deterrence models. Focusing on game theory models and formulation, there is a discussion done by both Steven Brams [92] as well as by Zagare [157] and their analysis was from theoretical and practical perspectives. The advantages of game theory is that it gives a chance to a acclimatize the model to the real problem in real life and analyze the strategic interaction. Plus, game rule assist in setting boundaries to the model to the research problem. For example, the assumption of players pre-committing to threat opponent is accepted by the game rules.

Generally, deterrence game model is mainly based on the two player chicken game. Chicken game is similar to the prisoner dilemma; each player within the game can swap between either strategies: Attack (D) which reflects behavior of Non-cooperation or strategy of Non-attack (C) which is confirming the behaviour of Cooperation. From deterrence perspectives these two strategies can be closely titled as attacking and Not attacking. These two strategies will consequence four possible outcomes shown in Fig. 3.1.These strategies can be summarised as:

- Both Players follow strategy of Cooperation (C). The payoff for both is the next best (3,3).
- One player prioritize strategy of Cooperation (C) while second player prefer Not-cooperate (D) and the next worst. In this case, the second and third outcomes are either (2,4) or (4,2).
- In the fourth outcome, both players are not willing to cooperate and they end up with (1,1).



Row \ Column	Cooperate (**C**)	Not Cooperate (**D**)
Cooperate (**C**)	**(3,3)** Compromise	**(2,4)** Column "win" Row "Lose"
Not Cooperate (**D**)	**(4,2)** Row "win" Column "Lose"	**(1,1)** Disaster

Game Key:

(**x**, **y**) = (Row pay off, Column pay off)

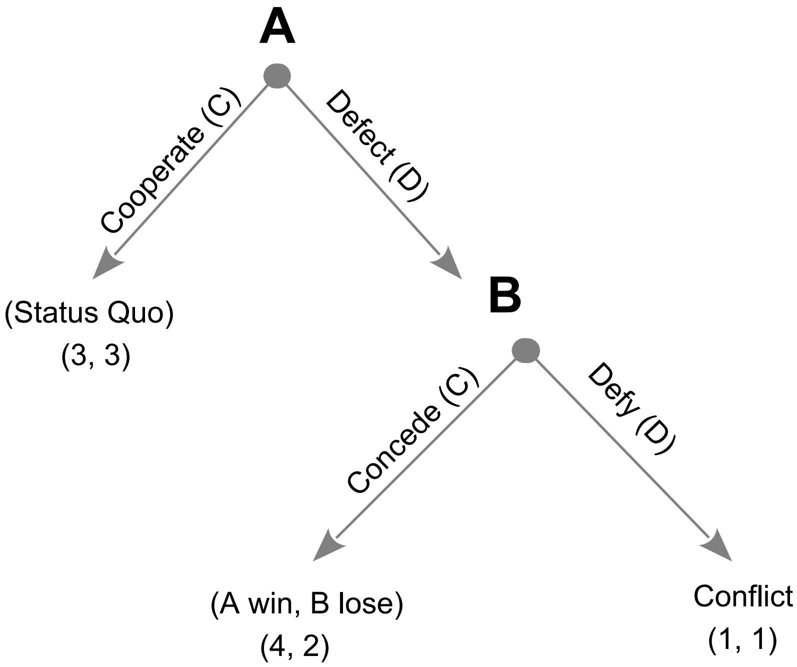
4= Best **3**= Next best **2**= Next worst **1**= Worst

Normalization: **4 > 3 > 2 > 1**

Fig. 3.1 Outcome Matrix of Chicken Game [92]

In this game model the Row can gain more if he select to attack where Column is not attacking and this will end up with payoff (4,2). In opposite, Column will end with a better outcome if attacking while Row is not attacking to get the payoff (2,4). But the problem here when any player confront opponent and choose Attacking (D), he will maximize but the risk here he might lead to mutual disaster (D,D) conflict.

The classical deterrence game as mentioned earlier was constructed mainly on the same rules of chicken. The expected payoff for both players Row and Column is limited to four outcomes between Cooperation, win/lose and Conflict. In this game there are two player: State (A) and State (B) in a conflict. State (A) may try to attack (B) while (B) is maintaing deterring (A) from initiate any attack. The challenge here what could make (A) not to attack (B)? How state (B) can maintain (A) to be deterred and enforced to *Status Quo*.



(A, B) = (Pay-off to challenger **A**, Pay-off to Deterrent **B**)

4= best; **3**=next best; **2**= next worst; **1**= worst

Fig. 3.2 Classical Deterrence Game [157]

Classical deterrence model shown in Fig. 3.2 is limited and there is a need to change it to the extensive game model. This will assist in expanding the model and widening the explanation, classical deterrence theory offers two main solutions for the deterrence challenge [68].

First, deterrent state -which considered in this model is State (B)- should make unchangeable commitment to burn the bridges to limit its opponent options for any back down [68]. This commitment should be confirmed and communicated clearly for the adversaries. This communication will keep State (A) in a position either to maintain *Status Quo* and cooperate with State (B) and this is where deterrence working. Otherwise, (A) challenge and attack State (B) and at this point a conflict with high probability starting.

Second, it is the threat that leave something for chance [93]. This threat will allow deterrent State (B) to surround the problem of irrational action via threatening to take action. This approach will raise the risk level that the situation may lead to miscalculation and lead to escalation and it is the nuclear conflict that will result into nuclear catastrophe. Between these two solutions there is a possibility of each player to act irrational and to go for a great risk of mutual assured destruction for pursuing their goals and here where credibility is required to face the irrationality.

In the deterrence game, there are two stages: First stage, each state (A) + (B) choose either to cooperate or not to cooperate. The second stage, each state can choose either to retaliate (defy) or not to retaliate (concede). In case state (B) retaliate to (A), this retaliation could lead for further escalator ladder within the conflict. If not retaliate, it will let (A) succeed in the attack and win the battle.

At this stage, consider the outcomes of the second stage and State (B) acting upon:

- State (B) choose Not attacking at the second stage in the case his opponent choose Attacking, Or Attacking in case Not attacked, which is more to preemption and lead to (tit-for-tat) outcomes

- State (B) choose Attacking regardless what State (B) opponent selected at the first stage, (Unconditional Cooperation) and this keep threat of retaliation high for deterrence mission.

Because State (B) decision is based on its capacity and capability into threatening its opponent. Moreover, it is reflecting its strategic information about opponent intentions into next stage. Threat credibility of the deterrent state playing vital role at this stage aligned with the perfection of strategic decision reflecting model payoffs.

Deterrence game outcomes gives each state three possible outcomes. First is the *3 = cooperation* (Status Quo), Second is *4 = Winning* by attacking and preemting, and Third is the *1 = conflict* between both actors. These outcomes from each state rational point of view can be structured like:

1. State (B)= (*Winning=4* > *Cooperation=3* >*Conflict=1*)

Outcomes	**Payoff for (A)**	**Payoff for (B)**
Status Quo	3	3
A wins	4	1
B wins	1	4
Conflict	1	1

Table 3.1 Outcomes of Classical Deterrence Game

2. State (A)= (*Winning=4 > Cooperation=3 >Conflict=1*)

In this structure, each state prefer Win the conflict rather than cooperation (4>3) and Maintain Cooperation (Status Quo) rather than letting opponent go for any preemptinve strike and win the race (3>1). So, each state acting with on going Maximization of its outcomes on every stage within the game. As the maximization force state to select the maximum possible strategy.

Nuclear deterrence theorist have debated about relative importance of credibility, rationality and the behavior of the state opponent and the national security strategists. orF example, McGinnis [94] has discussed deeply the rationality and argument related to adversary. He has discussed how actor acts rationally within the model and at the same time how deterrence model should be carefully developed to explicit assumption about the nature of choices within the model.

Another article has discussed deterrence theory and especially the issue of bias. O'Neil discussed the bias between game models and the psychology or the case study of the model [95]. In this article he discussed the neglecting promise of credibility in deterrence models and many other arguable issues. He has concluded his article with a very excellent conclusion which is *"Many critics miss the point that the theory is not a body of facts, a set of known truth to apply to conflicts. It is a process of grappling with these paradoxes and lead us to understand more about strategic behaviour. we struggle to solve them, but each success leads to new problems, which is as it should be. If we ever succeeded finally, the field would lose its interest and our process of gaining understanding would be over."*

Before concluding this section, deterrence model should involve two critical factors which are threat and promise and both factors must have enough credibility for making state adversary to believe on state capability to cause the promised harm. If there is no credibility for the promise of causing the promised harm, there will be no functional deterrence. Failure of deterrence often refer back to the failure of these condition that aid in injecting the fear that stimulate opponent behavior for cooperation.

For that, the attempt in this research to go deeper in analyzing credibility of cyber threats to enhance our understanding. This will shed lights over role of cyber threat credibility in cyber deterrence and to benefit resolving State-State cyber conflict and if not what is the nature of state-state cyber escalation. Then looking for a best approach for optimizing deterrence in state-state cyber deterrence.

Deterrence Theory Waves

Deterrence theory like many other theories begin, continued, developed and sometimes argued with so many philosophic questions regarding durability of the theory. Some of these scientific theories became partially incorrect after a period of time due to a new theory brought to the scientific field demolishing what previous theory had been trying to prove.

This section will discuss the progress of the traditional deterrence theory presenting the most distinguished characteristics of each wave. Theorists like Freedman [89] categorised deterrence theory to three waves while other scholars added fourth wave like Knopf [96]. While discussing each deterrence theory wave, lessons learned are going to be deduced for the seek of construction cyber deterrence theory.

1. *First Wave* of the deterrence theory was established and died in the early years of the nuclear era. The approach was more of holistic approach than narrow and the main idea of this wave is to establish deterrence strategies for the purpose of threatening of complete war but not to stop it completely.

   During first wave most of the concepts and terminologies of the deterrence domain appeared although the real practice of deterrence was there before second world war or before Hiroshima bombing [97].

   Cyber deterrence benefit from the first wave of deterrence theory literature to establish the general concept, definitions and main ideas for the benefit of establishing cyber Deterrence field in considering the differences between these two domains. The general concepts aid to develop Cyber deterrence theory as ground for other efforts supporting effectiveness of cyber deterrence.

2. *Second wave* of the deterrence theory was emerged early of 1950s and was continuously functioning till early of 1970s. During this period, Deterrence became the central motivating factor for US foreign policy. Also, during this period theorists began utilizing novel methodologies born in the social sciences like game theory, prisoner's dilemma and the analogue of chicken game. This integration of science fields brought up deterrence models in an attempt to make deterrence theory more rigorous [99].

Cyber deterrence inspires from the second deterrence theorist constructing deterrence theory based on the game theory models. Utilizing game theory to analyze the nature of cyber deterrence for deep looking at principles and assumptions.

3. *Third wave* of deterrence theory as claimed by the publication of George and Smoke's book, *Deterrence in American Foreign policy* (1974), was identified as the start of the third wave of deterrence theory [98]. This wave emerged in the a wake of US after the failure in Vietnam and allow theorists to become critical against second wave of deterrence theory. They argued that the theory had been relying on abstract- deductive reasoning rather than empirical evidence or experimental output. Also, theorists asked about the use of force which could be manipulated to gain bargaining advantages as a tactic for gradual escalation like what happened in Vietnam. During this wave, there was clear recommendation for measuring achievements of deterrence.

   The lesson that cyber deterrence could gain from the third wave is to address the need for more specific, identifiable and measurable studies to give measurable answers to the claims that deterrence is not going to work. Until the writing of this words there is no certain study produced yet to measure implementation of any national cyber deterrence policy and measured proving either success or failure. Most of studies generalized the conclusions about cyber deterrence either it is very complex or very difficult. For that, mathematical model based on game theory developed to analyze the problem toward provide a reasonable strategies as a solution.

4. *Fourth wave* of deterrence theory began simply, after 9/11. The attack against US trade centers has sparkled the need for deterring non-state actors. The challenge is how to exercise deterrence against terrorists (Non-state actors) willing to commit violence while they do not have any "return address". The research concentrate with state developing effective strategies that deterring non-state player and rogue states [96]. There are variety of criminals conducted by non-state groups and they are hiding under different covers like religious, political, and payable criminals.

   The lesson for cyber deterrence from the fourth wave of deterrence theory has introduced the most challenging issue with cyber deterrence which is deterring Non-state attackers known as "no return address". Cyber attack need to get attributed to identify the source of attack either originated by State or Non State. Different type of cyber teams are there like anonymous or other red teams and to trace back their footsteps is a serious challenge.

Role of Rationality in Deterrence

Looking to the deterrence between two states or from state prospective, it can be described as attempt by first state decision maker to force or to offer set of alternatives that is possible for the decision maker of the opposed states. Threatening or giving incentives as alternative is a set of option that are possible to happen between two states.

Manipulating rationally with an opponent when threatening lead him to decide not to attack is simply the philosophy of deterrence. This would normally let the adversary count the benefits as well as the cost of his actions. The opponent would see that the cost of confrontation is highly harmful and would tempt to be logical to avoid himself that harm by not acting the way he decide. That's why deterrence theory has been called one of the most influential product of social science. When person is dealing with strangers "odds" usually tends to be more rational, the way deterrence often is practiced. So, when the decision maker is thinking rationally, normally choose to act after doing a "cost-benefit" analysis [85]. In general, justifying rationality in deterrence is recommended because the development of cooperation decision should be rationally considered better than escalation.

Normally, something is described to be credible when it can be taken rationally seriously. In other words, a credible threat is the threat that is rationally believed to be significant when, "the credibility of threats is sometime also closely linked with their rationality" [157]. If threatener gives a credible threat, the threatened is rationally supposed to judge what extend the threatener is serious to execute it.

A good example in this case is the dropping of credible atomic bombs on Japanese cities Hiroshima and Nagasaki in 1945 [86]. If Japan had decided to retaliate against US, the payoff would be totally disastrous for both opponents. As Japanese leaders believed if they retaliate it could not be stopped at the second strike and this could drive to third strike and so on. Their decision can be counted as a rational decision based on classical deterrence game model [157]. Overall, this taught us that the world before 1945 was indeed different from meantime world as the deterrence doctrine was nurtured. It can be concluded that there is a big connection between credibility and rationality of the conflict actors. Assuming the adversary is rational,when confronting credible threat will priorities rational decision of cooperation rather than losing.

Role of Credibility in Deterrence

The deep meaning of the credibility in the strategic studies is the believability of the state threat and its capability in executing that particular threat. What is giving state credibility in nuclear deterrence is the nuclear threat that state is already holding it and at the same time its commitment to retaliate against any nuclear attack. Credibility of deterrence can not be separated from the state political objectives since the deterrence mission is supposed to support the state reputation [85].

For the deterrence, state need to have credible threat that will help in developing the deterrence by punishment or by retaliation against attacker. This was the main reason for nuclear state opponent to believe on state nuclear threat and its credibility. In case state opponent knows that state is not capable to retaliate, the dominant strategy will be to attack with no fear from any retaliation and this will be dominant unless the state change its capacity and move to develop its credibility to a better outcomes.

Credibility is related to rationality, because the cost of threat defend against something worth less than what it deserve to defense can be irrational. This is because the cost of defense is higher than what state is trying to deter. Within credibility, rationality still play a good role in deterrence strategy and should be counted carefully [157].

Credibility role in deterrence can be understood from the prospect of the deterrence by punishment strategy. For that, state credibility is the magical ingredient of the deterrence strategy. Defining threat credibility and its role in deterring cyber adversaries have to be deeply explored. Because the need to know how credibility shape the strategy of cyber deterrence assist in manipulation of the behaviour of state adversary.

Mutual Assured Destruction and Mutual Assured Disruption

The concept of Mutual Assured Destruction (MAD) appears in 1950 when the U.S. believed in massive retaliation and despite the attempt to rename it with more modified contemporary terms like flexible response and nuclear deterrence, it has remained the central theme of American plan of defense. As impact of challenges during the cold war between US and Soviet union the Mutual Assured Destruction (MAD) has begun. It was driving both adversaries to challenge each other via putting one city of opponent at risk of nuclear attack. The message resulted from MAD is “if you decide to attack me, I am going to destroy you”. It is a commitment for both opponent that I am assuring to retaliate immediately with no further discussion [100].

There are some examples of neighboring nuclear countries and mutually deterred from aggression by both having the ability successfully initiate a nuclear attack such as Indian with Pakistan. For that, during this research we need to investigate if MAD could be influential in cyber deterrence.

Mutual assured destruction is to guarantee the destruction for both opponent and that was partially accepted in traditional deterrence. On the other hand, mutual assured disruption create a case of chaos. A simple scenario for this concept is Estonia case. It was a moral lesson to value the scale of cyber attack affects particular national sector to get destroyed or creating disruption for both opponents.

Cyber attacks in general affect critical infrastructure and could result a disruption to economics and business within the country. In general recovery from the cyber attack is practically possible. For that, it will not demolish every infrastructure compared to nuclear.

Is mutual assured destruction going to work within cyber domain or mutual assured disruption? One of my research objectives is to find out the possibility of mutual assured destruction in cyber domain. This theory has been introduced in Chapter 3 as MAD theory was like a result or replacement of deterrence strategies during cold war. This research will investigate the situation of mutual assured destruction in cyber domain.

- First, we have to understand what is the differences between MAD by nuclear weapons and MAD by cyber weapons.
- Second, what is the target of both nuclear and cyber weapons?
- Third, why did this theory fail? What are the costs and gains if mutual assured Destruction in cyber domain was selected?

Let us assume Country (A) attacked by country (B). A serious damage to (A) has happened and country (A) decides to retaliate against (B). country (A) can initiate the retaliation and at the same with cooperation with third country (C) can attacks (B) on behalf of (A). As the cyber domain is open for different players, they can cooperate to establish a situation of Mutual assured disruption against specific target.

American nuclear weapons can not be given to UK to initiate nuclear attack on behalf of US. But, cyber domain nature is dynamic and it is open space between adversaries. It is easily to expect in future to see massive attacks coming from countries but these attacks initiated by another country on behalf of another one. As the target of cyber attack is not to kill human but to cause damage to infrastructure or deliver a message or force opponent to lose some money.

From my point of view, there are certain questions need to double think about, as these questions could open the gate for further deep investigation about differences between mutual assured destruction and mutual assured disruption concept in cyber space.

1. Is it a single or multiple cyber attack will be initiated as MAD?
2. Against specific or multiple targets, could be the MAD cyber attacks?
3. What is the availability of Vulnerability Database among Adversaries?

4. What is the fastest and easiest attack to be executed as immediate retaliation and could cause massive interruption for the targeted?
5. Direct or hide beyond covering technologies to avoid attribution and cyber defense controls, to deliver the message clearly or keep silent?
6. Immediate or after period of time the cyber MAD will be executed?

Answering this questions will further our understanding about mutual assured disruption (MAD) compared to mutual assured destruction within nuclear deterrence theory. These questions may help us to better understanding the core differences between deterrence in cyber compared to nuclear.

3.5 From Nuclear To Cyber Deterrence

Nuclear deterrence is the greatest example for successful deterrence strategy. It has clearly demonstrated the success of nuclear deterrence between state like USA which armed with nuclear weapons to deter Soviet Union which also weaponise with nuclear weapons during cold war. The core of deterrence strategy idea was between two states have the same capability to wipe its opponent with the nuclear attack and this shared power has resulted into MAD concept that each state are ready to retaliate against its opponent and this credible confirmation of retaliation stimulate both states not to think for attacking from the beginning. Because of result expected from nuclear confrontation, both states were not welcoming the end of nuclear confrontation [101].

Nuclear deterrence theory has been expected to contribute on deterring the raises of cyber threats. The idea here is to transfer nuclear deterrence theory and to apply it against cyber threat. Specifically, it is for the benefit of state deterring another state. Traditional deterrence theory objective was to stop the attack not to happen via making the cost of attack and the consequence exceed expected benefits. Deterrence strategy can be achieved via two approaches. First approach, developing strong defense and if state succeed in developing defenses that fail any attempt of attacking, this will force attackers to give up. This approach is a practical strategy in cyberspace especially against known cyber threats. Second approach, threatening the attacker with a massive retaliation and this could work in the case attacker is attributed and state have the capability and capacity to retaliate. This approach could work to deter cyber opponents. Lack of attribution will fail any deterrence attempt that state think to establish and this issue is one of the main differences between nuclear and cyber deterrence.

Deterrence theory to work in cyber era, it needs to consider cyber space uniqueness compared to the nuclear and this what we are trying to achieve by the end of this chapter.

Before that there are critical fundamental issues to understand it for the benefit of establishing cyber deterrence theory. Issues like cyber attacks, actor status, cyber defense, offense and deterrence [102].

What is Cyber Conflict?

Libicki has defined cyber attack as “The deliberate disruption or corruption by one state of a system of interest to another state. The former state will be referred to as the attacker; the latter state will be referred to as the target. In some contexts, the target may also become a retaliation. The affected system will be referred to as the target system” [107]. Another definition reflecting cyber attack and political conflicts is “the conduct of large scale, politically motivated conflict based on the use of offensive and defensive capabilities to disrupt digital systems, networks, and infrastructures, including the use of cyber-based weapons or tools by non-state/transnational actors in conjunction with other forces for political ends” [103].

Cyber deterrence is different from nuclear deterrence in different perspectives. First of all, nuclear attack is a direct physical threat to human life, killing, destroying with no recovery of the killed and destroyed infrastructure while cyber attack consequences can be recovered if you have another backup copy of similar attacked systems or databases. Nuclear weapons are known weapon and can be easily attributed and identified it belongs to whom. Likewise, cyber weapon can be distinguished (malware, DDoS, worms, SQL injection, etc.) but who has developed and who has utilized it (Attacker) [106].

Second, nuclear attack is between known states and the capacity of these states are known while in the cyber domain the attacker is mostly anonymous and it is very challenging to trace back the source of attack.

Understanding Cooperation, Competition and Conflict

Before moving to review the differences between cyber and nuclear deterrence it is essential to explain the actor status. This is related to the actor (State) status within the conflict and useful to know the differences between these conditions. This understanding will assist while analyzing how each state act. The situation of the adversary within the conflict are limited to three status: Cooperation, Competition and Confrontation.

Differentiating between these three situations between adversaries in all types of conflicts is explained through a table reflecting the state objective attached with example to know the exact meaning of each status:

Table 3.2 Understanding Cooperation, Competition and Conflict [110]

	Objectives	*Example*
• **Cooperation**	It is the practice of exchanging mutual benefit, especially privileges granted by one country or organisation to another.	Nuclear Superpower Cooperating to maintain Nuclear peace (Status Quo) and share agreements regarding nuclear disarmament, US vs Russia,
• **Competition**	It is the position of improving or increasing oneself which can produce overall raise the conflict between adversaries	The Nuclear arm races among international superpower, N.korea, Japan, India Vs Pakistan and many other cases of arm races like cyber arm races or state-state challenge
• **Conflict**	It is the position of concerning about one gain with an absolute LOSE for the other part or state opponent	Second Word War, US vs Vietnam Iraq vs Iran

Defense, Offense and Deterrence in Cyber Space

It is advisable to let states strategists to understand the three phases of conflict and how to differentiate between them within cyber space. Obviously, the aim of this section is to reduce the overlap between the concepts of Defense, offense and Deterrence. The approach will be via clarifying each term definition and elaborate via giving different cases and examples. Moreover, defining these core strategies will segregate which strategy should come first and will help us to understand how defense, offense and deterrence should work in harmony with the state strategies.

- **Cyber Defense:**

  The concept of defense in cyber is similar to traditional defense but when it comes to the practice, cyber is different. Cyber defense scope of work within Cyberspace, dealing with digital actors to defend against cyber soldiers whom utilizing digital tools for initiating attacks. Cyber defense has been developed to defend state cyber vulnerabilities that cyber adversaries aim to get benefit via targeting and create a disruption or destruction. States around the world are familiar with traditional defense strategies and concepts and with the growth of relying on cyber states need to speed up the changes with as it will offer many advantages in term of securing its cyber spaces and maintain productivity [78].

Traditional deterrence activities are generally as a reaction against attacks already begun and the attack reached or passed the borders. Cyber defense function when attacker starts to exploit any cyber vulnerability and the defense should prevent attacker from achieving the mission of exploitation. Defense in depth strategy in cyber goal to employ different layers of techniques and combine then together for the purpose of weakness of some of these cyber security solutions will be mitigated by the strength of another solution. The concept is similar to the traditional belief for "trustworthy systems can be built from untrustworthy components" [79].

The idea beyond the strategy of defense-in-depth is for state to harden its cyber defense. So, this will force cyber adversary to double thinking by judging the cost of achieving cyber attack will exceed the expected gain in case cyber attack is accomplished. Unfortunately, it depend on how serious the opponent is and his insistence to find cyber vulnerabilities. The advantage of defense-in-depth strategy is to help state to avoid the mistakes of previous attacks reflecting cyber attacks. It will help avoid weakness of other cyber security solutions as well as the misconfiguration vulnerability. Cyber opponent will always keep allocating resources to achieve these missions especially if there are sufficient objectives beyond. Advantages for state raising cyber defense are not limited in protecting civil sectors but it get extended to strengthen deterrence by denial approach.

- **Cyber Offense:**

  Cyber offense is the action when state attack another state utilizing cyber space as a domain for delivering cyber attacks. State aiming to develop its cyber deterrence strategy need to have its cyber offense and at the same time state should treat this capacity carefully as it could lead to unwanted escalator interaction and as mentioned earlier that all states are vulnerable to cyber threats [80].

  Still the challenge of initiating cyber offensive attack against state adversary is related to the attribution and the accuracy of the attribution. It reflects the achievement expected from the offensive strategy. When miscalculation happens and the offensive attacks are executed the response is not certain. Cyber and its vulnerability is different compared to the traditional conflicts domains (Air, Land and Sea).

  When state prioritize cyber offense strategy in cyberspace, this can stimulate instability between states within cyber space. Moreover, states in cyber are strong by holding offensive capacity but at the same time vulnerable for a plenty of cyber-attacks. Offensive cyber operations is adding more complexity for the international relation and cooperation. Assuming cyber offense is the best optimize strategy that will deter cyber adversaries is not the correct assumption although it has some advantages for supporting deterrence in term of credibility of cyber threat. Offensive cyber capacity will help to make cyber threat as credible threat and it will aid state deterrence strategy in making cyber threat more believable by the state cyber adversaries but it is only for threatening not to use it [81].

- **Cyber Deterrence:** Extending the concept of nuclear deterrence to the cyber deterrence, we can describe cyber deterrence as a strategy aim to dissuade cyber adversaries from initiating any cyber attack via injecting fear from the retaliation. To assure capacity of retaliation, state need to have preparedness for send a signal of retaliation certainty and this is more closer for the state to have offensive capacity. Deterrence strategy in cyber space need to work together with cyber defense and cyber offense via three dimensions [82]. Before pursuing the work to explore other elements related to cyber deterrence, it is essential to set the base. The cyber deterrence base is to define cyber deterrence terminology.

  What is cyber deterrence? cyber deterrence as a deterrence in kind to test the proposition that any state need to develop a capability in cyber space to change their bad intention towards manipulating cyber space to harm the state. State developing cyber attack capabilities have a big interest in cyber deterrence than state armed with a conventional capability [107].

  What is Cyber Deterrence? ***"Cyber deterrence is a strategy by which a defending state seeks to maintain the status quo by signaling its intentions to deter hostile cyber activity by targeting and influencing an adversary's decision making apparatus to avoid engaging in destructive cyber activity for fear of a greater reprisal by the initial aggressor" [105].***

  First, effective cyber deterrence strategy will need to have a credible defense that protect state cyber space infrastructure and make the attack very hard to succeed. The effort of hardening cyber defense will help deterring cyber adversaries even if opponent attempt many time to achieve the attack. This will let opponent to recalculate and to give up after different failed attempts. Second, it is the state ability to retaliate against the threat source. Retaliation to success need to create some sort of damage even bigger that what the attacker are expected. This effort should be aligned with the capacity of identifying the exact attacker rather retaliate and attack randomly. So, it is the capacity to identify correct attacker and then decide to retaliate or not. Third, it is the willingness of the to retaliate against the threats sources. State should be prepared for any retaliation and should be ready for the consequence in case of retaliation.

Cyber deterrence is a preemptive strategy against anticipated threats and in practice in the middle between offensive and defensive strategy and benefiting from both. In the cyber domain, this conceptual view means observing, detecting what is going on with the cyber space traffic as well analyzing the good and bad traffic. The defense, offense and deterrence operations are different in term of the practice.

These differences can be summarized as follows [83]:

- Defense is the capacity to defend oneself against an act of attack.
- Deterrence is the capacity to discourage opponent from committing the attack.
- Defense comes after the failure of deterrence.
- Deterrence is based on the threat of punishment.

Obviously, Fig. 3.3 explains the relation between Deterrence, Defense and Offense strategies within cyberspace. These three strategies are like the old concept "Old wine in new bottles" it was traditionally practiced and now states need to implement them against cyber threats affecting national security. State Cyber strategists need to look at these three strategies and align it with the current and future demand. Plenty of research been conducted in cyber defense [84].

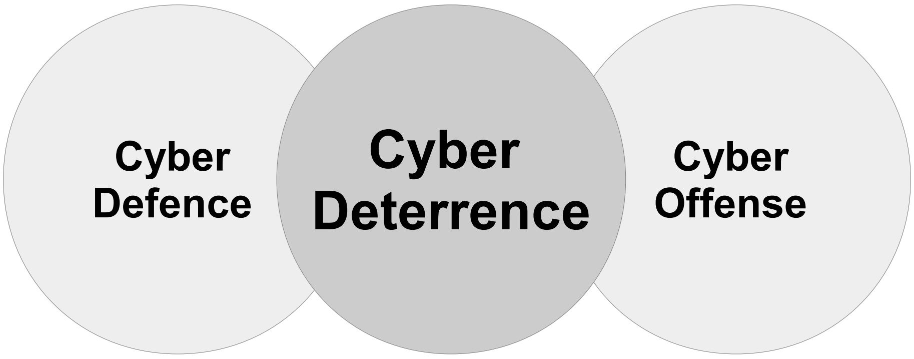


Fig. 3.3 Cyber Defense, Deterrence and Offense

Cyber defense, offense and deterrence should work together and each one relies on the other to accomplish its mission. Cyber attack is faster than other traditional attacks and the cost of development is lower, It can be executed from around the world while connectivity is available (delivery system), cyber threat can programmed to replicate itself like malware threats. , and it can be reprogrammed for targeting another cyber infrastructure. For that, cyber offense can help in threatening opponent. Cyber defense can assist in attributing the attacker. Cyber deterrence benefit from cyber defense attribution and cyber offense threatening as threat of punishment. In summary, deterrence is a traditional practice for security purposes and this project aiming to bridge traditional deterrence theory into the cyber deterrence domain considering cyber uniqueness following a scientific approach.

Traditional deterrence focus on the capacity of each opponent to deter each other. Similarly, cyber deterrence focusing on state capacity in deterring its opponent not to attack. Attacks within cyber environment is more complex compared to other conventional attacks. Small country holding zero day vulnerability can form a real danger even to a superpower state. This work effectively when this cyber weapon destruct opponent critical infrastructure and produce a real massive destructive situation. This lead to understand how superiority in cyber power is supportive factor to have strong cyber deterrence. Deterrence works based on two main strategies called deterrence by denial and deterrence by punishment [108]. Here we need to make these two strategies undergo to the cyber deterrence domain:

Cyber Deterrence by Denial

Deterrence by denial in cyber space domain can be defined via developing defense layers to make the attack very difficult or make it as hard as possible to deny the cyber attack. This development can happen through:

- Technology: via developing different layers of protection via Firewalls, Intrusion Detection/Prevention systems, Unified Threats Management (UTM), SSL, Encryption, and Maintain best practice of Defense on depth procedure within all theses infrastructure.

- Human Resources: via developing the skills, knowledge and capacity of human resources how to utilize tools and technology to harden defense in cyber domain to deny cyber attacks.

- Policies and Procedure: developing rules and regulation for enhancing the efficiency of security controls and enforce human resource to assure these security controls are up to best practice to deny cyber attacks. Implementing cyber deterrence by denial will establish the ground for the strategy of punishment as the detection and attribution of cyber threats happens during denial strategy.

Cyber Deterrence by Punishment

Referring to the nuclear deterrence and the strategy of deterrence by punishment, it was known for adversaries that the punishment of nuclear state is a nuclear retaliatory attack. The commitment for nuclear retaliation was committed and states was strategically ready for retaliation. Moreover both states US and Soviet Union are vulnerable to the nuclear retaliatory from each adversary which was deterrence by punishment practice in deterring nuclear state.

Returning to the cyber, the threat of punishment in kind (Cyber Attack) via retaliatory cyber-attack can be considered as deterrence by punishment in the cyber space. This can be practiced in cyber via hack the hacker, but the challenges in cyber is hacking the exact hacker is semi-impossible due to the problem of attribution. In the case state standing behind attributed cyber-attack it could be punished by retaliatory by its cyber adversaries which is a punishment from the attacked state. At this point attacker should believe that if he attack he will get punished either state or non-state and guarantees his loose.

Deterrence by punishment in the cyber space is more of offensive strategy and states need to be ready for offensive retaliations but careful not to use it. Such action are needed to send signals about state readiness to punish its adversaries and its commitment to punish and it is having the right to defend against its cyber threat.

Similarities and Differences between Nuclear and Cyber

In this section, the objective is to review transformation of ideas from traditional nuclear deterrence to the cyber deterrence. The mission was to look at the lessons that could be beneficial for the cyber deterrence and to consider it all the way when developing the strategies.

- Key Similarities between Nuclear and Cyber Conflict [104]:

- Nuclear and Cyber conflict are operate at all military operations levels: Strategic, Operational and Tactical, with the potential to have effects range from small to wide population scale.

- Both conflicts have the capacity to create large scale, even more existentially, destructive effects.

- Both can be conducted between States-Nations, or States/Nations and Non-State/actors, or between hybrids involve State and Non-State actors proxies.

- Nuclear and Cyber conflict can present the adversary with decisive defeat that cancel the need to fight conventional wars.

- Both can intentionally or unintentionally cause consequence result beyond the scope of the main attack target.

- Key Differences between Nuclear and Cyber Conflict[104]:

- Attributing nuclear attacker was not a problem but in cyber conflict it is the central problem
- Cyber conflict are actively working on a Man Made domain and most of this domain under the private sector while nuclear conflict actively working in major domains like state airspace, land and coastal waters or global domains like airspace, sea and space.
- Cyber attack is having lower cost compared to nuclear and high accessibility. This means millions of users around the world have the access to to cyber attacks tools where in nuclear there are a limitation for view states with sufficient resources to build up its nuclear capacity.
- Nuclear confrontation can be conducted under the condition of violence while cyber conducted over violence and nonviolence and creating both physical destruction. Cyber could attack air traffic controllers resulting airlines crashes and it could be conducted against civil normal virtual destruction like wiping the data.
- Cyber attack can be conducted with very high strict confidence and non traceable while nuclear attack is impossible to get conducted under these conditions of secrecy.
- Nuclear attacks are clearly considered as an act of aggression and with no doubt need immediate retaliation while in cyber still there are plenty of issues surround cyber retaliation or any cyber offensive operation as retaliation in cyber confrontation.
- In Nuclear the weapons used either for offensive and defensive can be distinguished easier compared to the cyber offensive and defensive tools.
- Cyber tools for offense and defense can be used for both opponents while in nuclear the situation is different.
- Nuclear attacks consequences are scientifically known and measured while still not certain how clear attacks consequences are calculated and measured
- Cyber networks for the government and military are scanned with cyber security solutions and this make more complex to retaliate and escalate in cyber than in nuclear.
- Second Nuclear attack is still powerful in term of destruction similar to the first nuclear attack while in cyber second attack could be prevented as at the first attack force state to enhance its vulnerabilities used for exploiting first attack.

- Nuclear counter force was possibly to get used against nuclear attack while in cyber this capability only limited to the known cyber attacks. Unknown and unpredictable cyber attack still cyber defense not capable to take actions regard it.
- In nuclear confrontation, third parties involvement are not make any worry while in cyber there are a worries from third parties to get involved especially in the case main adversaries are welcoming such like involvements.
- Private sector within the state are responsible to defend themselves in cyber conflict while in Nuclear State are responsible to defend against on their behalf
- Finally, nuclear confrontation is the highest level of confrontation which no escalation after nuclear while in cyber the question are till under discussion regarding escalation from cyber to nuclear.

These similarities and differences between nuclear and cyber conflict are the key factors to be considered for cyber deterrence strategy. Overall, cyber conflict is a certain activity that can be conducted by both States and Non-State against different types of targets. This type of conflict is effecting individuals, private sectors organizations and State and at the same time it could effect traditional military and state intelligence operations. Cyber conflict is wider than traditional definitions which consider the PCs, Software and Networks and involve plenty of activities conducted by different kind of actors.

This research aim to understand the nuclear deterrence key success and how to benefit from these factors for the benefit of cyber deterrence. The literature review in this section and the coming sections aim to investigate the general understanding and modeling the cyber conflicts for the purpose of succeeding the deterrence strategy.

The lessons can be summarized from this section, first, is the differences between deterrence in nuclear compared to the cyber. Second, Status of adversaries within traditional or cyber conflicts could be Cooperation, Competition or Confrontation and how essential to understand the differences between each status. Third, three different strategies that were traditionally in practice and then transformed in cyberspace. Finally, similarity between cyber deterrence and nuclear deterrence are explained.

3.6 Cyberspace Characteristics

States around the world rely on the networks, systems, communication systems and electronic services for running day to day business. This growth has formed the newly integrated domain titled as cyberspace.

Table 3.3 World Internet Users [109]

World Regions	*Internet Users Dec 2017*	*Penetration Rate (% Pop.)*	*Growth 2000-2018*
Africa	453,329,534	35.2 %	9,941 %
Asia	2,023,630,194	48.1 %	1,670 %
Europe	704,833,752	85.2 %	570 %
Latin America/Caribbean	437,001,277	67.0 %	2,318 %
Middle East	164,037,259	64.5 %	4,893 %
North America	345,660,847	95.0 %	219 %
Oceania/Australia	28,439,277	68.9 %	273 %
WORLD TOTAL	**4,156,932,140**	**54.4 %**	**1,052 %**

Millions of machines connected with each other facilitating human daily life. It starts from switch on our smart car early morning till switch off our mobiles before going to bed late night. The growth of utilizing Internet and connectivity has resulted into creating a challenge of stabilizing the cyber domain. Thousands of cyber attacks are happening daily reflects a real challenge to stop or to avoid it preemptively. It is not affecting the electronic services only but there is a strong relation between cyber attacks and national security of every country.

Estonia is the most famous case to be studied as an attack that completely shut down the national financial system [111] and it could be possible to initiate similar attack to the same country targeting another very sensitive sector i.e electricity grid, hospitals,....etc. Estonia case taught decision makers of the country the importance of investing in developing an advance effort to control attacks before they happen.

Hence, the need of preemptive strategies for all states is highly required to resolve the challenge of cyber attacks before national critical infrastructure get affected. To achieve this preemptive action, the cyber deterrence is the nominated solution for each country approach [112]. From International relation prospective, we have witnessed different countries around the world trying to cooperate with other countries proceeding to deal with cyber threats. From technological prospective, cyber deterrence requires innovating technologies that will help to deter cyber attacks.

As states aim to be involved in the highly communicated world within cyber space, securing cyber space became a fundamental requirement. Building highly secured cyberspace is a fulfillment of national and International security, as well as international economical and business exchanges. No doubt this domain enables societies and multinationals to communicate culturally.

likewise any invention, users start utilizing it positively, later, they misuse it as natural behavior of human-beings who tend to enjoy breaking rules. Since early 90s, technology witnesses a significant exploitation of the vulnerabilities found within technologies to gain unauthorized access to network resources or to exploit malicious attacks aiming to harm their adversaries.

These attacks can be initiated from anywhere around the world harming the farthest connected system. An attacker can exploit and cause a real damage to any vulnerable company/ state and bring down electricity grid system similar what happened to Black-energy malware [113]. As a result, Estonia -one of the most connected country- has witnessed a disruptive and sever cyber attack utilizing malware targeting electricity grid of the country that ended up with approx 75 percentage down. It is not a lesson for Estonia only but for all countries around the world to comprehend the risk of having vulnerable systems within critical infrastructure. Vulnerabilities tend to welcome attacker to utilize it [114] to stop or at least create a situation of disruption within critical infrastructure.

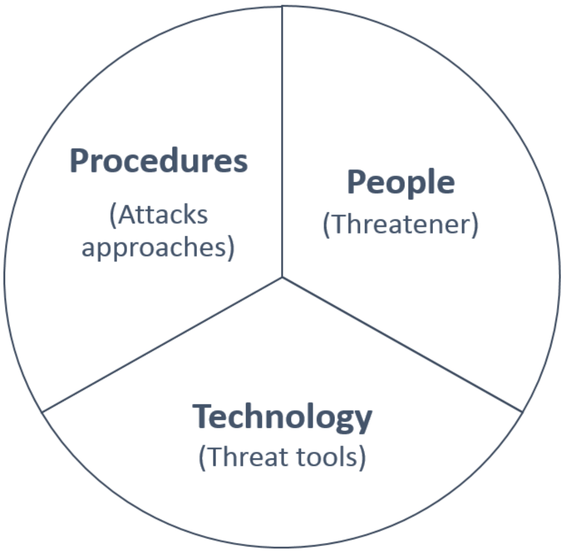


Fig. 3.4 Cyber Domain Pillars

Before moving to cyber deterrence theory, this section explains uniqueness of cyber domain and more important is look to cyber space from three prospective as a cyber space pillars. These pillars are people, technologies and procedures as figure 3.4 present them. Moreover, the section comparing how cyber attacks are different from nuclear attacks. It also, explore cyber attacks high-lightening the stages of cyber attack. Also, it answers this question: What is the capacity of modern technologies to detect cyber attacks and at what stage these detection happens? How strong is the observability of current cyber detection technologies?

From the literal definitions done, the Department of Defense Terminology Program which includes a dictionary of military and Associated Terms known as the DOD Dictionary gave a sufficient comprehensive definition for cyberspace, *"A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers"* [115]. This definition serves this research because it concerning about the military and the security aspects compared to other definitions. Besides, it clarify that there are certain operations occur in this interactive domain.

Cyber Operations has also been defined by this program as, *"The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace" [76].* Fairly, most of these operations are created for the benefit of people. However, some operations are meant for the destruction and causing harm like cyber attacks. Thomas Rid and Peter Burney have stated that cyber attack are computer codes that are designed to be used for the target of threatening or causing physical, functional, or mental harm to systems and networks infrastructure that basically serve daily human life [116]. This definition give general concept of how cyber attack look like. Moreover, further details are still needed to be digged out to have a deep understanding of cyber attack uniqueness. Specifically details about root cause of cyber attacks, attackers motivators and goals gained. Deep technical understanding about cyber domain will play a major part in benefiting successful nuclear deterrence strategies toward developing successful cyber deterrence strategies. Cyber environment is simply consist of three pillars people, procedures and technology [117]. In order to gain better picture about cyber threat environment, a drafted figure to provide a close understanding how three parties are working together.

Table 3.4 Cyberspace differences compared to other Domains [118]

	Cyberspace	**Air, Space, Sea, Land**
Size	Unbounded	Essentially fixed
Rate of change	High	Low
Governed by	Technology	Physical Laws
Ownership and jurisdiction	Private	Sovereign and International
Cost of Entry	Low	High
Attribution	Diffcult or semi impossible	High due to physical evidence
Dimension	Connectivity	Geographic
Cost of attack	Little or None	Expended munitions

In conclusion, there are a variety of cyber attacks, cyber attackers and procedure of executions cyber attacks. Definitely, these three non-separate components of cyber domain are crucial areas of cyber deterrence.

Cyber Attackers

Table 3.5 Sources of Cyber Threats [110]

Threat Source	***Motivation***
Intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. These include exploitation and potential disruption or destruction of information infrastructure.
Criminal groups	Criminal groups use cyber intrusions for monetary gain.
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, attack tools have become more sophisticated and easier to use.
Hacktivists	These groups and individuals conduct politically motivated attacks, overload e-mail servers, and hack into websites to send a political message.
Disgruntled insiders	The disgruntled insider, working from within an organization, is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the US economy, and damage public morale and confidence. The CIA believes terrorists will stay focused on traditional attack methods, but it anticipates growing cyber threats as a more technically competent generation enters the ranks.

Attackers in cyber domain could be state, organized groups/ red teams or even individuals. Unlike the players of nuclear domain is limited between governments of states.

In the nuclear confrontation, the players are known for both sides and has specific location which make the observability and certainty easier. On the other hand, the players in the cyber space are masked which make observability a real challenge in cyber domain.

Simply, cyber confrontation can be described as (state - state), (State - Groups) and (State- Individuals). For that, deep understanding of root cause of attackers motives enables developing effective cyber deterrence strategies. Cyber deterrence strategies should treat the motives in the first stage to avert the decision of attackers not to attack. Such kind of classification will help toward analyze the need of each player to get deterred. Deterrence strategy dedicated for single hacker could not fit deterring state or group of networked people. Cyber attack capacity and capability of these players are not the same.

- Internal individual within state get traced and attributed easier than an external hacker. External hacker live under another state which may not cooperate with harmed state authorities which requires different deterrence strategies to convince his state to cooperate. Convince attacker state either by threatening or incentives (Stick and Carrot Strategy). This type of interaction between states is a deterrence strategy by itself to groups and individuals of cyber attack.

- Coordinated groups or Red Teams need different strategies of deterrence. Because members of these groups are usually not located in one geographical spot; they tend to be from different cities or sometimes different states. What make tracing these groups more challenging is that it basically depend on the cooperation of the state among each other. There are certain strategies to deal with this type of attacker, It could be via legal procedures, or offensive technologies or direct military operation against their infrastructure.

- Regarding the third case when state confronts another state, cyber deterrence strategies is more political. However we should look at it from different prospectives such as intelligence, economy, credibility and motives. Cyber attacks could start as consequence of bad political relations and for deterring such kind of confrontation need to concentrate to encourage the other state for cooperation. Strategies like signing cooperation agreement, economic and political sanctions could help to deter cyber-attacks. Otherwise, direct threat as escalation against state is a further powerful strategy of deterrence and the consequence are unmeasurable.

It is essential to study each case separately to identify what is suitable to deter a particular state adversary. This will direct state strategist to think rationally more in-depth. The table explain main types of attackers and explain each category differences and motivators of each player [119]:

In conclusion, Player in the cyber domain has varies intentions compared to nuclear domain. Deterrence in cyber target to deter the players not to decide for attack. To deter the decision of these players, deterrence strategies should be strong enough, precisely vivid enough to guarantee successful cyber deterrence.

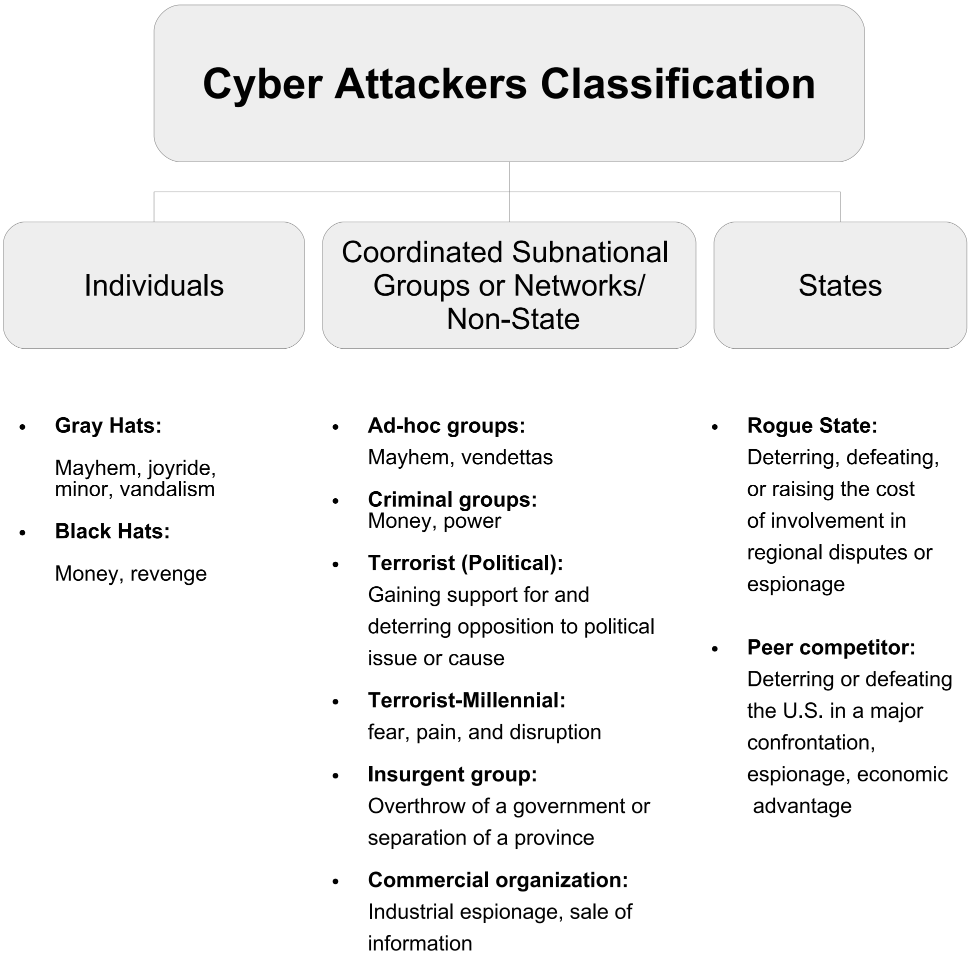

Cyber Attackers Classification
Individuals
Coordinated Subnational Groups or Networks/ Non-State
States
Gray Hats:
Mayhem, joyride, minor, vandalism
Black Hats:
Money, revenge
Ad-hoc groups:
Mayhem, vendettas
Criminal groups:
Money, power
Terrorist (Political):
Gaining support for and deterring opposition to political issue or cause
Terrorist-Millennial:
fear, pain, and disruption
Insurgent group:
Overthrow of a government or separation of a province
Commercial organization:
Industrial espionage, sale of information
Rogue State:
Deterring, defeating, or raising the cost of involvement in regional disputes or espionage
Peer competitor:
Deterring or defeating the U.S. in a major confrontation, espionage, economic advantage

Fig. 3.5 Cyber Attackers and Motivations Classifications

Cyber Attacks

Cyber attacks are widely variant and technologies utilized for initiating vary as well as the target of each attacks are different. Moreover, the location of cyber attack is unlike traditional attacks; because hackers from the farthest connected machine anywhere can initiate a cyber attack against any vulnerable machine around the world. This establish another challenge to attribute the attack to a certain player due to the smart technology of masking the attacker identity.

The technologies utilize in cyber attacks vary by the purpose they achieve. These technologies could be email attachment, malware encapsulated within image file, executable file embedded in email, etc. A good description for this type of these technologies is they are deceptive and stealthy. Technical understanding of how these technologies function will facilitate attributing the sources of attack. When Comparing between cyber weapons and

Table 3.6 Cyber Threats Definitions [110]

Threat	***Definition***
Botnet	A network of zombie machines used by hackers for massive coordinated system attacks. Employing a botnet to send massive simultaneous requests to servers prevents legitimate use of the servers and produces a denial-of-service attack.
Logic bomb	Camouflaged segments of programs that destroy data when certain conditions are met.
Trojan horse	Stealthy code that executes under the guise of a useful program but performs malicious acts such as the destruction of files, the transmission of private data, and the opening of a back door to allow third-party control of a machine.
Virus	Malicious code that can self-replicate and cause damage to the systems it infects. The code can delete information, infect programs, change the directory structure to run undesirable programs, and infect the vital part of the operating system that ties together how files are stored.
Worm	Similar to a virus, a worm is distinctive for its ability to self-replicate without infecting other files in order to reproduce.
Zombie	A computer that has been covertly compromised and is controlled by a third party.

nuclear weapons will conclude that nuclear weapons are limited and known in term as a weapon. On the other hand, the technologies used for the cyber attack are initially meant for positive usage then manipulated by hackers for harmful purposes.

Countries which have the capability to develop or own nuclear weapons are very limited and they are well known by international community. For that, if any nuclear attack happen, it is easily to get attributed. In contrary, cyber attacks technologies are accessible for everybody in this massive connected globe which add extra challenge to attribute the doer.

In fact, it is very difficult to split between this two pillars (Hackers-Technologies) because they are substantially integrated. The graph below aims to provide clear idea about classification of cyber-attacks based on attack vector, operational impact, defense, information impact, and target [120].

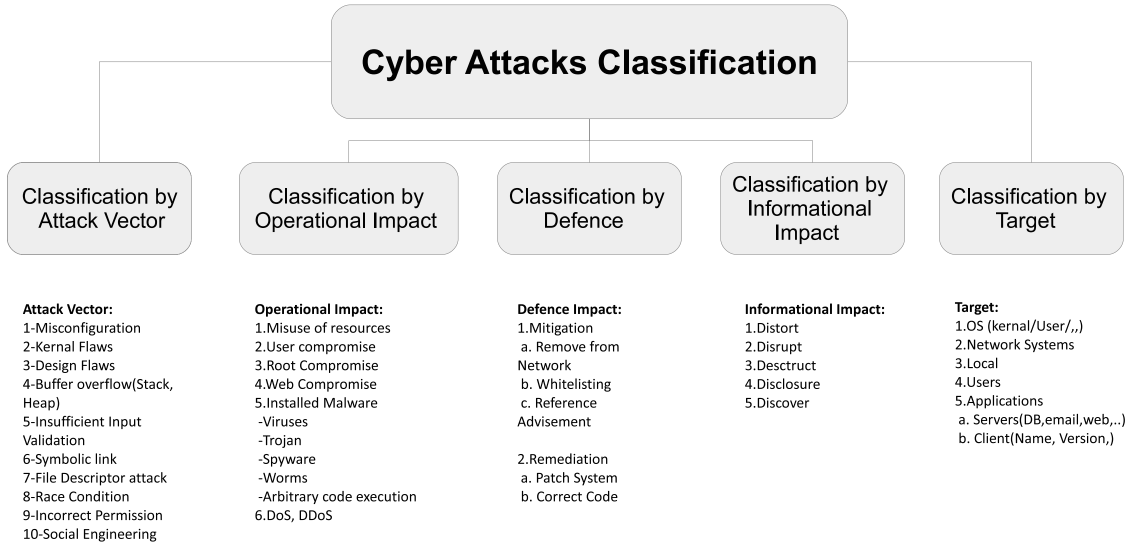


Fig. 3.6 Cyber Attacks Classifications

Cyber Attacks Life Cycle

There are a plenty of procedures used to execute cyber attacks like DDoS, SQL Injection, Malware and many others. Each of this attacking procedures is different from the other procedure and need specific technology or tools to identify, report and analyzed.

Deep looking at the gradual phases of the cyber attack starting when attacker's decision ending up to the execution of the attack. Technical understanding of these phases is beneficially useful for establishing cyber deterrence strategies matching each phase. Keeping in mind, each phase is full of deception, stealthy and usually sneaky. The phases can be summarized as follows [121]:

1. Reconnaissance:As a first step, hacker or attacker conduct research on a systems and human to find out the vulnerabilities to be utilized as a target and think of a best way to exploit it. The attacker decide on specific point to start the attack either via phishing emails or direct attack.

2. Weaponization: Hacker find out the tools that are successfully helpful for gaining access and putting the figures on the triggers which normally requires careful decision

3. Delivery: This step attacker utilizes the gained access to escalate the level of privileges to the admin level which enable him to manipulate with systems freely.

4. Exploitation: The attacker reach the confidential data and vulnerable systems in order to steal date or exploit the vulnerable systems.

5. Command and control: The attacker will maintain gained unrestricted access throughout the network for the purpose of command and control. To carry on silently install malicious programs like root kit that aid attacker to return access to the same systems.

6. Installation and execute: During this phase hacker alter the functionality of the systems hardware or disable the services provided by the targeted system. Here the organization cannot defend itself easily because the attacker is already strongly stealth and in control position. Classically, the stuxnet attack against Iranian nuclear infrastructure.

7. Maintain: after all above phases done, hacker usually work to hide their tracks by log cleaning and sometime they purposely leave some messages as a show or proof of evidence “that they are here”.

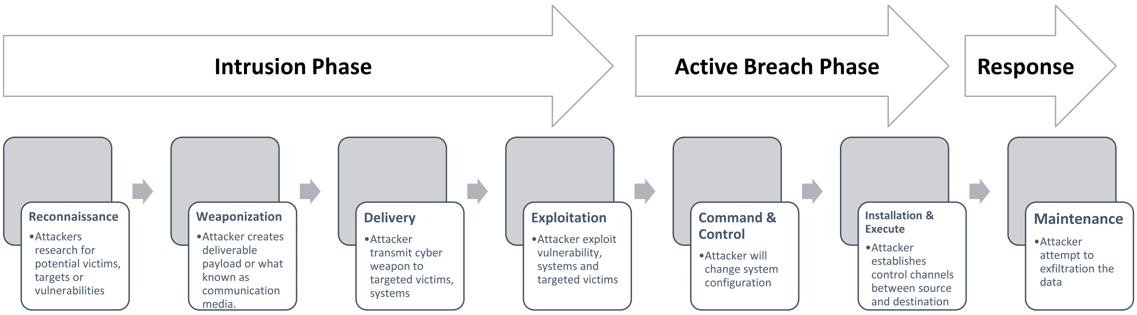

Intrusion Phase
Active Breach Phase
Response
Reconnaissance
•Attackers research for potential victims, targets or vulnerabilities
Weaponization
•Attacker creates deliverable payload or what known as communication media.
Delivery
•Attacker transmit cyber weapon to targeted victims, systems
Exploitation
•Attacker exploit vulnerability, systems and targeted victims
Command & Control
•Attacker will change system configuration
Installation & Execute
•Attacker establishes control channels between source and destination
Maintenance
•Attacker attempt to exfiltration the data

Fig. 3.7 Cyber Attacks Life Cycle

Cyber security technologies in alignment with cyber attack life cycle can play a facilitating role in detection and reporting attacks. Generally, there is variety of cyber attack methodology. For example, SQL injection happen when attacker keep trying to inject database with random code to obtain the access to database tables. This attempts can be detected and observed via different technologies.

Another more advanced example is when attackers utilize networks of infected zombies from all over the world and initiate the attack targeting one particular victim and this is what is called as distributed denial of Service DDoS attack.

Other more complicated example is when the opponent utilize very advanced technology like zero day attacks or malware. Reaching such kind of vulnerabilities and utilizing this for causing destructive attack is another total challenge. Stuxnet, Shamoon and many other malware were like revolutionary attack methodology.

Observability and Cyber Security Technologies

The main mission of cyber deterrence strategy is to prevent cyber opponent from organizing and conducting any cyber attack by manipulating with their decision. For effective cyber deterrence, state must have a credible threat of retaliation. As a main condition for retaliation is the ability to detect attacks and ability to retaliate.

Cyber deterrence can be achieved via threatening or giving state adversaries a different incentives that stimulate the cooperation. For developing the strategy, state requires having a high level of cyber observability over its cyber domain.

Observability will support reduce the level of uncertainty surrounding cyber attacks. As a national security states need to know what is going on within cyber domain and what cyber threat could effect its cyber infrastructure.

There are a different motivators for cyber attacks but state need to keep an eye on the cyber domain and assure its capability for attributing cyber attacks and assure readiness for security teams to deal with cyber attacks. Cyber attacks can be stimulated by political as well as economical conditions between states. Technologies will aid state maintain its superiority even in case retaliation is selected as a deterrence response against cyber opponents.

State to retaliate in cyber need more of certainty about the target other wise the retaliation will effect another innocent target and this could spark another escalator cyber interaction.

Observing cyberspace will help states indicate cyber threats level growing or descending, what is the opponent going to do and willing to do. For the cyber deterrence state will rely on this cyber threats indicators for feeding its decision either to retaliate or not, what is the credibility of its opponent.

Observability is not a simple task and at the same time is not impossible to develop it. State in cooperation with cyber security technologies for the purpose of observability will need to change its rule of engagements with cyber opponent. It is national security need to transfer traditional practice to the cyber and to develop decision of what to do with the adversary. State at the end will need to do something and the decision depend [122] state capability of:

1. Detection of expected attack
2. Identifying the attacker
3. likelihood of adversary's retaliation
4. Consequences of lashing out a wrong attacker

Cyber security technologies have recognizable capacities in detecting, collecting logs, analyzing ingress and egress network traffic. These facilities among these technologies helps cyber deterrence partially in attributing cyber attacks. In other way, these technologies could help send signals informing opponent that we (The State) are observing the income and outcome traffic. That message sent means we are prepared for retaliation and escalation.

Observability function of cyber security technologies in support cyber deterrence can be generally summarized -according to my own point of view- as explained underneath.

1. Identification: identify all income and outcome traffic, so when users “hackers or attacker” initiate a new session incoming to any cyber infrastructure it gets identified with full details, even new technologies claim that it can decrypt encrypted traffic for the purpose of malicious software filtration. Despite of all these smart technologies, there are still plenty of highly advanced cyber attacks that can not be identified by these technologies.

2. Recording: Recording what has been identified during previous phase. Information gathered accomplishes the observability purpose in term of complete information about source of attack, potential target, destination of attack plus history of attempts. Clever analysis of these information enables to point to suspicious cyber threat sources (Adversaries).

3. Reporting: Reporting phase is the final step of this process, by offering reports about whatever identified, recorded and analyzed for decision maker. The reporting is supposed to present detailed figures about threat level, threat source, threat target, threat type, and expected consequence of attack in the case if exploitation is accomplished. State decision makers are usually responsible of next step regarding the direction of the cyber conflict.

The purpose here is to review some of the cyber security technologies that can aid in the mission of cyber deterrence. The main objective of these technologies is to raise the level of observability within state cyber domain which will reflect to state capability to attribute cyber attacker. States to enhance its capacity in observing cyber space need to invest in these technologies and at the same time to assure sufficient training and practice for the cyber security teams. The ongoing preparedness aligned with technologies like:

- Intrusion Detection and Intrusion Prevention

  Intrusion detection technology mainly works for detecting cyber traffic and can be defined as “the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource. More specifically, the goal of intrusion detection is to identify entities attempting to subvert in-place security controls” [123].

  There are three well known intrusion detection technologies functioning over three different layer of detection:

  – Network Based (Network IDS): That function to identify unauthorized and irregular rarely based on network traffic. Network IDS using network tap, port span for detecting suspicious traffic in contrast of intrusion prevention system, Intrusion detection system does not block any network traffic. So, the network Intrusion detection system is gathering, identifying, logging and alerting security team and systems administrators. As explore of this technology is SNORT open source system.

- Host Based (HIDS): That function to identify unauthorized and irregular rarely based on device or specific host traffic. HIDS mainly get involved with an agent installed on each system for monitoring and alerting any suspicious activities on OS or applications by combining rules, signature and heuristics. As example of this technology, OSSEC - Open Source Host-based Intrusion Detection System, Tripwire, AIDE - Advanced Intrusion Detection Environment, Prelude Hybrid IDS
- Physical (Physical IDS): It is the act of identifying cyber threat to the physical systems and is usually considered as physical control to ensure confidentiality, integrity and availability. In addition, it works as a prevention system. Security Guards, Security Cameras, Access Control Systems (Card, Biometric), Firewalls, Man Traps, Motion Sensors are example of Physical Intrusion detection Systems.
- Intrusion Prevention Systems (IPS): It is adding the ability to block (prevent) the malicious gathered and identified data and behavior, which differentiate Intrusion prevention system from Intrusion detection system.

- Digital Forensics Tools

  Digital forensic field is mainly responsible for identifying the evidence of “who did it?”. In cyber domain it becomes essential that the attacker must be identified and known exactly “Who did this detailed cyber attack?”. Answering this question guides the cyber deterrence strategies for specific doers. Deterrence against unknown address is not effective and retaliation against undefined address is worthless. Digital evidences are not similar in cyber domain in term of source of evidence and procedures of data collection. For that, digital forensics specialists work hardly to identify source of cyber attacks.

  Cyber attack attribution is to link the cyber attack to the exact attacker as result of precise evidence. Directly or indirectly the improvement in digital forensic field support cyber deterrence strategies to attribute attacks and attacker. In short, there are different tracks on digital forensics, - Digital forensic for Operating systems: This track is concerned with operating systems forensics and evidence gathering like windows, android and IOS.

- Digital forensic for Networks: this track is interested in networks peripherals forensics like switches, routers and firewalls logs analysis.

- Digital forensic for mobiles and handhold devices: This track is mainly for mobile forensics and evidence tracing.

In the coming days of the research, the contribution of digital forensic for supporting cyber deterrence will be explored. Digital forensic contribution is the ultimate capacity of identifying attack and attacker for the purpose of deterrence.

- Security Information and Event Management (SIEM):

  Security information and event management (SIEM) systems are working to collect logs from variety of sources within organization. These sources could be from different operating systems, applications and on top of these are security technologies. Logs get collected and standardized in one format for the purpose of analysis and generate certain alerts. Some of the SIEM are facilitated with blocking of malicious traffic. It is available in different versions Cloud based SIEM, Hardware appliances virtual appliances and independent server system[124].

  In summary, the necessity of having high level of observability for the purpose of reducing the level of uncertainty is a foundation of figuring the adversary and his potential.

3.7 Cyber Deterrence Principles

Deterrence in general is a strategy for peace and it is developed for stimulating adversaries behavior and decisions that any offensive decisions will not be accepted in all means. Deterrence Principles provide states with a wide understanding of how to deal with other states and these principles will act as a systematic approach for managing deterrence strategy. Overall, principles are more of basic conditions compared to the policies or objectives but it is fundamental for governing both.

The attempt here is to review these principles and try to bring them from traditional deterrence practice to the benefit of cyber deterrence program. It is usually helpful to apply these traditional principles to the new deterrence domain like cyber domain for developing a systematic way for understanding the cyber deterrence as well developing the practice of the deterrence in cyberspace. Another objective here is to understand how to practise these principles and to enforce all these principles in every deterrence case or only for certain cases. Moreover, will these principles be treated equally in governing deterrence or it will differ from one case compared to other cases.

Before reviewing the principles of deterrence, it is good to think about the causes of conflicts. The preventive and preemptive traditional military attacks are still successful in making differences when calculating (Gain-Lose) between adversaries especially if the opponents are very weak. This will not work if the opponent is strong because the defense of the opponent will raise the risk of lose more than expected gain due to the defense the opponent is having. Readiness and superiority between adversaries make difference for stimulating conflicts or hold any expected conflicts. This view about the conflict is more related to the traditional military confrontation and with the technological development the causes for conflicts change especially after second world war.

This research is about deterrence in cyber space and this newly developed domain states rely on for civil usages, like control critical infrastructure of the electricity and communication networks as well as to access military systems, energy control systems and control systems for nuclear power plants. Unfortunately, it has become a field of competition in many areas and has become the base for many geopolitical conflicts. Cyber space has become a field for competition between super powers that have the capabilities and competencies in developing offensive technologies in the cyber space.

Referring to the literature, only two references has studied this critical issue. The first reference was a book specialized in military strategy principles and historical perspectives written by john m.Collins and the second reference was a research paper made by Andrew P.Hansen. Collins has produced the traditional deterrence principles and he concluded these principles: *Preparedness, Non-Provocation, Prudence, Publicity, Credibility, Uncertainty, Paradox, Independence, Change and Flexibility* [125]. The second best reference has assume another list of principles which are *Define the Domain, Defend the Domain, Destroy Threats to the Domain, Beware of Treaties, Establish Escalation Precedence, Ensure a Flexible Response, Institute a Collective Defense, Demilitarize Foreign Policy, Determine the Focus of the Deterrence Effort and Continually Incorporate History* [135].

Deterrence is mainly developed seeking for peace, to persuade the opponent in acceptable way that attack of any kind or even escalation is not desirable for both sides. To develop cyber deterrence program, a state needs to establish cyber deterrence principles that can work as a framework for the whole strategy. Cyber deterrence was originally inspired by traditional deterrence and at this point of the research investigate the traditional deterrence principles and to explore how these principles can shape the general cyber deterrence strategy.

The Principles are fundamentals or proposition that serves as the foundation for any system. In other words, deterrence principles are like a linked chain forming any deterrence program to get established. So, For deterrence there are some basic principles should be in place before establishing the deterrence program that state need to consider every single principle. The concept of deterrence has been utilized for multi-purposes not only in military strategy and accumulative support for these principles will reflect on governing deterrence whole strategy. The variation can be aligned case to case. So, the traditional deterrence principles that are essential for establishing any deterrence strategy are inferred from historical incidents and will try to review and address how each of which serve the core missions of the deterrence [125]:

- Principle of Purpose:

  Conflict prevention is a fundamental objective for the states deterrence strategies. Therefore deterrent strategists and national security strategist should specify the purpose from initiating the deterrence policy before establishing any strategy. This is because each deterrence case need a different treatment compared to other cases due to the uniqueness of each of which cases. Plans exercised to preempt offense do little to discourage malicious operations and it encourages the need to extend the deterrent umbrella. Sometimes, deterrence timing create limitation either to activate the implementing of strategy or postpone the course of action till other factors fulfilling the need for activating the deterrence. Moreover, strategist need to decide whether to extend or to limit the period of deterrence strategy in the case the main purpose achieved.

  Another dimension is the the purpose of align deterrence with alliances. This add to the principle of purpose another challenge either state to involve with alliances or to limit purpose of deterrence with its direct threats classifications. Common interest between allies can form cooperation under deterrence umbrella which requires deterring threats against the common interest. In case state distinguishing between full or limited involvement in alliance deterrence, it can be for state to establish a pragmatic independent deterrence.

- Principle of Credibility:

  Principle of credibility is mainly about ability to utilize the reward that and punishment for the purpose of manipulating with opponent to take it seriously. Credibility increases the adversaries likelihood to change the opinion from possible to probable regarding particular conflict. The principle of credible deterrence that raise the cost of the attack can not be achieved unless the the promises of punishments and incentives look like more reasonable.

  Its is simply the threat of retaliation or promise of reward that should be credible enough to get believed by the opponent. It should be clear enough that if you did X I will do Y and I am known by the threatener that I am serious enough to do it. This approach fulfill the principle of credibility, because if the deterrent said that he will do X if threatener did Y, then Y happened and nothing changed from the deterrent. This practice will spoil the threat credibility. State to develop its credibility must be clear and committed. Otherwise, the opponent's expectation will not be build based on a solid credibility.

- Principle of Uncertainty:

  The principle of deterrence based on the uncertainty is the alternative principle that may be used in the case of credibility principles for any reason not possible to be achieved. State with a changeable situations will give opponents with uncertain intention. It will lead the opponent to have uncertain expectation weather state is going to retaliate or not and this will maintain high level of fear from deterrent or between adversaries.

- Principle of Pain:

  The principle of Pain is to establish deterrence via painful penalties and this principle can support the demand for deterring opponents. Deterrence strategies can not be exactly taken from one case and applied the same to another case. It is essentially preferable to modify either the punishment or incentives according to the uniqueness of each individual case.

  The high level of threats used for the purpose of deterrence could seem look like unrealistic. But, promises to punish very severely and at the same time could keep opponents leaders to double think before initiating any unacceptable actions. Deterrent need to send clear message about the severity of threat will be utilized in the case threatener exceed the permitted lines. Raise the certainty of painful threat is an effective principle and it will keep causing difference in deterrence calculations.

- Principle of Pleasure:

  The principle of giving pleasure or satisfying the opponents is working. State need to consider what could deter opponent in order to give some sort of pleasure to give up from another higher risk threat expected by the threatener. This principle support deterrence strategy to balance between punish or reward opponent for aiming to drive the decision to hold from another higher threat that adversary could go for or to limit the conflict.

  Deterrence strategy should provide enough flexibility between threat and incentives to ensure its success. Rewards may effectively deter opponents and their allies. It could cost less than to keep threatening by retaliation where state need to confirm the benefits from rewards that opponent will gain by signing the agreement or treaties of cooperation.

- Principle of Preparedness:

  The Principle of Preparedness is to continuously keep state prepared to encounter an attack even during peace time. State readiness is considered as a great deterrence principle due to commitment that this principle can give to defend against opponents threats.

  Robust defenses and preparedness for retaliation will reduce the risk but sometimes decision makers and other crews lack institutional memory or historical memory,so they forgot to learn from previous cases or learn from this cases too late. Poor armed teams, poorly equipped and badly outnumbered could cause a deterrence damage and will stimulate opponent to take preemptive action in attacking. This principle can be observed in any conflict where state need to assure preparedness to have a credible deterrence.

- Principle of Non Provocation:

  Non Provocation principle means not to initiate any strategies considered as provokable acts by state opponent. Violating this principles could collapse the whole deterrence and sparking the conflict. The strategist who aim to avoid this impression will carefully try not to use the power or maintain the balance.

  Provocation with weak state could be considered as preemptive strategy and it could deter limited threats. But, provoking a strong state will open the door for other unexpected challenges. There is a need for certainty about states weakness or strength. Otherwise, the surprise of retaliation from strong state will change provocation to lose (From attacker prospective). Strong defenses aligned with enough level of readiness not to initiate any preemptive strategy could provoke opponent to protect deterrence strategy.

- Principle of Prudence:

  The principle of prudence as a result recommends military to utilize shields and civil defenses which could help to reduce the damages, and limit the losses. Also, it will force adversaries to pay more than expected in the case they select to go for the conflict. Carefully observing the domain and benefit from true indicators about the status, counting both: gain and loss of the action will help state to forecast deterrence improvement.

This happen when two states confront each other in nuclear and first state confirm its capability in destroying its opponents completely and this strength of response is there to drive the wisdom between both opponents to got for cooperation. The confrontation will result lose for both, Logically, partial loses are better ending.

- Principle of Publicity:

  The principles of publicity consider sending various signals either for the purpose of threatening or promising or rewards. It is conveying a message of observability for the suspected threat. So, state intentions and capabilities whether to penalize or reward adversary should be mentioned in public. For achieve deterrence, state should clearly mention its intention and let opponent decide how to act.

  State strategist need to be very careful to decide what information should go for public and how to form information that encourage opponent to cooperate. In some cases, state aim to trap its opponents via sending public signals via invalid public information. Both cases -trapping or deterring- state need to have its capacity to signal publicly. Conveying the messages can be conducted directly or indirectly, verbally or nonverbally, officially or unofficially, once or repeatedly. Moreover, messages sent by seniors are more credible than messages sent by juniors.

- Principle of Paradox (contradiction):

  The principle of paradox is for state to decide either to follow the philosophy of war as the best assurance for maintaining peace between states. The military conflict discourage the overconfidence between enemies and encourage the friends to keep being state friend. This doctrine will prevent or delay a conflict in future. In other words, this principle give confirmation that strict defense will spread large benefits for the deterrence via convincing opponents to cooperate rather than confront. So, the decision of war used paradoxically to end the conflict by peace. The threat of initiating a war will deter high expected future wars.

Traditional deterrence principles inspire the cyber deterrence research for further optimization. This encourages us to look deeper to these principles and give state strategist guidelines of developing cyber deterrence principles suiting the cyber uniqueness. This will be investigated in Section 3.6. Cyber deterrence principles will serve expected scenarios within cyber conflicts toward advancing deterrence strategy [135]. This research enhance these principles and align them with cyber domain to come up with clear principles considering the uniqueness of cyber domain. National deterrence strategy will be the first step to the direction of deterring cyber threats.

Table 3.7 Deterrence Principles

Traditional Deterrence Principles [125]	**Cyber Deterrence Principles [135]**
Principle of Purpose	Define the Domain
Principle of Credibility	Defend the Domain
Principle of Uncertainty	Destroy Threats to the Domain
Principle of Pain	Beware of Treaties
Principle of Pleasure	Establish Escalation Precedence
Principle of Preparedness	Ensure a Flexible Response
Principle of Non Provocation	Institute a Collective Defense
Principle of Prudence	Demilitarize Foreign Policy
Principle of Publicity	Determine the Focus of the Deterrence Effort
Principle of Paradox	Continually Incorporate History

The table list the deterrence principles suggested by [125] and the principles given in the second reference [135]. The table attempts to list assumed principles and find out which could be more efficient to be highly prioritized. Looking at second reference [135] list. This list simply describing procedure of what state should follow to approach cyber deterrence strategy. While first list is more of principles in term of its generality in shaping the concepts. For that, the below subsection would explain how the second reference approach define the principles. From the first glance, the reader can understand that these principles are closer to be practical procedure rather than solid principle.

- Define the Domain:

  Cyberspace is more managed by the private companies and states has attempted to define its cyber boundaries. US government has produced a clear vision regarding securing its cyberspace via its national cyber security strategy [126]. The strategy does not limit its operation within openness and collaboration that characterized internet growth, the strategy has defined what sort of activities are prohibited and not accepted within cyber space.

  States to develop cyber deterrence strategies need to define what is accepted and what is not in its cyber space and for the unaccepted state willingness to response. Moreover, state need to be more selective in term of approaching any engagement with cyber adversaries due to the nature of cyberspace and the expansion happening on a different dimensions.

- Defend the Domain:

  States to develop cyber deterrence strategies need to be enough equipped not with cyber technologies only, but other tools like strong diplomacy and capacity to raise different sanctions against threat state. Relying on cyber defense will not give any guarantee to deter cyber attacks as the sequential cyber attacks cases is enough to confirm the failure of defense in deterrence [127].

This does not mean cyber defense is not important but it shed the light over the importance of having strong cyber defense and at the same time to align defense with other strategies that will support the mission for deterring cyber adversaries. State to give priority in cyber defense as a first line for the mission of cyber deterrence aligned with other tools.

- Destroy Threats to the Domain:

  During the nuclear arm races, USA was very clear in term of threatening its opponent and has declare that it will destroy its adversary with nuclear attack as retaliation if USA get attacked and this commitment has sent a clear message if you did this I will do that and the result of nuclear confrontation was very clear for both adversaries. As the George Washington mentioned in his speech for the congress in 1793, “If we desire to avoid insult, we must be able to repel it; if we desire to secure the peace, one of the most powerful instruments of our rising prosperity, it must be known that we are at all times ready for war” [128].

  The idea for state to deter cyber threat, it must guarantee a credible threat of retaliation and there must be a clear commitment to proceed the threat of punishment against its adversaries in case it was attacked and state has attributed the attack sources. Moreover, there is a need to have some sort of transparency about the capacity of state cyber retaliation without specifying what is the targets and how to target opponent in cyber. This idea will create a sort of ambiguity with the opponent and could inject the fear of destructive retaliation and deter the opponent.

- Beware of Treaties:

  Establishing the treaties between states will help to hold or reduce the arm races. It has helped in prevented superpower from developing weapons on the space domain and that’s why we witness a limitation in arms development. This confirm one of the deterrence dimension by restrain adversaries from developing weapons. This treaty has resulted between all adversaries either USA or other superpower not to challenge each other and enforce the cooperation not to weaponise the outer space [129].

  In cyber, if this approach has been followed before witnessing this race on the cyber attacks between states expected to make a better cyber space. Cyber attack like

STUXNET has confirmed that initiating cyber attack against Iranian nuclear infrastructure has provoked Iran to develop its cyber offensive capability and this case was like opening the Pandora box and this is what NcGurk stated on TV interview [130]. After STUXNET attack any attacker can download the actual source code of it and re engineer it to use it against another state infrastructure.

- Establish Escalation Precedence:

  State need to prepare the escalation precedence and the conditions of being considered more important than something else. Cyber deterrence in relation to crises management need further study and careful policy consideration. It is the issue of either to integrate the cyber with nuclear or to limit the escalation ladder within cyber.

  In addition, international community agree about the need to secure the cyberspace but the challenge with the credibility of cyber threats for deterring. Then the idea of response with nuclear attack if cyber attack occur to state, and the Stuxnet attack has sparkled this debate and this scenario or the need of recalculation and re-evaluation [131].

- Ensure a Flexible Response:

  States are expanding with the growth of cyberspace solutions. In the case state selecting to respond, the response need to be flexible and calculate the consequences. Cyberspace are very fragile domain in all states and US on top of them. For that, flexible response is still the same as a concept but in term of practice are different compared to traditional practice.

  Flexible response within cyberspace is highly recommended due to the fragility of cyber and state dependencies on cyber and the use of force as a second option as a best structure of threat for retaliation. In nuclear, the response was clear via nuclear retaliation. Challenge in cyber is when cyber response is sufficient enough to deter from the first response (Cyber retaliation). State preparedness benefit from cyber offense capacity and the USA has authorized the section 954 from the national defense authorization to act for fiscal year 2012 [132]. Despite of this permission, the complexity of cyberspace is still dominant over the permission.

- Institute a Collective Defense

  Cyberspace is shared domain between all states and there is no physical borders compared to other threats domains (Land, Sea, air and space). It force states for more cooperation with other States to draw the lines of collective cooperation to defend against cyber threat. There are historical treaties like Australia, New Zealand, and united States security treaty or as Short titled as (ANZUS) signed in California 1951 for the purpose of providing mutual support in the case of any aggression and for settling disputes by peaceful means and this kind of treaty is one of the first treaty mentioning cyberspace and how states collectively should cooperate [133].

Initiating such like collective coalitions in cyber deterrence is helpful in different dimensions and especially in tracing the Non-State actors. One of the worst challenges within the cyberspace is the non-actors compared other deterrence missions and collaboration between states. Worth mentioning, deterring non-state adds value to the cyber deterrence strategy.

- Demilitarize Foreign Policy:

  State need to to develop its capacity in term of equipment, training, testing the best practice, and review the readiness related to the cyber deterrence strategy. But this does not mean that state should keep threatening randomly. This capacity is needed for threatening the potential cyber adversaries and it is for the purpose of sending a credible message about the State ability to deal with this types of threats. The show of unequaled military is good to confirm for others that the state is better than everyone or everything of the military capability. This help to develop a peaceful international environment and drive more diplomacy and demilitarization [134].

  Combining traditional military with cyber capabilities give state the ability to activate non-military. The diplomacy to encourage other states to act more peaceful. The strategy of demilitarize the foreign policy for deterring cyber space will encourage opponent toward incline to attack to cooperate.

- Determine the Focus of the Deterrence Effort:

  Deterrence is more complex than defense of offense in term of mission and how to focus the mission. State need to consider the how focus are the deterrence policy and identify the opponents decision maker as a target for deterrence to work. Opponent decision maker is decisive or critical, especially in the success or failure of cyber deterrence.

  So, states need to assure communicating the cyber deterrence messages in a clear and very precisely practice. This practice could be achieved via direct signaling against adversaries leaderships.

- Continually Incorporate History:

> The previous points and what I would like to title it as cyber deterrence procedural steps give practical process for the state aiming to establish its cyber deterrence strategy. It is like a general condition for the state to keep in mind it is not the final decision. For developing effective cyber deterrence strategy state need to look at the previous historical conflicts and retrieve the learned lessons for the future strategies.
>
> Cyber deterrence is a different problem compared to other deterrence strategies and this raise the challenge to the strategist, historians, security specialist and decision makers to double thinking while developing cyber deterrence and avoid any unwanted mistakes that could end into any unwanted escalation.

As mentioned earlier, the approach of Hansen [135] in defining the deterrence principles is more to a procedural guideline than a principles that can be utilized to govern the deterrence strategy. The principles should be more generalized and more of conceptualizing the targets as well as draw general lines. Then, it is supposed to be followed by procedural steps that reflect general principles. It can be debated but in conclusion, any state attempt to develop cyber deterrence strategies recommended to follow the approached structure in the Fig. 3.8 as a road-map.

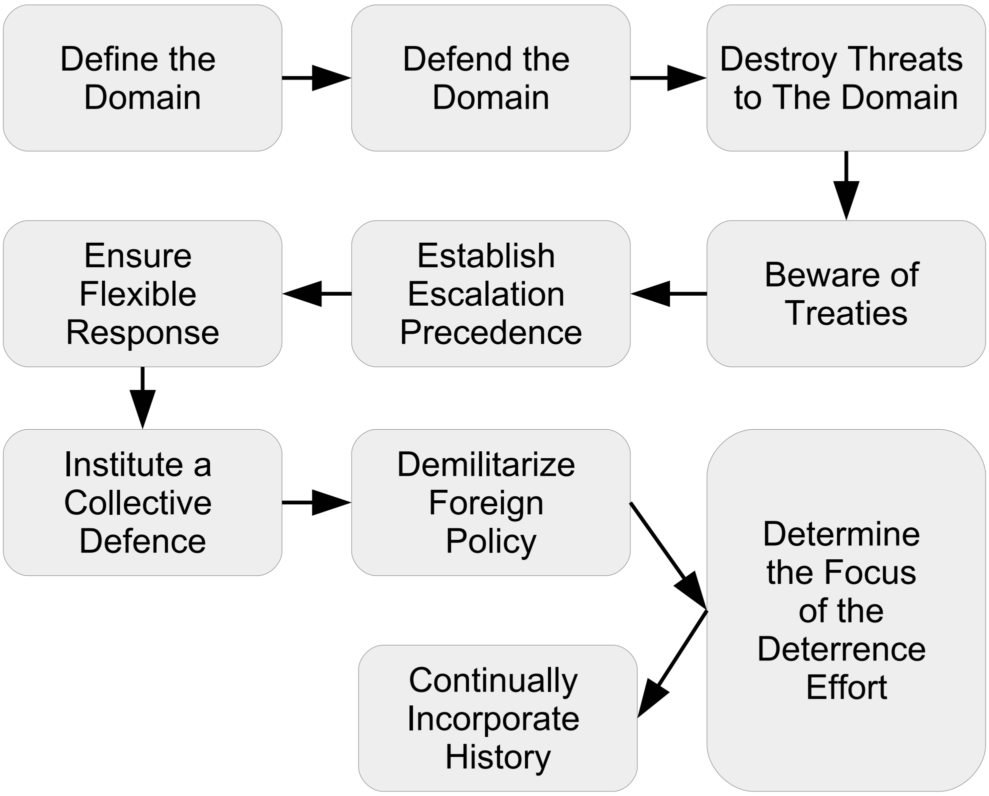

Define the Domain
Defend the Domain
Destroy Threats to The Domain
Beware of Treaties
Establish Escalation Precedence
Ensure Flexible Response
Institute a Collective Defence
Demilitarize Foreign Policy
Determine the Focus of the Deterrence Effort
Continually Incorporate History

Fig. 3.8 Deterrence Implementation Process

Referring to the mathematical analysis in the nuclear deterrence theory section (3.5) the role of each principle will be more clearly understood. The detailed analysis of deterrence model will give insight look about the relation between the principles and its necessity for the success of the deterrence strategy. As example, "Non Provocation" as a principle is similar to preemptive strategy. The question here, If state provoke its opponent, will it deter them or escalate the conflict?

As a conclusion, for having a robust cyber deterrence principles it is fundamentally to look at the general traditional principles as main cyber deterrence principles and combine together both approaches to aid state to produce a robust principles that will shape the national cyber deterrence strategy. Still more work is needed in this area aligned with the deterrence model to validate each principle role in shaping the deterrence strategy.

3.8 Cyber Deterrence Challenges

The concept of deterrence in general has its characteristics and basics. Referring to the nuclear arm race and cold war, the unbelievable power of nuclear weapons gave enough credibility to scare opponent from nuclear retaliation. For that, when we consider deterring motorists who use alcohol above the authorized limit [136] is different from studying deterring employees who do not comply with organizational information systems policies [137]. Each of these contexts has its own uniqueness.

This research focuses on the applicability of deterrence strategies in cyberspace. Therefore, investigating the zone between deterrence and cyberspace is the scope of this section and in order to deepen the understanding of the effectiveness of cyber deterrence, the challenges must be studied. Cyber deterrence is similar to many other scientific fields encountering challenges in its successful implementation. Achieving cyber deterrence strategy for any state requires to hold threat of retaliation, that will force cyber opponent not to initiate any cyber attack. To achieve the objective of cyber deterrence, there are many difficulties [138] that weaken the process of activating cyber deterrence strategies.

The aim of this section is to review the literature that studied cyber deterrence challenges [139]. It will shed the light over the differences between the traditional and cyber deterrence challenges. These challenges that cyber deterrence face, is reflection of new emerge technologies. Therefore, it needs new approaches to deal with. In addition, the section summarize them in a scientific way and link them to the reality of daily practice.

Studying the implementation of deterrence strategies within the cyber space need to consider the challenges that could confront these strategies or feed the success or failure. There is a complication with the cyber space technologies and connectivities, but would like to be more realistic in term of justifying these complexity. Cyber space involves tremendously different players with extreme different potentials. It consist players from governments, companies, users, networked hacking teams, individual hackers. In addition, hackers in cyber space can be coordinate under different umbrella as sub national groups, networks, non-state teams, and anonymous red teams and these coordinations gives example of how complex are to deter them.

Cyber domain operated by technologies that are developed by human and these technologies expanding and growing in alignment with the different layers of connectivities with a mixed societies lead to establish the art of deception practices between all players. This results into challenge of identifying "Who has done that?" [139]. Identifying exact attacker who usually in cyber have "no return address" is a complicated process. Despite theses challenges, there is a progress in development of cyber security technologies and this could help cyber defenders to detect cyber-attacks during attack and in some cases before attacks happen by providing current status/ behavior of inbound traffic. Not all cyber attacks can be detected and missing detection of some of these attacks confirming the gap of attributing attacker due to the lack of technologies that fulfilling the need for full detection and attribution and provide indicators about threat sources.

In general, the difficulties for implementing deterrence in cyber compared to other deterrence like nuclear deterrence issues that are directly connected to the nature and uniqueness of the cyber domain compared to other domains and it could be summarized as [138]:

- In cyber, no physical borders between countries and network addressing is not enough, all communicating with each other.
- In cyber, no exact physical address or return address can be traced for cyber attacker due to the complexity and practice of deception.
- In cyber, justifying who is beyond the attack/attacker either state or non state and the up to what extend limitation of targeting.
- Speed of transmitting cyber attack to affect target is different compared to other traditional attacks.
- In cyber, there is no limitation for spreading infections or attacks among different states.
- Intelligence teams can play a good role in term of forecasting cyber capacity of adversaries but it is very limited compared to the other conventional deterrence.

These issues are in general reflecting the nature and uniqueness of cyber space and its infrastructure. For that, from my point of view states to have cyber deterrence need to integrate cyber deterrence with other sources of information and not to limit the strategy within the cyber security technologies. Cyber deterrence should benefit from intelligence sources for forecasting the capacity of cyber adversaries. Different cyber attack has occurred and at the beginning of identifying these attack it was very difficult to get attributed but after period of time and with the cooperation between cyber security technologies and intelligence, the attribution and pointing who is standing beyond such like attack has been achieved.

Before investigating the challenges, we need to look at the questions asked that stimulat cyber deterrence challenges. These questions and its impacts look like factors forming the core challenges of the cyber deterrence policy. Having a deep investigation from a different prospective gives a robust ground for allocating the solutions required.

Table 3.8 Questions Shaping Cyber Deterrence Challenges[140]

Questions	Effects and Impact
• Do we know who did it?	• Cannot identify whom to retaliate against
• Can we hold their assets at risk?	• Do not know retaliation effectiveness
• Can we do so repeatedly?	• Cannot know whether retaliation repeatable
• If retaliation does not deter, can it disarm?	• No second prize for failure to deter
• Will third parties (alliance) join the fight?	• Will interfere with singling
• Does retaliation send the right message?	• Deterrence Policy may create moral hazard
• Do we have a threshold for response?	• Will interfere with signalling
• Can we avoid escalation?	• Risks of reduce credibility of retaliation
• What if the attacker has little worth hitting?	• Retaliation could be an exercise in futility

The impact of these questions give a hint about the impact if the answer of the raised question is not there. For that, a separate discussion about each challenge separately and look to any literature discussed this matter

- **Challenge of Attribution:**

  Attribution in cyberspace can be described as the art of answering the question raised with the above table “Do we know who did it?” Answering this question can be considered as the first step for punishing who is standing beyond the cyber attack [141]. Several literature concluded that cyber attack attribution is either impossible or extremely hard to be achieved. Their conclusions were not technological enough because these studies were based on political scientist. By looking at literature published by computer science and engineering scholars it is opposite to political based conclusion. Understanding technicality of cyber-attacks enables the attribution to be achievable though it is extremely hard.

One of the best inspiring publication about the cyber deterrence challenge from my point of view is produced by Clark and Landau [190]. They confirm that attribution is possible when all stages of cyber attack are analyzed carefully. Although certain attacks are established by controlled machines,it is still possible to get traced and attributed as example DDoS. The ability to identify the attacker within cyber domain is not an easy task since it requires a collaboration between different cyber security technologies to traceback the sources of attack. Let us assume computer (A) is controlled by computer (B) and the computer (A) is detected as attacker while the real attacker is computer (B). This type of complexity in cyber domain need a deep analyses to understand each attack technicality besides the possibility to attribute attack.

Last two previous decades the main purpose of technological development was for expanding connectivity and spreading the networks. In other words, the concentration was mainly for networking and routing not for securing inbound and outbound traffic. As a consequence, sophisticated cyber attacks continued to bypass defenses perimeter. Then the need to know “Who Did it?” was raised as it is essential to have answer for this question as the response depend on the attributing the attack. This demand has motivated the development of technologies with new features for identify source and destination of traffic, as well as trace the spread of malicious infection like malware spreading over the networks [143]. The development of technologies will not stop at this point but we are going to witness developed technologies that add extra advantages to the attribution and control.

Tracking cyber threats sources with technologies that are having visibility features is available and producing incoming and outgoing traffic but not up to the expected level. It is not providing full scale of identification for the sources but slightly give some information about traffic [144]. Also, it provides features that help remove some sort of uncertainty about who is beyond particular traffic. The anonymity still there with the traffic but it has been reduced by the revolutionary cyber security technologies. Cyber security technologies is more concentrating with what is called “Network Visibility” [145]. These facilities became available within firewalls and many other cyber security perimeters. They will be continuously helping investigators to identify source of threats. Intrusion phase within cyber attack life cycle 3.9 essential phase for collecting information about cyber threats and develop different indicators on what to do regard it. These information will drive the success of cyber deterrence and as example of the information that will be good to be gathered and analyzed are [146]:

- Actor/ Attacker [One or Many][State or Non-State]

- Assets Targeted [DBs, Servers, Military Systems, Control Systems, Individuals]
- Motivation beyond attacking [Destructions, Gain the conflicts, Spoil reputation]
- Time/ duration of attack [timing related information]
- Attack vector [Severity]
- Vulnerability [Prevention requirements]
- Malicious Software or Tools used [Open Sources, Infected Zombies,,,,,]
- Botnet Reliance [Exploitation mechanisms]
- Origin [Sources of threst]
- Destination

If these information harvested, it will be a progress for the state to build upon and support the decision of allocating cyber security resources that supporting the mission of cyber deterrence. The figure below attempt to simplify the idea of alignment between attribution and cyber attack life-cycle. It highlights cyber attacks stages and what the state will need to invest to raise the attribution challenge.

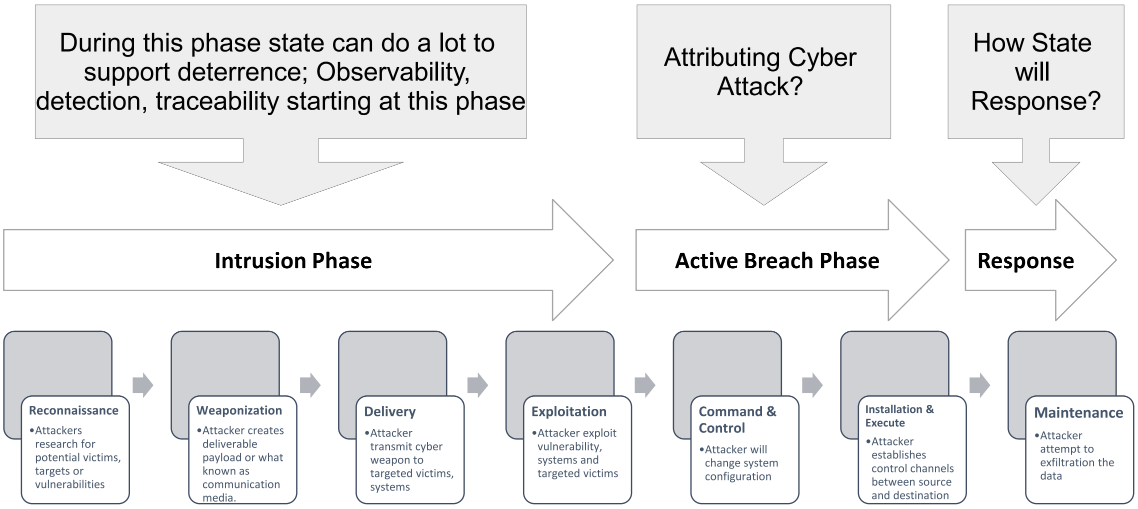

During this phase state can do a lot to support deterrence; Observability, detection, traceability starting at this phase
Attributing Cyber Attack?
How State will Response?
Intrusion Phase
Active Breach Phase
Response
Reconnaissance
•Attackers research for potential victims, targets or vulnerabilities
Weaponization
•Attacker creates deliverable payload or what known as communication media.
Delivery
•Attacker transmit cyber weapon to targeted victims, systems
Exploitation
•Attacker exploit vulnerability, systems and targeted victims
Command & Control
•Attacker will change system configuration
Installation & Execute
•Attacker establishes control channels between source and destination
Maintenance
•Attacker attempt to exfiltration the data

Fig. 3.9 Attribution alignment with Attack Stages

Attributing cyber attacks it is not just a pure technical issue and to achieve high level of attribution States will need to develop the skills, tools and the maintain high readiness of the national teams to deal with cyber attacks. The procedure of Attributing cyber threats having a different layers and national security teams need to be trained well to react professionally. As we have discussed that the cyber attacks are growing in term of complexity and it is not one step attack like traditional attacks but it is different, it is integrated and at the same time complex processes. So, state need to consider this difference when planing for attribution [147].

In conclusion, attributing cyber attack is a fundamental condition for the cyber deterrence strategy, and it is possible to attribute and point over the attacker but it is hard due to the nature of cyberspace. In comparison with nuclear attacks, nuclear weapons are easily to be identified, they belong to which country? But in cyber domain, deceptive and crafty mechanisms of communication make it complex. Hence, states need technologies with high visibility features to attribute cyber attacks.

- **Challenge of Geography:**

  The geography issue connected to the attribution issue as the cyberspace are connected globally. Cyberspace connectivity are expanded over most of the countries around the world and each state can communicate to another state without considering borders or any physical boundaries. This raises challenge for the state to develop its capacity to attribute cyber attack and identify the sources of threat.

  Another dimension for the geography and cyber deterrence is that state opponent can effect state infrastructure with cyber attack while he is sitting in his bedroom in a country at the end of world. Compared to the conventional conflicts, cyber attack easily for the state to deny that state are beyond the attack but conventional conflict its is not easy to deny the any attack due to the the nature of traditional attack are more tangible than cyberspace.

  Cyber threats against state infrastructure could be internal and it could be external and this categorization are based on geographical location. From the state point of view, deterring internal cyber threat is different from deterring external threats. Internal threats sources are within the State local law and governmental authorities, so it is easier to trace and deal with. But, the challenge when cyber threat geographically from outside state. It should be attributed either from state or from non-state actor, then if state was beyond the attack the deterrence strategy will be different and state deny the attack, non-state actors are the nominated and to deter such like group need different strategies which are not similar when state working to deter non state. Moreover, in both cases (State or non-state) you need to have opponent cooperation for deterring cyber threats and if there is no cooperation between both state there will no possibility to expect any optimization [148].

  All reasons discussed in relation to the geographical challenge reflecting international cyber threat against state infrastructure, this give obligation for all states and international community to cooperate due the fragility of cyber domain is shared between all states.

- **Code of Silence Challenge:**

  The third challenge with the cyber deterrence is the silent infection or silent spreads of the malicious codes. This challenge is because of the cyberspace uniqueness and when comparing cyber to other domains it will be like a new type of threat. It can infect State infrastructure while state does not detect the threat, and does not know when the execution of the attack is going to happen, and what is the target and what is the consequence of this attack in the case it get successfully executed. This happen in the case security controls are not capable to detect such cyber attack definition. These cyber threats that would prefer to describe it as "unknown, undetectable and unpredictable" cyber attacks. So, we can imagine how difficult is to deter threat with these characterization.

  Comparing cyber threats to other threats like nuclear threat from the above mentions descriptions give a glimpse about the nature of cyber threats and clear picture how challenging is to deter these type of attacks. Moreover, it confirms that we need a different deterrence approaches that are considering these uniqueness and to be more effective despite these challenges.

  Another dimension for deterring silent code is is to keep developing and updating the cyber security controls to a level to keep discovering process on going to optimize hardening the domain and make it difficult for the attacker to achieve the attack due to the cost expect to gain is lower than cost of attack.

- **Challenge of Regulations:**

  States needs to have its national security strategy for securing cyber space, this strategy encourage to shed the lights over the issues like regulating cyber space. Regulations are needed for the internal and external cyber threats and it is essential step to clarify the state readiness to deal with cyber threats either these attacks source internal or external [149]. Regulation and developing the norms are helpful [150]. It will support sending credible signal for state adversaries that if you get detected it will not stop to the point of attribution, it can be proceed for further actions. This approach could reduce the incentives for internal threatener to attacks and not sure about the external attacker as the external who need to have the cooperation of the other states that attribution lead to. From this point the regulation of cyber conflicts are a wide challenge for the deterrence strategy.

In April 2017, a meeting for the foreign affairs ministers of the G7 countries has approved what has been titled as " Declaration on responsible States Behavior in Cyberspace (G7 Declaration 2017). This declaration has addressed the issues like international stability and security of cyber space. As the growth in escalating cyber attacks occurred between states during last decade [151].

"*about the risk of escalation and retaliation in cyberspace [. . .]. Such activities could have a destabilizing effect on international peace and security. We stress that the risk of interstate conflict as a result of ICT incidents has emerged as a pressing issue for consideration. [. . .], (G7 Declaration 2017, 1).*"

This declaration shed light on the relation between the states and its responsibility in term of observing the behavior within the cyber and cooperating with other states in establishing norms and regulation especially for de-escalation confrontation in cyber space. These declaration from countries like G7 is an example to show how important to keep cyber space a peaceful domain.

- **Challenge of Spy versus Treaty:**

  Cyberspace has witnessed development of international treaties and regulation for the cooperation between states. The challenge is how to bring the cooperation between states despite the treaties while cyber space is full of ambiguity. The expected cooperation is for sharing information about offender teams, criminal networks or tracking attacks and attackers. This agreements will need to have mandatory technical practices to achieve its objectives [152]. It will add some sort of enforcement over states to invest in securing its domains and at the same time to keep observability practice over the domain. Also, it will encourage law enforcement organization to comply with these treaties as well intelligence teams. Another dimension for this issue is the type of international relations (good or bad) between both states and this dimension play a vital role for respecting or ignoring.

  Related to the issue of developing international norms and regulation, there are different states that reject to comply with these agreement and initiate operation like spying or what is known in cyber security as reconnaissance. This issue effecting the reputation of the state that initiate these operations and it can be considered as violation against the concepts of international democracies and a clear rejection of international agreement. The risk here is that reconnaissance activities can be detected between states and it can be considered as break for the treaties and easily will sparkle other states to initiate similar activities as the technologies for conducting such like operations are available.

For that, in cyber i assume that states are doing reconnaissance operations between each other silently and it is not a good approach as it will reflect on deteriorating the trust between states for the purpose of deterrence. So, it is a challenge and for the benefit of cyber deterrence states need to respect the treaties and not to allow any spying or reconnaissance operation against other states as it can be detected and it could stimulate opponents to do the same which will increase the challenge of deterrence in the future.

- **Offensive incentives Challenge:**

  Cyberspace have advantage and at the same time it is disadvantage. Avoiding international agreements and initiating offensive operation against cyber threats sources can be an option for the state cyber security strategy as there is no clear physical borders in cyberspace. In other hand, it could be a disadvantage to follow offensive strategy in cyber as it could destroy the whole cyber deterrence strategy and stimulate the conflict.

  Offensive operation is a preemptive strategy in cyber but it is not an easy option due to difficulty to assure the accuracy of the opponent and how effective is the operation in deterring the potential cyber threats. Practically to deter cyber opponent is not to preemptively provoke opponent without take account the response expected. There are real challenges in initiating any offensive cyber attacks for the purpose of cyber deterrence because of the nature of cyber infrastructure and the mistakes that could lead to cyber catastrophic between states.

- **Challenge of Social Norms:**

  Another cyber deterrence challenge is the development of social norms that governing the individuals behavior in cyberspace. Historically, different norms been developed for the purpose of deterring crimes, espionage and other warfare related issues. These norms can work to support deterrence policy up to certain point but it can infuse common understanding regarding the proper and improper behavior. Governments will distinguish between what can be categorized as cyber crimes act of war or it is just cyber espionage. In case cyber attack consequenced stealing one million pound is different from cyber attack targeting shutdown electricity grid. Each of these cyber attack are different in term of motives and target and the challenge here that the role of social norms to get developed for the purpose of deterring social cyber criminal acts where other opponent will not consider cyber attack initiated by individual as a ct of war by the source of the threat as wrong calculation.

For the accountability either internally and externally [153], states need to have social norms and it will help state to deter internal cyber threat at the beginning [154] then to establish understanding ground between cyber adversaries for the external arena. Another example, assuming state initiating a cruise missile which will result damage costing state ten million pound. This attack will be considered as act of war. In other hand, state initiate cyber attack result twenty millions pound as result of damage and this attack may will not be categorized as act of war compared to the cruise missile attack. This ambiguity or random categorization is a result of not having clear norms that differentiate between what is in the level of social cyber interaction and what is strategical (state-state) and above the social interactions.

- **Challenges of National Security:**

  Cyber domain is a share domain for private and pubic usage. This result a challenge for state cyber deterrence mission. States national security strategies are between traditional practice of direct interact with opponent cyber domain via scanning looking for the vulnerabilities and initiate cyber attacks that result a damage to the cyber infrastructure and limit the conflict within cyber and assure not to escalate to any kinetic war [155]. In other hand, state dealing with other private groups or red teams for conducting massive cyber operations against opponent. This kind of approach help the state to deny any responsibility form to the cyber attack. The challenges surround deterring non state actors and how challenging is to deter such like groups of criminal. Non-state players are another complex challenge to the cyber deterrence made by the cyber domain.

  Cyber domain has enabled this new methodology of confrontation between states [156]. While reviewing recorded cyber attacks in the last decade, we will conclude that there was escalation in frequency and severity of state sponsored cyber attacks. Our concern is the challenges of the cyber deterrence and if states keep this cyber strategy hidden, the consequence will not be for the beneficial for cyber deterrence.

  Deterrence by punishment can utilize the threat of retaliation for threatening but not to use it in real life and this make a huge difference for the national security. State threatening another state is different from other state using cyber threat to damage another state cyber infrastructure. First state practicing deterrence and second state utilizing the offense is easily leading to provoke opponents causing confrontation.

In summary, cyber deterrence in not a simple strategy compared to cyber defense. It is a complex strategy with a lot of consideration like avoiding escalation, Involving non state actors, international relations issues, norms and law enforcement. Challenges are there but

I would like to argue that these challenges are exist because there is no enough investment allocated for development. That's why most of the literature we review conclude that it is either impossible or it is very complex to achieve the deterrence in cyber space. But, with more development and investment in each of these challenges, cyber deterrence will work and it is going to work as most of states need to keep the cyber space safe. I think the development should follow more narrowed approaches rather than broader approaches. The development should select each of these challenges separately and pursue on how to optimize these particular challenges in the target to serve cyber deterrence strategy. Holistic approach will never lead to any result unless it get narrowed under very specific objective.

3.9 Successful Cyber Deterrence

The success of cyber deterrence is related directly to the level of development or improvements in the challenges that has been reviewed in the previous section (Section 3.8). Which means, as far as state is able to achieve the highest level of capacity and performance in each of these challenges will strengthen the success.

Cyber deterrence theory need to be polished by proving it with mathematical model analyzing the cyber conflicts and attempting to answer the assumed hypothesis. Moreover, developing cyber deterrence strategies that convince opponents that cooperation is more beneficial otherwise the confrontation will lead to keep his cyber infrastructure under punishment of retaliation. In other hand, cyber deterrence challenges at some point can be considered as indicators for success and failure of state cyber deterrence policy. For that, working on advances cyber deterrence should scope on optimizing cyber deterrence challenges.

As the cyber deterrence theory inspired by the traditional (nuclear) deterrence theory, it is aiming to provide clear answers for the fundamental deterrence questions [157]:

- When is cyber deterrence most likely to success?
- What is the most important determinant of cyber deterrence success?
- When is cyber deterrence most likely to break down?
- If cyber deterrence break down, how will it be resolved?
- Which one immediate or extended deterrence strategy is most effective, and under what circumstances?
- Which deterrence strategy can be more effective compared to other strategies against particular cases?

- Are limited cyber conflicts possible and, if so, under what conditions?
- When could escalation happen in cyber deterrence domain?
- How could escalation happen in cyber deterrence domain?

Effective Cyber Deterrence Program, One of the best statement that can explain how should the deterrence be in the very dynamical domain like cyber domain. This could lead to build cyber deterrence strategies aligned to what has been explained by Thomas Schelling literature when he said “One need to know what the adversary treasures and what scares him, and one needs the adversary to understand what behavior of his will cause the violence to be caused and what will cause it to be with held” [91].

Effectiveness of cyber deterrence should be aligned with assurance to react when targeted deterrence domain occurs. It is similar to say when a conflict by normal gun happen “one more step and I will shoot, and if you stop I won’t” [158]. This could be a scenario in cyber deterrence when accompanied by clear assurance.

Strong deterrence can be achieved via ultimate prevention of cyber-attack and ability to deter attacker or even potential attacker not to act. This will lead to reduce the likelihood of attack success and at the same time will increase the cost with the attacker to lead him to decide what we want him to decide. These concepts need to be re-shaped to serve cyber deterrence domain to achieve alignment between concepts and expected practices.

For that, main hypothesis for state cyber deterrence strategy can be summarized as:

1. Cyber Attacks can be observable, detectable, and can be attributed in various accuracy and can be reversed as a threat of retaliation.
2. Observability are there and the its practise in cyber space reflecting forecasting most expected sources of threats and identify the urgency or priority for initiating deterrence strategies against.
3. If attacker (State) assures will be detected, observed, attributed and will face retaliatory action either immediate or after period of time. So, they assumed to think rationally before exploiting any cyber attack.

These hypothesis will be tested within the developed models to validate its functionality. Cyber conflict in term of concept are similar to many other conflicts balance between wining and losing. The challenge here is to understand how actor in cyber space looking at the wining and losing.

Dynamics of Cyber Deterrence

Cyber domain is flexible in term of customizing cyber technologies which make it possible to develop new solutions to attribute cyber attacks. More specifically, growth in cyber technology reflecting growth in the demand in securing these technologies. At this particular issue the cyber deterrence strategies need to consider the dynamics of cyber space uniqueness. New technologies are needed to be developed to fulfill cyber deterrence requirements.

As example, assume one state suffering from multiple cyber attacks and at the same time want to establish cyber deterrence strategy. The strategy expected to control opponent to stop all or at least some of the attacks via strong cyber defense. In cyber domain, the defense layer are there to protect from whatever possible but it should work to provide extra service for the purpose of attributing cyber attacks. Technology should be enough flexible to get customized to serve the objectives of attribution. Because observing cyber domain is a top priority for the states concern about its national security. The cyber technologies need to provide ultimate support and highly consider challenges opposing deterrence in cyber space:

- Attribution
- Observability

Cyber deterrence are a mission for a dynamical domain (cyber) and due to the dynamic feature of cyber space there is a need for dynamic strategies that can be functioning in a different scenarios, it should get customized from time to time. Moreover, strategies can be shifted against another state adversaries. By considering the nature of cyber space and its dynamical changes in term of development, dynamical deterrence strategies are needed and then the assumption for successful deterrence can be highly possible.

General Conditions for Successful Cyber Deterrence

Diverting cyber conflict to stability and avoiding escalation between adversaries is one of greatest achievement for cyber deterrence. Therefore, cyber deterrence should be preemptive enough to assure prevention of unwanted actions from the opponent. Cyber deterrence working to manipulate with behavior of opponent to convince him with the consequence of loose at all options. Cyber deterrence can be successfully effective but we should understand the necessary conditions that usually decision are based on.

As this research is inspired by traditional deterrence these conditions will be revised within the coming chapters to meet cyber deterrence uniqueness but will list hem at this section for the purpose of grounding the modelling assumptions. The analysis and investigations to assure validity of these conditions for deterring cyber attacks [159] is part of the modelling responsibility.

- The general conditions for assuring successful deterrence can be assumed like two states in a a confrontation within a cyber conflict. First state can be considered as a Player (A) and it is acting as **Threatener** state and second state acting as Player (B) and its mission is to be continuously acting as **Deterrent** state that attempt to deter (A) not to attack via cyber space.
  - Player (B) deterrent must be able to detect the attacker bad behavior or unwanted cyber traffic especially during cyber reconnaissance stage.
  - Player (B) must have a visible and adequate capacity to carry out the deterrence threat of punishment, and keep this capacity ready. That means, player (A) must not be able to carry out a preemptive cyber attack that reflect player (B) capacity to punish.
  - Player (B) must be seen by Player (A) to be willing to perform the deterrent threat of punishment (as cyber deterrence strategy) or Otherwise committed to carrying it out continuously.
  - Player (B) must consider opponent capacity carefully and make rational calculations about whether to attack as retaliation or give up from attacking as a punishment strategy.
  - willingness of Player (B) to carry out the cyber deterrence strategies is usually the most uncertain condition, because of carrying out the threat does not (usually) protect or re-gain the prize.
  - Retaliatory cyber attack consequences are (usually) visited on Player (A) as well as Player (B) and both can repeat it.

In cyber, initiating immediate retaliation is not an easy assumption due to cyber complexity and lack of complete information about source of attack. Despite the challenges within cyber deterrence strategies, some other assumptions and its reflection to the deterrence model are need to be analyzed how possibly enhance the deterrence in cyber space. The assumptions for succeeding traditional deterrence might be slightly different from cyber deterrence due to the nature of cyber space and the dynamics of cyber threats. These assumption could be summarized as:

1. Decisions of attacking for both actors within cyber conflict based on rational calculations of (Gain-Lose) within the cyber. Specifically, It reflect accurate evaluations

regarding each case aligned with careful assessment about opponent capabilities and this should stimulate the decision.

2. High level of cyber threats (high level of scanning from attacker, up-normal behavior of traffic, exploitation attempts ... etc.) can deter or sometimes provoke opponent. For instance, nuclear weapons deters rather than provokes opponent to act aggressive behavior while cyber may do the opposite.

3. Cost hierarchies of gain and lose for both attacker and deterrent are similar, at least to the point that each one avoid large-scale violence at or near top within the cyber space due to need for keep cyber sustainability in exchange business and many other benefits.

4. Both states attacker and deterrent have similar frames of analysis about opponent cyber capacity, capabilities. So, these can give signals of resolve and reassurance. This lead to maintain tight centralized control over decisions that might involve or encourage the use of strategic (Cyber) weapons or not.

- Technical Assumptions:

1. States to assure its superiority in cyber defense technology as it is the first deterrence strategy (deterrence by Denial) and it help deny attackers and discourage their motives by Maximize the value of attack compared to expected payoff (gain) from attack.

2. States need to assure cyber attacks are partially detectable and possible to get attributed correctly but not all attacks in same level of attribution. Detection technologies need further development to fulfill the need for accurate attribution. This will help in developing strategy for threatening attacker via strong retaliation that will be more than their expectations.

3. Other assumption, every state have developed its cyber security technicality readiness for cyber deterrence strategies as well as ready to distinguish between political and economical sanctions as responses reflecting cyber conflict.

4. Assuming developing cyber offensive technologies to utilize when in need could make balance between adversaries and it help deterrence strategies effectively. State need to let opponent know that they are ready to take further actions in the case of threat reach not/agreed level.

For that, adversaries will keep monitoring each other and observing each other cyber space for different objectives and on top of all to understand opponent behavior. This race lead to stimulate a situation between both adversaries and specifically can be described as "I know you know and you know I know" what i am currently doing. The conflict and race to weaponizing cyber domain are there but there are a space between. Both adversaries think about consequences in term of cost (gain/lose) and risk before take any decision of attack. For that, cyber offensive/ defensive technologies are needed to manipulate with opponent decision within cyber conflict and balancing the power between adversaries for the benefit of cyber deterrence policy.

3.10 Research Directions

Literature review chapter has traced traditional deterrence theory, defining the deterrence terminology and exploring lessons learned that made traditional deterrence (nuclear deterrence) work. The chapter has attempted to investigate the cyber space uniqueness and differences with comparison to the nuclear. This exploration aids to segregate similarity and differences between these two domains of conflict. It also tries to present the challenges with deterrence in cyber to scope the work on these challenges to achieve expected optimization in the states strategy. These challenges are gathered from different literature and summarized into a prioritized approach. The chapter has investigated main principles that shape state national strategy for cyber deterrence and shed lights over importance of these principles in establishing comprehensive strategy. Summarizing the literature chapter, there are few challenges with the efforts made in previous cyber deterrence literature can be squeezed into three dimensions:

1. First, many attempts mentioned the idea of utilizing cold war deterrence strategies for the benefit of cyber deterrence. History has taught us that deterrence during cold war has been successfully kept cold war cold, but the crucial point is: will deterrence following the same approaches (nuclear) keep cyber (state-state) confrontation cold?.

   When it comes to the cyber space, United State is considered as a credible state because it is far advanced compared to other states in term of cyber innovations and cyber security solutions. Unfortunately, this development has brought some drawbacks. It is depending on cyber for running plenty of critical infrastructure while its opponent is less dependent which make the opponent less vulnerable compared to US. In other words, USA is supposed to be more credible and stronger in cyber security capacity and this credibility is assumed to deter its adversaries in cyber space while in reality it seems not.

For that, credibility of cyber threat for deterring cyber opponent compared to nuclear threat credibility is not the same and it should be considered carefully before implanting same approaches to a different conflict domain (nuclear to cyber). In chapter four, a model will analyze cyber conflict between two states attempting to show the role of cyber threat credibility in the success of cyber deterrence. The analysis approach is to investigate the effect of credibility of cyber threat in deterring states adversary emphasizing the role of cyber threat credibility in cyber deterrence strategy.

2. Second, in cyber space it is very hard to convince state adversaries (leaders, military, intelligence, hackers, etc.) that the cost of hacking can really outweigh the expected benefit. Here where deterrence should function; When the opponent perceive that he is losing more than gaining. Deterrence in general is more about perceptions between both adversaries.

   For example, a state might believe that escalation utilizing cyber threat is enough to manipulate with opponents perception to prevent him from initiating any further cyberattack. So, the state will select attack as a dominant strategy. With the same logic, the opponents can develop cyber credibility easily compared to nuclear due to logistics and availability of cyber threat. This mutual credibility will stimulate escalation between cyber opponents.

   Due to the different perceptions about each other (state-state) priorities aligned with the uncertainty or ambiguity of the other state intension in cyber space, the probability of escalation is high and this is where chapter five is attempting to investigate.

   In case credibility fails to deter state cyber adversaries, a model of escalation between cyber adversaries is to be developed to clarify consequences of mis-perceptions between adversaries. Within the model, a situation of mutual escalation either within the cyber space or other conflict domains will be involved between opponents. Chapter five will analyze whether cyber escalation aid cyber deterrence or it lead for a further instability in the cyber space between states which normally cause mutual ongoing loses.

3. Third, justifying functionality of cyber deterrence is a real challenge to know if cyber deterrence work or not will need an evidence that support the theoretical assumptions. Actually, cyber deterrence mission is to prevent cyber-attacks not to occur between cyber adversaries. This needs more analytic studies that justify no attacks occurred whether they are a result of deterrence success, as a result of fear from punishment or a result of deterrence by denial. In other words, the deterrence approaches of punishment and denial are facing plenty of challenges in cyber space and as alternative there is

another approach to be tried by the state in achieving cyber deterrence missions. There are some factors that play a vital role in succession cyber deterrence like mutual interest in deterrence and keep cyber space more of peaceful domain for exchange benefits via cyber space.

It is chapter six where the research try to call another approach that could work in cyber deterrence. This approach is trying to list the difficulties that deterrence face in other approaches and shed the lights over the approach of entanglement as it is based on the mutual interest in deterrence. It is more of self-deterrence

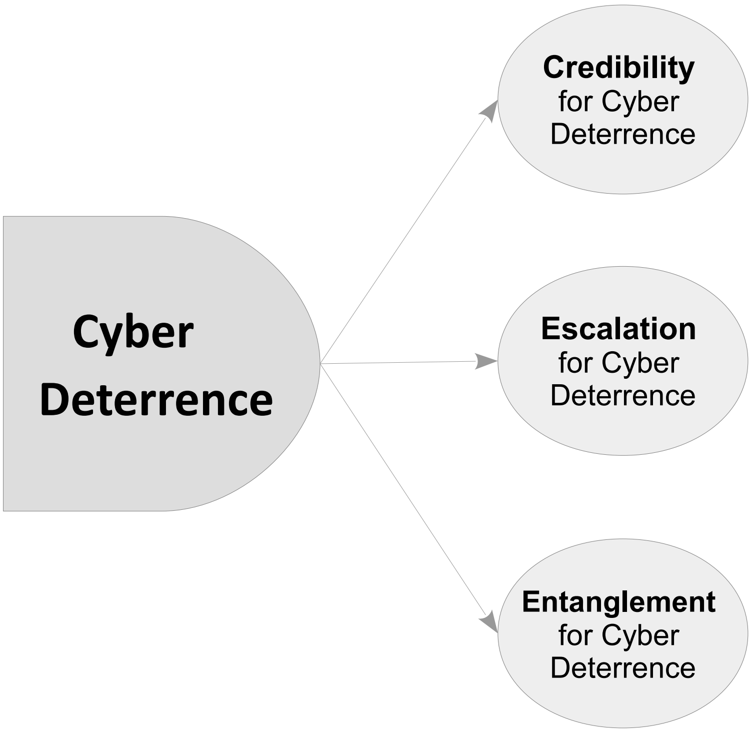

Cyber Deterrence
Credibility for Cyber Deterrence
Escalation for Cyber Deterrence
Entanglement for Cyber Deterrence

Fig. 3.10 Research Directions

From the research direction Fig (3.10), it will be clear that this research project is a response of the knowledge gap via developing mathematical models that analyzing:

- Chapter four: Role of cyber threat credibility (↭) in deterring state cyber adversaries and investigate the credible ways of manipulate adversaries decisions either by more enforcement that might further the cooperation behavior (deterrence) or winding down.
- Chapter five: Escalation (⇈) of cyber confrontation in the case of failure of credibility of cyber threat model. The chapter exploring the nature of cyber escalation ladder either it is going to be limited within the cyber or it can exceed to involve other domains of conflicts.

- Chapter six: Deterrence by entanglement model ($\leftrightharpoons$) as a new and could be the best approach for succeeding cyber deterrence strategy compared to other traditional deterrence model approaches (Denial or Punishment).

Chapter 4

Credibility for Cyber Deterrence

This chapter demonstrates the reasons for associating credibility with cyber deterrence and highlighting the role of cyber threat credibility with either success or failure of cyber deterrence strategy. It analyses the relevance of credibility to cyber deterrence assumptions in case of developing credible strategies.

A selected case study will be presented for motivation. The case will help to generate an understanding of the pivotal role of credibility in supporting cyber deterrence strategy from real life context. The observations are gathered from different resources and this will help to support assumptions raised positively or negatively.

An analytical model will be used to study the role of credibility in the success of cyber deterrence between two adversaries. The model considers several factors that assist in establishing credibility in cyber space like detection, attribution, defense, and offense. The model will help to raise essential critical questions like the importance of credibility in cyber deterrence strategy. With the same logic, other questions are raised within the model to highlight the essential ingredients shaping credibility in cyber space and reflecting the role of credibility between actors within cyber conflicts.

This chapter is concluded with a section that prescribes certain strategies which states can benefit from in real life practice. These strategies and learned lessons will assist states to understand the essential requirements for developing credibility in cyber space and draw the lines for states to develop or optimize its cyber deterrence policy.

4.1 Credibility Concept

The concept of credibility has played a central role in different national and international relations related studies and before jumping to demonstration of threat credibility, I will try in this section to investigate the credibility conception and the literature that was defined in [160]. Despite the claim of credibility and its importance in deterrence strategy, little attention has been given in the literature of traditional deterrence about the importance of credibility and its relation to deterrence. For that, this research examines the the theoretical connection between the cyber threat and its credibility in deterring cyber adversaries (State - State). Credibility was the cornerstone for nuclear deterrence and the certainty of damage that nuclear bombs will result are known and clearly calculated for both opponents.

As Freedman [157] characterizes credibility as the "magical ingredients" of deterrence and he mention that vast majority of strategic analyst believe that the "credibility" term is transparent enough and for that there is no formal definition to agree upon. So, he concludes that "Threat credibility is generally taken to mean that the threat is believed" [91] [98] [161] [163] by the opponent and this will be examined within the coming sections and this belief will reflect state adversaries and deterrence overall.

On the contrary, a threat that is unpredictable can be characterized as *incredible* or non believable by the opponent. As example, the nuclear conflict between the U.S. and Soviet Union during the Eisenhower administration could be described as conflict in (Status Quo). It is due to the threat credibility committed by the U.S. to respond in case Soviet Union violate in nuclear stability. Even after establishing the Massive retaliation Policy, it was widely criticized this policy is unbelievable by the Soviet Union and as consequence it is lacking credibility [164].

Smoke has claimed that the threat was not credible enough to stop the growth of Soviet Power because the Soviet arsenal of atomic bombs and long range bombers to deliver them grew during the mid to late 1950s. So, this led to less belief that the U.S. can launch any atomic war over any invasion in Asia or elsewhere [165].

Another school of strategist looked to credibility from the rationality point of view. This can be understood from the difficulty to give credibility to the state claim to go to war during the nuclear conflict because the adversary know the irrationality of such like threat [166]. Therefore, the concept of credibility is either directly or indirectly connected with rational behavior of the actor [165] [167]. For that, credible threat is the believed threat; threat can be believed only if it is rational accepted and applicable in the current condition. So, only rational threats are credible threats. But, what is shaping rational threat? The answer for this question depend on the rationality and its definitions.

From the above literature, a conclusion can be gained that the procedural rationality can identify rational threat by carefully describing the real world conditions and it will help to justify the retaliation response done by the state against its adversary. As a result of this procedural identification, the deterrent can separate those situations (Credible - Incredible) threats and then know if the threat is rationally credible (believed) or not. As a result of that, deterrent state can estimate its threat credibility from incredibility of the threat utilized in the promise.

Looking deeply at the U.S. and its threat of massive nuclear strike against Soviet Union, this action will trigger the Soviet Union to respond with nuclear attack. Under this condition, Soviet have “nothing left to lose” and they will retaliate against the U.S. in kind (Nuclear). Now, it is for the U.S. to measure its credibility in response to Soviet credibility before initiating any nuclear attack. There is a challenge of how each adversary anticipate opponent credibility response upon the attack and it is the responsibility of policy makers to justify this either to response or not.

From above discussion, threat credibility can be described as extend when deterrent prefer to execute the threat. For that, to measure the credibility of deterrent threat we should assume the player prioritizing to initiate the threat till the expected point and if it exceed that expected point it will be not worthy to continue and it could lead to defeat the threat rationality and hence it will be incredible threat.

Nuclear threat and credibility of state threat of retaliation in kind was one of the solid deterrence studies which has been confirmed from the result of no nuclear war has occurred between superpower. The core assumption was clearly assumed that the nuclear state is a credible state to threaten its opponent to cause catastrophic level of damage and it can be for both actors. If the nuclear threat that shaped state credibility for nuclear does not exist, state will not be able to send credible (believed threat) for its adversaries. This assumption will open the door for another large question which is: Under what condition, circumstances and what reasons threatener could receive the credibility of the threat? and What the state must do to convince its adversaries that this threat is real, not only bluffing?

Before going further, there are three possible influences that can shape state credibility [168]:

- **Reputation:** It is reflecting state image that adversaries believe about the state aligned with the state record especially the recent records related to the responding to the challenges either in the same region or anywhere around the world. Reputation could stimulate adversaries to roll back in certain situation as a result of deterrent promises and previous commitments. But, reputation is not enough to deter adversaries especially when sequence of failure occurred in the deterrent history. Relation between reputation and credibility is straightforward and it has to be consistent to impact robustly. In addition, some cases can impact upon state reputation equally while other cases can cause stronger impact. This is left to the state and its strategist to calculate the expected impact to its reputation.

- **Interest:** The influence of interest reflect state interest to respond to the given case and it can be practiced by different approaches. One approach can be via weight factors like the Value of gain or lose, amount of public population, logistic materials or other interests like relation of the issue to the state nation and its national security. Some cases have no interest for the state and it does not deserve to get any further attention while other cases are to be utilized for the purpose of strengthening the credibility.

- **Commitment:** It is State commitment to define what land to defend against, actions to be taken for assuring defense, punishments to be followed in case attacker initiate the attack. These declarations should be defined by the state clearly and the commitment will follow with some considerations. Commitment can differ depending on opponent cooperation and responses whether to signing treaties or execution by the deterrent. Sometime commitment overlap with the reputation and this overlapping lead adversaries sometimes to estimate the likelihood of the deterrent commitment and observing his responses record to estimate his direction in the future. Deterrent state gain credibility from its ongoing commitment whether it was a strong or a weak commitment.

These three dimensions (Reputation- Interest- Commitment) shape the state credibility within the international arena which needs careful calculation for the successful development of credibility. The model in the coming section will look at these influences and how they increase or decrease the level of credibility.

4.1.1 Credibility of Cyber Threat as a Punishment

Credibility may have different meanings in different contexts but the attempt in this research is to scope in analyzing credibility of cyber threat in supporting state cyber deterrence policy for developing long term strategy that could help increase peace between states within cyber space. Credibility is a multidimensional concept [160] and in this research will limit the investigation within the context of credibility of cyber threat as a threat of retaliation for deterring cyber adversaries.

The argument in this chapter is that state can develop its credibility in cyber space in supporting the strategy of cyber deterrence. The analysis approach aim to address first how state should develop its credibility in the cyber space and then explain factors that could shape credible and rational cyber threat. Achieving credibility in cyber space is not a simple task compared to other conventional conflict domains because of the uniqueness and complexity surrounding the cyber space.

Threat credibility means that the threat is believable by state adversaries and for that state need to understand the influencer for credibility in cyber space. First influencer, state reputation in the cyber space are playing vital role and it is important to get built aligned with state capability that the state hold enough amount of cyber threat that will effect its adversary up to level of assuring loses not to gain if the opponent initiate any cyber attack. In addition , state need to develop its capacity in detecting cyber threat and respond in a level that maintain the state reputation.

Second influencer, state should practice its interest in responding to cyber threat and giving enough attention to cyber threat to enhance credibility. Each state receive thousands if not millions of cyber attacks on a daily bases and not all these attacks have same interest because cyber attacks differ from DDoS, SQL, APT to a malware targeting critical infrastructure. So, not all these cyber attacks will steal state interest but at least state need to assure enough attention to be paid. In the case of single personal computer attacked will not be equal in impact than attacking SCADA system managing electricity grid of the state capital. In this case state interest should be more increased to match with the level of attack. In this case state need to define its interest practically to defend and deter its cyber adversaries.

Third influencer, state commitment to define its critical cyber infrastructure and these critical infrastructure will be like red lines that is not accepted to get crossed and if the opponent cross these lines by initiating any cyber attack state commitment to retaliate will be under examination. United state as example has defined its critical infrastructure and it has been clearly mentioned in its cyber strategy. Commitment to punish and retaliate should be defined by the state. State commitment for case after another will feed the credibility record how strong was the responses. Moreover, state should maintain consistency on same practice as it will strength the signal for its adversaries.

The argument that cyber attack is not credible enough in deterring cyber adversaries is not completely correct and need a careful critical assumption. For a state to become credible, it needs to follow and sustain a solid approach that assures its opponents about its credibility to retaliate effectively and repeat the threat to a level that could consequence high amount of losses. There are technical challenges but also in opposite there are plenty of opportunities that state can benefit from cyber space uniqueness to increase its credibility. The technical part of the cyber credibility begin when state develop its capacity to detect threat and attribute then credibly assure its willingness to threat by retaliate in a sequential situations. Threat of sequential attacks is possible in cyber due to vulnerability that cyber space can offer and it is plenty compared to nuclear. State reserve the right to have its credibility to threat its opponent but it is not having the right to use these threats. International system will not accept the use of threat if there is no reason but it is respected from state to develop its credible in the cyber space and it should be one of state objectives and the case study will present how credibility has been developed.

4.2 Motivational Case Study

Chapter argument is the credibility of cyber retaliation as a threat of punishment and the analysis aiming to understand role of cyber retaliation in cyber deterrence. Despite the claim that cyber attack does not effect human lives or devastate state infrastructure compared to other conventional attacks but there are other types of loses consequences by cyber attacks that should get enough consideration and a careful analysis. Cyber attacks has begun as a simple attack with a limited damage and over years has been developed in term of consequences and ways of attacking. Moreover, vulnerabilities spread all over cyber systems which can be utilized easily for effecting states critical infrastructure. More critical, when military infrastructures of state become vulnerable to a cyber threats. Yes, it can be one probability of successful cyber attack and it is a limited attack but no guarantor that in future to witness unlimited (replicated) cyber attacks and on going repeating itself which will impact with sever and harmful consequences.

For furthering explanation of the chapter argument and looking deeply to the argument, chapter sheds the lights over Iran and USA cyber conflict and how this particular cyber interaction has stimulate non-credible state against highly credible state to speed up and become as credible state and considerable state with respected cyber threat. Iran has developed considerable cyber capabilities to further its internal and external national security strategies and this development led to increase its capacity into the highest level of worldwide cyber credible states similar to Russia, China and USA. Stuxnet attack in 2009 was the most noticeable case that has initiated the race in Iran for develop cyber capability [169].

Considering Iran as a credible state in cyber space is based on the credibility influences that mentioned earlier in this chapter (Reputation, Interest and Commitment). Iran has a long record and solid reputation in the readiness for confronting its opponents and to response to any conflicts. When cyber attacks joined the political conflicts in recent years Iran clearly was not ready for it. Iran before stuxnet attack was not considered as credible in cyber and I assume that USA and Israel thought that Iran will not retaliate due its weakness in the cyber space capacity and the attack will succeed in demolishing the nuclear infrastructure.

But, despite assumption that Iran is not having enough capacity to response but it has developed its reputation via seriousness to respond and not letting attacker to run away without punishment. Then, Iran has practiced its interest in securing its cyber space and this was clear via stuxnet case responses and what has happened after developing the capacity.

Iran has confirmed its commitment to response to the cyber threats and attacks and has done it. These influences has confirmed Iran and its credibility in cyber space. Clearly each of these influence has impacted on Iran credibility and to identify within the model how each influence increase or decrease Iran credibility within state adversaries.

Looking at the historical cyber events between Iran and USA, there are a significant improve in Iranian cyber capacity. The correlation between cyber threat credibility and state cyber capacity is obvious and listed events in the coming sections is only as example help to understand the journey of Iran in developing its capacity in the cyber arena [170].

In 2009, and after Iranian president election, a political movement called "Green Movement" has protested against elected government attempting to remove new president and they utilized the social media heavily. This incident has convinced Iranian leaders about the need for more additional cyber capabilities to stop such like protest or for trace and arrest the oppositions.

Then by 2010 the western sanctions escalated against Iran and on top of sanction is stop selling any advance cyber security technologies to Iran. This has resulted to force Iran to develop its own cyber capacity domestically. Surprisingly, in the same year of the sanction 2010, Stuxnet malware attack targeting Iranian nuclear infrastructure has occurred and after long investigation the claim about the sources of operation was collaboration between Israel and US.

In 2012, Iranian cyber army has been formalized and led by the Revolutionary Guard and this army structured to operate under the Supreme council of cyberspace which has been established by supreme leader Ayatollah Khamenei. Establishing and nominating cyber army is one of the best evidence reflecting the interest of Iran to go further with the cyber space despite the sanctions. The Iranian cyber operation has begun since then with limited objectives like cyber espionage but after then world has witnessed another Iranian cyber threat.

Early 2016, and after long time of investigation US prosecutors raise that 7 Iranian supported by Islamic Revolutionary Guard Corps (IRGC) beyond DDoS attack conducted between 2011 - 2013 and the attack was targeting different systems related to around 46 US banks.

Iran has seriously developed its cyber capacity and has utilized its cyber capabilities to retaliate against its regional and international cyber adversaries like USA and its allies in the region (Israel and Saudi Arabia) from Iran point of view. In addition, Iran cyber threat has been admitted by Israeli leaders themselves and they have confirmed that Iran has become a cyber superpower and it is clear for them it is the fourth biggest cyber army in the world [171].

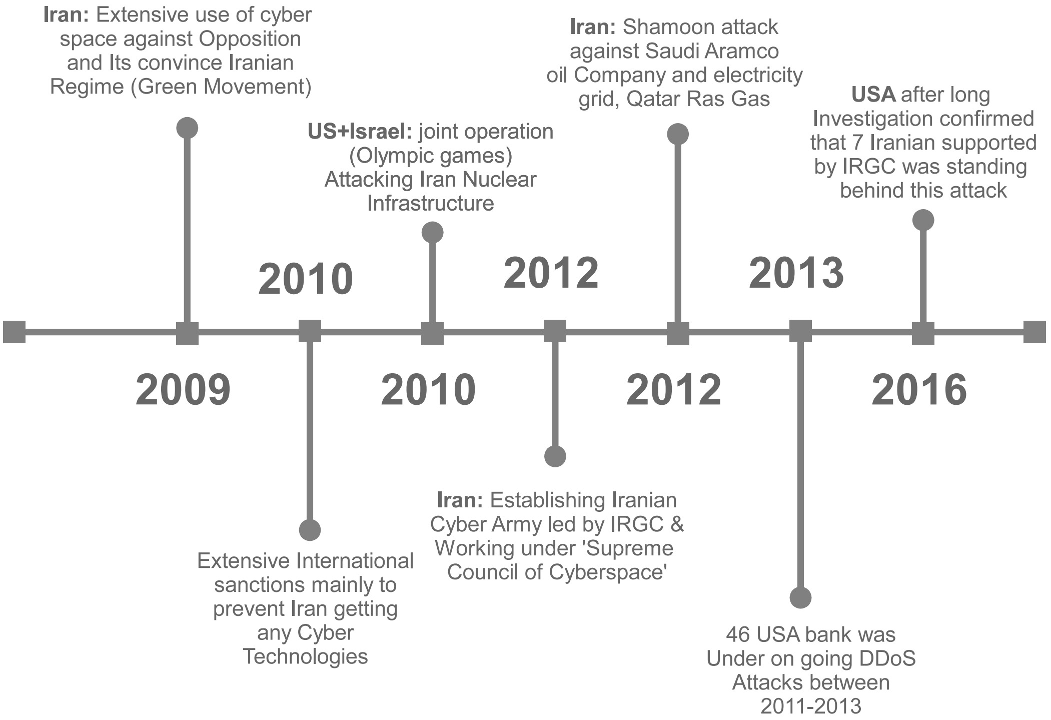

Iran: Extensive use of cyber space against Opposition and Its convince Iranian Regime (Green Movement)
2009
2010
Extensive International sanctions mainly to prevent Iran getting any Cyber Technologies
US+Israel: joint operation (Olympic games) Attacking Iran Nuclear Infrastructure
2010
2012
Iran: Establishing Iranian Cyber Army led by IRGC & Working under 'Supreme Council of Cyberspace'
Iran: Shamoon attack against Saudi Aramco oil Company and electricity grid, Qatar Ras Gas
2012
2013
46 USA bank was Under on going DDoS Attacks between 2011-2013
USA after long Investigation confirmed that 7 Iranian supported by IRGC was standing behind this attack
2016

Fig. 4.1 Iran Cyber Credibility Time line [172]

Another Challenge with threat credibility is to measure the credibility and the intention of state opponent to confront and this require inside information about both actors cyber (Offensive or Defensive) capabilities and what both player are going to do the next step.

Looking at the conflicts and real life practise and considering people involvement in executing these missions are highly selected, it is difficult to get a complete information about what is going on but by attempting to guess from result that might reflect what is going on and the interactions, reputation and interest the opponent intention can be estimated. Sequence of cyber incidents listed in the Fig. 4.1 is enough to estimate Iran next step in the case get attacked and its adversaries has known what is the usual Iranian prefer to response in the case get attacked.

Before Stuxnet, credibility of Iranian cyber threat was not enough to signal USA and its allies like Israel to double think before initiating Stuxnet attack operation. Stuxnet attack has encouraged the Iranians to go for as I would like to name as Iranian "cyber arm race" to develop their own cyber capability. Then, after short time Iran cyber capacity and its threats was known it is on and its cyber threat is respected by its opponents. This is where believability (credibility) begins when opponent knows that you have a threat that is capable to affect and cause harm. This respect happens after enough detection about Iranian cyber threat by different intelligence or cyber security specialist and community.

USA within 2015 deal, has tried new approach with Iran that may hold Iranian continuous development of their cyber capability but it seems the problem is not simply can be successful solved. Cyber space is different and traditional approaches seems not sufficient due to different reasons and on top of these reasons are the availability of the resources on-line and a different suppliers can produce the cyber threat and technologies. In other hand, USA cyber threat credibility was believed enough by Iranian and it was the reason or a motivator to accept to cooperate with USA in the 2015 agreement. Both actors believed that each other are credible (in Cyber) enough to effect its opponent within the same political conflict.

Before closing this discussion, another important issue need to shed light over the possibility to develop cyber capacity compared to other conflict domains (air, Sea, land and Space). States have wide resources compared to non-states actor, this will make states more and faster capable to develop their cyber offensive and defensive capability compared to other conflicts tools. Developing F16, F18, Nuclear missiles, or many similar tools need much of logistics and not all states will be capable to offer. In nuclear domain as example, states need plenty of logistics and international relations to develop their nuclear infrastructure, but in cyber the situation is totally different due to the availability, and connectivity of cyber space. This will simplify operations like reconnaissance and gathering plenty of information about state adversaries.

In reviewing Tehran vis-a-vis Washington within the cyber space confrontation and review the Washington vulnerability to a cyber retaliations, we can estimate how Washington was very careful not to respond to Iranian cyber attacks and threats with other massive cyber attacks as it could lead to unwanted cyber escalation or miscalculated cyber confrontation [173]. So, the damage expected to occur from cyber attack between both actors has stimulated careful calculation and this is due to credibility established between both actors after the stuxnet operation.

In this situation, where USA aim to deter Iran cyber threat [174], we can assume that it is going to be an easy task for USA to follow traditional strategies of deterrence like deterrence by denial or deterrence by threat of punishment as the the threat of cyber retaliation as a punishment. But, the challenge is that the confrontation is within the cyber space and Iran has developed its cyber threats and it is considered as a credible state in the cyber space. For that, each deterrence strategy (denial and punishment) is not going to work and for that US need to find alternative strategy for deterring Iran cyber threats especially with credible state like Tehran. In addition, the previous point is that USA is more relying to the cyber space compared to Iran and this issue is very critical and considerable not to go for further (cyber escalation) as the most looser is expected to be USA not Iran.

The most important role of state threat credibility is to inject its adversaries to believe that retaliation stamped with a clear commitment. If this believe (credible cyber threat) successfully injected to the opponent believe it will be enough to deter. Moreover, it will enforce to precaution before any cyber confrontations. Referring to Iran and USA, Iran commitment was examined after stuxnet cyber attack. Iran commitment to retaliate was there and it was sever enough for its adversaries and their alliances in the region (USA and Saudi Arabia). Shamoon attack [175] as well as many other cyber attacks exploited by Iranian cyber teams was the commitment and it is the confirmation of Iranian cyber threat credibility.

Despite the delay in the Iranian retaliation, but from the point of view of extended deterrence the late retaliation can be considered and it can be executed even later if the delay will help in term of getting more accurate and complete information. Both incidents stuxnet and shamoon cases was a real examination of how cyber credibility was not there and when first attack occurred has result for the attacked State (Iran) stimulated to develop its cyber capacity in urgency for getting the necessary credibility in confronting cyber space adversaries.

To wrap up the section, threat credibility means that the threat is believable by state adversaries, Iran has successfully developed its credibility in the cyber space and Iran cyber threat credibility believed by its adversaries and they know it can cause a real damage. In opposite, it is not simply to assume Iranian cyber threat was enough to deter its opponent to stop any future cyber attack as the deterrence is not limited only to the credibility of threat of retaliation punishment. The credibility of Iranian cyber threat has been developed over last decade and the above time-line has present the progress of Iran toward developing its credibility as cyber threatener state and to add to this, President Obama has confessed that Iran is a credible state in the cyber space and this is a confirmation about the stage that Iran has reach. In opposite, US cyber threat credibility also credible enough by looking to the reputation, interest and the commitment of US in response to cyber threat and threatener. Clarifying chapter argument in details will be part of next section and it will be within the model.

4.3 Credibility Model for Cyber Deterrence

There is little published literature that has discussed credibility and its role in deterring state adversaries. Most studies in the field of strategic deterrence have only focused on importance to develop its credibility without detailed analysis. To the best of our knowledge, our research is among the first conducted on credibility of cyber threats in deterring state cyber adversaries and the model developed is the contribution for the field of strategic cyber deterrence. This section investigates the relation between credibility in cyber space and how states can particularly utilise cyber threat as a threat of retaliation in cyber arena.

Conventional approaches for deterring state opponents is either to denial the threat or threaten to retaliate and both approaches will be explained within the model. Cyber deterrence by denial is practically possible by developing another defensive capacity that assure state capability to fail the expected threat. Then, in case state does not have the sufficient cyber defensive capacity that assure failure of adversary threat, state will follow the second strategic approach of deterrence which is threaten to retaliate in case threatener decides to attack.

Threat of retaliation from the state (deterrent) perspective should be believed by the threatener (attacker). The belief about state retaliation (Threat) should be both credible enough and effective severely as a retaliation. States' credibility and its strategic reputation in cyber space is different compared to the nuclear deterrence. Credibility of nuclear weapon within the nuclear conflicts is clear from the consequence that the nuclear bomb will result but in cyber, both actors practice within the conflict is full of mis-perception and this cause miscalculation between players.

Before progressing in this section, it is good to notice that within the process of analyzing credibility of cyber threat there will be a strategic requirement supporting the assumptions will be mentioned and nominated automatically. These requirements reflecting the technical side of the cyber space and it can be considered as learned lessons within the model. Because these tactics state without it will not achieve the main objectives of deterrence.

By referring to conventional nuclear deterrence game model, it was clearly known that the threat of nuclear retaliation from nuclear state is there and it is credible enough. The credibility of nuclear threat was understood between both states and Cuban missiles as a best example to explain how deterrence played vital role in preventing any nuclear conflict between both adversaries USA and Soviet Union. Both actors were nuclear states and confirmed if they get attacked, they will immediately retaliate by nuclear attack. This mutual confirmation of retaliation was assumed as a reason for injecting the fear (Credibility and Believability) between opponent.

Scope of Credibility Model: *scope of this model is to analyze cyber threat credibility and its role as a threat of punishment in deterring state cyber adversaries. This model is not considering other threats in developing state threat credibility for deterring state cyber adversaries.*

So, credibility of nuclear threat as retaliation was known and understood due to consequence of nuclear attack is known, the state opponent is a nuclear state and has the motives, the willingness and reputation in confronting USA is also there. The probability of miscalculation was highly expected and it could have occurred at any moment between both adversaries. Looking at the game model in Fig. 4.2 will help to understand the nuclear deterrence model. The model assumes two nuclear states and one state aiming to deter its opponent. Simply, each state has two strategies: either to attack or to cooperate with the opponent by not attack.

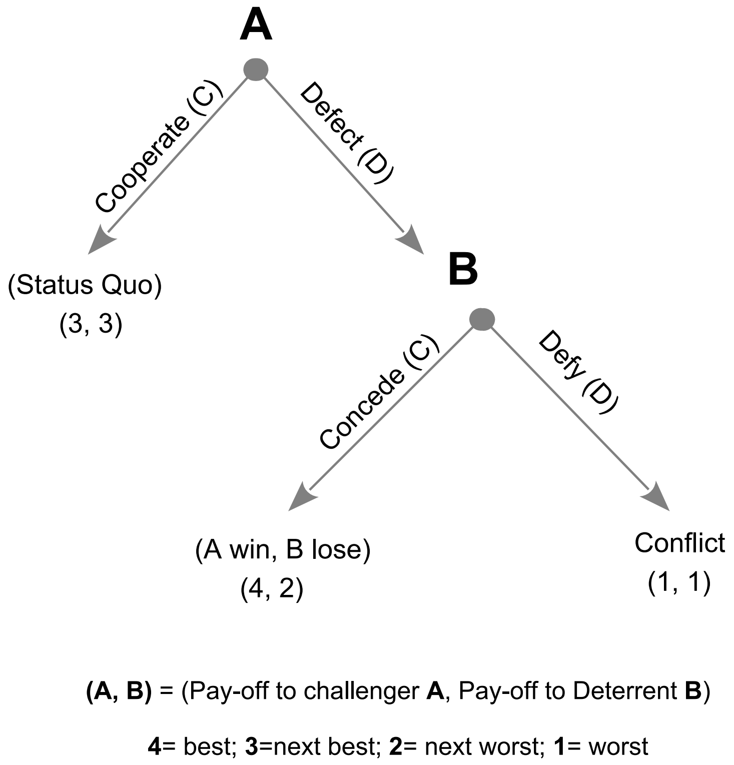

A
Cooperate (C)
Defect (D)
(Status Quo)
(3, 3)
B
Concede (C)
Defy (D)
(A win, B lose)
(4, 2)
Conflict
(1, 1)
(A, B) = (Pay-off to challenger A, Pay-off to Deterrent B)
4= best; 3=next best; 2= next worst; 1= worst

Fig. 4.2 Classic Deterrence Game [68]

According to the traditional deterrence game model, both nuclear states in a political conflict and both states work to cause some damage or effect its opponents for different reasons. Each state has two strategies to play with and possible to choose either:

- C = Cooperate (Not Attack)
- D = Not Cooperate (Attack)

In nuclear model, the aim was to assess the possible outcomes from the nuclear conflict and understand how nuclear deterrence has worked within the model as well as in real life. Model assumptions have four possible outcomes within the same nuclear conflict and each outcome is different from another outcome due to different possible reasons that are analyzed below:

- First outcome: State (A) prioritize the strategy of (non-cooperation) and follow the (attacking) strategy against its opponent which is State (B). Then, State (B) will not respond (not-attack) and this will result for (B) to get defeated. Maintain same scenario will stimulate (A) to maintain selecting (attacking) strategy as a dominant strategy. So, State (A) is the winner within the conflict and the game end at this point.

  Simply the case here is that (A) = C > D, while (B) did not respond to (A), the Strategy of C > D has succeeded and the reasons beyond this success could be lack of defense, surprise of attack, or weakness in state (B) defenses.

- Second Outcome: Second situation of the conflict is when both states prioritize to attack each other in any possible situation without considering gain or loose via miscalculation where each individual state is expecting to win while the in real life is not going to achieve any wining. Proceeding this strategy separately from each state point of view will assure the result of conflict between both states. The conflict in nuclear domain mean a mutual nuclear holocaust.

  This is the worst outcome of the model because (A) = C > D and at the same time (B) = C > D. continuous commitment to maximize the **C** (Attacking) Strategy from both (A) + (B) will result continuous loses from both states especially if both states rely on a good amount of resources to support maintain the same strategies that will maintain the result of (Conflict).

- Third Outcome: Final possible situation from the nuclear deterrence interaction within the model is the cooperation between both state (A) and state (B) and maintaining Status Quo (SQ). It is achievable when both (A) + (B) maximize the (Not attacking) as prioritize strategy for both states. For that, State (A)= C < D and the same situation with the State (B)= C < D.

  Maintaining the $Status\ Quo$ outcome between both actors is the core for deterrence stability and will result assurance that there is no decision for any preemptive nuclear attack between adversaries. This outcome is achievable under strict conditions for example strong defense that trip up any attempts of attacking or fear from retaliatory punishment that consequence loses more than any expected gain. Within both situations credible and believable threat are essential to stimulate the opponent cooperation behavior.

Third output of the general deterrence model $(Status\ Quo)$ figure 4.2 is where a mutual credibility of nuclear threat has played a vital role in shaping peace between nuclear power and has maintained peace even during cold war. Moving from traditional to cyber and developing a probabilistic model for analyzing cyber threat credibility is the final destination of this chapter. The approach of developing probabilistic model that help to understand how to bring both opponents to the outcome of (Cooperation , Cooperation) or what is called (Status Quo) where there is no intentional deliberate cyber attacks. This is essential for state in deterring its cyber opponents is to have credible cyber threat that help enforce for cooperation and assure sustainability of cyber deterrence strategy.

4.3.1 Threat Credibility and Cyber Conflicts Outcome

Comparing both traditional games Fig. 4.2 and 4.3, the main difference between both games is the credibility of threat and its reflection to the payoffs consequence for each state in the situation of two credible states in confrontation. In this case, both states can $Maximize(Attack) \geqslant (Cooperation)$ the strategy of attack and at the same time opponent can respond and its response is credible enough for causing enough damage for its adversary. In comparison with State have no credible threat the conflict payoff will not be the same. It will be more probably credible state will dominantly act with superiority due to credible threat under the hands which make the difference in confrontation calculation.

In the deterrence game with players holding credible threat for retaliation Fig. 4.3, the payoff of both states (A) + (B) when holding credible threats assumed to end up with (2,2) while in conflict between two states with no credibility to threat it is expected to be (1,1), see Fig. 4.2. This is because the credible threat will assist state to defend and retaliate against external threats. Moreover, it will strengthen its capacity within international system.

There is a significant correlation between threat credibility and the outcome for each state within the same conflict. State with credible threat could cause a different level of damage to its adversaries and at the same time for the adversaries with the credible threat is not the worst due to availability of the credible threat and probabilities to retaliate against first strike and cause mutual damage. So, when state assure that its opponent hold credible threat and based on the expected outcome when confronting with credible state, the state need to recalculate carefully whether to move further or try another approach for winding down the conflict. State payoff with the credible threat is not the worst payoff due to high probability for the attacked state to retaliate. In this situation when both states get confronted and they have credible threat within the model, the expected outcome is going to be like:

$$State(A) = C < D = 2 \tag{4.1}$$

$$State(B) = C < D = 2 \tag{4.2}$$

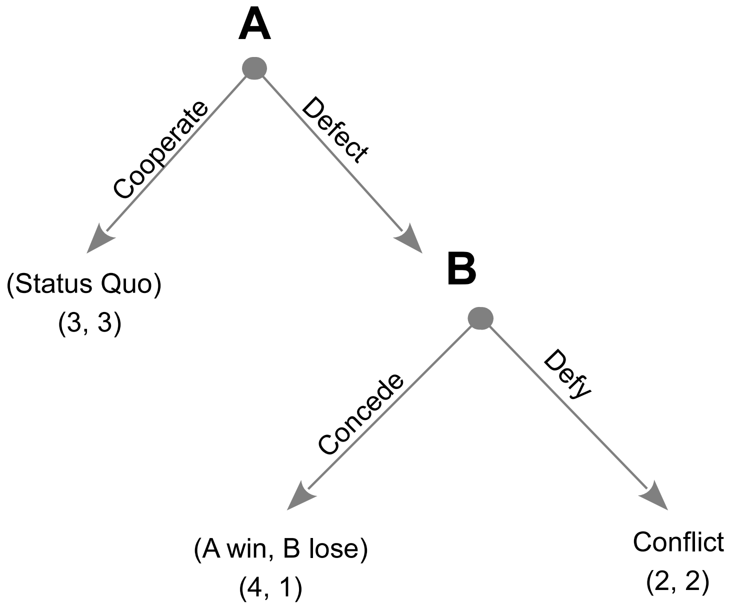


Fig. 4.3 Simple Deterrence Game with a Credible Threat [68]

Credibility of threat was clear in nuclear deterrence models. The cost of nuclear attack and consequence of attack are expected and known between both states. The challenge is when threat credibility is not clear between actors due to lack of information about cost of threat or cost of damage possibly resulted from the attack. In cyber, there is no clear measurement about the damage that (X) cyber attack from state (A) will result (Y) amount over state (B). Yes, in case scenario of attack is defined and specified exactly, estimation is likely to be measured. It is because a procedural experimental with clear and defined sampling while in real life the situation is different. Moreover, cyber attack is unpredictable as the vulnerabilities are unlimited within both states (B) and (A) cyber space.

For that, no state will know what other state is capable to do with its cyber infrastructure until state get attacked. Cyber attacks are ongoing and the deterrent state is gathering information about who is standing behind these attacks. This process provide more information about cyber threat credibility and attributing these attacks stand out in this information. At this point attacked state can retaliate with its credible threat in kind (cyber attack) or if the state is not having any credible cyber threat then it will have nothing to rely on.

Threat of retaliation in kind (Cyber Attack) is the first step for the state aiming to develop its credibility in the cyber space arena. Once state begun to confirm its commitment to deter and confirm its interest to deter its adversaries within cyber space the credibility is the corner stone. Deterrent retaliation (cyber retaliation) could be similar to the first cyber attack and utilize the same malware as retaliatory threat and it could work to send signal about willingness to threat to retaliate. In addition, state can replicate the same cyber attack for causing more credible damage for its adversaries. Referring to the Stuxnet malicious code it can be found on the cyber space and then it can be re-engineered and utilized against the threatener by the deterrent. This replication is one of the uniqueness of the cyber space which permit the same scenario to get repeated. Cost of developing main cyber threat could not be the same compared to customizing or replicating second generation of the same original cyber threat and this is a another factor should get considered deeply.

The outcome from cyber attacks are not similar from the state national security perspective. If the attack targets independent banking systems, it is not similar to another cyber attack target biggest national power station. The result of attacking power station will consequence a total shutdown for the whole city as well as the banking systems. So, cyber attacks or cyber threat outcome shape the credibility of cyber threat that is needed for deterring state adversaries. The level of threat effectiveness is correlated directly into deterring adversaries and it is the state decision to develop the credible threat for deterring the opponents without considering the consequence. Another advantage from developing and keeping the preparedness in cyber space is not to use it but only for the purpose of deterrence.

Morgan [85] argues in his book that there is only one deterrence theory while Quackenbush [68] argues against Morgan that there are at least two types of deterrence theory which are Classical deterrence theory and Perfect deterrence theory. ***First***, *Classical deterrence theory rooted to the basic assumption where that the high cost of nuclear war make conflict the worst outcome for everyone*. ***Second***, *Perfect deterrence theory rooted to the assumption that different states have a different preferences that cause some states prefer to backing down or roll back from the fighting*. In opposite, other states prefer to pursue on fighting because these states holding credible threats supporting state strategy for maintaining longer fighting.

Detailed examination for both theory assumptions are needed and the approach for justifying the accuracy can be through selecting case by case. I think the differences between both deterrence theories are linked to the outcome of conflict and the differences in perceptions between each state about threat credibility. The model will help to get more understanding about both deterrence theory assumptions. Here, I will renew the traditional assumption to a new assumption that are fitting cyber deterrence and cyber threat credibility;

- First assumption; Raised by classical deterrence theorist that the highest cost of damage could caused by the attacker will shape state credibility. In our case, the highest damages that could be caused by initiating cyber attack could shape state credibility, or

- Second assumption; Raised by perfect deterrence theorist that assuming that it depend on State perception about the threat value and importance. In this research, it reflect cyber threat and how each state believe about cyber attack consequences and its credibility (destructive attack or not).

Credibility of cyber threat for the mission of deterrence is relevance to the above assumption but we need to look deeply to the real world in practice. Prior to stuxnet and other cyber attack targeting critical infrastructure, States was considering cyber attack as a single cyber attack and it will go. But, when cyber attacks start targeting states critical infrastructure the calculation has changed. Cyber threat considered as a serious threat affecting national security and need to do something regard it. In order to investigate the correlation between cyber threat and state perception about each cyber attack we have to have a better understanding how cyber threat can occur repeatedly as in Fig. 4.5 and could target the low level outcome and at the same could affect high valuable cyber asset within same state cyber infrastructure. So, relying on traditional deterrence model without repeated game mode to analyse cyber deterrence will not work and for that new model as a fundamental cyber deterrence model is developed. This model is the ground for other cyber deterrence model mainly to analyse repeated cyber interaction between two states and it is the figure 4.4. In this case, states with the ongoing cyber conflict will realize the value of loses. First cyber attack can play a role of awakening or like sparking the attention to the importance of cyber threats then it is for the state to calculate where to move next.

Before moving more deeper in the credibility analysis and its role in cyber deterrence, I think it is essential to elaborate in differentiating between deterrence in nuclear and cyber. Nuclear deterrence model 4.3 assume state (A) believe that the probability of (B) retaliation is certainly and it is going to wipe (A) most valuable assets. The Nuclear threat was targeting big cities for assure casing massive damage. Nuclear threat of retaliation was certain and credible enough and dissuasive to stop state (A) from beginning not to attack (B). State (A) payoff in the case of attacking (B) is $(A_i) < (b_j)$ which is not worthy to go for the attack from the beginning. The high certainty about consequence of nuclear confrontation was enough to stimulate the fear within (A) decision owner from attacking adversaries with nuclear attack.

The assumption of nuclear deterrence model that the credibility of nuclear threat is enough to deter opponent does not work in cyber as it is with nuclear. The argument, if it is working we will not witness hundreds of thousands of cyber attacks around the world. Because simply each state is ready to claim to retaliate against any cyber attack supported y state opponents.

But, what if the cyber threat of retaliation is declared by the attacked state and it is not just a retaliation but it is going to be a repeated retaliation till exceed the previous attack.

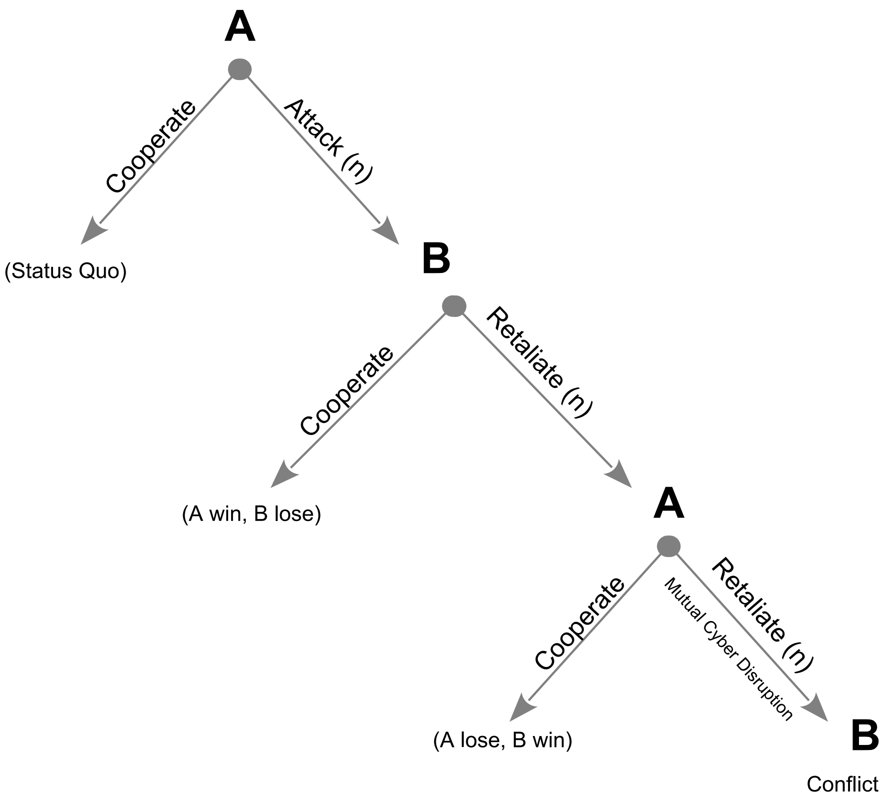


Fig. 4.4 Cyber Deterrence Model

Repeated threat of retaliation for the purpose of deterring state cyber adversaries I assume will make difference in conclusion and will assure ($Maximize = Lose > Gain$). For optimizing credibility of state cyber threat, it requires more than one stage of interaction between the adversaries due to the nature of cyber attacks and need to realize the capacity of states opponents. At first, cyber attack can be considered as a general attack from non-state actors but after further attribution a more complete and accurate information gathered. Second, if the target was under different context like what has occurred in Iran nuclear infrastructure it will reduce the misperception and it will raise the state beliefs about the cyber attack credibility with its adversary especially if there is a long journey of exchange cyber attacks between these two states mixed with different cyber target like what figure 4.5.

In summary, its not easy to assume threat of retaliation within the first round of cyber confrontation will assist state in developing its credibility and it will deter State cyber adversaries. So, the classical deterrence model seems has worked in preventing nuclear confrontation but i don’t think with its current assumption will work in the cyber space. In cyber space, state reputation, credibility and its willingness are not clear within the first game until its adversaries gather more information via attributing these attacks. Then, state

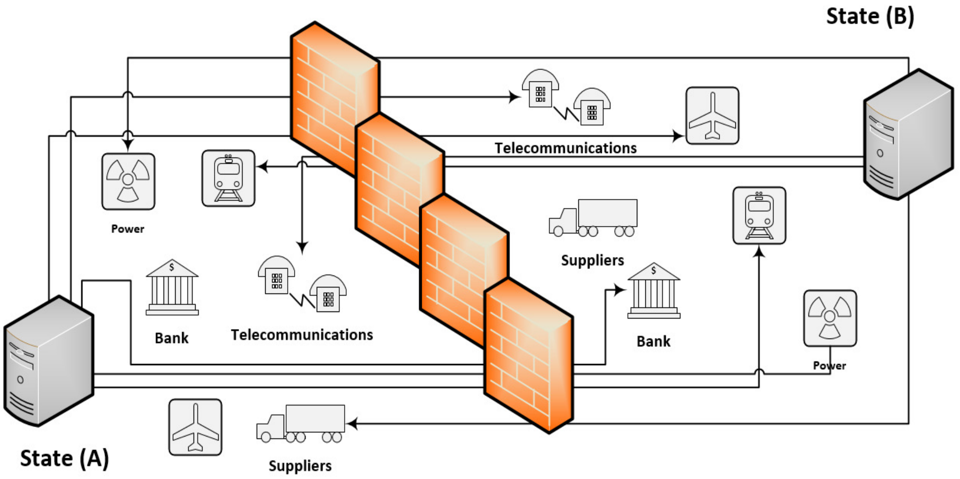


Fig. 4.5 Cyber Attacks Exchanges between State (A) and (B)

credibility is examined and assured, which will increase the certainty about its intention for the coming interaction. State need a model with a nature of sequential game model to analyze sequential interaction and shed the light over the growth of cyber threats credibility. The model will exceed the assumption of the classical deterrence model to develop new model with a model having more than one sub game (Fig. 4.4). This model aid in aligning nature of cyber deterrence problem and provide bigger image about the complexity of cyber deterrence.

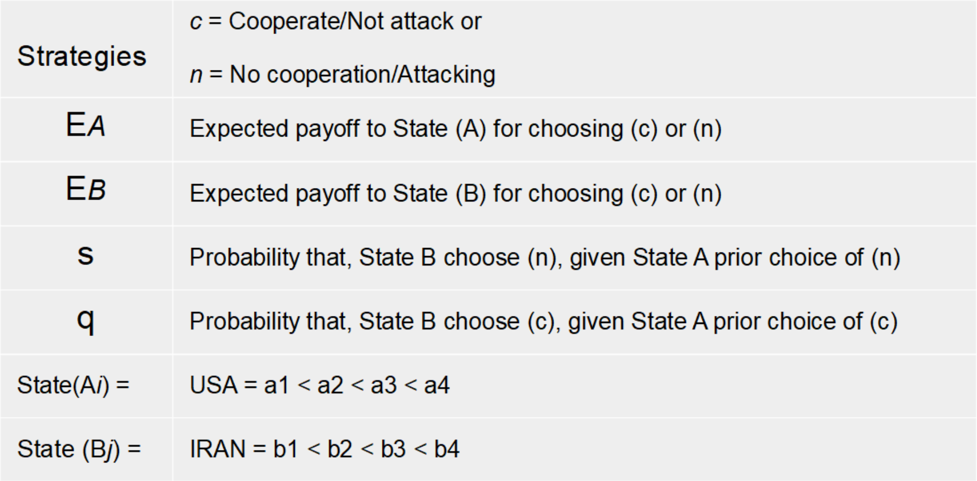
Cyber attack with high level of damage is having a high level of expectation to stimulate retaliatory interaction rather than observing the consequence from the attacked state point of view. Moreover, retaliation from state (B) will lead to another cyber interaction between both actors and this is the difference between nuclear and cyber deterrence models. In further thought, this multi stages of cyber interactions within the cyber deterrence model and cyber space will assist in confirming credibility of cyber threat and within the coming sections will observe the role of threat credibility in deterring each other or it may further the cyber challenge.

4.3.2 Credibility of Cyber Threat under Complete Information

Unknown cyber threat can be classified as incredible threat due to incomplete information about the attack timing, its target and its expected consequences and damage. In opposite, others can argue that unknown cyber threat is highly credible due to its unpredictability. It will keep state in foggy situation of difficulty to predict time, target and amount of loses that could create. The answer to this argument is when state has its credibility the adversaries are supposed to expect the worst within the conflict and keep the preparedness up to higher possible situation.

Complete information that aid a state in pointing at threat sources (cyber adversary) is limited due to shortage in cyber attribution. Additionally, the superiority with state opponent remind us about credibility influencers discussed in Section 4.1 (Reputation, Interest and Commitment) and how this mixture reflect into developing credibility model. The general credibility in cyber is expected to get developed over sequential and repeated cyber interactions. The state proves its credibility in every attack that gives precise or at least semi-precise information about how credible it is against adversaries. State practise should sustain reflecting its strategic commitment in developing cyber credibility.

Moving to the credibility of cyber threat model and its role in cyber deterrence, the assumption consists of two states (A) and (B) and each state moving with two strategies. First, **- c -** Cooperate by (Not attack) and second **- n -** Not Cooperate by (Attacking) the opponent. One of the game rules is that each state can get other opportunity to change between these two strategies within the sub game. Each change in state strategy will be considered as a retaliation if attack and defeat if not attack within the model interaction.



Strategies	*c* = Cooperate/Not attack or *n* = No cooperation/Attacking
E*A*	Expected payoff to State (A) for choosing (c) or (n)
E*B*	Expected payoff to State (B) for choosing (c) or (n)
s	Probability that, State B choose (n), given State A prior choice of (n)
q	Probability that, State B choose (c), given State A prior choice of (c)
State(A*i*) =	USA = a1 < a2 < a3 < a4
State (B*j*) =	IRAN = b1 < b2 < b3 < b4

Fig. 4.6 Credibility Model Definitions and Notations

Fig. 4.7 shows two states acting as a player within deterrence game in extensive form representing the cyber conflict. Normally, players assumed to be rational and always seeking the best strategy for maximizing their payoffs. In this game, players represent two nation-states in cyber conflict. State (A) assumed as challenger threatening to attack state (B), while (B) wants to deter the attacker within the cyber space via developing its credible cyber threat. The payoffs for State (A) and State (B), respectively, are noted as (B_i, B_j) and this payoff assumed in order:

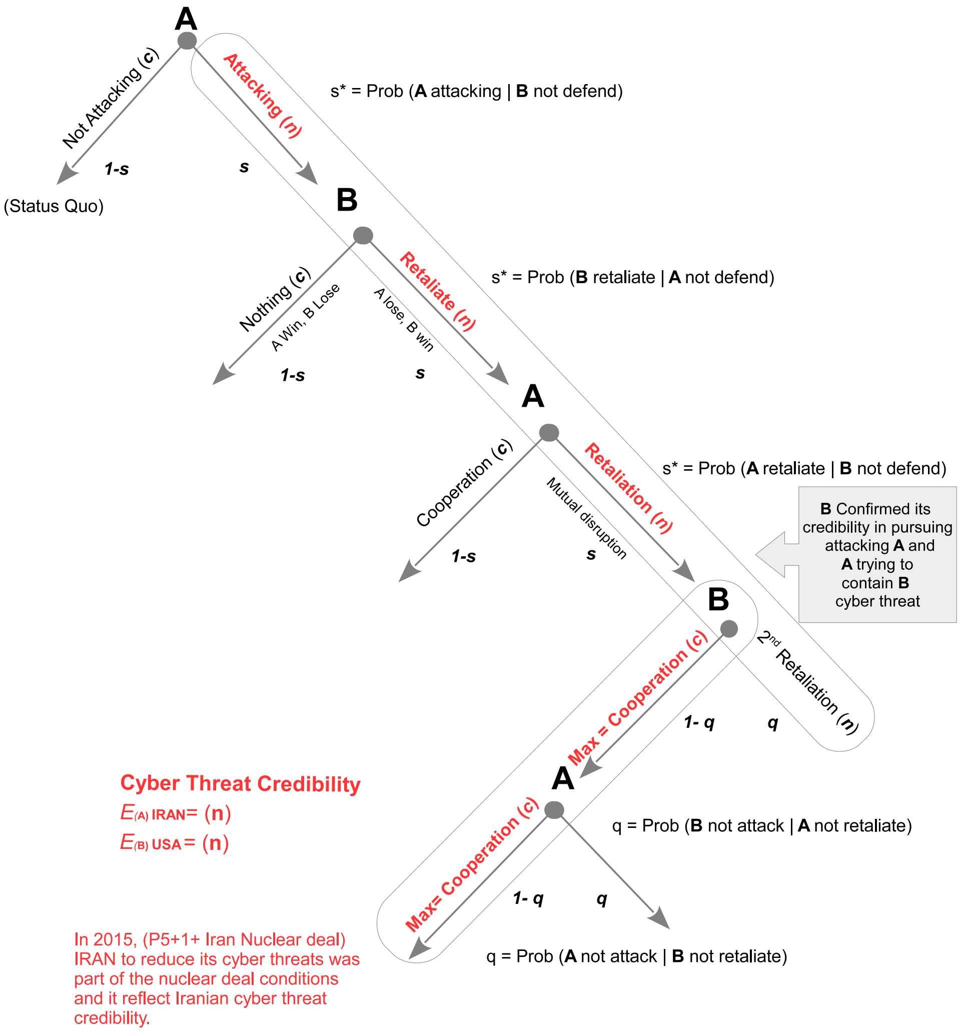

A
Not Attacking (c)
Attacking (n)
s* = Prob (A attacking | B not defend)
1-s
s
(Status Quo)
B
Nothing (c)
A Win, B Lose
Retaliate (n)
A lose, B win
s* = Prob (B retaliate | A not defend)
1-s
s
A
Cooperation (c)
Mutual disruption
Retaliation (n)
s* = Prob (A retaliate | B not defend)
1-s
s
B Confirmed its credibility in pursuing attacking A and A trying to contain B cyber threat
B
Max = Cooperation (c)
2nd Retaliation (n)
1- q
q
A
q = Prob (B not attack | A not retaliate)
Max= Cooperation (c)
1- q
q
q = Prob (A not attack | B not retaliate)
Cyber Threat Credibility
E(A) IRAN= (n)
E(B) USA= (n)
In 2015, (P5+1+ Iran Nuclear deal) IRAN to reduce its cyber threats was part of the nuclear deal conditions and it reflect Iranian cyber threat credibility.

Fig. 4.7 Credibility of Cyber Threats Model

- State $(A_i) = USA = a_1 < a_2 < a_3 < a_4$
- State $(B_j) = IRAN = b_1 < b_2 < b_3 < b_4$

  In addition to credibility of cyber threats model keys, each state will utilize c or n notification as a reflection to the strategy followed within one limited cyber interaction.

- Strategies **(c)** = Cooperate/Not attack or **(n)** = No cooperation/Attacking

  Both actors within the model changing between these two strategies and the expected outcome going to have notation going to be look like:

- E_A= Expected payoff to State (A) for choosing **(c)** or **(n)**
- E_B= Expected payoff to State (B) for choosing **(c)** or **(n)**

Then, analysis probability within the model reflecting various situations within the cyber conflict but in this model the analysis going to be only limited to scope within the **q** and **s** situation and it will be analysed intensively. Referring to the credibility influences, state should consider other situation that reflect:

- p = Probability that, State B choose **(c)**, given State A prior choice of (**n**)
- q = Probability that, State B choose **(c)**, given State A prior choice of (**c**)
- r = Probability that, State B choose **(n)**, given State A prior choice of (**c**)
- s = Probability that, State B choose **(n)**, given State A prior choice of (**n**)

Ideally, credibility in cyber space should not get developed for the mission of attacking and spreading cyber conflicts but it should target strengthening the strategies like deterrence and defense. State need to prioritize development of its credibility not for attacking but for the purpose of deterring cyber opponents. For deterring opponent threat should be effective for maintaining mutual deterrence between both actors A and B. It is the $(Status\ Quo)$ where each state strategy are limited not to attack or not to further any confrontation and this mutual strategy are strict to the outcomes of;

$$\text{Status Quo} = a_3 = b_3 = 0 \tag{4.3}$$

Who is to say this, states are confronting each other. Cyber attacks are ongoing and every state is spying on another state. Cyber attack begin with reconnaissance as a first phase where each state gather information about its targets and adversary vulnerabilities. During cyber reconnaissance the mutual payoff for both actors can be considered as (a_3, b_3) as both actors observe each other without any interaction of wining or loosing.

Cyber threat credibility and its effectiveness are directly related to the amount of damage that cyber attack can consequence. So, if any state ignores cyber threat effectiveness it will reflect to strength deterrent credibility by reducing the cost of the threat delivery (From Deterrent). This could happen because the attacker is not prepared enough to defend against deterrent threat or it has low prospectives about deterrent threat (Cyber Retaliatory) and that's where *(A) = n > c*. Threatener who move from Status Quo can occur under different circumstances like miscalculation or motivated by achieving superiority over its traditional adversary. When State (A) initiate its first cyber attack the expected payoff from selecting the strategy of ***n*** is:

$$E_A(n) = a_4 p + a_1(1-p) \tag{4.4}$$

State (A) by weighting the strategy of attacking ***n*** expectation was to gain superiority over its adversary. For that, US and Israel idea of attacking Iranian nuclear station and the expectation was the cyber attack may cause speedup the processing and will lead to a complete internal explosion or damage. Unfortunately, the damage was there but not as per expectation. There was a stop in operational procedures but after that everything resumed as it was before.

First game round between US and Iran or (A) and (B) in Fig. 4.7 show possibility of State (A) attacking (B) and succession of the cyber attack. In other hand, the expectation was that Iran is not an advanced country especially in cyber technologies. So, very sophisticated and complex cyber attack will not get traced or attributed by Iranian weak cyber capacity. In addition, they assumed that Iran was not capable to retaliate as it was not having any credible cyber threats compared to any other advanced state. For that the calculation about Iranian cyber threat is limited to a weak position and the assumption about cyber threat is:

$$b_3 > b_4 p + b_1(1-p) \tag{4.5}$$

Second node of the game Fig. 4.7 is to observe the consequences from attacked state and what is going to happen next. After period of time, Iran has retaliated although the retaliation was not immediate. It was after period of time. State (B) cyber retaliation has happened and it was massive in terms of cost and targets. Threat of retaliation from state (B) has been confirmed. The expected outcome from (B) retaliation is:

$$E_B(n) = b_4 p + b_1(1-p) \tag{4.6}$$

The retaliation in cyber attack from State (B) could be executed whether attribution completed or not. Due to possibility offered by cyber space vulnerabilities (opponent space) for executing cyber threat under different scenarios, Retaliatory threat for deterring cyber adversary (A) from selecting the strategy of repeating the attack strategy of n again, Cyber threat should be under the condition from (B) perspective:

$$a_3 > a_4 p + a_1(1-p) \tag{4.7}$$

The assumption here that (B) as a deterrent state with certainty should not stop threatening its adversaries as it begins utilizing cyber threat for its political conflicts agendas. In case miscalculation occurred and deterrence did not work for any reasons and (B) get attacked again by (A), It (B) to evaluate its threat effectiveness in deterring (A). The point here is what (B) need to do as another response to the failure of first attempt of credible threat is to review the efficiency of cyber threat to maximize the cost of damage (To the threatener) and to reduce the cost of threat delivery (To the Deterrent). This new approach will establish another possibility to raise the credibility of cyber threat (deterrent state) by Minimize the cost of delivery for the (B) and maximize the consequence of damage to the (A).

$$\text{- Maximize (Lose)} = (A_i)$$
$$\text{- Minimize (Cost)} = (B_j)$$

This approach of increasing the cyber threat credibility can be practiced by increasing the frequency of threat of attacks or by changing the value of targets. Critical infrastructure of any state is highly valuable cyber assets and the consequence of malfunctioning this infrastructure is uncountable. So, threat to retaliate or retaliation against threatener critical infrastructure will enforce to recalculate and reconsider the credibility of the deterrent state cyber threat credibility.

Assuming this is what happened in Iranian case, different cyber attacks attributed source from Iran, United state has begun to think rationally that pursuing confronting Iran has stimulate its strategy to developed its cyber capacity. Then Iran has become as a cyber threat source and has confirmed its retaliation and for optimizing USA strategic situation it is better to deal with it carefully and not to pursue the strategy of confrontation.

It is because cyber threat efficiency and its consequences have increased and there is no guarantee about next cyber attack and its consequence. In the model, state (A) has calculated the credibility of state (B) cyber threat and has realized it is credible enough to consequence an effect damage to cyber infrastructure and this could be a valid reason to deter (A) not to attack or at least to think carefully next time. For that, we can assume this what has happen in USA in confronting Iran, USA is more relying on cyber space and at the same time it is more vulnerable to a different kinds of cyber attacks. Moreover and from USA point of view, carrying on cyber confrontation will result in mutual disruption that every cyber attack certainly will end up. Ongoing process of cyber attacks followed by retaliation or threat of retaliation by (B) will not establish any solution between both states and due to vulnerability within USA cyber space, USA outcome will be ($E_A = Lose \geqslant Gain$).

In the case of state (A) preemptively attacks state (B) and state (B) does not show any response. It is clear that state (A) *Win* and State (B) *Lost* the cyber confrontation. This scenario could happen despite (B) pre-commitments to retaliate if (A) attacks. This scenario could occur in different scenario and one of these scenarios is that State (B) does not have any threat that can be utilized to accomplish the punishment of retaliation against (A). This is where threat credibility is making difference. When State hold credible threat, strength of its strategic situation in confronting its adversaries are totally different compared to a situation where state does not have any credible threat.

In referring to Iran, at the beginning it was not ready to retaliate against Stuxnet attack. But, Iran was provoked and after short period of time Iran has developed its cyber capacity as in Fig. 4.1. By the same logic, Iran was capable to develop its credibility in the cyber space and became a consider threat source for the cyber threats. Since USA was the the challenger in the game. USA has prioritized the choice of first move to attack Iran as state (B). After close attribution for the Stuxnet attack Iran got the message and has made what can be considered as cyber arm race in developing its cyber capacity. USA has assume that in case it has maximize its probability of attacking Iran $E_A = Maximize(p)$ and for sure Iran are not going to response due to lack of credibility. Preemptively attacking opponent in the cyber space will not prevent second retaliation due to cyber uniqueness but preparedness and maintain *Status Quo* could be better. For that, state need to assure developing its credibility within cyber space and not to use it preemptively due to high probability for Non- Credible state without cyber space to develop its cyber credibility within a short period of time and retaliate with massive attacks that will over weigh gain achieved by first attacker.

For a state aiming to develop its credibility in cyber space, It makes no sense for Iran as a state (B) to follow strategy of $Donothing$ if USA as a state (A) has attacks and attributed. For the cyber deterrence strategy to be effective, (B) should pre-committed to retaliate immediately if (A) attacks; thus, (A) is certain about mutual disruption if (A) attacks. Otherwise the dominant strategy by USA against Iran will continue as $attacking$.

4.3.3 Cyber Threats Credibility Through Multiple Stages

Credibility is basically believability and to let adversary keep in mind (believe in) cyber threat (cyber damage) that state is capable to cause, state should develop a level of reputation that is sufficiently enough to get believed by its adversaries. The problem with cyber attacks is that not all attacks reflect high cost or high impact to the state adversaries. In addition, state adversaries infrastructure have different perceptions about its value and link to the national security even if it is attacked with the same cyber attack. Actually, some of these attacks affect state critical infrastructure and consequence a huge disruption and big amount of loses. To let opponent to believe state cyber threat need an enough experience to believe in state credibility and its willingness and commitment to practice it.

One of the cyber space advantages is the possibility to cause repeated cyber attacks due to availability of vulnerability in each state cyber space. Repeated probability of causing damage from one state to its opponent will support (directly or indirectly) the credibility of cyber threat. So, If State A $Max(n) > (c)$ then attacking Stat B. State B with same logic can $Max(n) > (c)$ and then repeatedly State (A) can execute repetitively strategy of attacking B.

Moreover, it could be aligned with gradual retaliation strategy. The gradual cyber retaliation can start with a purpose of sending a signal for the opponent and to assure commitment for retaliation and this is what has happened with Iran-USA case. Iran has responded to different targets figure 4.1 and strategically this target was either directly belong to USA infrastructure or belong to some of USA alliances in the region like Saudi Arabia or Israel.

Iran has confirmed its commitment to retaliate $Maximize = Gain > Lose$ via repeated cyber retaliation. It was not only one attack and one target, but it was different targets with different kind of cyber attacks. After first round of attacks, Iran adversaries began to realize that Iran now become serious to respond and now has developed its cyber offensive capacity and it is serious to use it to cause harm over its adversaries cyber infrastructure and willing to increase the level of damage if needed.

Referring back to the beginning of the game tree Fig. 4.9, assumption here has begun with Iran as state that does not expect any kind of cyber attack which might possibly target its nuclear infrastructure. Cyber vulnerability was there in nuclear plant machines but there was lack of discovering or mitigating this particular vulnerability. USA and its regional alliance Israel to be assumed standing behind of Stuxnet operation has gathered information about the vulnerability and found it as a golden opportunity for effecting Iranian nuclear infrastructure via speeding up the production or causing different kind of damage and when this mission succeed it is considered as gain from USA prospective $E_A = Gain > Lose$. After deep investigation, it can be clearly observed that the attack has succeeded in reducing the operation. Reversing this particular cyber attack by national and international association, Iran has been shocked and at the same-time stimulated to act seriously regarding this newly emerged threat and prepare for future cyber attack and this is where state credibility is developed. At that point, there was no guarantee Iran will retaliate or will repeat the same scenario and utilize gained experience from the attack against its opponent (USA its regional alliances). But, Iran has retaliate and what has happened was massive and has raise Iran payoff $E_B = Gain > Lose$ and this outcome what has established its cyber credibility. Iran retaliation against USA and its regional alliances is supporting Iran cyber threat credibility. repeated cyber retaliation is a repeated signal to Iran cyber adversaries about its cyber threat credibility and its willingness to pursue cyber threat.

One of the cyber uniqueness is the complexity and possibility of deception in hiding cyber evidences. Cyber attack need sometime to investigate or reverse the attack to identify the source of attack. Attacker might assume to attack and clean the evidence, but this is not always true in all cases especially if the attack needs plenty of logistics like stuxnet, it was clear that a state as an actor was behind this attack because it is difficult for non-stat actor to arrange the logistics for developing and testing this particular attack. For that, the game between these two states was not the same before and after the Stuxnet attack as shown in Fig. 4.8.

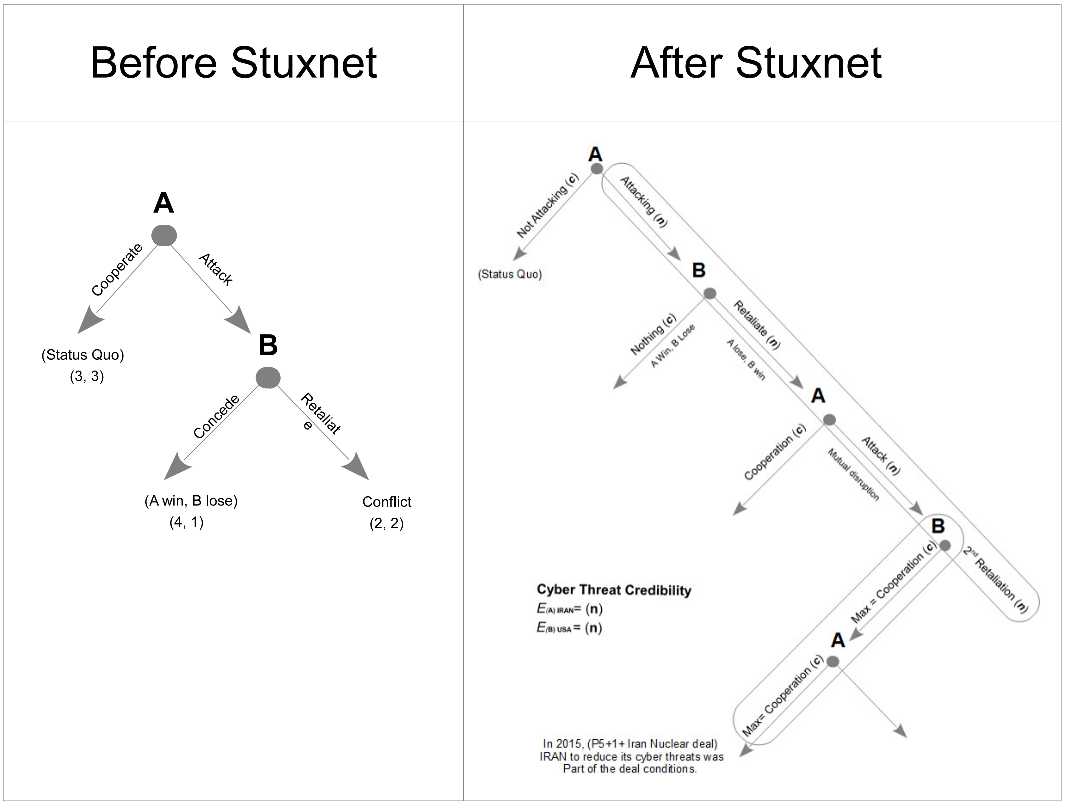


Fig. 4.8 Before and After Stuxnet

Another uniqueness of the cyber space, is the development of credibility that can be shaped via re-producing the same cyber threat that state (B) get attacked by. It can utilize it for retaliation and threatening its adversaries. Cyber compared to nuclear, logistics for developing cyber threat are much easier than developing nuclear threat. So, it is also easier to keep threatening for the purpose of strengthening state credibility. Yes, retaliation might not be possibly to be automated but it can be done sometime after depending on state strategist and decision maker to select time and target. Cyber threat gives state variety in developing its credibility and it gives variety in the responses approaches under different context. It could be for sending clear signal and it could be gradual and flexible response. Moreover, it could be one massive attack. This justification is lifted to the sate strategist to estimate what could be enough to force opponent cooperation behavior.

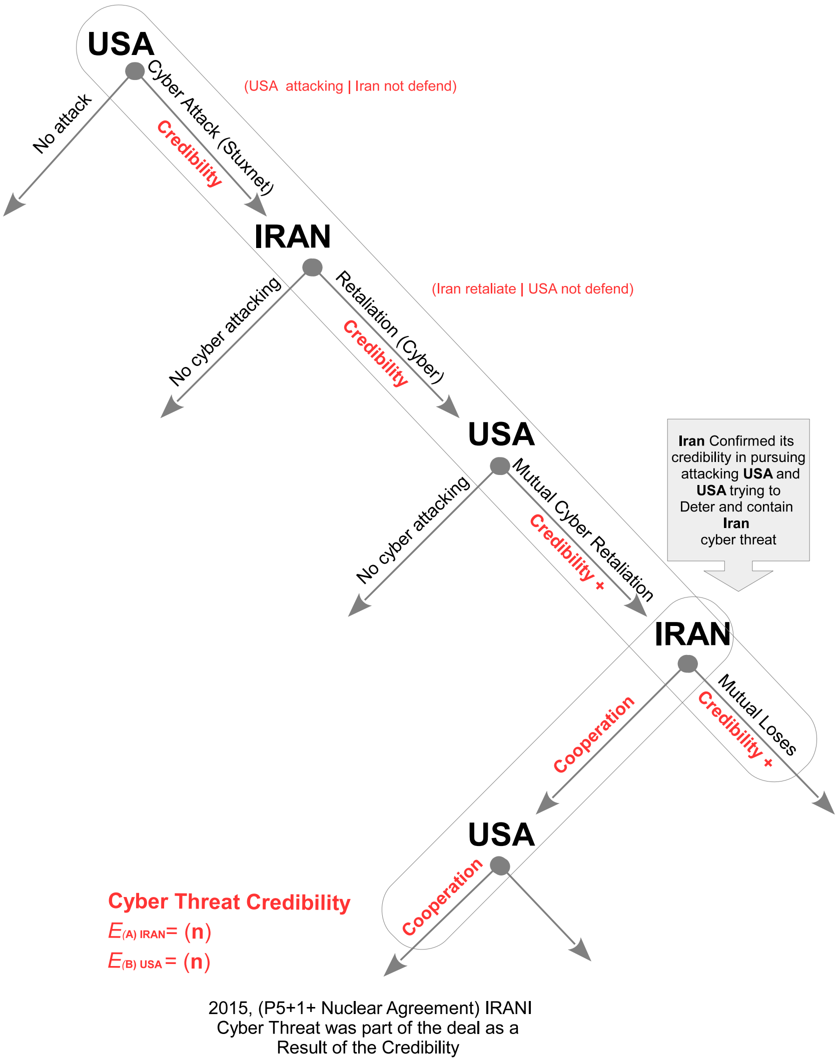

USA
No attack
Cyber Attack (Stuxnet)
Credibility
(USA attacking | Iran not defend)
IRAN
No cyber attacking
Retaliation (Cyber)
Credibility
(Iran retaliate | USA not defend)
USA
No cyber attacking
Mutual Cyber Retaliation
Credibility +
Iran Confirmed its credibility in pursuing attacking USA and USA trying to Deter and contain Iran cyber threat
IRAN
Cooperation
Mutual Loses
Credibility +
USA
Cooperation
Cyber Threat Credibility
E(A) IRAN= (n)
E(B) USA = (n)
2015, (P5+1+ Nuclear Agreement) IRANI Cyber Threat was part of the deal as a Result of the Credibility

Fig. 4.9 Iran vs USA Cyber threat Credibility

At this point, state strategist need a careful consideration of mutual vulnerabilities that each state have in cyber infrastructures which might spark cyber escalation due to miscalculation. Game tree below is attempting to analyze the cyber confrontation and each state decision. This game shed the light over the mutual decision between Iran and USA to understand how credibility of cyber threat has been stimulated to grow within the USA (A) and Iran (B) geopolitical conflict. Mainly, its present how Iran (B) has develop its cyber credibility stimulated by USA confrontation that sparkled by Stuxnet cyber. Iran credibility has been developed and formulated by state interest, commitment to interact. This growth of Iran cyber credibility and reputation is not yet confirmed in deterring state cyber adversaries like USA or its alliances.

The figure present the sequence of interaction between case study actors (USA-IRAN) and within this interaction the particular movement that add value to state (B) as Iran credibility. Internationally, states in cyber space are vulnerable to the cyber attacks and this vulnerabilities like a mutual situation. In other hand, cyber threat of retaliation effective to cause damage to the other state despite the debate about the disruption or damage that could result from cyber attack which is completely unwanted by the both states.

The assumption here is that both states can possibly interact via cyber attacks that might start as a simple attack then get worse to unaccepted level by both opponent at a certain degree where opponent will attempt to find alternative approach within the conflict. The scenario here is reflecting the time line (Fig. 4.1) and Credibility of cyber threat model (Fig. 4.7) model and the analysis conducted from the different triangles.

4.3.4 Cheap Fighting and Cyber Threats Credibility

Despite the technological sanction from western countries against Iran (Fig. 4.1), Iran was capable to develop its cyber threats for initiating different operations that can be considered as Iranian cyber retaliatory attacks. Developing conventional threats like strike fighter need plenty of resources and efforts for the testing compared to the cyber threat. For that, cyber threat is much possible and cheaper to develop it and utilize it for causing different kinds of loses. It can be used repeatedly and this give cyber threat advantage in manipulating with State opponent as it is not directly affect human life and can cause damage.

In the real world, states developing its cyber capacity for different missions and one of the newly addition to the civil missions is supporting state in maximizing it payoffs in Geo-political conflicts. Iran after Stuxnet attack has been shocked how this unpredictable cyber attack occurred and then Iran has speed up its cyber arm race.

Looking at the outcomes in the Fig. 4.10, it is simplify the Sequence of interaction between Iran and US. At the **T** payoff Iran has confirm its commitment to response to the sources of threat. At this outcome, someone could argue that the response was not against direct governmental organization. Yes, but it is part of the state opponent infrastructures and the retaliation send a credible message that “I am as Iran State and I am willing to retaliate and here is the proof”.

The message beyond these particular retaliations was to confirm willingness t maximize payoff and build up Iranian cyber threat credibility. It is to prove the capacity to threat even if the attacker was not USA Banks or US alliance like Saudi Petrol Company (Aramco), but this retaliatory strategy against this kind of targets for Iran will confirm its commitment and credibility despite the target was not governmental bodies. In addition, repeating cyber threat and it is one of the cyber space advantages for states. Cyber threat can be repeated against different targets within adversary critical infrastructure and utilizing different vulnerabilities because at the end this will cause an extra pressure to the state opponent to find a solution even if the attacked target was not a government.

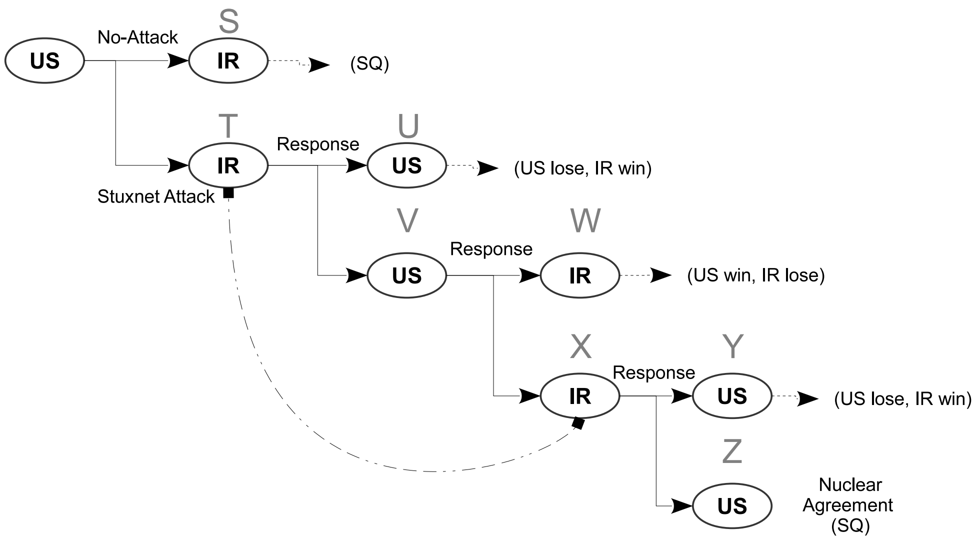


Fig. 4.10 Iran Cyber Credibility Multi stages Analysis Tree

Iran after Stuxnet has continuously pursued threatening different institutes and attacking US Banks. Fig. 4.10 listing both states (USA- Iran) payoff within the game model and by following the payoff of Iran particularly will understand the sequential payoff of attacking has assisted Iran in developing its cyber credibility. Iran has continuously committed to *Maximize* strategy of attacking and this Iranian strategic situation reflecting :

$$\text{Maximize}(E_B)via = b_4 > b_1 \tag{4.8}$$

For that, Iran expected payoff by maximizing strategy of retaliation within the conflict with USA will be more of:

$$E_B = b_4q + a_1(1-q) \tag{4.9}$$

Since state is not interested in cooperation or not in the position to justify its success or failure from the particular conflict, it is expected to pursue in challenging its adversaries and this what has happened with our case study after sequential cyber interaction. At this point, we have seen how Iran has retaliated sequentially against USA and its alliances. Then strategically Iran has became known as a credible state in the cyber space. The assumption within the model has changed to consider Iran as a credible state confronting USA as another Credible state in the cyber space. So, the cyber confrontation between USA and Iran can be spliced to two phases:

- First phase: State (A) = USA as a credible state within the cyber space in confrontation with non credible state (B) which reflecting to Iran. In this scenario, USA best strategy in challenging Iran is to Maximize strategy of Attacking $E_A = (n) \geqslant (c)$. This strategy will guarantee USA ($Win \geqslant Lose$) against Iran.

  Conversely,

- Second Phase: State (B) = Iran as a credible state in the cyber in confrontation with USA (A) as another credible state. This confrontation can be considered as a response or another correlated strategy to the previous strategy made by USA via Maximizing strategy of attacking $E_A = (n) \geqslant (c)$. At this phase, Iran situation changed from non-credible to a credible state and USA dominant strategy of maximizing the attack payoff will not be the same as before. Iran by achieving credibility in the cyber space can Maximize it strategy to keep attacking USA $E_B = (n) \geqslant (c)$ and the maximization in strategy of attacking confirm Iran credibility in cyber space and stimulate USA strategy to have second thought before attacking Iran.

At this point, I assume that USA and President Obama believe that pursuing confronting Iran will not maximize its payoff and it will cause more of escalation status within the conflict. It is clear that USA are more dependent on cyber space in operating its infrastructure and this will confirm its vulnerability within the cyber. So, in a rational comparison when USA confronting credible state like Iran it should be more logical to select the chicken position in attempt to maximize its payoff within the cyber space. Developing some sort of cooperation with Iran (As cyber threat) might wind down the cyber and stimulate Iran to change its strategy from $E_B = (n) > (c)$ to the strategy that have more of cooperation $E_B = (n) < (c)$. The challenge is what state will do in case of red lines are crossed by its cyber opponent. Repeated outcomes are shown in Table 4.1.

Outcome	**Description**	**Iran Ordinal Payoff**	**USA Ordinal Payoff**
S	Status Quo in Cyber Space	b_3	a_3
T	US Attack Iran(Stuxnet)	b_1	a_4
U	Iran developed nd Retaliate	b_4	a_2
V	US - Response	b_4	a_2
W	US Continue (Sanctions, etc)	b_2	a_4
X	US - Response	b_2	a_4
Y	Iran keep Attacking	b_4	a_2
Z	Iran Credible/Containment	b_3	a_3

Table 4.1 Conflict Outcomes and Threat Credibility in Multi stages

Collective review about Iranian payoff with the above table will assist confirming Iran capacity in maximizing its payoff in different cyber interaction and strengthening its cyber credibility. From strategic point of view, the capacity in succeeding cyber threat in a repetitive approach. This will confirm Iran as a credible cyber state despite all kinds of general economical and political sanctions and specific sanction to prevent Iranian hands from western advance cyber security technologies.

4.3.5 Credibility of Cyber Threat and Communication

In any given situation related to the cyber conflicts and for the benefit of strengthening state cyber threat credibility, politicians or state decision maker should clearly communicate about what are they willing or not willing to do regarding cyber threats sources. This declaration will signal state opponent about its strategic intention and this signal should be strong enough.

Even in the case state still not having complete information about the attacker, it can pretend that it is having information but it is not the time to disclosure it completely. This tactics will aid in strengthening its strategic position and should keep signaling that it is going to punish to a level to assure losing more than any expected gain. At this stage, state (deterrent) strategy of retaliation State $E_B = (n) \geqslant (c)$ are dominant. Dominant strategy of threat by retaliation is correlated directly in strengthening state credibility and strategically reflecting:

$$Maximize.Prob(Retaliation) = GoodThreatCredibility = GoodCyberDeterrence \quad (4.10)$$

Clear communication will assure state commitment to its adversary and at the same time state must avoid signaling adversaries with any weak or empty threat. This mean, State need to benefit from developing cyber vulnerabilities DBs that can be called upon need for the purpose of assuring success of threat credibility.

State reputation get developed over history as well as sustainable time-line within international arena. It could be one case that help developing the credibility like what has happened with our case study Iran vis-to-vis USA. After stuxnet Iran were capability to develop its cyber capacity for the purpose to retaliate against USA as well as its regional alliances.

Referring to Table 4.1, Observing the outcomes of Iran after sequential cyber retaliation which is considered as retaliation reflecting stuxnet attack. At the same time, these sequential cyber retaliatory attacks develop Iran cyber threat credibility and it has stimulated Iran adversaries to calculate the next attack carefully due to fear from its retaliation. It does not mean Iran adversaries do not have cyber capacity but it means that Iran retaliation is unpredictable and the consequence of continuously challenging Iran will lead to escalate the confrontation rather than wind it down.

State alliances as well as state adversaries observe state commitment to what has been announced and then the believe on state credibility is believed or not. Iran vis to vis USA case, Iran has confirmed its commitment of retaliation and effecting USA or its regional alliance with loses either financial or operational in different cases listed in Fig. 4.1. Iran has confirmed its strategy of retaliation within cyber space via maximizing attacking more that any possibility of cooperation in the case get attacked. Iran practise was via the approach of Maximizing $E_B = (n) \geqslant (c)$.

For that, state communication should get the best possible level of commitment with practice for the purpose of optimizing state credibility within cyber space. Iran has surely gained the credibility.

In opposite, any state signaling its adversaries with weak or non credible communication will not add any value to its credibility. Weak communication will demolish state credibility more than any expected construction. State should assure its capacity and credibility aligned with communication reflecting its cyber threat credibility. For that, weak communication reflecting low profile of retaliation against cyber attacks will encourage state adversaries to keep Maximizing the strategy of attacking $E_A = (n) \geqslant (c)$ state. In this case, if Iran did not retaliate and not respond against USA and its regional alliances with strength, the adversaries will keep attacking and causing different level of possible damage.

Credible communication could strength and weakening cyber deterrence strategy and then it is to the State adversary to decide next step either to pursue the *Attacking* strategy or drive to *Cooperation* due to $E_A = Lose \geqslant Gain$. Correlation between weak communication and bade non credible threat of retaliation can be summarized in:

$$Minimize.Prob(Retaliation) = BadCyberCredibility = BadCyberDeterrence \qquad (4.11)$$

Minimizing the probability can be due to the lack of resources but there are other strategies that can be utilized like strategy of bluffing and its should be strong enough to get believed by state Adversary. Otherwise, state will fall in the same trap of weak communication and lose its credibility.

Iran in the outcomes T and X has maximized its payoff and the same time has maximized its probability of retaliation to the most possible value. For state (B) as deterrent this maximization will feed credibility record among other states. In both T and X, Iran outcome was (b_4). This list of payoff in Table 4.1 clarify how Iran has successfully develop its cyber threat credibility over sequential cyber retaliation targeting USA strategical business and its alliances.

In addition, at the Z outcome within Fig. 4.10 and after different rounds of cyber challenges between USA and Iran, attempt here was to find out a better outcome from the growing cyber confrontation between these two states. Iran has committed to its threat of retaliation and at the same time USA has not stopped challenging Iranian system with different economical sanctions. Then, 2015 nuclear agreement has created some sort of raised expectation about probability of cooperation or reduction in this particular conflict.

Nuclear agreement was signed by USA and other western countries and the signal beyond this agreement is that "If you are willing to cooperate -In the geopolitical conflicts + cyber conflict-, I will certainty cooperate, But if you don't respond with Cooperation I will retaliate without hesitant but it will be effective will assure to reduce or Minimize any expected gain $E_A = Gain \leqslant Lose$.

4.4 Strategies and Lessons for Credibility

Primary objective of this research is to help states in developing cyber deterrence policy to preventively protect state from unpredictable cyber attacks. For a successful cyber deterrence, it is important for a state to develop its credibility in cyber space. Credibility of cyber threat as punishment need to be understood and then to be enhanced for the purpose of succession of cyber deterrence strategy. The strategic approach to achieve national cyber deterrence strategy is possible via two directions: (1) Strengthening the cyber defense (denial) to assure failure of any attempts of cyber-attack or to make it highly costly compared to the gain expected. (2) Strengthening the cyber offensive which will give state superiority over other state in term of threat of retaliation within the cyber space.

But, there are more details between the lines requiring deeper understanding especially the approach for the state to develop its credibility. It needs to have credible threat that is effective, achievable and it is believed by state opponent. Despite this assumptions, in real world nobody really knows exactly how advanced is the state in the cyber space as the cyber domain is a complex domain with multi layer of connectivity. Superiority in cyber could be measured form different perspectives and from different triangles. State can be superior in term of its cyber offensive capacity but not in defensive field and this could be because of the various reasons for technologies failure or lack of resources.

Credibility (believability) of Iranian Cyber Threat was enough to encourage USA to look at a new approach to for deterring Iranian cyber threat or at least to practice semi-containment. In other hand, USA cyber threat credibility was believed enough by Iran from experience and it was the reason to motivate or drive to get closer to cooperate with US during president Obama administration. It was like a containment strategy by USA as a failure of US deterrence stopping Iranian nuclear program. So, it looks like both actors (US-Iran) believe that each other is credible enough to effect its opponent cybrally and at the same time both are weak in matter of cyber vulnerabilities.

Referring to the model analysis and literature, the research within this chapter ended up with number of conclusions that state should consider developing cyber credibility. Within model discussion and the analysis conducted it has shed the lights over essential strategies that state should be in practice for developing its credibility in the cyber space and without these strategies the assumption of developing cyber deterrence strategy will stand over a weak position. This section attempt to totalize the lessons learned from the analysis and prescribe different lessons for the state national strategist for the purpose of supporting national cyber deterrence strategy. Credibility of cyber threat is the corner stone for the sate cyber deterrence policy and for achieving the deterrence in the cyber space, strategist need to know what is the fundamental requirements for developing credibility from top to bottom.

4.4.1 Credibility of Cyber Threat Model General Lessons:

- Credibility of cyber threat is incomparable with nuclear threat, because cyber threat is more provocative when utilizing it against another state. It will stimulate cyber arm race to develop cyber credibility for the purpose of retaliation. In addition, developing cyber credibility is possible and more flexible compared to nuclear which required plenty of logistics.

- Credibility in cyber space can be mutually developed among states due to availability of resources for helping developing cyber threats.

- States need to consider repeated cyber threat model against its adversaries as in cyber states credibility is established by repeated rounds of threatening

- Detection of state cyber space known and unknown and maintain observability over the cyber space up to highest level for measuring source of threat and categorizing sources of threats. Then state need to communicate to the highest expected sources about the its findings. This practice will add to the record of state interest to deal with these threats seriously.

- Communication and Signaling and Sometime bluffing: State in deterring cyber adversaries should threat to retaliate in a sequential approach to assure its credibility expected from its cyber threat of retaliation

- State need to consider or implement strategies like Defense-in-depth for optimizing capacity of cyber threat detection as the Cyber Security Technologies rely on limited information about the known threat and the unknown threat also can be tracked via its behave within the networks and infrastructure. Despite these advances, still there is a wide range of threats can succeed in attacking different state critical infrastructure.

- Coupling cyber defense strategies and cyber readiness for retaliation (Cyber offense) and declare these readiness to assure credibility for cyber opponent.

- State need to develop a national strategy for Integrating threat management systems together and to benefit from new approaches like Machines learning and its applications in analyzing sources of threats. This will assist states in prioritizing cyber threats for the purpose of deterring these threats.

- Cyber Offense and Retaliation: State need to develop its capacity of initiating immediate cyber offensive attack especially in the case the attribution of threat source was clear and a need to initiate such like hack-back procedure against threat source

- Cyber Defense and Protection: State should evaluate its cyber defense capacity in defending against different type of cyber threats and to conduct ongoing cyber assessment to assure up to date defensive capacity.

- Detection and Attribution: Within cyber defense State need to evaluate its capacity in detecting cyber threat targeting its critical infrastructure and develop its capacity in attributing the source of cyber threat to the level of knowing who is standing behind the attack either State or non-state actors. This capacity will drive State decision to threat credibly the exact or at least semi-exact source of threat.

- Vulnerability DB's: Cyber attacks is based on vulnerabilities that are exist within state opponent and it can be utilized by the State to threat its adversaries. For that, state recommended to develop its vulnerabilities database that can be utilized for threatening cyber opponents. Without having these vulnerabilities State will not be able to success any Cyber threat. There is a different type of cyber threat that can be utilize either to get it from reconnaissance operations that state can conduct it.

- Repeated cyber threat: State need to consider its capability to threat its cyber opponent with a repeated cyber threat and it should be credible enough. The repeated threat can be via targeting different targets or same targets with different types of cyber attacks/threats.

- Different types of target: For strengthening credibility of cyber threat state needs to know its opponent cyber infrastructure. The clear understanding of adversary infrastructure will help to signal clear message that the state know where to hurt its opponent either to select soft targets like civil infrastructure which is known as (counter value). It is linked to civil services or to select the hard target that is known as critical infrastructure to the state especially those linked to the national security. These targets are called (counter force) which cause a real force to the opponents to stimulate cooperation.
- Commitment and Willingness to use the cyber threat: State need to practise its commitment via practical exercises for signaling its adversaries about its readiness in retaliation or any confrontation.

4.4.2 Credibility and States Strategies:

- Strategically, credibility of cyber threat for the purpose of deterring state cyber adversaries can function under the strategies that IRAN should act upon. For the state (B) Iran stand point to deter State (B) -USA- from conducting any further cyber attacks against Iranian cyber infrastructures it should act:

  1. Minimize (p) : Convince (A) USA that attacking Iran will end up with $E_A = Lose > Gain$ and cost of attack is more than expected gain. So, minimize any success of USA cyber attack will deter USA attacking Iran.
  2. Maximize (r) : State (B) Iran should Keep threatening USA by retaliation for the aim of not to give USA chance to preempt within cyber space.
  3. Maximize (s) : Iran to increase the cost of success any cyber attack from (A) -USA- stand point which will increase $E_A = Lose > Gain$.

  At the same time, USA (A) position to assure its credibility in the cyber space, it should assure its strategies going under strict conditions. For a strategic and credible responses, USA should keep Iranian cyber threat down via:

  1. Minimize (r) : USA to minimize the probability of cooperation with Iran (B) and to assure $E_B = Lose > Gain$
  2. Maximize (p) : State (A) Keep maximizing the probability of non cooperation despite the attribution of cyber attacks sources from USA.

3. Maximize (s) : It is the worst strategic situation between (A) and (B) where USA keep challenging Iran within cyber space expecting the assurance of $E_B = Lose > Gain$ strategy will enforce Iran to wind down and give up.

A deep understanding of the strategies that each state need to have for developing credibility of its cyber threats will clearly assist in gaining the respect from state adversaries.

Chapter 5

Escalation for Cyber Deterrence

This chapter discusses the nature of escalation in cyber space in case credible cyber threat -as a threat of punishment- fail in deterring state cyber adversaries. It analyses the relevance of cyber escalation to deterrence assumptions and strategies. The chapter further investigates what is expected to occur in case deterrence failed to prevent state from unwanted cyber confrontations. The chapter begins by discussing escalation concepts and its definitions in the conventional strategic studies and more specifically its relation to the deterrence.

A selected case study will be presented as motivational case study that stimulates the argument of the chapter. Selected case will help to generate a deep understanding about the nature of escalation in cyber space and what state can expect regarding cyber conflicts in real life context. The observations generated from different resources will help examining assumptions raised positively or even negatively.

Analytically model has been developed to analyze the nature of escalation within cyber space between two adversaries. The model has considered different factors stimulating escalation in cyber space. The analysis within the model will help to explore critical situations. One of these situations is state approach regarding escalation with credible or incredible cyber adversaries. In addition, the model aims to explore limitation of escalation in cyber and state policy for conflicts reductions. Moreover, model will shed the lights over state consideration before furthering any escalation. Chapter has concluded with a section that discuss strategies and different learned lessons that state can follow before selecting any cyber escalation. These strategies and lessons will assist states to understand the fundamental requirements for escalation in cyber space and draw the lines for states to develop or optimize its cyber deterrence policy withing escalation ladder to develop cyber de-escalation.

5.1 Escalation Concept

Escalation as a concept has several meanings within the context of international conflicts [176]. Theorist like to define it as a process by which conflicts growing in severity over the time [177]. This definition reflect the conflict between individuals, groups or even between state-state conflicts. Deterrence strategies could not sustain longer and for many reasons deterrence could not work for the governments that are not investing enough to maintain effective deterrence.

The conventional conflicts and the escalation occur between state-state, strategist in both sides of confrontation has different tactics to utilize and sometimes they call it under the rules of engagement as they expect to attain the conflict by escalating the confrontation with the adversary [178]. This can work in case the first state succeed in controlling its opponent reaction for a period of time that allow the state strategist for developing new trap or pursue the opponent. Interaction between conflict actors need careful observation for justifying direction of conflict and understanding differences between deterrence and escalation. State strategist need to understand stages of conflict and at what stage the conflict is current [179].

Deterrence strategy is responsible in preventing confrontation and maintain peace between actors but when conflict conditions are changed and further intensity observed growing up between adversaries, at the point when conflict move from the deterrence (Status Quo) to an escalation (Intensity increased), this movement can be claimed as a failure in deterrence and each actor is not willing to act cooperatively with the opponent. During the deterrence there are mini-interactions between adversaries but they are limited and might be only bluffing. The challenge is when tangible escalation begins it is a painful decision for both state to decide either to escalate and fight or to cooperate and surrender. State decision reflects the power of state and how long is the crises is expected to sustain [180].

This research is about deterring cyber threats and in the case of two credible states are confronting each other and non of each state is willing to cooperate, escalation is highly nominated to begin withing the cyber conflict. The differences in cyber compared to other conventional conflicts is that cyber attack does not target human life directly. First, state needs to decide either to go for full scale of cyber confrontation or just limit cyber conflict escalation to limited cyber attacks. Second in cyber, State in cyber need to set clear objectives for the decision of cyber escalation and de-escalation rather randomize the responses. Another important issue in cyber is that state need to consider that cyber space is a shared space before burning the bridges [181].

In this chapter, the aim is to analyze escalation process in cyber space in case of cyber deterrence strategy has not successfully worked. Plus, credible cyber threat has not clearly succeeded in deterring cyber threatener. Before moving to the next discussion, I should specify the concept of cyber escalation process and from the earlier mentioned definitions and from my point of view, the simplest and easiest definition to describe cyber conflict escalation is when the intensity of cyber attacks increase. This increase reflects frequency of attacks, consequence resulted, value of the attacked targets. Cyber conflicts between states have grown and are going to be more in term of frequency, intense and severity. Escalation in the conventional conflicts has been given a plenty of thinking while in this chapter the attempt is to understand the nature of cyber conflict escalation and to give inside thoughts that help optimizing cyber deterrence as well as managing cyber crises.

Nevertheless, the reasons behind selecting escalation strategy is that the repetition of cyber attacks can be arguably considered as a process of escalation. It is because both opponents in the same conflict are investing to add more threat expecting to deter the opponent while attacked state consider it as retaliatory and respond with another retaliatory attack. Yes, first cyber attack can be a DDoS attack targeting view and limited institute, but the retaliatory attack maybe more sever and its mission as a threat for a purpose of deterring threatener. At this point, no one would believe that first attacker would accept to hold its cyber threat and it is highly expected to pursue threatening. Cyber conflict escalation is a gradual regression from an acceptable level of confrontation to an unacceptable stages. Each stage of cyber escalation has its own characteristics in term of lose and damage.

Escalation and International Relations

State – state cyber conflicts are part of the international relations and this domain of studies is very deep complex field of studies. A wider view about challenges reflecting cyber conflicts added to the complexity of international relation will give hints how critical is the cyber conflicts as well as giving the solutions. Moreover, integration between states-states cyber space adding another dimension to the cyber conflicts escalation as both states need to exchange business rather than exchange cyber bombs. Cyber space integration is different compared to traditional conflict domains (land, sea, air) and this differences reflect the nature of confrontation [182].

Traditional confrontation in conventional conflicts occurs via limited weapons that gives deterrent limited scope to develop threat that denial these (Conventional) threats and if defender succeed in developing these defensive threats, attacker will get deterred due to unavoidable loses aligned with losing any expected opportunity of partial winning within the same conflict [183]. So, understanding the usefulness of escalation or de-escalation in deterring cyber conflict compared to another conventional conflicts is one of the research objectives. This investigation will help figuring criteria that shape selection of both escalation or de-escalation strategy and it dependencies for the benefit of cyber deterrence strategy.

However, sometimes incorrectly cyber threats are described as a threat that doesn't cause any sort of escalation between state-state cyber conflicts and it is only limited incidents. But, we need a holistic view about the context of cyber-attacks and the motivators for state to initiate attacks against its opponents. Cyber attack happens with motives an state-state cyber attacks under political motivations. For that, it could be part of a total conflict and cyber attacks utilized for an escalator mission.

Cyber threats are not limited to attacking, hacking systems but it can be utilized for plenty of operations that affect state national security and this threat has appear in US election and how cyber space is utilized for effecting the national security of USA democracy. Cyber space gives threatener flexibility to shape the threat for serving nature of conflicts between both states. Conventional conflicts use traditional weapons for affecting opponent in a way of causing damage that force to cooperate with threatener while cyber give each adversary to play the same game for causing same damage for many times. For that, a historical review over different cyber-attacks can confirm that the assumption of cyber escalation is possible to occur and it is in practice within state-state conflicts. Yes, it is different in term of cost of loses and consequence but it is the same in term of loses and damage.

Additionally, cyber incidents attributed source from another state no matter whether this state is credible or not but there is no law enforcement from one state against another state except the international law enforcement and it is very long journey till issues gets solved. Moreover, cyber space is a border less domain as well as the nature of complexity in connectivity add a highly probably to stimulating cyber escalation between adversaries. The resources that states can allocate for the purpose of escalating cyber conflict are more than what non-state actor can offer. Aligned with the cost of developing cyber threats and utilizing it for escalating cyber confrontation is cheaper than other conventional weapons. So, states involvement in cyber confrontation add an extra strength to the strength of escalation strategy aligned with cyber uniqueness that allow this escalation to occur on a high frequency.

Developing norms or what some theorist call it as "accepted standards of behavior" in the international arena (State-State) and call all states to join and agree with, will help to avert cyber crises from mis-perception in cyber conflict, missing the attribution or any unwanted mistakes. Moreover, it will help to develop mutual cooperation in term of investigation and build up the confidence. In avoiding any sort of escalation all states should sign for these norms and on top of them USA, for assuring mutual trust no exception from joining this norms. Usually, norms help to shape state behavior in the domain and it will function as governor for state not to exceed the acceptable level of cyber practice and what has been agreed with [184]. Norms can be helpful even during the conflicts escalation by adding more enforcement over states to limit the conflicts within certain targets like military infrastructure and not to target the civilian's cyber infrastructures.

Escalation Management and Cyber Deterrence

Deterrence by threat of retaliation in cyber space is very critical as it could stimulate cyber escalation spectrum easily. So, in case of cyber escalation starts both adversaries would prefer to get low level of cyber disruptions and destruction within actor infrastructure. This preferences are shared between both opponents and then it will depend on each state and its preferences to pursue the escalation or hold. Escalation is not one step conflict and state need to justify its objectives rather than keep escalating with no valid and rational reasons.

Deterrence strategy in cyber space need credible threat and the credible threat need to confirm its capability to affect its opponent severely (believability) but the risk here when threat of retaliation get change its status from – threatening to retaliation - to – Attacking and Escalation. At this point, state need a careful calculation to limit escalation within the cyber conflict for the benefit of cyber deterrence rather than pursuing uncalculating escalation.

In this situation, strategy of "tit-for-tat" can add explain explain the managing of escalation between cyber adversaries [185]. Logically, the idea here for State (B) to deter State (A) give a clear commitment that "if you attack my (Cyber) critical infrastructure, then you will be regretful for exceeding the lines". These lines can be defined from state perspective as critical infrastructure and if cyber adversary exceed the red lines (B's Critical Infrastructure) and attacked any of these infrastructure it will not be fit the conditions that state (B) declare and the ball will be under (B) hand to act upon. Cyber red lines (B's critical Infrastructure) must be mutually understood to prevent each state not to exceed acceptable level of risk. Tit for tat approach need a careful responses and believe of immediate response at the speed of the light is not easy to work in cyber due to cyber complexity and challenges related to attribution and technologies.

By the same logic, when escalation exceed the cyber deterrence strategy to join another conflicts. States willingness to escalate from cyber-cyber to cyber-conventional or rational calculation should reinforce to limit cyber conflicts within cyber rather than involve other threats. Analyzing conflict escalation ladder (wining or losing) with cyber context is a bit complex as the cyber can be utilized for different political conflicts. States in deterring its opponents need to consider the scenario of managing the escalation ladder and what steps can fit in managing the escalation. Steps like reducing the ambiguity about state intentions and raise the practice of cooperation with other states [186].

5.2 Motivational Case Study

The historical conflict between USA and Russia is not limited to cyber space but the challenge here is the road-map of the conflict weather it is going for further escalation or it is limited to what we have witnessed within cyber. As known, these two states are both cyber as well as nuclear credible states and they are willing to cooperate as well as confront due to capability and capacity they hold.

The case of cyber escalation between USA and Russia is very complex situation due to credibility of both states own and the behavior of challenging each other which does not result any signal that could help to build up any step of cooperation. Cyber arm race is ongoing and there is no clear expectation between both Cyber superpowers whether to limit confrontation within cyber space and utilize cyber for sparkling other geopolitical issues or escalate to a different approaches.

In this section, I will try to explore the nature of escalation ladder within Cyber-Cyber and Cyber- Other conventional/ Nuclear military confrontation. The attempt here to explain different approaches may help understanding the nature of cyber escalation. The confrontation between USA and Russian is one of the best case studies that reflects the attitude of escalation. The history of this confrontation is not newly discovered but it is historically there But, what is added to this is the utilization of cyber space for confronting as another dimension. Another dimension of cyber escalation added to the USA-Russia cyber conflict the claim of Russian interference in USA election and its willingness to retaliate and cause damage.

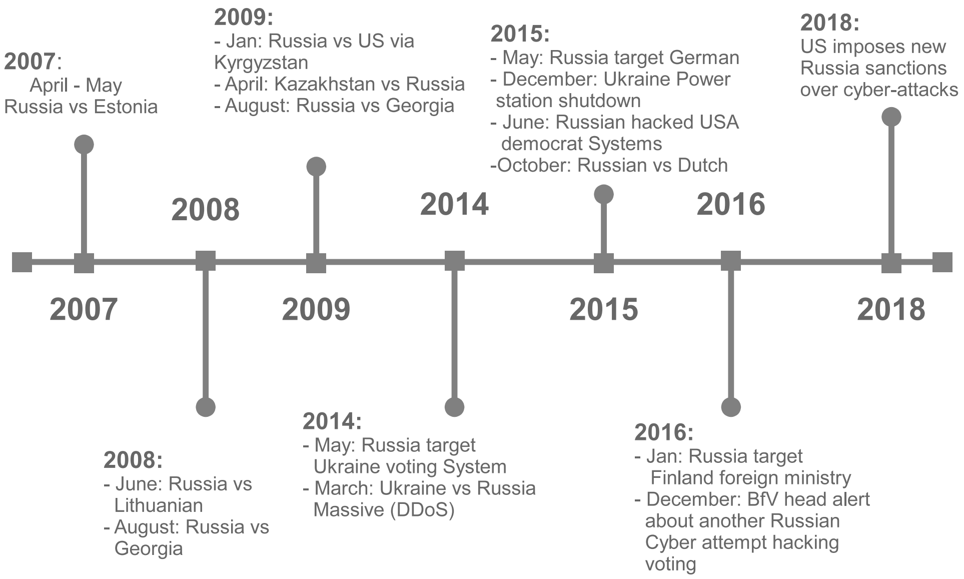

2007:
April - May
Russia vs Estonia
2009:
- Jan: Russia vs US via Kyrgyzstan
- April: Kazakhstan vs Russia
- August: Russia vs Georgia
2015:
- May: Russia target German
- December: Ukraine Power station shutdown
- June: Russian hacked USA democrat Systems
-October: Russian vs Dutch
2018:
US imposes new Russia sanctions over cyber-attacks
2008
2014
2016
2007
2009
2015
2018
2008:
- June: Russia vs Lithuanian
- August: Russia vs Georgia
2014:
- May: Russia target Ukraine voting System
- March: Ukraine vs Russia Massive (DDoS)
2016:
- Jan: Russia target Finland foreign ministry
- December: BfV head alert about another Russian Cyber attempt hacking voting

Fig. 5.1 Russia vs US and allies Escalation Time line [187]

This time line mainly present ten years of Russians cyber threats against other nations and it is confirming Russian credibility and readiness and willingness to utilize cyber space for any minor rather than major political conflict [187].

- April-May 2007: Estonia, annoyed Moscow and planning to move a Russian World War II memorial and Russia retaliate by shutting down and result out of action Estonia's internet via massive distributed denial of service (DDoS) attack targeting on government offices and financial institutions, focusing on disrupting communications.
- 2008:
  - June 2008: Russian utilize similar cyber-attack to punish Lithuanian government because the Lithuanian government forbidding any display of soviet symbols and Russians red teams response with cyber retaliatory targeting governmental web pages and deface it with hummer and sickles with five stars.
  - August, 2008: When Georgia pro-western government and then sent troops into breakaway republic backed by Moscow. Russia initiate new scenario of attacking by gather together land, Sea, and Air units for the mission of invading the Georgia. This was aligned with Cyber operation by Russian hackers and consequence of internal communication shutdown.
- 2009:
  - January 2009: Russia trying to encourage Kyrgyzstan president to recover American military base, Russian hackers shut down two out of four Internet service providers with a DDOS attack. This has worked and Kyrgyzstan removed US military base. Thereafter, Kyrgyzstan received two billion as aid and loans from the Moscow.
  - April 2009: Kazakhstan media published a statement by Kazakhstan president criticized Russia regarding political situation, an immediate DDoS attack was attributed to Russian teams shut down the media outlet.
  - August 2009: Russian hackers has shutdown Facebook and twitter within Georgia as memorialize the first year anniversary for Russian invasion the Georgia.
- 2014:
  - May 2014: 3 days before Ukraine's presidential election, a Russia-based hacking group, shutdown country's election systems in an overnight attack and back-up system was also shutdown, but Ukrainian computer experts were able to recover

the system before Election Day. This attack was aimed to create chaos and hurt national candidates for helping the pro-Russian candidate. In think this case was stimulating Russian to play the same game with USA elections.

  - March 2014: For the second time, Russian government harmonised military and cyber action. Another DDOS attack 32 times larger than the largest known attack previously used during Russians invasion of Georgia disrupted internet in Ukraine while Russian -armed pro-Russian rebels were seizing control of the Crimea.

- 2015:

  - May 2015: German digital forensics found hackers had penetrate the networks of German Bundestag and it was the most significant hack in German history. The BFV German domestic Intelligence Service claim that Russia was behind this attack and the target is information about Bundestag, German leaders the chancellor Angela Markel's and the NATO.
  - December 2015: Russian hacker's shutdown the central Ukrainian power station utilizing malware called black energy malware. This attack has consequenced 235,000 homes without power.
  - June 2015 - November 2016: Russians hackers penetrate Democratic Party networks and got to access to the personal emails of democratic officials and then it was leaked into global media like WikiLeaks. CIA and FBI now believe the intrusion was intended to undermine the election, the deep mission is to effect Hillary Clinton and support Donald Trump.
  - October 2015: Cyber security professionals claim that Russian attempting to hack Dutch Government networks for pulling reports related to the shoot down of flight MH17 over Ukraine. Because Dutch safety Board conclude that plan was attacked by Russian made missile and it was fired from area held by pro-Russian rebels [188] .

- 2016

  - January 2016 : Cyber Security Company announced that they believe Russian hackers were standing behind multi cyber-attacks on Finland's foreign ministry for a several years ago.
  - December 2016: BfV head warned " There is growing evidence of attempts to influence the federal election next year" he is referring to the German election and he critics Russia cyber threat and their attempts to effect Chancellor Merkel

because of her support to the sanctions against Putin personnel association after Russia annexed Crimea.

The U.S. has been targeted by repeated cyber attacks by foreign cyber powers and US seems to have limited power to stop this attacks. This confirm the assumption that even if the state is categorized as superpower but it is still vulnerable to the cyber-attacks.

During the 2016 presidential campaign Russian hackers has play a vital role in manipulating with the America democratic election. Claim was they have hacked national committee email server and made plenty of efforts to influence the elections outcome. As the special counsel Robert Muller specify 13 Russians and another 3 Russian entities. Then in February US intelligence with law enforcement officials warned that the government of Russia will try again to use the cyber space for conducting another operations for interfering with the midterm elections during November 2018. During the same month, white house publicly has blamed the government of Russia for the most destructive and costly cyber-attack in the history and the claim was about the 2017 NotPetya malware. This malware has disabled the government of Ukraine before spreading to a different multinational corporations like Maersk, FedEx and many others consequence billions of dollars as a damage.

Clearly, it is not limited to the Russians only who is hacking the United States cyber infrastructure. Chinese hacking groups are there and they have stolen plenty of US intellectual property related to the industrial sectors and to the critical military sectors as well.

China has weaponised what is known as “Great Firewall” and has conducted a massive DDoS attack against different US websites like GitHub, as a punishment for hosting content that the leadership of china found it as undesirable. In 2014, North Korean hackers has initiate a cyber-attack against Sony Company as a reflection of the “The Interview” movie which also represent the attempt of assassination of North Korean leader Kim Jong Un. Sony attack has erased content of thousands of computers and released internal emails. Also, has frightening Sony into canceling the movie from being released. Also, Iran has also attacked US financial institutes and cause immeasurable damage to the banks and other financial institute in New York.

So, cyber threats are capable to cause damage for the Superpower despite the superiority in defenses and offense capacity each state own. The nature of cyber escalation between superpowers can renewed calls for nuclear deterrence cooperation and particularly in cyber confrontation between USA and Russia. This case has not witnessed any signal of collaboration and this is due to different reasons reflecting the status of both actors behavior in cyber space:

- First, both Russia and USA are credible states and both actor act rationally attempting to maximize their payoff for causing some sort of loses over each other. This expectation because cyber space is not effecting human life directly and for that no worries to pursue challenging without considering cost of loses consequence ongoing cyber challenging.

- Second, USA as actor in the same game not clear about Moscow intentions and they still have a deep doubtful either Moscow willing to cooperate or not yet. Russia still acting offensively against USA especially after US sanctions. Russia conducting serious cyber operations against US and these operation exceeding normal operation like what is normally conducted during peace time.
- Third, Russia not willing to cooperate due to different perceptions about the nature of winning and losing within cyber space. This misperception lead to misunderstanding and accuracy upon what to agree and what to keep as floating between both states.

Escalation process of cyber confrontation is not limited to above reasons but I think in (Russia-USA) context deterrence can work under the context of mutual deterrence and mutual fear of loses. These two states are both credible states and enforcement approach cannot bring them to the table of cooperation. In this situation, need another approach relying on advancing mutual benefit and enhance the promise to go for mutual trust.

In summary, the nature of Russian cyber threat confronting USA and many other western countries having nature of cyber escalation. Different questions here, will escalation ladder be limited to confrontation within the cyber or it is possibly to exceed cyber to another domains of conflicts (Nuclear)?

5.3 Escalation Model for Cyber Deterrence

The previous chapter analysed the possible role of cyber threat credibility in deterring state cyber adversaries similarly to nuclear deterrence. One of the chapter findings was that credibility is not sufficient in deterring state opponent fully from pursuing any cyber attacks. So, the next expected situation of the cyber conflict is to move to more escalator stage between both opponents. In this case, this chapter analysis scope around escalation and expected gain from the decision of escalation and consistently attacking.

Cyber escalation model is based on deterrence game model where players are able to choose either to Cooperate (Not Escalate) or Not to Cooperate (Escalate). The problem with escalation is when the more cooperative player (If there is one) decide to retaliate at a certain degree will end up both states are prioritized to attack as dominant strategy. In cyber space, we assume states are going for escalation (Increase the intense of cyber attack) but at certain degree both states may recalculate the situation and agree to cooperate and deescalate the cyber conflict before it gets out of control. In the process of conflict deescalation, state can work to develop new (Status Quo) by threatening its opponent with more (ongoing) escalation cyber threat expecting opponent with more positive response reflecting willingness to cooperate.

The problem with escalation is that both states cannot avoid it when the crises begin and state will not progress unless it maintains growth in threatening more than the threat at the beginning of conflict. It is closer to increase the intensity of cyber conflict and it is unavoidable between both states to go for several repeated cyber interaction until realizing the need to reducing the intense via moving to more cooperative position.

Referring to the nuclear deterrence and escalation strategies, the expected advantage of state preemptively attack its nuclear opponent is not working at all because of earlier commitments to retaliate (Escalation) with any nuclear attack and there is no trust between both players. This will reflect no advantage from preemptive strike. But, who is to say preemptive cyber strike is not possible in cyber space? States can initiate cyber attack and challenge here is that immediate cyber retaliation is not expected to happen (Even if it is Pre-committed) due to different technical issues reflecting the nature of cyber space like attribution and states perceptions about that particular target.

In this model, the assumption will consider threat of retaliation against first cyber strike is not enough to prevent state from a preemptive cyber attack. With the same logic, State can threat its opponent with a massive cyber retaliation and it may prevent first strike but it is with low level of probabilities. Escalation in cyber occurs after first strike and second actor is retaliating and then still both states have the motives to pursued attacking. Therefore, de-escalation in cyber space can be assumed to begin when both states escalate and challenge each other till mutual belief that the conflict will reach uncontrolled point and it could get exploded. At this point, both states will reduce the incentives of any further preempt in cyber opponent.

Cyber deterrence between two credible states like Russia and United States -with assurance of second cyber strike capability- would seem to give the necessary level of threatening and assurance that is needed within cyber space. But the challenge, will cyber threat help to create motives for cyber de-escalation and prepare the ground for cooperation between these two superpowers or does it needs more intense in escalation to develop the fear from losing the control of conflict and then each actor will prefer to signal the opponent about possibility to cooperate.

Analyzing conflict escalation and attempting to model escalation in cyber space is the goal of this section and within the escalation situation I assume there is a preference within both states decision makers to damp down the conflict and if not working then try the next possible strategy that is to contain it rather than shift to a full scale war which will lead to a mutual suffering and lose. Assume this cyber escalation occurring between two credible superpowers (Cyber Credibility) causing serious damage and even between superpowers and other non superpowers is causing an effective damage.

Scope of Escalation Model: *scope of this model is to analyze the consequence cyber threat credibility failure and the expected outcome from escalating cyber confrontation and its role in deterring state cyber adversaries.*

Our case in this chapter reflects two superpowers in a historical confrontation and they have recently added to the conflict utilization of cyber space in confrontation via different approaches. Russia and America have been in different escalation cases and one of the top cases was Cuban Missiles. This case was a real example how nuclear escalation could begin and how escalation is later get stabilized. The cyber confrontation between Russia, United State and many other western States as explained in previous section and time-line in Fig. 5.1 reflect on going escalation and Russian cyber threat growth. Not all interaction was directly between Russia and US but some have involved allies. Escalation between superpowers is either direct confrontation or via allies, will be considered as a direct confrontation and need collision for deterring these threats.

The decision tree presented in Fig. 5.6 has attempted to establish the logic of Russian willingness to escalate utilizing cyber space against its adversaries and this was clear in different cases listed in Section 5.2. Russia has consistently demonstrated cyber threat as a tool for military operation like what has occurred in Ukraine. Sequential cases attributed to Russian government support the assumption of escalation between these two superpowers.

Russia has mixed the utilization for the cyber threat, in some cases it was part of military confrontation like Ukraine case and in some other cases like Estonia it was only limited to a cyber attack. Logically, Russia as actor in cyber space was on going *(Maximizing the Probability)* of attacking in cyber as well as retaliating. This observation is essential for its opponent to consider. However, stabilizing scale of escalation should offer both actors freedom to move or act upon availability of non-provocation from each other.

5.3.1 Cyber Escalation and Deterrence

Accordingly, analysis begin by setting up escalation game and just to remind our self escalation game is based on deterrence model as mentioned earlier. In addition, in real life cyber confrontation is ongoing between states but the difference is the heat level of the confrontation. Nuclear confrontation has not occurred compared to cyber and this make difference in the game model by assuming that the conflict is on going and the deterrence is deterrence within the conflict. This means cyber deterrence is mainly to stop ongoing attacks and at the same time deterring the future expected (state-state) cyber confrontation.

Within cyber escalation model, payoffs for state (A) and state (B), respectively are noted as (A_i, B_j) and this payoff assumed in order:

- State $(A_i) = Russia = a_1 < a_2 < a_3 < a_4$
- State $(B_j) = USA = b_1 < b_2 < b_3 < b_4$

  Both actors (players) within the model can change between two strategies either to **attack** or **not to attack** and within the analysis going to give notation look like:

- Strategies **(c)** = Cooperate/No attack or **(n)** = No cooperation/Attacking

  By selecting each of these two strategies the expected payoff for each state will be listed within the model figure 5.3 as:

- E_A= Reflecting the Expected Payoff to State (A) for choosing **(c)** or **(n)**
- E_B= Reflecting the Expected Payoff to State (B) for choosing **(c)** or **(n)**

Escalation model aim to analyze probability of each state strategic situation and the decision of escalation within cyber space. Cyber conflict outcome expected to be one of the four outcome listed below. While the scope of this model is to analyze escalation, model will focus on one notation which is s :

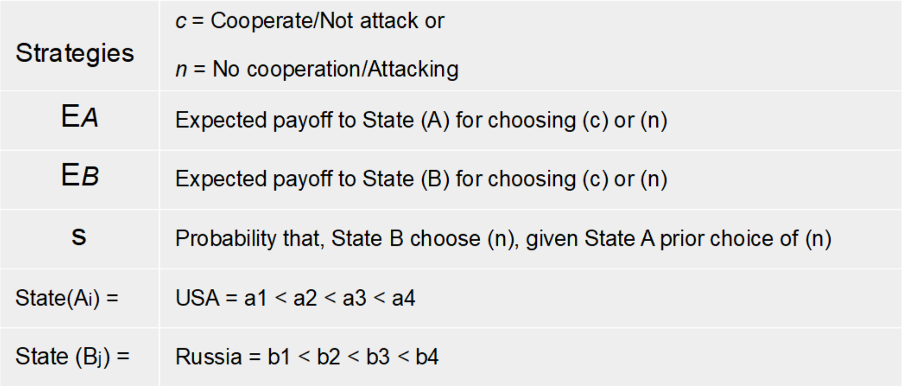
- s = Probability that, State B choose **(n)**, given State A prior choice of (**n**)

In accordance with the rules of the escalation game model, players should act strictly to the model general rules:

+ Each player, either (A) or (B) do have the flexibility to choose and change between (attack) and (not to attack) strategies,
+ It is 2*2 game which consequence four strategic payoff for both states within the game either for USA and at the same time for Russia,
+ Both states can prefer not to escalate and priority (c, c) which reflect best outcome for both states (a_3, b_3),

+ One state either (A) or (B) might *not to escalate* and both the E_A and E_B can be (c, n) or (n, c). This outcome might reflect best outcome for state that are not willing to cooperate (a_2, b_4) and (a_4, b_2),

+ Both State are not willing to cooperate (n, n) and this outcome might be the worst outcome for both states (a_4, b_4) as it is reflecting mutual conflict, and need further analysis.



Strategies	*c* = Cooperate/Not attack or *n* = No cooperation/Attacking
E*A*	Expected payoff to State (A) for choosing (c) or (n)
E*B*	Expected payoff to State (B) for choosing (c) or (n)
s	Probability that, State B choose (n), given State A prior choice of (n)
State(A$_i$) =	USA = a1 < a2 < a3 < a4
State (B$_j$) =	Russia = b1 < b2 < b3 < b4

Fig. 5.2 Cyber Threat Escalation Model Definitions

The interest here, is to model (State-vs-State) cyber escalation situation reflecting failure of cyber threat credibility in deterring state cyber adversaries. Usually, escalation begin when both players move up into escalation ladder. Scope of cyber escalation model reflecting situation where confrontation begun by the high probability of one state preempt another state and the attacked state retaliate and move to other action that may provoke opposition to escalate for further involvement like conventional military. A single retaliation is allowed at the beginning of the model that could establish for "Right the balance" for initially more cooperative player "Expected".

So, the model begin by State (A) preemptively attack (B) and State (A) expected outcome reflecting $E_A = n > c$ and initiate the cyber attacks against carefully selected targets. State decision from maximizing *attacking* strategy reflecting different geopolitical/economical conflicts. By executing cyber attack, first state expect to gain certain objectives. One of expected objectives that attacked state will not be able to defend the cyber attack.

By attributing first (Considered) cyber attack it is most likely that State (A) is the attacker and the ball will be in State (B) side since (B) is going to decide the next step within the model. Cyber space compared to other conflict domains give states high probability for succeeding second strike which mean attacked state can retaliate within cyber space. At this point, State (B) assume maximizing *Cooperation* strategy will not cause the exact response

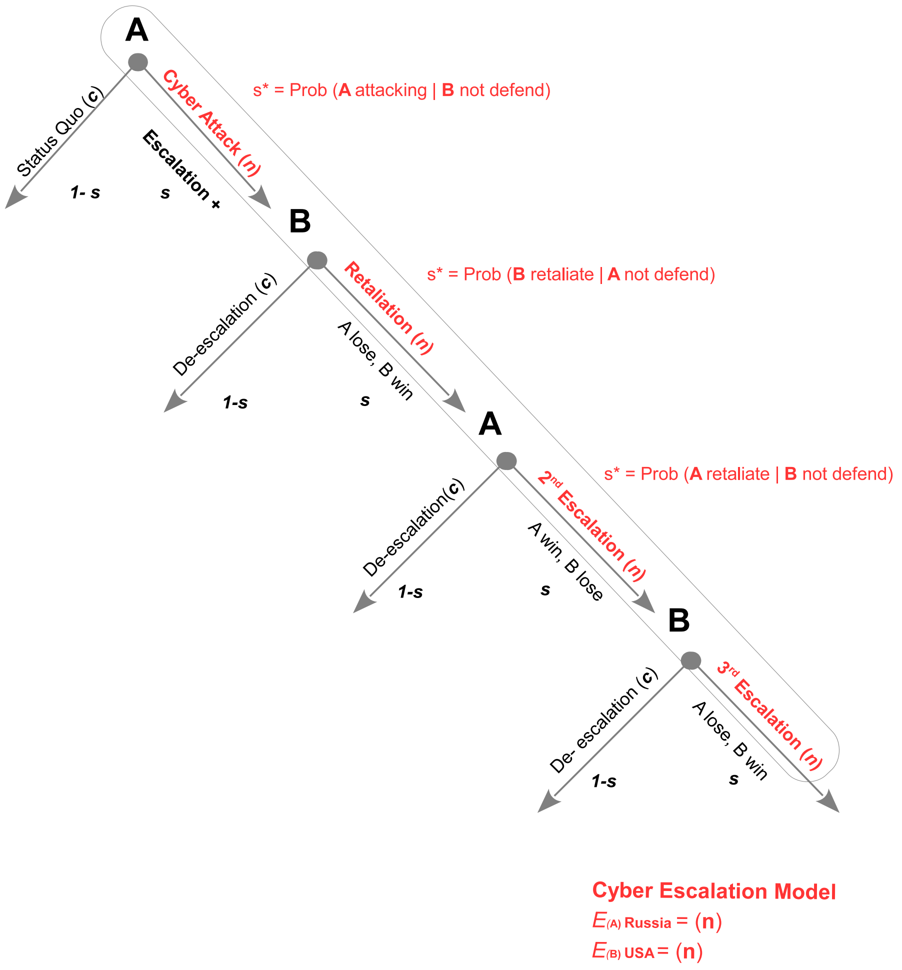


Fig. 5.3 Cyber Threat Escalation Model

for State (A) and selecting the strategy of cooperation will not aid State cyber deterrence as it will give signal of weakness from (B) to respond against (A). Moreover, it will help State (A) to continuously select n as dominant strategy.

In case (B) decided to respond with retaliation then the $E_A = n > c$ and for pursuing this strategy a state need to consider target that is valuable to the (A) for assuring this retaliation with cyber attack may give a concrete response and may deter opponent not to repeat any similar cyber attack. It worth noting that the advantage of state holding cyber threats and readiness to response is to signal its adversaries regarding its interest in defending against its cyber space. Moreover, it will signal about state capability for assuring observability over its cyber infrastructure and willingness to act against predictable threats.

Escalation model in cyber space reflecting failure of first round of deterrence game happen and when there is no preemption occurred $E_A = c$ and both players are assured to stick with it. But, escalation start when one state change the strategy to take preemptive cyber attack and when attack certainly happen and get attributed then E_A= n and at this point it will establish the ground for a new model that will lead for cyber escalation model.

In this case, first equilibrium is certainly started by State (A) resulting preemption where State (A) attacking (B):

$$E_A(n) = a_4 p + a_1(1-p) \tag{5.1}$$

Escalation payoff for mutual cyber attacks situation reflect the intention of both states to maximize strategy of attacking. It is the situation where Mutual non cooperation and it appears when:

- State (A) Assured Payoff E_A= $n > c$, and at the same time
- State (B) Assured Payoff E_B= $n > c$

Fig. 5.4 is a game model attempt to explore the nature of growth in cyber confrontation in correlation with the value of loses consequence each cyber attack. State(A) vis-to-vis State(B) are in a cyber escalation and both state strategic situation is highly probably expect to occur and sustain due to different reasons. This scenario is reflecting reasons like:

a. Failure of cyber threat credibility in deterring state cyber adversaries

b. Cyber space have no borders and it is an open space for all to confront,

c. Signaling adversaries about state cyber capability, capacity and its willingness,

d. Different perception regarding cyber attacks (destructive or not),

e. Possibility in removing attacker foot print and digital evidences,

Stage 2, in cyber escalation game tree is more of clear provocation between both states. It reflects the commitment of opponent in pursuing conflict via attacking state (B) expect to achieve the objective of attacking strategy. Main objective from attacking (B) is to gain more of lose. But, the point here is to justify level of gain expected by state (A) as attacker. State (B) outcome from this particular attack could be reflecting $E_B(c) = b_1$ or it could reflect the value of $E_B(c) = b_3$. Cyber attack have a value from state point of view and it would reflect to stimulate state next step in retaliation or ignore the attack and not to retaliate. It is mentioned within game model that the value of $b_1 < b_4$ and for that not all successful cyber attacks would deserve the state intention to retaliate.

Moving to stage 3, escalation is the general character at this stage of the game model where both players are working to prove their abilities to respond and make progress as

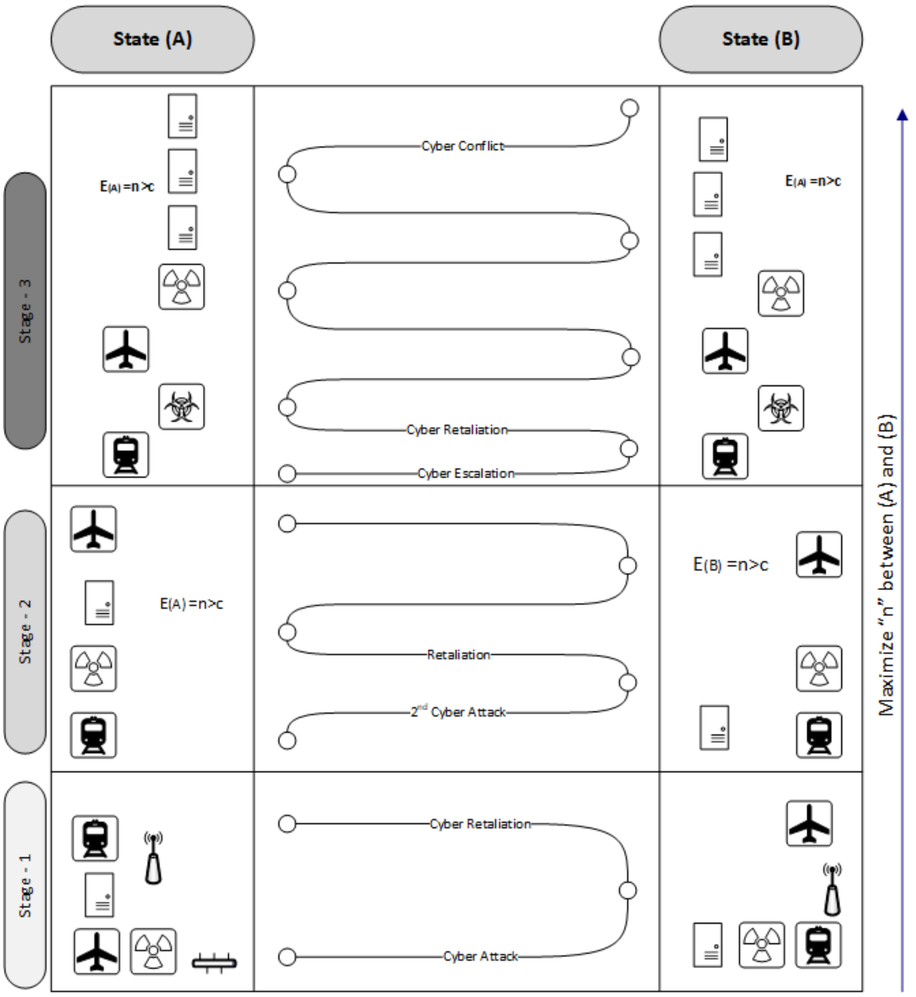


Fig. 5.4 Escalation in Cyber Space Model

well as achieving the possible losses in the cyber space. During this stage it is clear that both players attempting to utilize cyber targets and attacks to achieve the maximum possible losses within adversary cyber space.

State (A) will attempt to keep its loses close to $E_A(n) = a_1$ and at the same time its adversary loses are more close to $E_B(c) = b_4$ which reflect more valuable loses aligned with low cost of loses for excuting cyber attack from (A) prospective. It could practised via targeting adversary most critical infrastructure. Both players attempting to utilize cyber targets and attacks to achieve the maximum possible losses in the adversary cyber space.

Presumable, the decision maker in both states (A) and (B) would rationally limit the escalation within the cyber space for the purpose of let other strategies to get involved in supporting cyber deterrence policy. This does not mean to involve other conflict domain and at the same time not to exclude it. Of course, the adoption of a cyber-scale escalation strategy is possible in terms of the variety and intensity of cyber attacks, as well as in the diversification of targets to be a real pressure on deterring attacking state.

5.3.2 From Cyber to Nuclear Escalation

The argument here is that cyber escalation may go beyond cyber domain. The assumption of the state-state conflict scenario begin via utilizing cyber and then will not stop within cyber and will extent to the full escalation ladder till reach utilization of nuclear threat as a threat of retaliation.

Up to today, the assumption that cyber escalation between both (A) and (B) to exceed and to involve nuclear domain for confronting opponent is not working. It is because nuclear threat by itself has succeeded in stabilizing international system. Over five decades since exploration of nuclear weapons and the world has not witnessed any nuclear confrontation due to success of deterrence within nuclear domain. That's was because most superpowers perceptions about the consequence of any nuclear confrontation was clear. For that, they would prefer sustainability of nuclear deterrence (Status Quo) rather than breaking it and confronting each other.

Referring to the nuclear deterrence model and its assumption, it is clear that first state know that the certainty of nuclear retaliation from first state is assured. For that, probability of winning is lowering expected outcome $E_A = (Lose > Gain)$. Then, there is no guarantee from adversaries not to retaliate and the probability to retaliate will confirm $Lose > Gain$ and at the same time not have any second nuclear retaliatory. For that, superpowers know the consequence of nuclear confrontation and at the same time know the consequence of cyber confrontation but it seems cyber threat by it self is not enough to deter state cyber adversaries. It could be working in repeated interaction due accumulative confrontation and accumulative cost of loses but with single round of interaction model is not going to raise the fear within adversaries.

It known that attacked state want to threat the attacker via send a strong signal about its certainty of retaliation. The challenge here is to answer the question will the cyber retaliation send the expected message to the first cyber attacker? If not, will high probability of frequent - massive - cyber retaliation against first attacker will make difference in deterring cyber adversaries or need to involve another kind of threat?

Assume, it rational from both states not to concentrate on utilizing the cyber offensive strategy as it could lead to cyber escalation. Sparkling cyber escalation will consequence to un measurable loses and disruption between both players. State (A) will $E_A(n) = (Gain < Lose)$ and at the same time for the state (B) while approaching the problem with careful diplomatic dialogue or following many other tools might assist in avoiding any sort of cyber escalation.

For that, the assumption to involve nuclear as a reflection of cyber threat is not accepted logically due to success of deterrence in preventing nuclear confrontation rather than cyber.

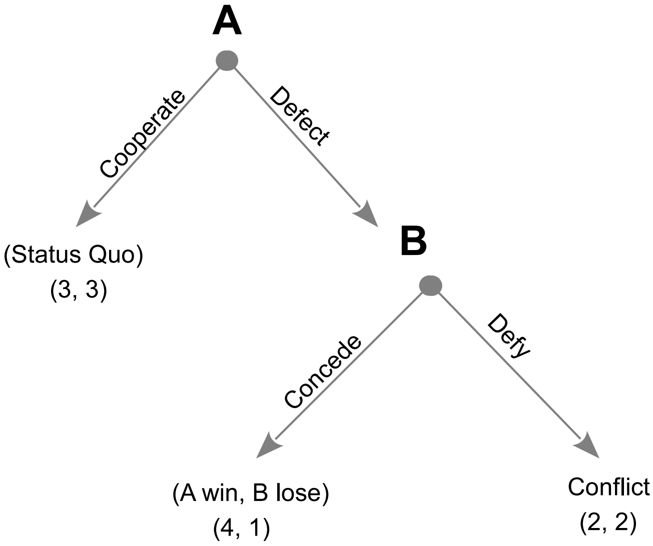


Fig. 5.5 Simple Deterrence Game with a Credible Threat [68]

Nuclear states are looking for sustainability in nuclear domain and not willing to go for any nuclear escalation and the respond to this argument is the success of nuclear deterrence in preventing any nuclear confrontation to occur over different cases over the history during and after the cold war. as example, Cuban missiles, India vis to vis Pakistan, Israel vs Arab states, North Korea, etc.

Simply, assumed the nuclear deterrence model worked in preventing nuclear confrontation via credibility of nuclear threat. It is known that the expected outcomes of the nuclear deterrence model are four strategic payoffs between both players, $[E_A]$ and $[E_B]=$ $(c,c)(n,c)(c,n)(n,n)$. Sustainability in nuclear deterrence efficiency since cold war has prevented the world plenty of nuclear confrontations. Sustainability in avoiding sparkling any nuclear confrontation are assured by all superpower around the world. For that, it is not possible to expect any escalation from cyber to nuclear confrontation due to credibility of nuclear threat and its deterrence to maintain $(StatusQuo)$ within superpower conflicts.

Therefore, the hypothesis that nuclear confrontation as a result of cyber threats is incorrect. It is because nuclear states did not face in the face of the destructive nuclear threat, which is more dangerous than cyber threats. Therefore, we do not expect any nuclear confrontation due to cyber risks from a nuclear or non-nuclear state. For example, Israel faces cyber-attacks from neighboring countries in the region but has not used or threatened to use nuclear weapons against these countries.

5.3.3 Escalation and Mutual Assured Disruption (MAD)

Ability to stabilize cyber confrontation (escalation) or at least to contain it is a mixed blessing as it helps to stop the growth of mutual damage on both sides of conflict (cyber space) and progress to deterrence objectives (stability in cyber confrontation). However, crises stability could lead to another step of provocation behavior by state adversary which will return to the escalation scale. Provocation can happen via direct cyber attack between state (A) and (B) or attacking the allies reflecting main conflict. This provocation will cause another round of cyber confrontation and result mutual cyber disruption.

The nature of cyber escalation is closer to consequence of mutual disruptions. Mutual assured disruption mainly reflect cyber attacks that cause shutdown infrastructures, wipe databases, power shortage, networks damages and many other technical consequences. In this situation, states can recover despite the high cost of this recovery. Of course, state doesn't like to get this high bill but this is the end of cyber attacks compared to traditional approaches of fighting where it kills human and wipe the infrastructure like nuclear attack. It is incomparable with cyber attack.

USA vis to vis Russia in cyber space are growing and it will not stop to the level of presidential election manipulation. It is cheap fighting domain and could cause a lot of chaos for state opponent via utilizing different kind of cyber interference. Repeated cyber interaction between adversaries will accumulative consequence high loses. Resistance of cooperation will reflect loses for both opponent due to high probability of cyber attacks success.

$$\begin{aligned} E_A(n) &= a_4 p + a_1(1-p) \\ E_B(n) &= b_4 p + b_1(1-p) \end{aligned} \tag{5.2}$$

Expected outcome for each state following strategy of attacking -n- is to accomplish but at the same time possibility of getting lose via opponent retaliation is high due to cyber vulnerabilities availability within state cyber space. Between these two equations (5.2), both states will suffer from the mutual disruption where both state can keep repeatedly attacking its opponents causing some sort of loses within cyber space.

Comparing cyberspace to other conflicts domain, cyber attack is not affecting human life directly compared to conventional conflict where human is the target. For that, states are highly interest to manipulate with its opponent via cyber space for cause maximum possible loses. Russia persistently challenging USA and attempting repeatedly to cause different kind of loses whatever possible to achieve. Continuously attempting to cause different kind

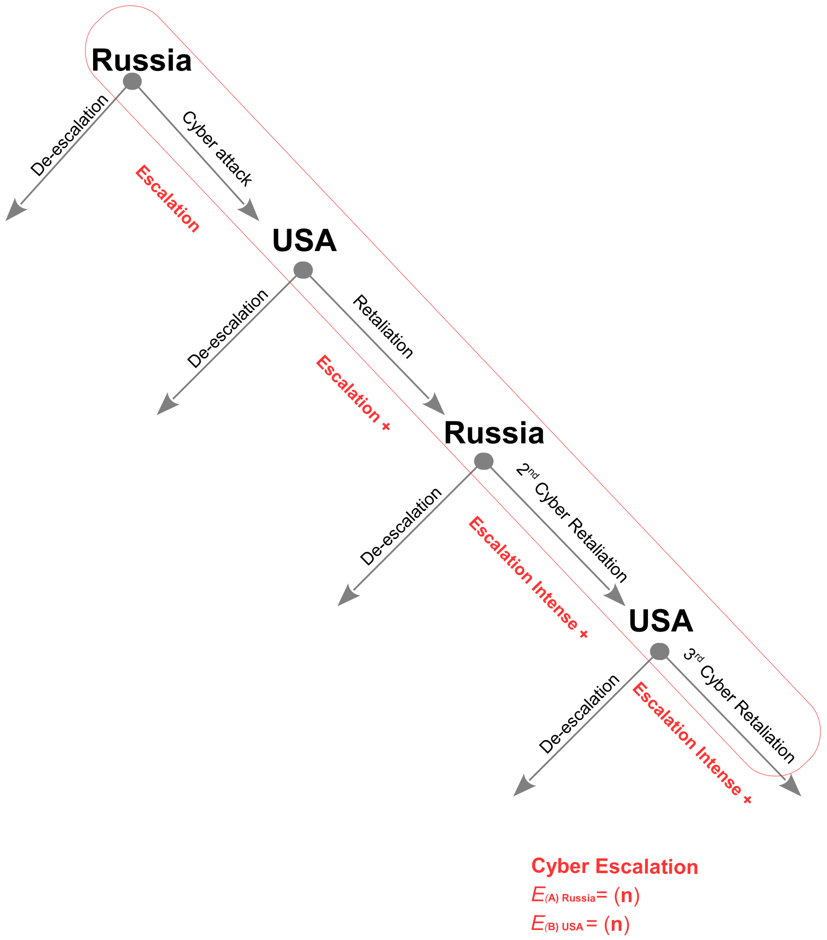


Fig. 5.6 USA vs Russia Cyber Escalation

of loses into USA cyber infrastructure. For that, USA and for maximizing benefit of its cyber deterrence strategy and rather than maintaining cyber escalation, might attempt to concentrate more on how de-escalate cyber confrontation. De-escalation is reduction in the cyber mutual disruption situation and it is meeting with deterrence objectives. Reducing threat intense is deterrence and deterrence might not stop threat fully but it can be considered as a success of deterrence while reduction in threat level. This reduction is reflection when state adversary decided not keep attacking and move to a decision of reducing the attack.

De-escalation is reduction in cyber attacks. It could happen under the commitment and acceptance of state adversary to reduce or hold the $Maximization\ of\ attacking$ strategy ($E_A = c > n$) and keep signaling about its strategical changes. Deescalation could be due fear from threat of retaliation, believe on mutual repeated loses between adversaries, shortage of resources or attempt to guess adversary willingness to cooperate and growth in adversary threat credibility. In practising deescalation, state (A) strategy should reflect more of cooperation ($E_A = c > n$) and should be full of commitment.

De-escalation is more of cooperation than confrontation within the model and within the real life practise of each state strategies. For that, assuming cooperation started it needs from both actors to terminate their payoffs reflecting their intention and it can occur under the mutual condition:

- Predictable payoff for E_A= c > n, concurrently and similarly,
- Predictable payoff for E_B= c > n

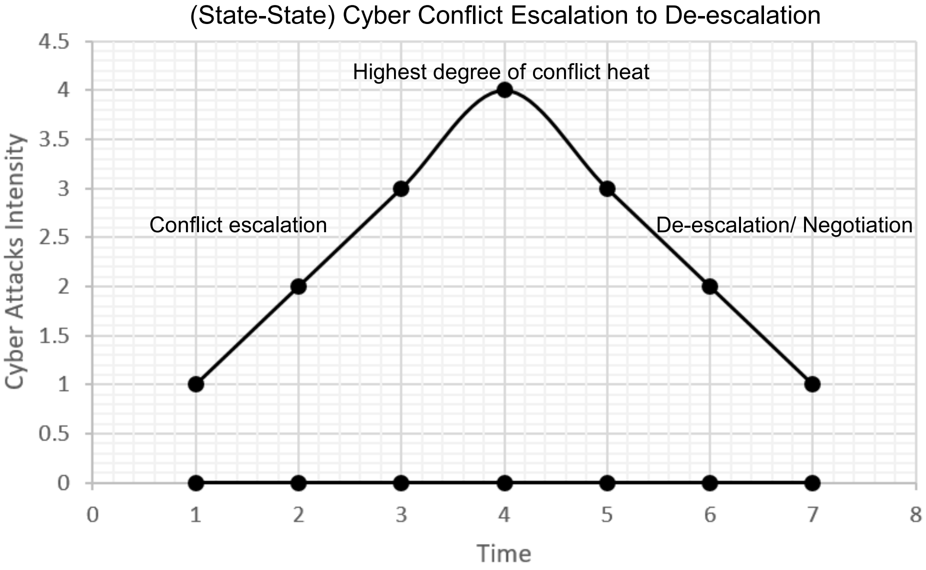


Fig. 5.7 State vs State Cyber Conflict Escalation and De-escalation Mode

Cyber escalation model is based on a deterrence game has been developed in (chapter.4). Both adversaries are assumed to be able to choose any level of initial cooperation or non-cooperation; the more cooperative player (if there is one) maybe then choose to retaliate. In cyber conflict, states are assumed to have escalated their cyber conflict. After realizing the growth in loss (Accumulative Loses) and reach the time to stabilize the escalation before it explodes.

State (B) can, by threatening it adversaries by repeated cyber attacks (Within the sequential game) against its cyber opponent, supposed to stimulate adversary behaviour to stabilize and establish new $(StatusQuo)$. The new $(StatusQuo)$ is a consequence of maximizing the probability of s strategy for both player point of view within the game model.

In addition, points of threat escalation are identified in early sections which neither state can prevent the adversary within cyber space from escalating further without threatening the opponent more severely (Repeated Games) than before the crisis explode, thereby heating up and already the tense situation between State E_A= $n > c$ and E_B= $n > c$.

Crisis in cyber space stabilization is aided by being driven close to the situation of full cooperation between both adversaries. Paradoxically, both players may benefit from having created a crisis for only escalating threats may resolve. The benefits are more supporting other strategic factors like reputations and credibility. In this case state might benefit from limited escalation. Controlled and limited escalation will assist state credibility in threatening adversaries. In this model, the attempt is to discuss ways of avoiding threat escalation and decrease risk of ongoing (state-state) cyber confrontation, especially cyber conflicts between superpowers that have the most advanced cyber technologies.

The report produced by National Intelligence in 2017 has assessed Russia cyber activities and its intentions in recent US elections. This report and many other reports reflect the nature of cyber escalation between Russia and USA [189] as a case reflecting our model. In term of modelling escalation and deescalation, such situation can be understood via tracing the repeated interaction between both players (USA and Russia). Each state seems pursuing situation of challenging.

Strategy of minimizing cooperation with state cyber adversary is exactly reflecting the growth in cyber threat and it is where cyber escalation.

$$\begin{aligned} &Minimizing\ Prob\ of\ (Cooperation) \nparallel Deescalation \\ &Minimizing\ Prob\ of\ (c) = Bad\ Deescalation \end{aligned} \tag{5.3}$$

Russia has tried repeatedly to effect USA cyber infrastructure utilizing different kinds of cyber threats on top of these threat was the suspicious of targeting US voting cyber infrastructure. As well as the Americans in the ongoing attempts to track and monitor weaknesses in Russia cyber domain, either for direct use or for future employment as a retaliation from the Russians cyber threats. Increasing the probability of cooperation within state vs to vs its cyber adversaries is where cyber deescalation beginning. It can be initiated by one state for the purpose of signaling its adversaries about its intention to change its strategy within the same conflict. Correlation between maximizing probability of cooperation and deescalation in cyber confrontation functioning in a parallel in reducing cyber threat heat.

$$\begin{aligned} &Maximizing\ Prob\ of\ Cooperation \parallel\ Deescalation \\ &Maximizing\ Prob\ of\ (c) = Good\ Deescalation = Good\ Cyber\ Deterrence \end{aligned} \tag{5.4}$$

So, it is state to decide rationally between escalate and deescalate cyber threat for the purpose of deterring its cyber adversaries. Different criteria state need to consider especially if it is confronted with a real sophisticated cyber state like Russia and China. Moreover, what is working between China and USA might not fit to establish any deterrence between Russia and USA.

5.4 Strategies and Lessons for Escalation

In summarizing the chapter and what has been observed from the cyber escalation model analysis as well as the case study, certain lessons has been concluded. These lessons can be transformed as a strategy that state would benefit in strengthening its cyber deterrence policy.

Escalation in cyber deterrence is a situation that comes after threat of retaliation as a punishment failure in deterring state cyber adversaries. Credibility of cyber threat can work in stimulating cooperation behaviour between adversaries while in many cases it does not. When credibility of cyber threat does not work, the intense of cyber confrontation is the next stage of the conflict where each adversary attempt to challenge and this will increase the probability of mutual loses (mutual assured disruption) which will basically cause damage for both state cyber domain.

Specifically, when a state get into escalation situation within cyber space it needs a careful analysis about the next step in escalation due to the complexity and unpredictability reflecting the ambiguity of cyber space threats. Escalation in cyber space can benefit from escalations of other conflict domains but it is does not mean it will give the same results. For that, the lessons from this chapter analysis can be briefly summarized:

5.4.1 Escalation of Cyber Threat Model General Lessons:

- State need to calculate carefully the decision of escalation when confronted with known credible state. This is because it is very fragile strategy as the retaliation from credible state might be heavily costly and will minimize any expected gain.

- Escalation in cyber space can assist state in Minimizing its cyber adversaries certainty about high benefits. This can be practise via signaling or practical exercise.

- Fluctuate between light escalation and non escalation as the retaliation from the credible state probable consequence with high impact of damage.
- It is known that credible state in the cyber space can go for escalation due the resources and capacity. But in opposite, it is also known that other state can keep the cyber escalation
- Escalation in the first cyber case will give state immunization and experience for maximizing strategic reputation within cyber space.

5.4.2 Escalation and States Strategies:

- Escalation in cyber space between two states (A) and (B) occur when credibility of cyber threat as a retaliation punishment fail in reducing the heat of ongoing cyber confrontation. Then, both states get involved in cyber attacks and the main conditions for cyber escalation is when both states USA and Russia pursue their intention to challenge its opponents and this is what is happening in real life. So, strategic situation for each state will be reflecting each state calculation.

  USA (B) escalation strategies will consistently follow strategies under the condition $E_B = n > c$:

  1. Minimize (p) : Keep attacking Russia via utilizing cyber threat either as a punishment or as a retaliation for the previous cyber attack. In addition, it does not give Russia chance to preempt within cyber space,
  4. Minimize (q) : Continuously assure to minimize any probability of cooperation with Russia,
  2. Maximize (r) : Keep maximizing the strategy of attacking Russia aiming to keep enforcing Russia to maximize probability of cooperation,
  3. Maximize (s) : Retaliate in ways to keep effecting Russian cyber infrastructures and strengthening USA cyber credibility,

  In opposite, Russia (A) to escalate need to follow a strategy that assures $E_A = n > c$ and under conditions of:

  1. Maximize (p) : Keep Retaliate against USA via repeated cyber attacks either as a punishment reflecting cyber attack. In addition, not to give USA chance for any second preemption,

4. Minimize (q) : Continuously assure to minimize any probability of cooperation with USA,
2. Minimize (r) : Keep maximizing the strategy of attacking USA aiming to keep enforcing USA to maximize probability of cooperation,
3. Maximize (s) : Retaliate in ways to keep effecting USA cyber infrastructures and strengthening Russia cyber credibility,

- Deescalation within cyber space can be achieved in case of both Russia (A) and USA (B) parallel and at the same time prioritize the following strategies:

1. Minimize (s) : USA convince Russia to reduce the probability of attacking and,
2. Maximize (q) : Then prioritizing the cooperation due to probability of maximizing cooperation will assure outcome of $E_A Max(q) = (Gain \geq lose)$

Chapter 6

Cyber Deterrence by Entanglement

In this chapter, the target is to explain a new deterrence approach that might be more efficient in optimizing cyber deterrence compared to previous traditional deterrence approaches (Denial and Punishment). This approach is based on entanglement. The chapter will introduce the concept of entanglement and the incentives for prioritizing entanglement approach. It will investigate the practical steps for approaching the deterrence by entanglement for deterring cyber threats. Practices that motivate states to develop mutual trust as a ground for the strategy of cooperation and at the same time show even credible state was lack to deter non credible state using credible cyber threat.

The next section of this chapter attempt to analyze the strategy that could replace the weakness of credible threats in deterring cyber threats which is escalation. Escalating cyber confrontation has different nature compared to other type of escalation of conventional conflicts and Each state can deliberately pursue cyber confrontation.

For that, this chapter tries to explore the deterrence by entanglement as a best optimistic strategy for the state-state cyber conflicts. It will analyze the relevance of entanglement to cyber deterrence and assumptions for developing strategies that develop concrete entanglement for the benefit of both adversaries. On further thought, the role of entanglement in cyber domain in supporting cyber deterrence will be explained.

Then, the chapter will present a case study as motivational case study that support the assumptions of success of the entanglement approach as a better strategical option for two credible cyber state. The case study reflect the situation of two states having close interest to cooperates showing mutual fear followed by mathematical model for analyzing the entanglement approach and how the model can work reflecting the situation of mutual cooperation. Chapter conclude with a section presenting strategies that help optimizing state entanglement and helping states with ultimate approach that consequence cyber deterrence working successfully.

6.1 Entanglement Concept

States developing their cyber power (Defense, Offense and Deterrence) for assuring their capacity to defend or respond against international cyber threats. This development will give states ability to show its credibility and readiness to approve its capability. Over history, states was trying to hide its military capacity and consider this capacity as a key success or advances for the states in challenging its opponents and surprises. But, this assumption changed during the recent history especially during the cold war between USA and Soviet Union. During cold war and with a little of transparency between both adversary. The transparency gives a transparent information or indicators about mutual nuclear capacity and this draw a clear expectation about the consequence in case of miscalculation happen between both nuclear superpowers.

In cyber space, states are developing its capacity similar to other states around the world even those states under international sanction can develop its cyber capacity and we have witnessed this with Iran as case discussed within credibility chapter. Despite western sanction to prevent Iran from getting any cyber security technology but after specific cyber attacks, the Iran cyber race has quickly started and it has became a credible cyber state similar to many other international credible states within a very short period of time. For sure, state can be credible in cyber but at the same time it is vulnerable to wide range of cyber threats. By the same logic, when state (A) develops its cyber offensive capacity its adversary can develop the same offensive capacity or other advanced once.

Developing cyber threats and replicating it is more simple compared to other conventional conflict domains. Moreover, the delivery of the cyber threat is simple and have different tactics within a well connected networked world. This uniqueness raise the level of possibility of suffering repeatably and unpredictably. In opposite, state opponent can do the same of getting cyber threats and utilize it for effecting state (Deterrent) repeatedly and this will not aid the deterrent state or main state on escalating process of cyber attacks and growing scale of cyber threats. Thats why no states can claim that its is secured from any type of cyber attacks as the decision maker know how fragile is the cyber space and it should be treated carefully.

The core goal of cyber deterrence strategy is to prevent cyber adversaries from taking the decision of attack. In addition, the general understanding of the deterrence practice was via two major sub strategies. First, deterrence by denial and the second is by punishment and both were practiced enough during the cold war.

Within previous two chapters, we have seen how credible state in the cyber domain (USA) was not capable to stop its opponent (Iran) from developing its cyber credibility and despite its credibility it has not succeeded in deterring Iran from threatening US within cyber space and this approach has resulted into another credible state that can utilize the cyber threat as retaliatory against its adversaries.

The analysis within previous two chapters have shed the lights over the lack of success in the deterrence approach by strategy of punishment by retaliation via credible cyber threat and it could lead to an escalator interaction between two credible states. The nature of escalation in cyber is not going to limit to certain expected targets but it is more of unpredictable and unknown. Also, this approach will not function as it is expected to deter cyber threats especially in case of cyber conflict between credible cyber actors. So, both cyber deterrence by denial which is reflecting hardening cyberspace vulnerability will reduce any probability of getting attacked neither cyber deterrence by punishment utilizing credible cyber threat aligned with other sanctioning will deter states from getting cyber technologies that help develop cyber threats.

These two approaches for deterrence were not successfully working in cyber due to the uniqueness of cyber space reflecting the misperceptions, misattribution and changes in the international system in term of conflict and cooperation. Comparing cyber to the nuclear, in nuclear the parameters for the deterrence was clear between USA and Russia and it was known that no nuclear attack is accepted and if attack occurs the retaliation in kind is confirmed. This happens when there is no misperception between both actors and both states know what is the consequence. While in cyber, strategies are still having a lot of ambiguity between states and need more work to get narrowed down and develop another approach. Different questions within the cyber deterrence strategy need clear answers: (1). Should cyber deterrence strategy deter one particular cyber attack? (2). Should strategy target deterring any cyber attack that may target any critical infrastructure disruption or destruction? (3). Should it deter malicious activities like political propaganda? (4). Should it deter newly complex cyber-attacks like ransomware or crypt jacking attacks? More deeper work is needed to be done in this field and with more precise approaches to achieve more measurable deterrence in cyber space.

Deterrence in cyber compared to the nuclear need more transparency similar to what has occurred during Cold War between the Soviet Union and USA. The transparency is reflecting the real intention of how state strategically is willing to utilize the cyber space and up to what extend it is willing to keep cyber a peaceful space. Another similar question with another dimension, will superpowers accept to be more transparent about its cyber capability with its adversaries especially if these states consider as a mini state in the international system.

We suggest that the best belief about state and its strategic situation in cyber space is that every state know that it is secure but at the same time it is vulnerable. It is secure, in the sense that states are investing to secure what is possible to secure in the cyber space specially the known cyber threats. But, vulnerable to plenty of unknown and unpredictable cyber threats as states are more opened and networked than ever before. USA is on top of these states who knows this mutual situation of cyber strength and vulnerability [190]. This mutual belief (state-state) should enforce the need for maintaining cyber as space for exchanging business and stimulate states for entanglement approach for the benefit of deterrence in cyber space.

Cyber threats is not limited to the malware, APT, but it is broader. A broader classification includes cyber espionage, cyber sabotage, and many others of disruptive cyber threats [191]. Furthermore, states are suffering from vulnerability where cyber defense technologies are not capable to protect state infrastructure from these wide range of cyber threats despite the development with the cyber defense aligned with the capacity of all states to develop and replicate cyber threats. This complex mixture enforce states to belief in the strength important and weakness at the same time. The cyber space is needed to be more peaceful space and at the same time individual states want to utilize it for more enforcement against its opponents.

The entanglement approach presumes each state are welcoming the cooperation more than confrontation due to the achievement to the believe about strength and vulnerability. For that, state welcoming the cooperation in cyber. This assumption need to be followed by practical steps in the real practice [192].

Trust Building for the (State to State) Entanglement

Transforming deterrence by entanglement to practical steps between states need tangible actions. The mutual interest is not enough to assure progress between states, for that, there is a need for developing mutual trust aligned with the mutual interest of making peace and cooperation in the cyber space.

some of the practical actions that can be initiated between (state-state) cyber deterrence by entanglement approach is like:

- An official high level members from both states to be nominated for responsibility of any critical cyber incidents and working more closer.
- Sharing information about cyber threats and threatener, via agreed mechanisms and trusted communications channels. It could be via intelligence community channels or other trusted governmental institutes.
- Forming a technical teams for closer technical work in the case of challenges in issues like digital forensics, reverse engineering or any other technical related issues.

Deterrence by entanglement as per Joseph Nye [193] is more of "Self deterrence" and it could be as a result of mis-perception between both actors within the conflict. The problem of mis-perception between both actors in cyber conflict is a complex issue and to raise the level of perception need an inside information about each state intention. Each state need more complete and accurate information about its opponent to reduce the level of uncertainty. Raising the transparency and exchange of information was there within nuclear deterrence during cold war between both US and soviet. Both states has exchanged information about each other nuclear intention more closely. This is not just exchange information but more related to the issue of transparency between two states. This exchange was the key to know about each other threat as well as a more deep signal about intention to cooperate rather than confront.

In cyber, the ambiguity about threats as well as vulnerability is high and at the same time each state attempt to hide any information about its cyber program and treat it under the classified information. This lead to a situation where states doesn't know what opponent is carrying as a threat and intention of utilizing the threat or not and this is where mis-perception play the role in deterrence. Essential issue like mis-perception between both actors in cyber conflict will not help to achieve any sort of deterrence and understanding of each other intention aligned with feel of mutual debilitation [194].

Assuming high probable success for the deterrence by entanglement strategy does not mean that other deterrence approaches are not essential for the state aiming to develop its cyber deterrence policy. This high probability is reflecting the nature of cyber space and challenges surrounding conflicts in cyber. Issues like (attribution, lack on norms,,,etc) give the entanglement approach more acceptance between two states aiming to cooperate compared to other deterrence approaches. Moreover, it will test how serious both states (A) and (B) to cooperate closely in preventing furthering any escalator cyber confrontations. The scenario is like state (B) is more advanced in cyber security technologies compared to the State (A) and in this case and by working more closely between (A+B), it could make a better progress in tracking red teams.

In summary, entanglement approach is closer to the cooperation between both states due to lack of credibility efficiency, fear from escalation and for mutual benefits. Another advantage, it could help to identify if state (A) stand behind the malicious activities or it is not the state. Entanglement approach will reduce the uncertainty between both adversaries and will examine seriousness of cooperation between both states in reducing the cyber threats. Next section objective to present a case study that explain the nature of deterrence entanglement and the motivators for both adversaries and the expected gains.

6.2 Motivational Case Study

China became known as the second largest world economy and at the same time it is a nuclear state. Moreover, China is the second largest defense budget in term of spending and this strategic and international position give China another strength in the deterrence calculation. Deterrence rely on threat and promises and not limited to these two factors when deterrence strategy between superpower like China and USA. China with its economical and military position in the international arena have the capacity to play with the factors of threat and promise similar to USA.

Another dimension in the China cyber power is the capacity of its cyber army. China has developed its cyber hacking army and recently has admits that it has developed this army and there are many units working on the same mission despite denying this claim for a long time. However, it is for the first time China admitted and then it was in the PLA publication called "The Science of Military Strategy." [200]

So, cyber confrontation between two states China and USA is another scenario compared between USA and Russia. For that, what could suite china decision maker could not suite Russia and similarly what could encourage USA for cooperation could not encourage Russia.

Dependency, Cyber Defense, China and United States:

Cyber space has become more critical for all states sectors of government, commerce, intelligence, military, academic, and not limited to many other public services. Unites states compared to many other states is highly depending on cyber space and it is the preferable medium for communications and many aspects of social life.

The more critical part in the US case is that the American military is also highly dependent and relying on plenty of global cyber networks consisting of 15,000 local area networks and more than 7 million computers connected to each other over more than 100,000 telecommunication circuits. These systems and networks are spread all over US bases around the world. The scary point, these cyber infrastructure process and transmit classified and unclassified, secret and the top secret information reflecting daily ongoing administrative tasks and not limited to the fighting operations [201]. Just to imagine that hackers successfully reach the information related to the military plans, capability, and different intelligent operations. This is information and just need to think about consequences if Chinese hackers get to such information.

The figures about US and its military usage of cyber technology is published on 2009 and we can estimate the growth in utilization new technologies. Yes, adopting new technologies give US and its military a step ahead in superiority compared to other adversaries but at the same time this reliance cause to increase exploitable vulnerability which aids cyber adversaries another superiority against US.

Deterrence by Entanglement, Why?

The aim of cyber deterrence policy is to discourage state opponent from starting or pursuing ongoing conflict and this can be via convincing that if state (A) continue on threatening state (B) there will be more to lose than to gain. This can be practiced by different deterrence approaches. First, deterrence by denial where state strengthening its cyber defensive capability, and this will prevent any success of the attack or get frustrated. Second, deterrence by punishment where state (B) threat its opponent with a massive cyber retaliation benefiting from its cyber offensive capabilities. Both deterrence by denial and deterrence by punishment need further credibility both in offensive as well as defensive. On top of these two approaches, state need to communicate clearly about its intent and demonstrate its ability to use this capacity.

Cyber deterrence by denial can work in reducing the threat from known cyber vulnerability via hardening cyber defense controls. This will keep deterrence by denial (Maximizing) the cost of attack from attacker prospective and (Minimize) the possibility of success. But still this approach is not capable to deal with unknown cyber threats. Advance Persistence Threats (APT) or Zero-day attacks where states challenging each other. So, this approach is not sufficient enough to deal with state cyber adversaries [195].

Cyber deterrence by Punishment also can work but with a lot of challenges. State can threat to retaliate in kind by reverse cyber-attacks to the suspected state with massive and replicated cyber attacks. In case of China and US, approach like deterrence by punishment is not highly expected to work due the power of both state plus capacity and capability aligned with the willingness. But, another way around the ongoing cyber confrontation will affect both of these two superpower states. For that, pursuing with not approach to deter cyber threat between both states is more of escalation and ongoing cyber escalation between two credible states consequence ongoing mutual loses reflecting mutual debilitation in cyber defense.

The problem with both approaches that State (A) can continuously maintain that cyber attack came from non-state actors or other red teams and they are acting upon their own sense of corrupt understanding about protecting nation or country. So, these cyber attacks is not on the any official orders by the state or the governmental agents. In addition, there is no clear or solid cyber evidences confirm that attack coming from State (A) and this is what is happening with our case in this chapter. China keep claiming that cyber attacks are not sources by its official agents and there is no evidence for this. From real world practise it is not easy to identify DDoS attack from source having IP address coming from china domain and this IP address under the responsibility of any Chinese agents. This technical complexity need a closer approach that help exchanging information between both States (A) and (B).

Credibility of USA as well as China is there [196] and fragility in cyber space also there aligned with willingness between both states for challenging each other[198]. The most important issue need to have more attention is the mutual benefit and the calculation of gaining and loses between both states. Aligned with the credibility of both states is the complexity of each other geopolitical situation that both superpowers have sort of interest to benefit each other and balance between cooperation and confrontation. Some can argue that China cyber threat is more of stealing information not destructive compared to Russian cyber threat. Answering this argument is possible: Stolen information is valuable and it has helped china to enhance its economy and political situation and at the same time reflect damage to USA business as well as strategic operations.

It is indispensable to understand motivators for selecting cyber deterrence by entanglement as another approach without replacing other deterrence approaches (denial, punishment and norms). For that, in this chapter the attempt is to explore entanglement as an effective deterrence strategy in deterring cyber threat especially between superpower.

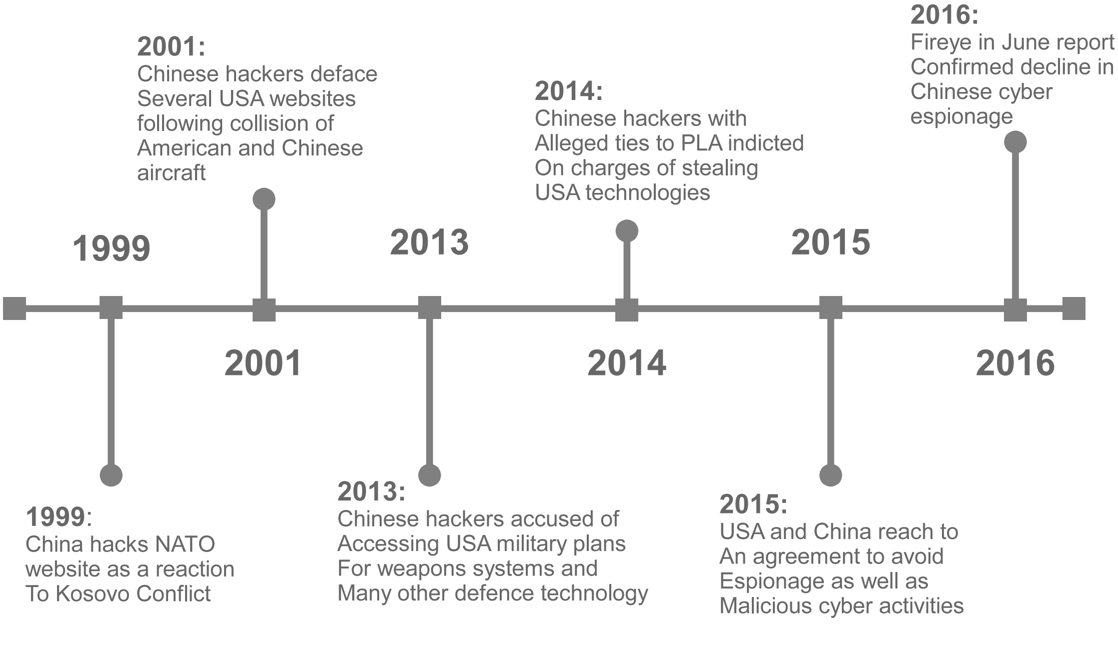

2001:
Chinese hackers deface Several USA websites following collision of American and Chinese aircraft
2014:
Chinese hackers with Alleged ties to PLA indicted On charges of stealing USA technologies
2016:
Fireye in June report Confirmed decline in Chinese cyber espionage
1999
2013
2015
2001
2014
2016
1999:
China hacks NATO website as a reaction To Kosovo Conflict
2013:
Chinese hackers accused of Accessing USA military plans For weapons systems and Many other defence technology
2015:
USA and China reach to An agreement to avoid Espionage as well as Malicious cyber activities

Fig. 6.1 China vs USA Cyber Espionage Timeline [197]

It is known that USA and China are on the top of list as first and second largest world economic as well as military budget. International strategic position for both states as superpower is an exceptional context compared to the relation between USA and Russia. For that, relying on both approaches (Denial-Punishment) of traditional deterrence is difficult to work efficiently in deterring cyber threats.

Balancing the belief about strength and weakness (vulnerability) within cyber space is a core factor that can stimulate rational calculations of both actors to bring them together with new approach for a first step of cooperation. The nature of cooperation is based on self deterrence as China and USA confirm they will not get involved or by knowingly support any cyber attack against its opponent. So, this self deterrence to assure no cyber espionage or any semi cyber crimes will be sponsored by the state against another state and the same with adversary. This is where self deterrence or deterrence by entanglement can begin.

The selected case study is the best case that reflect the situation where both states are having the intention to cooperate and at the same time have the fear from its opponent. Entanglement approach bring both states to first step of guessing the depth of water between actors and then build upon this approach another closer agreements or another norms to assure demilitarization in cyber space.

Plenty of strategist claim that the mission of cyber-attacks sourced from China is to steal secrets from foreign companies and government. Reasons beyond this attack is differ from political espionage to corporate espionage and everybody does the same thing with slight differences. The argument here, it is difficult to limit Chinese cyber capacity is for only political or economic espionage as it can be utilized for different destructive mission while the capacity are there and ongoing get developed [199].

China and USA Cyber Agreement

During the state visit of China President Xi Jinping on 24-25 September 2015, Chinese president and USA president stood together and declared that both state USA and China will not conduct or support any cyber enabled theft of intellectual property and it is including trade secrets or any other confidential business information.

President Obama said, “I raised, once again, our serious concerns about growing cyber threats to American companies and American citizens. I indicated that it has to stop.” Moreover he said “The United States government does not engage in cyber economic espionage for commercial gain, and today I can announce that our two countries have reached a common understanding on a way forward” [203].

Chinese president has confirmed that the two countries would not knowingly support any such practices and both states will remain strict to the norms of behavior within the cyber space. President Xi Jinping said on his speech September 2015, “The Cold War has long ended. [China and the U.S] should make joint efforts to build a new model of major-country relations between two countries, and realize non-conflict, non-confrontation, mutual respect and cooperation" [204].

Despite a high level of uncertainty surrounding this agreement and many could argue about the mutual commitment but this deal has reduced the risk heat of cyber threat between both states and establish sort of bilateral trust. What is confirming remaining uncertainty is president Obama announcement and his warning "We will be watching carefully to make an assessment as to whether progress has been in this area" [205] and White House has released in general what has been agreed between China and United State regarding this particular issue. Below the list a briefed of what has been published in White house official website [202]:

- Both agreed on timely responses should be provided and agreed to cooperate in a manner reflect to national laws and other relevant international obligation, investigation and collecting cyber evidences and mitigate suspicious malicious cyber activity and both agreed to update each other regarding investigation as appropriate.
- Both sides agreed to that neither country will conduct nor knowingly support cyber enabled theft of intellectual property including trade secrets or any other confidential information.
- Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyber space.
- The United States and China agree to establish high level joint dialogue mechanism on fighting cyber crimes and other related issues.

One year after the agreement, FireEye published a technical report in July 2016 claiming that the number of cyber attacks compromising US networks by Chinese attackers has dramatically dropped from 60 in February 2013 to less than 10 in May 2016 [206] and this give a positive progress in Chinese cyber threat reduction.

Absence of evidence is not the same thing as evidence of absence and when a technical report from a specialized company like FireEye [206] confirmed reduction in cyber attacks as well as a strategic research corporation like RAND confirm that this agreement is a good first step in reporting the advantage to achieve this agreement. Scott Harold on his report mention that after many years of suffering of losses costing US billions of dollar as a consequence of economically motivated cyber espionage [207] sourced from China.

As discussed above, the general economical and military situation of both states (China - USA) and complexity of geopolitical situation between both states. The need for new approach of deterrence became necessary.

From China perspective, this agreement may reflect what is president Obama confess that USA are not involve in any cyber espionage and it is willing to go for further cooperation and at this point China leadership thinks optimistically to welcome and response positively.

From USA perspective, this agreement is a vital opportunity to test the Chinese government intension in cooperation and willingness. Usually Chinese denying the cyber espionage or any other attacks. But, this agreement will help to test compliance with the agreement and possibly to deter cyber espionage. Moreover, it will help for furthering the cooperation especially in developing another norms for shaping State Cyber behavior between State to State.

A high level of agreement between USA president and Chinese President reflect mutual believes of both leadership regarding seriousness of Cyber Threats and at the same time importance for both states to keep cyber space functioning despite different assumption regarding commitments for transferring agreement to a practical actions. So, this agreement should be considered as first good step in the right direction, Yes it is not the final step for solving wide problem like cyber confrontation.

This agreement has been developed between optimism and at the same time skepticism despite a different claims that 2015 cyber agreement between Beijing and Washington is difficult to achieve its objectives but our point here is to response to a very deep question which is, What has stimulate USA and China to sit and agree to sign this particular agreement? It is because of mutual believe of debilitation and the best optimistic and strategic option is to go with an approach of entangle. This approach may will reduce the intention of confrontation and it does [206].

The agreement is a result of mutual assured debilitation and reflecting the practice of the deterrence by entanglement approach. It aids in maximizing rather than minimizing the cooperation and a good example for other states within international arena to work closer to achieving the objectives of demilitarizing cyber space.

6.3 Entanglement Model for Cyber Deterrence

Cyber deterrence main objective is to discourage state cyber adversaries from starting or pursuing ongoing cyber threat. As discussed earlier there are plenty of challenges weakening success of deterrence in cyber space like lack of attribution, deniability, misperception, uncertainty about adversary intention, and many other challenges discussed within literature review Section 3.8. For that, we assume deterrence by entanglement will assist in resolving these challenges. Then by resolving these challenges, the hope of achieving successful cyber deterrence probably will increase.

Deterrence by entanglement approach can be more of self-deterrence where each state at certain degree should accept to reduce the intense of cyber-attacks at the beginning for its benefit and then for its opponent to develop mutual trust and to accept to change the strategy of attacking by cooperation. On top of this, state need to communicate clearly about its intention not to use its cyber threats capacity as a first step for developing a trust ground for next step of cooperation.

Scope of Entanglement Model: *scope of this model is to analyze the deterrence by entanglement approach and the expected outcome from this approach in deterring state cyber adversaries.*

Cyber deterrence by entanglement model analysis begin by setting up the cyber deterrence model and just to remind our self about the credibility of cyber threat model as well as cyber escalation model analyzed in previous chapters. Within previous two model of analysis there is no clear willingness for cooperation between states due to complexity and different perceptions between cyber adversaries. Not withing the model between two credible states and its cyber threat nor with escalation approach as well.

The payoffs for State (A) and State (B), respectively, are noted as (A_i, B_j) and this payoff assumed in order:

- State $(A_i) = China = a_1 < a_2 < a_3 < a_4$
- State $(B_j) = USA = b_1 < b_2 < b_3 < b_4$

  Both actors within the model in figure 6.3 keep changing between two strategies either to attack or not to attack and going to give notation like:

- Strategies **(c)** = Cooperate/No Attack or **(n)** = No cooperation/Attacking

  In addition, the expected payoff for both sates within deterrence by entanglement model will take symbol:

- E_A= Expected payoff to State A for choosing **(c)** or **(n)**
- E_B= Expected payoff to State B for choosing **(c)** or **(n)**

  Then, the analysis between state (A+B) within the model will be following mixed

- p = Probability that, State B choose **(c)**, given State A prior choice of (**n**)
- q = Probability that, State B choose **(c)**, or given State A prior choice of (**c**)

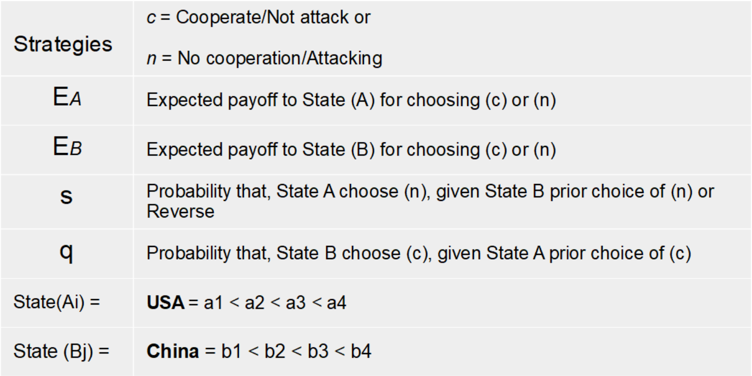
- r = Probability that, State B choose **(n)**, given State A prior choice of (**c**)
- s = Probability that, State B choose **(n)**, or given State A prior choice of (**n**)

In accordance with the rules of the entanglement model, player should restrict to the model general rules:

- Each player (State), either (A) or (B) do choose between ($n = Attack$) and ($c = NottoAttack$),
- It is 2 player model which consequence four strategic payoff within the game for both states either for US or China.
- Both states (China or USA) at a certain degree would prefer to entangle (cooperate) and priority (c, c) which reflect best outcome for both states: (a_3, b_3)
- One state may not cooperate (c, n) and (n, c) and it is reflect best outcome for the state that are not willing to cooperate (a_2, b_4) and (a_4, b_2) but will not sustain as best outcome.
- Both States are not willing to cooperate (n, n) and this situation will be the worst outcome for both states (a_1, b_1) which will reflect $Mutual\ Cyber\ Confrontation$ (escalation).

Cyber deterrence by entanglement model is also based on cyber deterrence game model consisting of two states as players and involved within a cyber conflict. Both states can select between two strategies either to *not to attack* (*Cooperate*) or *attack* which reflect situation of (*Not to Cooperate*). Deterrence model are mainly relying on analyzing *Gain* and *Lose* as a reflection of *Cost* shaping gain and lose from each actor prospective. Deterrence by entanglement approach mainly working on explaining situation that assumed to help in bringing both opponents to the table. Entanglement model manipulating with the calculating cost and benefit between these two strategies (n) or (c).

With the same logic of cyber deterrence model where probability of preemption from both actors point of view are with high probability due to different reasons reflecting the nature of cyber space and many other (State-State) domains conflicts. Both States are rationally trying to maximize their payoffs within cyber conflict and when conflict begin there will be lack of information about attacker. After period of time some information is gathered as a result of digital forensic technologies and many other related analysis. During attack, state (B) start pointing over the attacker state (A) and opposing with deniability from state (A). In this case, we assume attribution is there and reflecting frequent cyber attacks that has occurred between both states. In this situation, deterrent (B) aiming to bring the attacker (A) to the table for furthering the behaviour of cooperation rather than sustaining on confrontation mode. Cooperation is a self deterrence where adversary believe that cooperation will give more of $Gaining > Lose$.



Strategies	*c* = Cooperate/Not attack or *n* = No cooperation/Attacking
E*A*	Expected payoff to State (A) for choosing (c) or (n)
E*B*	Expected payoff to State (B) for choosing (c) or (n)
s	Probability that, State A choose (n), given State B prior choice of (n) or Reverse
q	Probability that, State B choose (c), given State A prior choice of (c)
State(Ai) =	**USA** = a1 < a2 < a3 < a4
State (Bj) =	**China** = b1 < b2 < b3 < b4

Fig. 6.2 Cyber Deterrence by Entanglement Model Definitions

In modelling cyber deterrence by entanglement approach we will consider two states with opposed interests within cyber space. Each state is *maximize* attacking (cyber attack) expecting gaining and in some attacks it is gaining from attacker prospective but cyber retaliation is not predictable which could be more sever to the attacker from the first attack due to consequence of the retaliation attack. When calculating *gain* achieved via first attack and the *lose* consequence from retaliation, a rational decision are needed. Rational decision is expected to be $Minimize$ attacking strategy and preventing pursuing attacking adversary. This decision is a consequence of fear in continuing Losing more than any gaining from confrontation with current adversary. This rational calculation is the ground for stimulating self deterrence.

Cyber confrontation at this stage between both superpowers (China and USA) reflect the intention of confrontation rather than cooperation. It is because each state believe separately can manipulate with its adversary and cause more lose than gain within cyber space. The strategic situation between both states reflect $Mutual\ Non-Cooperation$ and each state strategy:

- State (A) Assured Payoff $E_A = n > c$, and at the same time USA intention,
- State (B) Assured Payoff $E_B = n > c$

If theses strategies are continued, it will clearly not lead to any cooperation between USA as well as China and no deterrence will be expected to get establish. For that, one of both states need to spark the initiative to lead the entanglement process for establishing

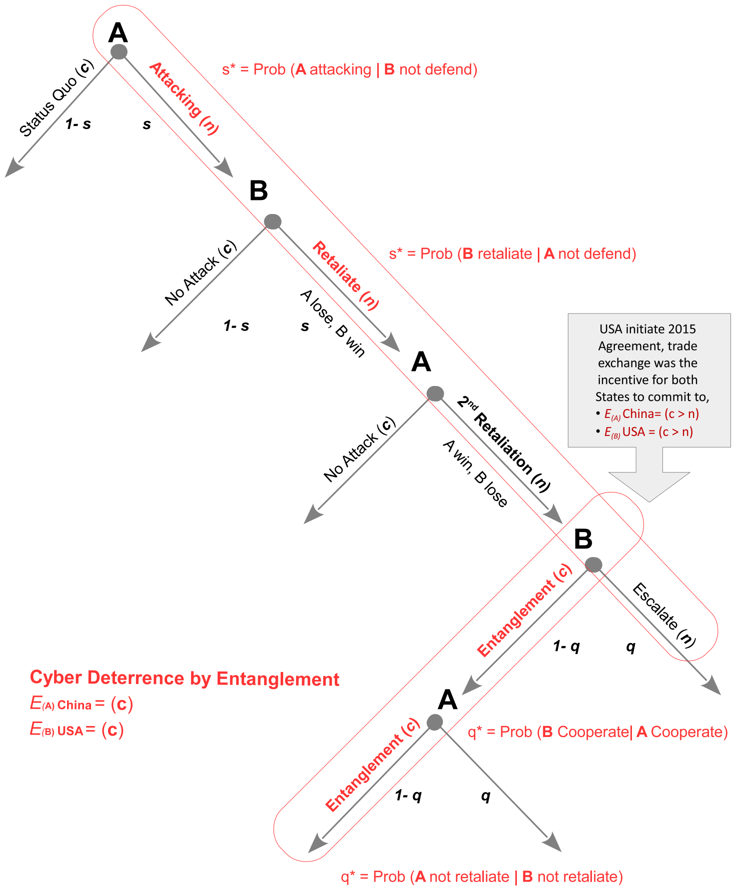

A
Status Quo (c)
Attacking (n)
1- s
s
s* = Prob (A attacking | B not defend)
B
No Attack (c)
Retaliate (n)
1- s
s
A lose, B win
s* = Prob (B retaliate | A not defend)
A
No Attack (c)
2nd Retaliation (n)
A win, B lose
USA initiate 2015 Agreement, trade exchange was the incentive for both States to commit to,
• E(A) China= (c > n)
• E(B) USA = (c > n)
B
Entanglement (c)
Escalate (n)
1- q
q
Cyber Deterrence by Entanglement
E(A) China = (c)
E(B) USA = (c)
A
q* = Prob (B Cooperate| A Cooperate)
Entanglement (c)
1- q
q
q* = Prob (A not retaliate | B not retaliate)

Fig. 6.3 Cyber Deterrence by Entanglement Model

sort of cooperation and it could be considered as a (Self Deterrence). The idea here, that the deterrent state approach its opponent via adding the cyber threat as one of negotiations agenda for testing the depth of the water of its opponent. Close negotiations about cyber threats and the need for further interaction between both States will help both player to justify the intention of opponent either to cooperate or not and pursuing the negotiation just a cheap talk. The negotiation should provide solid ground for mutual intention to allow the equilibrium to provide better profit for each player $(A)+(B)$.

Challenge with Entanglement model is the degree (the point), where both actors need to get convinced about his adversary intention to cooperate. Repeated cyber interaction via on going attacking and retaliation between both states might not be enough to stimulate the willingness for furthering cooperation decision due to lack of information about opponent willingness to cooperate and reduce the intense of cyber attacks.

In this case, the incentives between USA and China as both states are on top of list as economical power where each state need to keep exchange of business via cyber space running smoothly. As example, USA has amazon and china has Alibaba where millions of goods get imported and exported between these two states plus the global market.

Recall nuclear deterrence model, the certainty about threat of retaliation $E_B = (n) > (c)$ which high certainly will consequence mutual nuclear attack and mutual loses $E_A = (n) > (c) = LOSE > GAIN$. Pursuing strategy of nuclear attacking with high certainty of nuclear retaliation is not a rational strategy and will not lead to any optimization either to E_A or E_B.

But in cyber, certainty of retaliation and its success is possible due to vulnerability within cyber space. More specifically, when state know certainly that its opponent willing to change the curve of non attacking strategy to retaliate and cause more harm, it should calculate its next strategy. From both states point view, this situation is possible to occur. Yes, not all cyber attacks are equal in term of value and its relation to state national security. In this case, the general assumption here that China as State (A) with the model continuously committed to *Maximize* strategy of *Attacking* $(n > c)$ and in cyber space it is expected to reflect situation of winning the attack and achieve expected *Gain* within accepted cost of attacking aligned with gain.

$$E_A(n) = a_4 p + a_1(1-p) \tag{6.1}$$

It is more of *Gain* > *Loses* cyber attack and that is why State (A) strategically prioritize to keep *Maximizing* the strategy of cyber attack against its adversary assumed USA. In opposite, USA is a credible state in the cyber space and similarly have the interest to threat and cause *Lose* over its adversary presumed in this case as China. So, USA by repeatedly attacking Chinese cyber space will *Gain* via success these cyber attack but it seems China are not suffering as USA from cyber threat and this is because USA are more relying of cyber space in operating State infrastructure as well as its economy. USA by pursuing *maximizing* strategy of *attacking* expecting to deter China via threat of cyber retaliation would be successfully achieved by:

$$\text{Maximize } E_A(n) = a_4 > a_1, \tag{6.2}$$

China payoff by *Maximizing* strategy of cyber attack within cyber conflict with USA will be more of:

$$E_A(n) = a_4 p + a_1(1-p) \tag{6.3}$$

Both States (A) and (B) can maintain strategy of *Maximize* cyber attack strategy and moreover maintain success of this particular strategy within the model (6.3). Success of attacking via cyber space are highly expected as mentioned earlier and it is one of the cyber deterrence challenges. China expected payoff from attacking USA expected to be $E_A(n) = a_4$

and at the same time USA payoff expected by attacking China $E_B(n) = b_4$. So, correlation between possibility to success cyber attack and cause mutual ongoing loses between both states are the main point for stimulating entanglement and self deterrence. In caparison with nuclear deterrence this situation is not much likely to success due to logistic difficulties in proceeding second nuclear strike while in cyber is highly possible to success. That is why we assume in this model that both players at a certain degree should choose not to retaliate and begin a new approach can be titled as “Suspected Cooperation” which is more of mutual situation balance between optimism and at the same time skepticism. This situation is a result of different cyber confrontation between both actors (USA - China).

$$\text{Maximize } (E_B)Via = b_4 > b_1, \tag{6.4}$$

For that, USA payoff by *Maximizing* strategy of cyber retaliation within the conflict with China will end up look like more of:

$$E_B(n) = b_4 r + a_1(1-r) \tag{6.5}$$

Degree that has sparked entanglement approach is the expectation of getting more $Gain \geq Loses$ from this particular strategic exchanges. It could be argued that this approach via following $Minimizing(attacking)$ strategy and at the same time $Maximizing(Non-Attacking)$ within cyber space will work against the calculation of optimizing cyber threat credibility but in reality not. It is because following this strategic approach means to keep cyber defense as well as cyber offense functioning in place. *Maximizing not to attack* in cyber does not mean to remove state cyber defense and offense technologies but it means to keep it running for executing other missions like defense against other known cyber threats and observing cyber space threat for furthering threat analysis. Cyber defense as well threat of cyber offense will keep serving and there is no correlation between the decision of cooperation and these two strategies. Cyber defense are assumed to function against known cyber threat and cyber offense as well should be in place not for usage as it is risky to use it. Both, cyber defense and offense are supportive for state cyber deterrence.

Entanglement scenario between China and USA was during both players China and USA calculate the profit (Gain) from *Maximizing* strategy of *Not Attacking* that will consequence expected outcome for China $E_A = (c) > (n)$ and at the same time USA calculating the profit from pursuing *Maximization* the strategy of *Not Attacking* strategy $E_B = (c) > (n)$. It should be equivalent, parallel and at the same time between both players. At this period of mutual maximization of $(Cooperation)$ via *Not Attacking* strategy, the degree that sparkling the entanglement scenario is located and it will replace confrontation to a cooperation between

China and USA. It is a reflection of China Maximizing $E_A = (c) > (n)$ and at the same time and equally USA Maximize $E_B = (c) > (n)$. Here is where situation of optimism and skepticism begin, the expectation between both states will probable progress more of cooperation. The first step of cooperation can be via political negotiations and then to get followed by technological and practical negotiation to implement what has been agreed upon.

Entanglement model is looking to the probability of mutual cooperation between two states and it reflect the probability of $[q]$ and what is driving two player to maximize the probability of $[q]$. At the beginning of node three within the game tree Fig. 6.3, behavior of United States as State (B) has moved from pursuing challenging China as a State (A) to attempt to approach via another approach that may return to maximize the *gain* outcomes for the benefit of United states itself. Practical consequence of USA changing its strategy and behavior begin by initiating a negotiation process before Chinese president state visit to add Chinese cyber threat to the presidential visit agenda.

At this particular point within entanglement model, game has changed from ongoing cyber confrontation to attempt initiating negotiation between USA and China during China presidential visit. At this point, USA has taken the initiative with China and scenario is to test Chinese willingness to cooperate with USA regarding cyber threats. The expectation from USA that China expected to *Maximize* strategy of cooperation and *Not to Attack* and USA by taking the initiative can be assumed is willing to cooperate with Chinese and coming closer to negotiate the possible solutions for the cyber threat challenge.

USA by following this approach will get more closer involvement with Chinese government about solving the cyber threat dilemma. Chinese usually deny any claim against Chinese government and sponsoring the cyber threats. In the case of Chinese resist any closer negotiation will give a clear signal that China is still denying any sort of cooperation. But, what has happened is the opposite and China has *Maximize* the *Cooperation* and agreed to involve cyber threat within presidential visit agenda.

In addition, one of cyber deterrence by entanglement practice can be via agreeing to exchange information between USA and china about cyber threat sources and its full attribution. This will reduce the deception practise between both adversaries and raise the level of trust between (A) and (B) within cyber space. USA can involve China with technologies and experts that help in digital forensic or many other kind of technologies supporting attributing cyber attacker

Just for comparison, mutual *maximization* of *Attacking* strategy to a mutual *maximization* of *Not to Attacking* strategy within cyber space between two credible state (USA and China);

$$\text{Maximize } E_A(c) = a_4 q + a_1 (1 - q), \tag{6.6}$$

$$\text{Maximize } E_B(c) = b_4 q + a_1(1-q) \tag{6.7}$$

China strategy at the beginning of entanglement point within the deterrence model (game tree) are reflecting;

$$E_A(c) = a_3 \tag{6.8}$$

USA payoff by *Maximizing* strategy of cooperation within entanglement model with China will look like more of:

$$E_B(c) = b_3 \tag{6.9}$$

It is because a_3 and b_3 reflecting more of wining but it is not the ultimate winning due to slight amount of lose within defense and the investment in strengthening cyber defense and offensive capabilities.

Entanglement approach has resulted high level of agreement between USA president and Chinese President. At this point and when both presidents agree to go for more cooperation and reduce the deception surrounding cyber threats via raising the certainty of cooperation. The agreement has reflect mutual believes between both leaders regarding -possibility- to go one step closer and attempt with caution to cooperate as it is for both states benefit to keep cyber space functioning. Despite assumptions about China commitments for transferring agreement into practical steps. This agreement should considered as first good step in the right direction, Yes it was not a final solution for a wide problem like deterring cyber threats but it is a good step and might work in other cases as well.

6.3.1 Entanglement and Cyber Deterrence

It is because of the cyber space uniqueness and the challenges of cyber deterrence been discussed in section 3.8 the assumption of entanglement approach for deterring state cyber adversaries been raised. The reasons behind this nomination is that the entanglement approach will help in mitigating these challenges. As example, one of the biggest challenges in cyber space is that state can deny any claim against and its response can be like these cyber attacks are sourced by individual attacker. These attackers are influenced by other political conflicts but not hired by state government.

In cyber space, state can hire any red team to initiate different cyber attacks for the purpose of causing damages to its adversaries expecting this approach might deter its cyber adversary while its adversaries can do the same scenario without any worries. Practice like this will keep state in a serious challenge to attribute the attacker as well as defend against its unpredictable cyber attack. More changeable to deter these attackers. This complex situation seem influence USA to think little ahead via approaching Chinese cyber threats via entanglement. What have been observed in USA approach with China is the a semi-cooperation between two well known superpower. These two States have enough cyber capacity as well as threat credibility. If both, credible states (China and USA) sustain confronting each other state, the consequence is mutual damage *Lose* $>$ *Gain* due to mutual debilitation within cyber space. The scenario of continuous confrontation between China and USA will be like China Maximizing attacking $E_A = (n) > (c)$ and at the same time USA pursuing *Maximization* attacking $E_B = (n) > (c)$. Consistently pursuing this strategy from both actors will clearly result to cyber confrontation which will consequence to mutual continuous loses. So, rather than pursuing on persistent loses state will optimize deterrence via furthering cooperation rather than confrontation. Entanglement model as an approach working parallel with more cooperation with state adversaries.

$$Maximize\ Prob\ of\ Cooperation \parallel\ Cyber\ Deterrence\ by\ Entanglement \tag{6.10}$$

Which mean:

$$Maximizing\ Prob\ of\ (c) = Good\ Deterrence\ by\ Entanglement \tag{6.11}$$

Deterrence by entanglement model has explained the situation when the two actors go for conflict cyber conflict while both actors are benefiting from each other and need to exchange plenty of operations within cyber space. Within the model, each state attempt to drive its opponent to more cooperation rather than confrontation. The model has produce sort of optimization in reducing heat of exchanging cyber attacks begin when both adversaries believe rationally it is *Gain* when state (B) take the initiative and signal its adversaries about its willingness to cooperate. Rational calculation should look at the cooperation as gaining not losing because pursuing attacking strategy will consequence *Lose* $>$ *Gain* despite assumption of attacking (threat of retaliation) strategy as dominant in Nuclear deterrence but in cyber the concept might not work similarly.

Cyber deterrence by entanglement model has assumed two rational state as a actor and calculating threat of credible cyber threat that affecting state cyber space and both player reach to a believe of guessing each other intention to cooperate in the cyber arena for the benefit of each state itself via reducing cyber threat from its credible opponent and commit not to involve government with any support or involvement with any cyber operation that might cause any damage to adversary [208]. This belief has been achieved after repeated cyber confrontation.

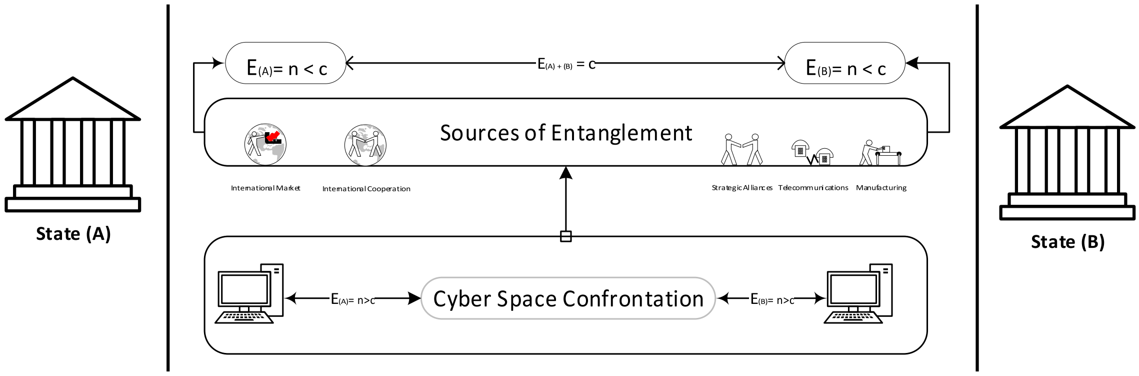


Fig. 6.4 Cyber Deterrence by Entanglement Mode

Figure 6.4 show how each states (A + B) has initiate the model with $E_A = n > c$ and $E_B = n > c$. At the beginning, both players commitment to confront adversary in cyber domain that the state by itself suffering from weakness has result lose. On the other hand and after signing the agreement, both states has changes to $E_A = n < c$ and $E_B = n < c$ and this simultaneous strategic commitment helped both player to achieve self deterrence and cooperate and gain sort of reduction in cyber confrontation heat. Yes, it can be argued that this situation might not sustain but the respond to this argument is that the approach can be repeated again expecting to optimize first deal. While the opposite of deterrence by entanglement is to minimize any intention of cooperation between adversaries and this is not in the benefit of each state. Minimizing probability of cooperation within the model is not parallel with cyber deterrence.

$$Minimizing\ Prob\ of\ Cooperation \nparallel Cyber\ Deterrence\ by\ Entanglement \tag{6.12}$$

Which mean:

$$Minimizing\ Prob\ of\ (c) = Bad\ Deterrence\ by\ Entanglement \tag{6.13}$$

By reach the believe about the need for self deterrence and entangle with state adversary, each state will minimizing probability of cooperation in cyber space between states correlate directly to develop uncertainty between adversaries. This uncertainty will consequence to demolish any deterrence attempts because cyber deterrence to begin need slight margin of cooperation for the purpose of sparking the deterrence by entanglement model.

6.3.2 Cyber Mutual Assured Debilitation

One of the cyber uniqueness is the spread of vulnerabilities all over state critical infrastructure and systems operating these infrastructure. This factor with ongoing optimization will help state -Maximizing- the cost of success cyber attack for the attacker. But, still in cyber there is a chance to win via re-engineer the same cyber threat to bypass the defense solution develop after the first wave of attacking. First attack from state (A) with high probability of (Success > Failure) = State (A) Best strategy is to keep attacking (B). Then, State (B) has enhanced its cyber infrastructure against known cyber threats. In this situation, the second attempt by state (A) to attack (B) will not be the same as previous attempt due to enhancement conducted by the (B). The next attempt will change the calculation between both adversaries and the situation is mainly from State (B) as a deterrent state and continuously attempting to deter its adversaries:

- Maximize the cost of cyber attack = (A_j)
- Minimize cost of cyber defense against A= (B_i)

The gap between cyber vulnerability in state (B) and optimizing these weakness is where state (A) can success its attack. This is where debilitation in state cyber space and its strategic situation begin. State (A) vis-to-vis State (B) is superior in detecting cyber vulnerability and utilize them and cause the lose within the equation of cyber conflict. In opposite, State (B) superiority in make difference with cyber conflict calculation is via detecting its vulnerability and enhance to a level that assure for the attacker $E_A(n) = Lose > Expected\ Gain$. Then when State (A) attempt to repeat the attack against (B) will discover that $E_A = (Cost\ of\ attacking) > (Expected\ Gain)$, and the rational assumption here is to defeat (A) from pursue attacking (B) due to enhancement made by (B) in the cyber defense. The challenge with (B) is to get complete and accurate information about the intention of (A) about attack type and the target of the next attack.

Challenges that preventing development an effective and comprehensive cyber deterrence strategy [138][139] are not limited to issues like attribution, Information sharing between states, legal and international institutions, cyber threats and mutual perceptions. One of the nearest approach to resolve some of these issues is to progress in term of cooperation in exchanging information instantly between state-states about threats sources. Overall, superpower states like China, United States, Russia and many other share the same situation within the cyber. It is a big concern about the vulnerability of cyber space to the offensive technologies and sadly to confirm weakness in cyber defense. Developing cyber defense capacity and at the same time offensive for threat of retaliation might help state in reducing cyber threat heat but still not bring cooperation from adversaries. In the situation where weakness are mutually and there are share interest in maintain cyber space for exchanging benefits states could approach opponent with more of cooperation signaling [194].

In summary, states growth in relying on cyber space in operating plenty of critical sectors and at the same time rely on a vulnerable cyber technologies should enforce the rational calculation to pursue the cooperation strategy rather than challenging and confrontation. States may not to confess easily about the vulnerability of its cyber space but the truth is truth and in practise cyber space are vulnerable and in the case state willing to reduce the heat in cyber space (state-state) conflicts.

6.3.3 Entanglement and Cyber Cooperation

Looking to both state -USA and China- presidents speeches and analyzing the signals within the context. The impressions about willingness to cooperate despite the skepticism are there and it was clear when:

President Obama said, “I raised, once again, our serious concerns about growing cyber threats to American companies and American citizens. I indicated that it has to stop.” Moreover he said “The United States government does not engage in cyber economic espionage for commercial gain, and today I can announce that our two countries have reached a common understanding on a way forward”. Particularly, at this point President Obama trying to maximizing the strategy of cooperation via $E_B = Attacking \ < Not \ Attacking$.

Simultaneously, when President Xi Jinping said on his speech in September 2015, “The cold war has long ended [China and the U.S] should make joint efforts to build a new model of major-country relations between two countries, and realize non-conflict, non-confrontation, mutual respect and cooperation” [204] response and agree to what president Obama clearly mentioned. This speech clearly reflecting the willingness of leadership to cooperate $E_A = \ Attacking < \ Not \ Attacking$.

So, these two speeches reflecting both state leadership intention for *Maximizing* Cooperation more than confrontation. Yes, there are a Grey zone about the degree of cooperation and how close involvement to achieve but the intention of cooperation has been agreed to develop it. Moreover, what is interested in selecting China vis-to-vis USA case is that both states are known as a superpower in the international system. Both states credibility in other domain was not sufficient in developing any deterrence against cyber threat, which mean the approach of cooperation was expected to maximize the expected outcome for both states (E_B) and (E_A). In addition, the atmosphere surrounding the presidential declaration aligned with approval for signing agreement was highly probably positive. Moreover, the road-map

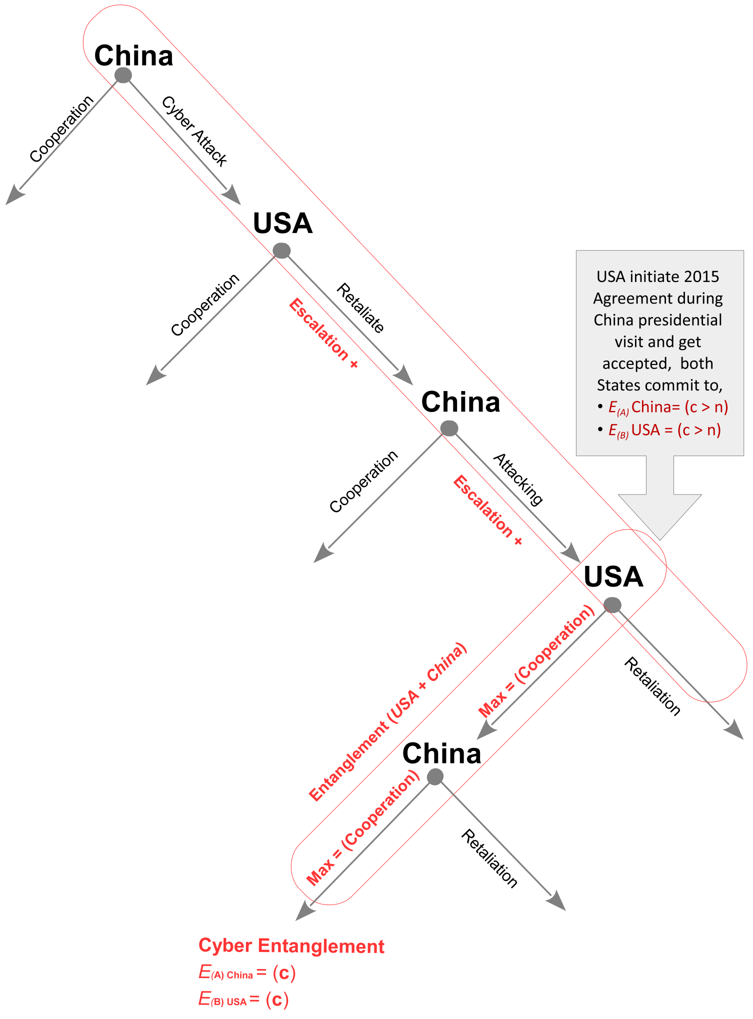


Fig. 6.5 Cyber Deterrence by Entanglement Case Study

of developing closer cooperation from the both states presidents and the expect benefits for maximizing each other outcomes.

Cooperation payoff reflecting both states China (A) and USA (B) intention to come closer for the aim of maximizing other mutual benefits as the figure 6.5. The situation of mutual cooperation in State-State cyber conflict and possible to success when:

- State (A) = China Committed to E_A= $c > n$, Equally and the same time USA,
- State (B) = USA Committed to E_B= $c > n$

In concluding this section, entanglement approach has worked in bringing two superpower (USA and China) into more of cooperation reflecting credible cyber threat. This approach can be assumed as self deterrence before deterring the opponent. Each state looking for maximizing the benefit from cyber space and reducing the cost of loses. In addition, each state relying on cyber space in exchanging different types of business.

6.4 Strategies and Lessons for Entanglement

In summarizing the lessons learned from the cyber deterrence by entanglement model, State will need to know that having credible cyber threat will not be sufficient enough to threat its opponent with massive retaliation and expect it to get deterred. In other hand, it does not mean that state need to preempt its adversaries with offensive cyber attack to assure preventing cyber attacks expected from its adversaries. Neither approaches not enough to bring state cyber deterrence closer to achieve its objectives.

But, the idea beyond entanglement model is to bring both adversaries to another approaches of semi-cooperation. Entanglement are mainly for the credible state and need to have certain criteria to assure achieving its mission.

Despite this assumption, in real world nobody really knows exactly how advanced is the opponent and superiority in cyber could be measured form different perspectives and from different triangle. State can be superior in term of its cyber offensive capacity but not in defensive and this reflecting different reasons. The context of cyber deterrence by entanglement can work in one case where it cannot work in other cases and the lessons that can be summarized from entanglement model analysis is:

6.4.1 Cyber Deterrence by Entanglement Model General Lessons:

- Deterrence by entanglement assisting state in reducing uncertainty (trust) about its cyber adversaries and raise the expectation about the intention for furthering the cooperation.

- Entanglement approach help in reducing cyber deterrence challenges. As example, attribution and when state cooperate technically and share accurate and complete information means there is no trap and there is a willingness in cooperation.

- State need to look at share interest between state itself and the state opponent. This mean when stat get attacked by its opponent is like the opponent attacking him self. It is due to mutual loses between both states especially in cyber space.

- Deterrence by entanglement in cyber space can be approached when both adversaries agree to formulate senior level from exchange its cyber capacity in term of technology like cyber forensics and attributions tools. This top level cooperation will reflect to further the cooperation practises between mid level government like intelligence, military and concern institute.

- State should approach its cyber adversary with issues that have mutual interested with its opponent. The case between China and USA, both states are mutually interest in exchange business and clearly cyber space is essential space for this exchange and it should be sustain and more peaceful between both adversaries.
- Entanglement approach will help to investigate if there is any claim that State try to escape from. China was claiming that cyber attacks threatening USA sourced by Non-state actors but when both superpower approach cyber conflict with entanglement, they can work closely and exchange information semi opened to resolve and trace red teams (Non-state) and there will be no excuse for china as well as USA.
- Cyber deterrence by entanglement is more of self deterrence where state need to strength and keep observing its cyber space. Observation mission to understand the threats that might affecting state and at the same time estimate suspected threats sources.
- Deterring cyber threat by entanglement work technically when both adversaries agree to come closely to identify the threats expected to get resolved. Both states can cooperate approximately $\approx$ when the degree of conflict between both reflecting "no winning" and at the same time "no losing".

6.4.2 Entanglement and States Strategies:

Strategically, for developing threat credibility for the purpose of cyber deterrence state like USA should be prepared with cyber threat that is sufficient enough to develop the fear within adversary mind as well as China (B) should do. Readiness and preparedness strategies is a good strategy but need careful calculation to avoid any miscalculation. For that, USA in deterring China need commitment to strategies:

1. Minimize (p) : Maintain strategy of threatening China with cyber retaliation. At the same time not to give China any chance to success in any preemptive cyber attack via hardening USA cyber space security controls.
2. Maximize (r) : Keep maximizing the threat of attacking which expected to inject the fear from USA cyber threat and assure that for china cooperation is better than confrontation.

3. Maximize (s) : Remain maximizing the threat of retaliation and willingness to go for any further escalation aiming for enforce China into giving up within cyber conflict.

At the same time, from China (A) strategic position and for maintaining maximizing its credibility of cyber threat. China toward maximizing its benefits from the cyber conflict with USA it should sustain with strategies like:

1. Minimize (r) : China to keep attempting to minimize the probability of USA attack. It should keep $E_B = Gain \leqq Lose$ for any expect cyber attack.
2. Maximize (p) : Maintain maximizing strategy of threatening USA ($E_A = Attack > NonAttacking$) and this strategy assumed to inject the fear from China cyber threat.
3. Maximize (s) : China to remain strengthening the strategy of challenging USA within cyber space for assure credibility and to defend against USA cyber threat ($E_A = (n) > (c)$), despite ($E_B = (n) > (c)$) expecting at particular point USA will give up.

In achieving entanglement objectives, both States should work toward maximizing the cooperation from the strategic point of view of both adversaries. By maximizing cooperation both state might reach to agreement under the strategies reflecting both USA and China. and this what has happened in 2015 agreement. So, both state (A) and (A) should:

1. Minimize (q) : USA to maximize the strategy of cooperation (c) and expecting china probability to maximize probability of cooperation (c), China leadership believe that approximately $E_B \approx Gain = Lose$,
2. Maximize (q) : At the same time China to maximize the strategy of cooperation (c) and expecting USA probability to maximize probability of cooperation (c), that mean USA decision maker approximately to believe in $E_A \approx Gain = Lose$.

Cyber deterrence by entanglement approach has approved its capacity to bring two superpower (USA and China) in the table and agree to reduce the heat of cyber confrontation. After one year, the result has been confirmed by one of leader in the cyber security technology company called Fire-Eye [206] and also has been confirmed by top strategist USA institute RAND corporation [207] that the approach followed by USA has helped to progress in reducing China Cyber Threats. But, the question is whether it will be sustainable.

Chapter 7

Conclusion

Conflicts in cyber space are not limited to cyber security technologies, systems vulnerabilities or cyber offense solutions. It is a unique domain where there are different players (States-Non State) having different interests to achieve and different agendas to accomplish.

The Motivations for conducting this research is due to the weakness of Cyber defense as well as complexity of Cyber offense which is very difficult to utilize due to its difficulty in identifying the source of attack. Logically, deterrence is assumed to fill the gap between defense and offence. Keeping in mind, what is applicable in deterring first state can't be applicable to the second state and a careful analysis for cyber deterrence strategies in deterring (state - state) cyber conflict was the broader scope of the research. Then, research was narrowed to find out the best optimal strategy to help state develop its capabilities for the mission of deterring cyber adversary.

The methodology for conducting the research was done by following game theory as a tool for analyzing the applicability of cyber threat as a credible threat for punishing state opponent with massive cyber retaliation. Then, to analyze the conflict in the case of cyber threat as a credible punishment was not successfully efficient in deterring state adversary and both opponents prioritize to escalate the cyber conflict intense and attempt to wind down the conflict

After investigating cyber escalation, the attempt was to examine different approaches for the benefit of cyber deterrence. The examined approach was deterrence by entanglement and the analysis was trying to bring new concept into the deterrence strategies where both states are sharing interest issues that can be utilized to cool down cyber conflict.

7.1 Review the Contribution

Answering the core question about whether deterrence is going to work or not in the cyber space, it is more related to whom to deter, how to deter him, and what approach will fit the case? The context of deterrence in nuclear is different to deterrence in cyber space.

Challenges in cyber deterrence like uncertainty about attributing cyber-attack and diversity of cyber adversaries due to wide connectivity within cyber space does not mean that deterrence in cyber is not going to work or it is impossible. Cyber deterrence can possibly work and there is a serious need to invest in the attribution solutions where organization can efficiently attribute attacker.

Optimizing cyber deterrence following deterrence by denial strategy works partially and plays larger role in deterring known cyber threats. States need to harden the cyber defense where cyber adversaries can't achieve any threat and at the same time fail its calculation because it's not worthy to attack while it is not going to succeed in the (Lose > Gain) equation. Credible state in cyber defense is more difficult for the attacker due to the capacity and its tolls to develop advance threats that cyber defense of the attacker will not be capable to deny it in case of retaliation committed by the attacked state.

Deterrence by punishment as a second strategy can work in threatening state cyber adversaries via repeated threat of retaliation that raise the value of (Lose> Gain). At this point attacker rationally assumed to wind down cyber confrontation. State strategist need to think about combining both cyber deterrence by denial with deterrence by punishment because combination can impact to stimulate the opponent cooperation due to the calculation of cost and benefit from pursuing cyber threats.

When both traditional deterrence strategies (Denial – Punishment) did not work, State strategists are responsible to optimize cyber deterrence strategy and must not limit themselves to the traditional approaches and try another approach like entanglement. Chapter six examined deterrence by entanglement approach which benefited from different strategic issues and the mutual interest in cooperation. Deterrence by entanglement approach is more of mutual self-deterrence and it has worked in bringing two superpowers as an attempt for more cooperation as because both actors keep escalating which ends up in hurting themselves. Since they have mutual interest, it is better to entangle and work more cooperatively.

On further thought, the role of entanglement in supporting cyber deterrence through convincing state opponent that cyber-attack is hurting the attacked state and at the same time, it causes lose to the attacker (state) itself. This means the lose is mutual and it is better to cooperate rather than maintain ongoing confrontation.

Specifically, It has proposed different models that analyzing how state should manage the cyber deterrence when it get confronted with credible state. The research has produced the following research contribution within this thesis:

- A systematic literature review for the cyber deterrence and the literature produced in the field. This work has helped to identify the knowledge gap and helped in setting up the research road map. Refer to chapter (3.1).
- A model for analyzing credibility of cyber threat in deterring state cyber adversaries. The approach was following different strategies which is expected to help in success threat of retaliation as threat of punishment and expected to deter state adversaries. Refer to section (4.3).
- A model for analyzing the nature of cyber escalation ladder between two cyber credible states. This model assuming two credible states confronted when the credibility of cyber threat was not sufficient enough in deterring opponents and this failure leads to escalation in the intense of cyber attacks between these two states and prepare the ground for the mutual assured destruction. Refer to section (5.3).
- A model for analyzing the assumption of deterrence by entanglement as a different approach compared to traditional approaches and it could work between two credible states. This model relying on shared interest of both actors within the same model. The model has investigate the motivation for deterrence by entanglement as well as what could enforce both adversaries for more of cooperation. Refer to section (6.3).

7.2 Identify and Address Limitations

Deterrence is well known concept in international security studies and usually strategist see cyber deterrence from nuclear deterrence prospective and for that they think deterrence would not work in the cyber era due to different players, full of uncertainty, high level of anonymity with lack of attributions.

Yes, these issues reflect the uniqueness of cyber space but it does not mean deterrence is not working completely. Limitation of credibility of cyber threat as punishment is correlated to the misperception between both actors about intentions either to attack or not as well as attack consequences. Then, maintaining ongoing cyber escalation is possible for stimulating deterrence by entanglement approach for the purpose of reducing the heat of cyber escalation reflecting mutual interest in maintaining cyber as a peaceful space between both states. Cyber deterrence is like deterring social crimes more than deterring nuclear superpower where it can work in deterring particular actors and at the same time can't work for other actors. What has worked to bring China and USA and sign agreement promising mutual cooperation has not worked between Russia and USA. Deterrence by entanglement was the approach and might not work in other cyber conflicts. So, the limitation that may weaken cyber deterrence functionality can be identified as:

- Cyber threats attribution need to be advanced and will assist identifying threats and threatners. This advancement will consequence in identifying applicable deterrence strategies. Identifying cyber adversaries will assist state in identifying the applicable deterrence strategy that might work efficiently.
- Misperceptions about consequences of cyber threats and the value of the targets for the attacked as well as attacker are a complex issue. Compared with the nuclear, consequence of nuclear attack is clear for both adversaries but in cyber it is not known what target is more to effective in threatening opponent. Reducing the perception between both adversaries in cyber will stimulate the rational decision for furthering cooperation rather than confrontation.
- Mutual assured debilitation situation in cyber space is there even with the superpower. While all states vulnerable to cyber threats there is a need to a narrowed technical approach. Tackling this vulnerabilities need a narrowed investigation about each particular cyber threat and this will be more measurable approach for deterring international cyber threat.
- Variation in cyber conflicts in term of threats used reflecting the nature of cyber defense and the value of wining and losing. Justifying wining and losing is a bit complex and cause limitation in justifying success of cyber deterrence.

Deterring cyber threat is an international issue and there is a technical and experimental efforts needed to be conducted around these challenges. Measuring attribution of different cyber threats. Cyber Attack compared to nuclear attack is less harmful but for measuring cyber deterrence and to justify success,

7.3 Directions for Future Work

Research and sciences cannot give a holistically answer for certain research problems while sometime it helps to open the door for more questions rather than answering existed questions. For that, in this research I assume a further research on cyber deterrence are highly needed for the benefit of deterring cyber threats and for making cyber space a peaceful domain as possible. Regarding, cyber threats attribution, I think the growth in cyber security technologies innovations will reflect in advance attributions and digital forensics. The development will help attribution process in term of accuracy, timing and efficiency.

Cyber-attacks reflect the advances in cyber offensives capacity that state have it and willing to utilize it. Advances in offensive cyber capacity will not sustain state in advances position compared to other state. This capacity could change in the future and get replaced by other cheapest cyber threats that give state cyber offense more efficiency. More understanding of cyber threat limitation and the consequences to each other state will give state strategists and decision maker a better robust standing. Future strategies should consider that one size will not fit all cases:

- Technology and Attribution: Deep investigation of cyber defense technologies and its capacity in attributing cyber attacks like SQL, DDoS, Malware, Botnets, (Each cyber attack individually) with high accuracy and track back.

- International and National Organizations: Collaboration to work on missions for stimulating new policies that encourage different states (Cyber Adversaries) following deterrence by entanglement approach via bringing adversaries and states together.

- Rationality and Cyber Threat Credibility: Cyber deterrence is more than just threat to retaliate state adversaries. States decisions maker rationality need to be convinced deeply about the (value) reflecting ongoing loses consequence from cyber attacks via modeling (Value + Cost).

- There are a similarity and slight differences between deescalation and deterrence by entanglement approach. For that, there is a need for future work on modelling both situations and analyzing each situation in a separate model for further understanding both strategies.

7.4 Closing Remarks

In this research, I have worked to produce theoretical models that help in understanding and trying to optimize cyber deterrence strategy and support state with new tactics that efficiently can deter state cyber adversaries.

Research has approached problem analysis via three dimensions beginning by looking at the Credibility of cyber threat in deterring cyber adversaries threats (Deterrence by punishment). Then, when credibility of cyber threat is not sufficiently working into deterring opponent the escalation of cyber confrontation is the next expected outcome between adversaries and its probability is highly expected to result. Finally, the best possible approach for the state to deter its opponent is to consider the deterrence by entanglement as a different approach that may work and lead for a good strategic deterrence.

Developed mathematical models contribute to analyze the problem and advance our understanding about cyber deterrence strategy. Contribution of this research is important in term of understanding cyber deterrence problem and in particular supporting states advancement in keeping cyber domain as peaceful domain. Cyber deterrence is closer to deter criminals rather than nuclear deterrence. Because deterrence strategies help to reduce cyber-attack not to stop it totally.

References

[1] Cilluffo, F.J. and Cardash, S.L., 2013. Cyber domain conflict in the 21st century. Seton Hall J. Dipl. & Int'l Rel., 14, p.41.

[2] Chahid, Y., Benabdellah, M. and Azizi, A., 2017, April. Internet of things security. In Wireless Technologies, Embedded and Intelligent Systems (WITS), 2017 International Conference on (pp. 1-6). IEEE.

[3] Lacinák, M. and Ristvej, J., 2017. Smart City, Safety and Security. Procedia engineering, 192, pp.522-527.

[4] Martellini, M. and Malizia, A. eds., 2017. Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges: Threats and Counter Efforts. Springer.

[5] Miller, B. and Rowe, D., 2012, October. A survey SCADA of and critical infrastructure incidents. In Proceedings of the 1st Annual conference on Research in information technology (pp. 51-56). ACM.

[6] Lupovici, A., 2011. Cyber warfare and deterrence: trends and challenges in research. Military and Strategic Affairs, 3(3), pp.49-62.

[7] Sean Lyngaas (2015, December 17) White House Sends Cyber Deterrence Policy to Congress, Available at: https://fcw.com/articles/2015/12/17/lyngaas-congress-cyber-deterrence.aspx (Accessed: 3-3-2018).

[8] President.ee (22.12.2015) Estonian President in Poland: NATO Deterrence Should Include Cyber Space, Available at: http://www.baltic-course.com (Accessed: 3-3-2018).

[9] Czosseck, C., Ottis, R. and Talihärm, A.M., 2013. Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security. Case Studies in Information Warfare and Security: For Researchers, Teachers and Students, 72.

[10] Farwell, J.P. and Rohozinski, R., 2011. Stuxnet and the future of cyber war. Survival, 53(1), pp.23-40.

[11] Zetter, K., 2016. Inside the cunning, unprecedented hack of Ukraine's power grid. Wired.

[12] Chen, T.M. and Abu-Nimeh, S., 2011. Lessons from stuxnet. Computer, 44(4), pp.91-93.

[13] Malone, P.J., 2012. Offense-defense balance in cyberspace: a proposed model. NAVAL Postgraduate School Monterey CA.

[14] Lynn, W.J., 2010. Defending a new domain: the Pentagon's cyberstrategy. Foreign Affairs, 89(5), pp.97-108.

[15] Shaheen, S., 2014. Offense–defense balance in cyber warfare. In Cyberspace and International Relations (pp. 77-93). Springer, Berlin, Heidelberg.

[16] Kugler, R.L., 2009. Deterrence of cyber attacks. Cyberpower and national security, 320.

[17] Betz, D.J., 2017. Cyberspace and the State: Towards a Strategy for Cyber-power. Routledge.

[18] Hughes, J. and Cybenko, G., 2014, June. Three tenets for secure cyber-physical system design and assessment. In Cyber Sensing 2014 (Vol. 9097, p. 90970A). International Society for Optics and Photonics.

[19] Foreman, P., 2009. Vulnerability Management. CRC Press.

[20] Schiller, J.I., 2002. Strong Security Requirements for Internet Engineering Task Force Standard Protocols.

[21] FIPS, P., 2006. 200, Minimum Security Requirements for Federal Information and Information Systems. NCSD March.

[22] Scandariato, R., Wuyts, K. and Joosen, W., 2015. A descriptive study of Microsoft's threat modeling technique. Requirements Engineering, 20(2), pp.163-180.

[23] Stoneburner, G., Goguen, A. and Feringa, A., 2013. Risk management guide for information technology systems. NIST.

[24] Sullivan, J.E. and Kamensky, D., 2017. How cyber-attacks in Ukraine show the vulnerability of the US power grid. The Electricity Journal, 30(3), pp.30-35.

[25] Luiijf, E., Nieuwenhuijs, A., Klaver, M., van Eeten, M. and Cruz, E., 2008, October. Empirical findings on critical infrastructure dependencies in Europe. In International Workshop on Critical Information Infrastructures Security (pp. 302-310). Springer, Berlin, Heidelberg.

[26] Parzyan, A., 2017. Cyberspace – A Manmade Domain for Wars. 21st Century, (1 (20)).

[27] Trautman, L.J. and Ormerod, P.C., 2017. Industrial cyber vulnerabilities: Lessons from Stuxnet and the Internet of Things.

[28] Hall, A.O., 2017. The Cyber Defense Review: Investing in Cybersecurity Solutions. The Cyber Defense Review, 2(2), pp.9-12.

[29] Rid, T. and Buchanan, B., 2015. Attributing cyber attacks. Journal of Strategic Studies, 38(1-2), pp.4-37.

[30] Slayton, R. 2017;2016;, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment", International Security, vol. 41, no. 3, pp. 72-109.

[31] Goychayev, R., Carr, G.A., Weise, R.A., Donnelly, D.A., Clements, S.L., Benz, J.M., Rodda, K.E., Bartholomew, R.A., McKinnon, A.D. and Andres, R.B., 2017. Cyber Deterrence and Stability (No. PNNL-26932). Pacific Northwest National Lab.(PNNL), Richland, WA (United States).

[32] J. S. Nye Jr. Nuclear lessons for cyber security. Air UNIV Press Maxwell AFB AL, 2011.

[33] Geers, K., 2010. The challenge of cyber attack deterrence. Computer Law and Security Review, 26(3), pp.298-303.

[34] Elder, R.J., Levis, A.H. and Yousefi, B., 2015. Alternatives to Cyber Warfare: Deterrence and Assurance. In Cyber Warfare(pp. 15-35). Springer, Cham.

[35] Nayak, J.K., 2015. Fundamentals of Research Methodology: Problems and Prospects.

[36] Kumar, R., 2005. Research methodology: A step-by-step for beginners.

[37] Bryman, A. and Bell, E., 2015. Business research methods. Oxford University Press, USA.

[38] Edgar, T.W. and Manz, D.O., 2017. Research Methods for Cyber Security. Syngress.

[39] Salter, M.B. and Mutlu, C.E. eds., 2013. Research methods in critical security studies: An introduction. Routledge.

[40] Treat, J.W., 1996. Writing ground zero: Japanese literature and the atomic bomb. University of Chicago Press.

[41] Powell, R., 2003. Nuclear deterrence theory, nuclear proliferation, and national missile defense. International Security, 27(4), pp.86-118.

[42] Powell, R., 1990. Nuclear deterrence theory: The search for credibility. Cambridge University Press.

[43] Jervis, R., 2002. Mutual assured destruction. Foreign Policy, (133), p.40.

[44] Welch, L.D., 2011. Cyberspace–The Fifth Operational Domain. IDA Research Notes, pp.2-7.

[45] Bennett, B.T., 2018. Understanding, assessing, and responding to terrorism: Protecting critical infrastructure and personnel. John Wiley Sons.

[46] Kothari, C.R., 2004. Research methodology: Methods and techniques. New Age International.

[47] Goertz, G. and Starr, H. eds., 2002. Necessary conditions: Theory, methodology, and applications. Rowman Littlefield.

[48] Correa, H., 2001. Game theory as an instrument for the analysis of international relations. Ritsumeikan Annual Review of International Studies, 14(2), pp.187-208.

[49] Kapor, P., 2016. Game Theory Approach To Conflict And Cooperation In International Relations. Economic and Social Development: Book of Proceedings, p.242.

[50] Shiva, S., Roy, S. and Dasgupta, D., 2010, April. Game theory for cyber security. In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (p. 34). ACM.

[51] Lye, K.W. and Wing, J.M., 2005. Game strategies in network security. International Journal of Information Security, 4(1-2), pp.71-86.

[52] Amadi Emmanuuel Chukwudi, Eze Udoka, Ikerionwu Charles. Game Theory Basics and Its Application in Cyber Security. Advances in Wireless Communications and Networks. Vol. 3, No. 4, 2017, pp. 45-49. doi: 10.11648/j.awcn.20170304.13

[53] Alpcan, T. and Basar, T., 2003, December. A game theoretic approach to decision and analysis in network intrusion detection. In Decision and Control, 2003. Proceedings. 42nd IEEE Conference on (Vol. 3, pp. 2595-2600). IEEE.

[54] Agah, A., Das, S.K. and Basu, K., 2004. A game theory based approach for security in wireless sensor networks. In Performance, Computing, and Communications, 2004 IEEE International Conference on (pp. 259-263). IEEE.

[55] Wu, Q., Shiva, S., Roy, S., Ellis, C. and Datla, V., 2010, April. On modeling and simulation of game theory-based defense mechanisms against DoS and DDoS attacks. In Proceedings of the 2010 spring simulation multiconference (p. 159). Society for Computer Simulation International.

[56] Jones, M., Kotsalis, G. and Shamma, J.S., 2013. Cyber-attack forecast modeling and complexity reduction using a game-theoretic framework. In Control of Cyber-Physical Systems (pp. 65-84). Springer, Heidelberg.

[57] O'Neill, B., 1994. Game theory models of peace and war. Handbook of game theory with economic applications, 2, pp.995-1053.

[58] Benslama, M., Boucenna, M.L. and Batatia, H., 2015. Ad hoc networks telecommunications and game theory. John Wiley Sons.

[59] Prisner, E. (2014). Game Theory Through Examples. Mathematical Association of America. doi:10.5948/9781614441151

[60] Libicki, M.C., 2017. It Takes More than Offensive Capability to Have an Effective Cyberdeterrence Posture. RAND.

[61] Freedman, L. 2004, Deterrence, Polity Press, Cambridge.

[62] Brown, M.E., 1977. Deterrence Failures and Deterrence Strategies (No. P-5842). RAND Corporation, Santa Monica, CA.

[63] Andres, R., 2012. The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence. Trans. Array Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Derek S. Reveron. 1st ed. Washington DC: Georgetown University Press.

[64] Budgen, D. and Brereton, P., 2006, May. "Performing systematic literature reviews in software engineering". In Proceedings of the 28th international conference on Software engineering (pp. 1051-1052). ACM.

[65] Zagare, F.C., 2011. The games of July: explaining the Great War. University of Michigan Press.

[66] Friend, J.M. and Thayer, B.A., 2017. 10. Biology and international relations. Handbook of Biology and Politics, p.165.

[67] Benson, B.L., Rasmussen, D.W. and Mast, B.D., 1999. Deterring drunk driving fatalities: an economics of crime perspective1. International Review of Law and Economics, 19(2), pp.205-225.

[68] Quackenbush, S.L., 2011. Understanding general deterrence. In Understanding General Deterrence (pp. 1-20). Palgrave Macmillan, New York.

[69] Brodie, B., 1959. The anatomy of deterrence. World Politics, 11(2), pp.173-191.

[70] Huth, P. and Russett, B., 1988. Deterrence failure and crisis escalation. International Studies Quarterly, 32(1), pp.29-45.

[71] “Deterrence.”Merriam-Webster.com, Merriam-Webster,www.merriam-webster.com/dictionary/deterrence. Accessed 2 May 2018.

[72] Morgan, P.M., 1983. Deterrence: A conceptual analysis (Vol. 40). Sage Publications.

[73] Jones, R.E., 1968. Nuclear deterrence: a short political analysis. Routledge and Kegan Paul.

[74] Eugene Rosi (ed.), American Defense and Detente (New York: Dodd Mead, 1973), p. 96

[75] Lebow, R.N. and Stein, J.G., 1987. Beyond deterrence. Journal of Social Issues, 43(4), pp.5-71.

[76] Staff, J.C.O., 2013. Department of Defense dictionary of military and associated terms. MILITARY BOOKSHOP.

[77] Paul, T.V., Morgan, P.M. and Wirtz, J.J. eds., 2009. Complex deterrence: Strategy in the global age. University of Chicago Press.

[78] Saydjari, O.S., 2004. Cyber defense: art to science. Communications of the ACM, 47(3), pp.52-57.

[79] Tirenin, W. and Faatz, D., 1999. A concept for strategic cyber defense. In Military Communications Conference Proceedings, 1999. MILCOM 1999. IEEE (Vol. 1, pp. 458-463). IEEE.

[80] Slayton, R., 2017. What is the cyber offense-defense balance? Conceptions, causes, and assessment. International Security, 41(3), pp.72-109.

[81] Saltzman, I., 2013. Cyber posturing and the offense-defense balance. Contemporary Security Policy, 34(1), pp.40-63.

[82] Rehn, S.D., 2011. Don't Touch My Bits or Else!–Cyber Deterrence. ARMY WAR COLL CARLISLE BARRACKS PA CENTER FOR STRATEGIC LEADERSHIP.

[83] McGuire, M.C., 1967. The structure of choice between deterrence and defense. In Issues in defense economics (pp. 129-169). NBER.

[84] Liles, S., Dietz, J.E., Rogers, M. and Larson, D., 2012, June. Applying traditional military principles to cyber warfare. In Cyber conflict (CYCON), 2012 4th international conference on (pp. 1-12). IEEE.

[85] Morgan, P.M., 2003. Deterrence now (Vol. 89). Cambridge University Press.

[86] Wilson, W., 2008. The myth of nuclear deterrence. Nonproliferation Review, 15(3), pp.421-439.

[87] Kahn, H. and Jones, E., 2017. On thermonuclear war. Routledge.

[88] Steff, R., 2016. Strategic Thinking, Deterrence and the US Ballistic Missile Defense Project: From Truman to Obama. Routledge.

[89] Freedman, L., 2004. Deterrence. Cambridge, UK.

[90] Snyder, G.H., 1959. Deterrence by denial and punishment. Woodrow Wilson School of Public and International Affairs, Center of International Studies, Princeton University.

[91] Schelling, T.C., 2008. Arms and influence: With a new preface and afterword. Yale University Press.

[92] Brams, S. and Kilgour, D.M., 1989. Game Theory and National Security. Blackwell.

[93] Schelling, T.C. 1960. The Strategy of Conflict, Cambridge, Mass

[94] McGinnis, M.D., 1992. Deterrence Theory Discussion: I: Bridging or Broadening the Gap? A Comment on Wagner'sRationality and Misperception in Deterrence Theory'. Journal of Theoretical Politics, 4(4), pp.443-457.

[95] O'Neill, B., 1992. Deterrence Theory Discussion: II: Are Game Models of Deterrence Biassed towards Arms-Building? Wagner on Rationality and Misperception. Journal of Theoretical Politics, 4(4), pp.459-477.

[96] Knopf, J.W., 2010. The fourth wave in deterrence research. Contemporary Security Policy, 31(1), pp.1-33.

[97] Quester, G.H., 1986. Deterrence before Hiroshima: the airpower background of modern strategy. Transaction Publishers.

[98] George, A.L. and Smoke, R., 1974. Deterrence in American foreign policy: Theory and practice. Columbia University Press.

[99] Snyder, G.H., 1971. " Prisoner's Dilemma" and" Chicken" Models in International Politics. International Studies Quarterly, 15(1), pp.66-103.

[100] Sokolski, H.D., 2004. Getting MAD: nuclear mutual assured destruction, its origins and practice. DIANE Publishing.

[101] Record, J., 2004. Nuclear Deterrence, Preventive War, and Counterproliferation. Cato Institute.

[102] Bendiek, A. and Metzger, T., 2015. Deterrence Theory in the Cyber-Century. INFORMATIK 2015.

[103] Mulvenon, J., 2005. Toward a cyberconflict studies research agenda. IEEE Security Privacy, 3(4), pp.52-55.

[104] Mulvenon, J.C. and Rattray, G.J. eds., 2012. Addressing Cyber Instability: Executive Summary. Cyber Conflict Studies Association.

[105] Iasiello, E., 2014. Is cyber deterrence an illusory course of action?. Journal of Strategic Security, 7(1), p.54.

[106] Nye, J.S., 2011. Nuclear lessons for cyber security?.

[107] Libicki, M.C., 2009. Cyberdeterrence and cyberwar. Rand Corporation.

[108] Christopher Haley (February 06, 2013) A Theory of Cyber Deterrence, Available at: https://www.georgetownjournalofinternationalaffairs.org/online-edition/a-theory-of-cyber-deterrence-christopher-haley (Accessed: 5th May 2018).

[109] Miniwatts Marketing Group (Page updated June 2, 2018) Internet Usage Statistics , Available at: https://www.internetworldstats.com/stats.htm (Accessed: 11-7-2018).

[110] Reveron, D.S. ed., 2012. Cyberspace and national security: threats, opportunities, and power in a virtual world. Georgetown University Press.

[111] Davis, J., 2007. "Hackers take down the most wired country in Europe". Wired magazine, 15(9), pp.15-09.

[112] Kugler, R.L., 2009. "Deterrence of cyber attacks". Cyber power and national security, 320.

[113] Khan, R., Maynard, P., McLaughlin, K., Laverty, D. and Sezer, S., 2016, August. Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid. In ICS-CSR.

[114] Gurevich, V., 2014. Cyber and Electromagnetic Threats in Modern Relay Protection. Crc Press.

[115] Pellerin, C., 2010. Lynn: cyberspace is the new domain of warfare. Retrieved July, 20, p.2011.

[116] Rid, T. and McBurney, P., 2012. Cyber-weapons. the RUSI Journal, 157(1), pp.6-13.

[117] Legris, P., Ingham, J. and Collerette, P., 2003. Why do people use information technology? A critical review of the technology acceptance model. Information management, 40(3), pp.191-204.

[118] Jabbour, K.T. and Ratazzi, E.P., 2012. Does the United States Need a New Model for Cyber Deterrence?. In Deterrence (pp. 33-45). Palgrave Macmillan, New York.

[119] Khalilzad, Z., 1999. Defense in a wired world: protection, deterrence, and prevention. RAND-PUBLICATIONS-MR-ALL SERIES-, pp.403-436.

[120] Simmons, C., Ellis, C., Shiva, S., Dasgupta, D. and Wu, Q., 2009. AVOIDIT: A cyber attack taxonomy. In Proc. of 9th Annual Symposium On Information Assurance-ASIA (Vol. 14).

[121] Ross Brewer, VP and MD EMEA (March 6, 2017) The six stages of a cyber attack lifecycle, Available at: https://www.helpnetsecurity.com/2017/03/06/cyber-attack-lifecycle/ (Accessed: 3rd May 2018).

[122] Mazzotta, B.D., 2011. Leverage in Cyberspace, Without Deterrence.

[123] Berge, M. and Young, E., 2014. Intrusion detection faq: What is intrusion detection?. SANS Security Training.

[124] Kotenko, I. and Chechulin, A., 2012. Attack modeling and security evaluation in SIEM systems. International Transactions on Systems Science and Applications, 8, pp.129-147.

[125] Collins, J.M., 2002. Military strategy: Principles, practices, and historical perspectives. Potomac Books, Inc.

[126] Nakashima, E., 2011. Obama administration outlines international strategy for cyberspace. The Washington Post, 16.

[127] Stiennon, R., 2010. Surviving cyberwar. Government Institutes.

[128] George Washington: "Fifth Annual Address to Congress," December 3, 1793. Online by Gerhard Peters and John T. Woolley, The American Presidency Project. http://www.presidency.ucsb.edu/ws/?pid=29435.

[129] Conley, C.A., 2014. Outer Space Treaty. Encyclopedia of Astrobiology, pp.1-1.

[130] Sean McGurk, interview by Steve Kroft, 60 Minutes, NBC, March 4, 2012.

[131] Cimbala, S.J., 2011. Nuclear Crisis Management and Cyberwar. Strategic Studies Quarterly.

[132] United States Congress, The National Defence Authorization Actfor Fiscal Year 2012 (Washington D.C.: Congressional Record, 12 Dec 2011), H.R. 1540, Volume 157, Number 190, H8356- 8726

[133] Maclellan, N., 2011. Australia and the global re-alignment of US military forces. Dissent, (37), p.18.

[134] Long, A.G., 2008. Deterrence: From Cold War to long war: Lessons from six decades of RAND Deterrence Research (Vol. 636). Rand Corporation.

[135] Hansen, A.P., 2012. Nothing New Under the Sun: Benefiting from the Great Lessons of History to Develop a Coherent Cyberspace Deterrence Strategy. National Defense University Norfolk VA Joint Advanced War fighting School.

[136] Yu, J., 1994. "Punishment celerity and severity: Testing a specific deterrence model on drunk driving recidivism". Journal of Criminal Justice, 22(4), pp.355-366.

[137] D'Arcy, J. and Hovav, A., 2007. "Deterring internal information systems misuse". Communications of the ACM, 50(10), pp.113-117.

[138] Wei, M.L.H., 2015. "The Challenges of Cyber Deterrence". Journal of The Singapore Armed Forces, 41(1).

[139] Geers, K., 2010. "The challenge of cyber attack deterrence". Computer Law & Security Review, 26(3), pp.298-303.

[140] Wrenn, C.F., 2012. "Strategic Cyber Deterrence". Fletcher School of Law and Diplomacy (Tufts University).

[141] Rid, T. and Buchanan, B., 2015. Attributing cyber attacks. Journal of Strategic Studies, 38(1-2), pp.4-37.

[142] Clark, D.D. and Landau, S., 2010, November. The problem isn't attribution: it's multi-stage attacks. In Proceedings of the Re-architecting the Internet Workshop (p. 11). ACM.

[143] Shipley, P.M., Shipley and Peter M., 2000. Intelligent network security device and method. U.S. Patent 6,119,236.

[144] Lindsay, J.R., 2015. Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. Journal of Cybersecurity, 1(1), pp.53-67.

[145] Lancope, Inc. Scalable visibility and security analytics across your business, Available at: https://www.lancope.com/solutions/security-operations/network-visibility (Accessed: 3rd May 2018).

[146] Kadivar, M., 2014. Cyber-attack attributes. Technology Innovation Management Review, 4(11), p.22.

[147] Clark, D.D. and Landau, S., 2011. Untangling attribution. Harv. Nat'l Sec. J., 2, p.323.

[148] Dogrul, M., Aslan, A. and Celik, E., 2011, June. Developing an international cooperation on cyber defense and deterrence against cyber terrorism. In Cyber conflict (ICCC), 2011 3rd international conference on (pp. 1-15). IEEE.

[149] Taddeo, M. and Glorioso, L., 2016. Regulating cyber conflicts and shaping information societies. Ethics and policies for cyber operations.

[150] Glorioso, L., 2015. Cyber conflicts: Addressing the regulatory gap. Philosophy Technology, 28(3), pp.333-338.

[151] Taddeo, M., 2017. Deterrence by Norms to Stop Interstate Cyber Attacks. Minds and Machines, 27(3), pp.387-392.

[152] Shackelford, S.J., 2014. Managing cyber attacks in international law, business, and relations: In search of cyber peace. Cambridge University Press.

[153] Knake, R.K., 2010. Untangling attribution: Moving to accountability in cyberspace. Prepared Statement before the Subcommittee on Technology and Innovation, Committee on Science and Technology, Hearing: Planning for the Future of Cyber Attack.

[154] Guitton, C., 2012. Criminals and cyber attacks: The missing link between attribution and deterrence. International Journal of Cyber Criminology, 6(2), p.1030.

[155] Stevens, T., 2012. A cyberwar of ideas? Deterrence and norms in cyberspace. Contemporary Security Policy, 33(1), pp.148-170.

[156] Dawson, A., 2013. Addressing cyber warfare: bolstering deterrence through developing norms (Doctoral dissertation, University of British Columbia).

[157] Zagare, F.C. and Kilgour, D.M., 2000. "Perfect Deterrence" (Vol. 72). Cambridge University Press.

[158] Morgan, P.M., 2002. Threats and Promises: The Pursuit of International Influence.

[159] MILLER, N. R (2010) Defense, Deterrence, and Compellence , Available at: http://userpages.umbc.edu/ nmiller/POLI388/DEFENSE AND DETERRENCE.5.ppt (Accessed: 5th May 2018).

[160] Levmore, S. and Porat, A., 2014. Credible threats.

[161] Freedman, L., 1989. The evolution of nuclear strategy (Vol. 20). London: Macmillan.

[162] Rubin, J.Z., Pruitt, D.G. and Kim, S.H., 1994. Social conflict: Escalation, stalemate, and settlement. Mcgraw-Hill Book Company.

[163] Mueller, J.E., 1995. Quiet Cataclysm: Reflections on the Recent Transformation of World Politics. Longman Publishing Group.

[164] Kaufmann, W.W., 1989. The requirements of deterrence. In US Nuclear Strategy (pp. 168-187). Palgrave Macmillan, London.

[165] Smoke, R., 1987. National security and the nuclear dilemma: An introduction to the American experience. Random House.

[166] Lebow, Richard Ned (1981). Between Peace and War: The Nature of international Crisis. Baltimore: Johns Hopkins University Press.

[167] Betts, Richard K. (1987). Nuclear Blackmail and Nuclear Balance. Washington, DC: Brookings Institution.

[168] Orme, J.D., 1992. Credibility and Deterrence. In Deterrence, Reputation and Cold-War Cycles (pp. 1-11). Palgrave Macmillan, London.

[169] Futter, A., 2015, February. Hacking the bomb: nuclear weapons in the cyber age. In International Studies Annual Conference (pp. 23-27).

[170] Eisenstadt, M., 2016. Iran's Lengthening Cyber Shadow. Washington Institute for Near East Policy.

[171] WAQAS (18th October 2013) Israeli Think Tank Acknowledges Iran as Major Cyber Power, Iran Claims its 4th Biggest Cyber Army in World, Available at: https://www.hackread.com/iran-biggest-cyber-army-israel/ (Accessed: 17th October 2018).

[172] Ali Soufan (August 11, 2016) Iran's Growing Cyber Capabilities, Available at: http://www.soufangroup.com/tsg-intelbrief-irans-growing-cyber-capabilities/ (Accessed: 12/12/2018).

[173] Schmitt, M.N. ed., 2013. Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press.

[174] Connell, M., 2014. Deterring Iran's Use of Offensive Cyber: A Case Study (No. CNA-DIM-2014-U-008820-FINAL). CENTER FOR NAVAL ANALYSES ALEXANDRIA VA STRATEGIC STUDIES RESEARCH DEPT.

[175] Alelyani, S. and Kumar, H., 2018. Overview of Cyberattack on Saudi Organizations. Journal of Information Security and Cybercrimes Research (JISCR), 1(1).

[176] Carlson, L.J., 1995. A theory of escalation and international conflict. Journal of Conflict Resolution, 39(3), pp.511-534.

[177] Herman, K., 1965. On escalation: Metaphors and scenarios.

[178] Davis, P.K. and Stan, P.J., 1984. Concepts and Models of Escalation (No. RAND/R-3235). RAND CORP SANTA MONICA CA.

[179] Lichbach, M.I., 1987. Deterrence or escalation? The puzzle of aggregate studies of repression and dissent. Journal of Conflict Resolution, 31(2), pp.266-297.

[180] Huth, P. and Russett, B., 1988. Deterrence failure and crisis escalation. International Studies Quarterly, 32(1), pp.29-45.

[181] Brecher, M., 1996. Crisis escalation: Model and findings. International Political Science Review, 17(2), pp.215-230.

[182] Manzo, V., 2012. Deterrence and Escalation in Cross-domain Operations. JFQ: Joint Force Quarterly, 66, pp.8-14.

[183] Azar, E.E., 1972. Conflict escalation and conflict reduction in an international crisis: Suez, 1956. Journal of Conflict Resolution, 16(2), pp.183-201.

[184] Libicki, M.C., 2012. Crisis and escalation in cyberspace. Rand Corporation.

[185] Hurwitz, R., 2013. Keeping Cool: Steps for Avoiding Conflict and Escalation in Cyberspace. Georgetown Journal of International Affairs, pp.17-28.

[186] Osawa, J., 2017. The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?. Asia-Pacific Review, 24(2), pp.113-131.

[187] Robert Windrem (Updated Dec. 18, 2016 / 8:53 AM GMT) Timeline: Ten Years of Russian Cyber Attacks on Other Nations, Available at: https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111 (Accessed: 3rd December 2018).

[188] Healey, J., Cantos, M. and Geers, K., 2015. What's next for Putin in Ukraine: Cyber escalation?. Cyber War in Perspecfive: Russian Aggression against Ukraine, pp.153-158.

[189] Office of the Director of National Intelligence, 2017. Assessing Russian activities and intentions in recent US elections. Unclassified Version.

[190] Clark, R.A. and Knake, R.K., 2010. Cyber War: The next threat to national security and what to do about it. New York: Ecco.

[191] Rid, T., 2013. Cyber war will not take place. Oxford University Press, USA.

[192] Brantly, A., 2018. Conceptualizing Cyber Deterrence by Entanglement.

[193] Nye Jr, J.S., 2017. Deterrence and dissuasion in cyberspace. International Security, 41(3), pp.44-71.

[194] Crosston, M.D., 2011. World gone cyber MAD: how "Mutually Assured Debilitation" is the best hope for cyber deterrence. Strategic studies quarterly, 5(1), pp.100-116.

[195] Akdag, Yavuz. "Cyber Deterrence against Cyberwar between the United States and China: A Power Transition Theory Perspective." (2017).

[196] Drazen, Allan, and Paul R. Masson. "Credibility of policies versus credibility of policymakers." The Quarterly Journal of Economics 109, no. 3 (1994): 735-754.

[197] Bluestone Analytics (AUGUST 14, 2018) Cyber Threat Report: China, Available at: https://www.bluestoneanalytics.com/news/chinathreatreport (Accessed: 3rd April 2019).

[198] Smeets, Max, and Herbert S. Lin. "Offensive cyber capabilities: To what ends?." In 2018 10th International Conference on Cyber Conflict (CyCon). IEEE, 2018.

[199] Inkster, N., 2018. China's cyber power. Routledge.

[200] Mohit Kumar (March 20, 2015) China Finally Admits It Has Army of Hackers, Available at: https://thehackernews.com/2015/03/china-cyber-army.html (Accessed: September 3, 2019).

[201] Wentz, L.K., Barry, C.L. and Starr, S.H., 2009. Military Perspectives on Cyberpower. NATIONAL DEFENSE UNIV WASHINGTON DC CENTER FOR TECHNOLOGY AND NATIONAL SECURITY POLICY.

[202] The White House (September 25, 2015) FACT SHEET: President Xi Jinping's State Visit to the United States, Available at: https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (Accessed: 9th December 2018).

[203] Harold, S.W., Libicki, M.C. and Cevallos, A.S., 2016. Getting to yes with China in cyberspace. Rand Corporation.

[204] Brown, G. and Yung, C.D., 2017. Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace. The Diplomat.–2017.–19 January. http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurityagreement-part-1-the-us-approach-to-cyberspace 27.03. 2017).

[205] KIM ZETTER (25 September 2015) US and China Reach Historic Agreement on Economic Espionage , Available at: https://www.wired.com/2015/09/us-china-reach-historic-agreement-economic-espionage/ (Accessed: 8th December 2018).

[206] FireEye ISight Intelligence (June 2016) Redline Drawn: CHINA RECALCULATES ITS USE OF CYBER ESPIONAGE , https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf: FireEye, Inc.

[207] Scott W. Harold, (August 1, 2016) The U.S.-China Cyber Agreement: A Good First Step, https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html: RAND Corporation.

[208] Cioffi-Revilla, C., 2009. Modelling Deterrence in Cyberia (pp. 125-131). Amsterdam: IOS Press.

Appendix A

Attributing Cyber Attacks

It is irrelevant to the research to explore the technical practices of how states practically develop its cyber attacks attribution procedures. I have mentioned in Section 7.3 the future work and the efforts needed to be allocated in supporting state cyber attribution more technically. So, i would like in this appendix to elaborate about attribution from technical perspectives and more closely from digital forensic point of view. Different cyber attacks need different kind of technologies for achieving the attribution required. So, as example state can select one particular cyber threat and the focus on deterring this one attack and design the approach to attribute it. Each cyber attack is different in term of approach, tools, targets, effectiveness and severity and need for intensive technical work to assure accuracy within future work.

The technical aspect of attribution cyber attack reflecting the process of attack. Specifically, the systems and solutions used for initiating the cyber attack and the target for the same attack.For more understanding about each cyber attack and the technological need in achieving attributions the road map for the system to be developed is to provide comprehensive (Complete and Accurate) information about the attack and the attacker.

As example, attributing ransom ware attack can be as example how state should practise the strategic operation in tracing cyber threats for the benefit of cyber deterrence. Ransom ware attack usually beginning by standard methods of attacking like email attachment, website and when infection arrives on user machine and start the process of communication with the encryption servers is where state can detect this communication. Then, a process of selecting files for the purpose of infection and then pursue for finalizing the encryption via rename, encrypt then rename again. The last step in ransom ware infection is when it start asking for the payment in case recovery are in demand.

State in achieving the mission of attributing this particular cyber threat need to approach the threat technically and evaluate its capacity. Attribution is not impossible mission but

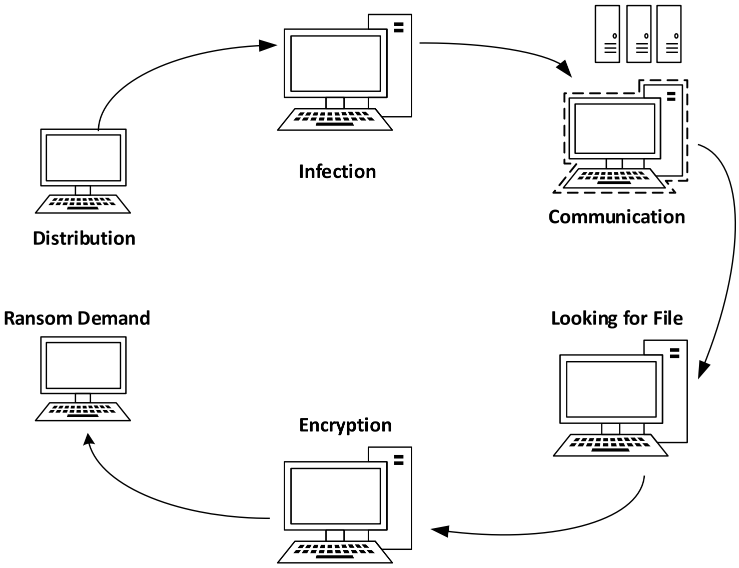


Fig. A.1 Ransomeware Lifecycle

I think it is little complex reflecting the uniqueness of cyber space complexity in term of multi-layers of communication.

Appendix B

List of publications

B.1 Journal Papers (Google Scholar)

- Al Azwani, N. and Chen, T., 2018. Cyber Deterrence by Punishment: Role of Different Perceptions. Cyberpolitik Journal, 3(5), pp.62-75.

- Cyber Deterrence by Entanglement: Analytic Model of Deterrence by Entanglement as result of Mutual Assured Debilitation [Submitted and Accepted]

- Credibility of Cyber Threat: Theoretical Model Analyzing Correlation between Cyber Threats and its Credibility in Deterring (State-State) Cyber Conflicts [Under Submission]

B.2 Conference Papers

- Al Azwani, N. and Chen, T., (2018). Deterrence from Nuclear to Cyber Deterrence, Istanbul Bosphorus International Cyberpolitics, Cyberlaw and Cybersecurity Conference, Turkey - Istanbul, MAY 11-14, 2018. Istanbul: Cyberpolitik Journal and Centre for Cyber Politics Research (http://cyberpoliticsconference.org)

- Al Azwani, N. and Chen, T., (2019). Cyber Deterrence by Entanglement Theoretical model for deterring (State-State) Cyber Threats, Istanbul Bosphorus International Conference on Cyber Politics and Cyber Security, Turkey - Istanbul, June 27-30, 2019. Istanbul: Cyberpolitik Journal and Centre for Cyber Politics Research (http://cyberpoliticsconference.org)

B.3 Conference Poster

- Nasser S.Al-Azwani and Thomas M. Chen, *"CYBER DETERRENCE. A STRATEGIC MODELS FOR DETERRING (STATE-STATE) CYBER THREATS"*, Cyber Security Workshop, 12th AND 13th March 2018, KENT UNIVERSITY (https://research.kent.ac.uk/cyber-security-workshop/)