Deterrence by Denial approach for the most known State Cyber Vulnerabilities

Nasser S. AlAzwani and Thomas M. Chen*

January 21, 2020

Abstract

Cyber deterrence by denial strategy can be practised by the state by making it hard for adversaries to succeed any attempt of attacking. It was practised during nuclear deterrence strategies as well as in many other conventional deterrence. This paper argues the functionality of cyber deterrence by denial in deterring cyber threats. In this paper, our attempt is to define cyber deterrence by denial, model it, explore operational roles of cyber security technologies in approaching deterrence by denial within cyber space. Model analysis shed lights over practicing deterrence by denial and its vital role in understanding how efficiently denial can work in maximize failure of any attack which will impact in maximizing cost of cyber attacks to the attacker. Due to limitations in cyber security technologies, unknown cyber threat might not be deterred with assumed approach. Proposed model confirmed that deterrence by denial strategy might works in deterring known cyber threats within instrumental model. As for the benefit of enhancing deterrence in cyber space there is a serious need to reduce the tendency to ignore exploring this strategy.

Keywords: Cyber security; cyber deterrence; cyber deterrence by denial; game theory; national security

1 Motivation

Deterrence has rescued humanity from nuclear holocaust for more than half a century. Cyber threats that threaten state cyber space is growing aligned

*email:nasser.al-azwani@city.ac.uk, email: tom.Chen.1@city.ac.uk, School of Math, Department of Electrical and Electronic Engineering, Computer Science and Engineering, City, University of London, UK

with growth in utilizing cyber technologies. Cyber defense and offenses technologies are there but still having different gaps in assuring full protection against cyber threats especially threats that are supported by state adversaries while others arguing that cyber deterrence might not work similarly to nuclear deterrence [6]. From this argument, cyber deterrence might help states in preventing unwanted cyber damage but it depend on the approach. Deterrence by denial strategy was practised within nuclear deterrence but it is not limited to deter nuclear threat but it can be practiced to deter other kind of threats and cyber threat is not exceptional. Cyber deterrence by denial can be practiced via applying cyber defense capabilities for the objective of denying state adversary success in achieving his targets from initiating cyber-attacks.

The motivation here is to understand the impact of practising deterrence by denial strategy between any two states by analysing repeated cyber interaction. The approach in this analysis is by selecting one particular cyber threat and measuring the success progress of the deterrence by denial. Main point here is to differentiate between deterring whole war from deterring one particular weapon within this particular war. More specifically, selecting one particular cyber threat as a model for state to implement deterrence by denial approach and measure the outcome. The motivator here is to narrow deterrence strategy to select one particular weapon and deter it. Specifically, in cyber is to select one particular cyber threat within cyber space and scope the deterrence strategy against this particular threat. By following this particular approach we can assume a measurable model for measuring cyber deterrence by denial and its efficiency. In cyber space players are plenty but with our attempt here is only to limit it within the state vis to vis state within cyber space.

There are three main outcomes from this paper that can be summarised to: First, to define cyber deterrence by denial and define its practical procedures in reducing the scale of cyber threat originated by state adversaries. Second, to model cyber deterrence by denial and analyse repeated cyber interaction and its reflection in optimizing deterrence by denial within cyber space. Third, to respond to the argument that cyber deterrence does not work by confirming its functionality in deterring known cyber attacks via practical approach. Practical approach in the cyber space is mainly within *cyber defense line* rather than *cyber offense line*. It suggests that greater investment in developing deterrence by denial in cyber space will not only lead to maximizing cost of attack to the state adversaries, but also to more failure in achieving successful cyber attacks as well. These outcomes are the answers of the research related questions:

- Are there any differences in the deterrence by denial definition between nuclear and cyber space?
- What are the evidences that support the functionality assumption of deterrence by denial in deterring known cyber threats?
- Is deterrence by denial working in cyber space similarly in nuclear deterrence?

This paper contributes to literature by providing answers to questions that are not only timely, but could inform current discussions on the potential effects of cyber deterrence by denial approach. States has experienced significant cyber attacks over the last few years and this increase in amount of mutual loses but in some cases is not. This research acknowledges the challenge in measuring success and failure of the deterrence by denial approach and the attempt to solve by bringing the concept to practise. More specifically, exploring the deterrence by denial concept from multidimensional approach.

2 Background

There is a growing literature considering the impact of investment in cyber deterrence strategies to reduce cyber threats targeting state infrastructure. The general concept of deterrence is the use of threats of punishment to threaten opponent to prevent him (Individual/Group/State/Institute) from conducting something unwanted. This concept is a simple and general conceptualisation about the deterrence [1]. Traditional deterrence strategies has been categorised to a different kinds of deterrence. This differentiation is based on the definition and the scope of each kind of deterrence. Deterrence been concluded to five kinds as per Ryan article and these kinds are deterrence by punishment, by denial, by association, by norms and taboos, and finally by entanglement [2].

Although some of the past literature assumes that cyber deterrence is not going to work because cyber is different from nuclear. Assumption like this is not enough to assure deterrence is not going to work in the cyber space [3]. For that,

Definition: 1 *Deterrence by denial means persuading state adversary not to attack by convincing him that his attack will be defeated, that he will will not be able to achieve his operational objectives from the attack [4].*

Our paper fills this gap for the benefit of deep understanding of cyber deterrence by denial by providing evidence that denial approach work in thwarting known cyber attacks, which means state adversaries are not going to benefit from initiating known cyber attacks because the failure is obvious due to cyber defense allocated. Likewise, It is clear that expanding in cyber defence efficiency increase in failure cost to state adversaries. In other words, the repeatably un-achievement in cyber attacks will grow repeatably the value of loses. Increasing the lose value correlate directly to adversary decision not to repeat these attacks as it has failed and it is just waste of resources to keep repeating similar cyber attacks. Just to remind our self, cyber defense and denial strategy working only against known cyber threats.

By reviewing the literature on traditional deterrence, cyber deterrence and game theory, this paper present new approach for analysing cyber deterrence by denial via looking to the cyber security technologies as a factor. This factor is to measure its efficiency in deterring known cyber threat within ideal and instrumental setup. Then analyse how this approach might reflect to the adversary decision. When any kind of cyber attacks denied by attacked state means the attacker already deterred. Yes, some would argue that this approach is more of defense rather than deterrence but the response is: It is defense for the purpose of deterrence. By deny the previous attack, attacker are not expected to attack or repeat the same attack against same target due to expected result which is failure. logically, attacker would get deterred automatically.

3 Case Study

For understanding deterrence by denial practise, the focus here to select one cyber threat as a case for a state to scope in. It is to narrow the analysis to achieve the deterrence by denial goals via practical and measurable tactics. Hardening cyber defences will assist state in minimize attacks success, maximize failure and maximize cost to state cyber adversaries. Practical strategy for achieving this objective will serve developing equation reflecting expected outcome for state (A) and can be noted as E_A and for state (B) expected outcome which can be noted as E_B. These expected outcomes correlated directly with state mission within cyber conflict.

Since it is the selection of one cyber threat for developing deterrence by denial approach, The process here is to select DDoS cyber threat as a case study reflecting the model analysis in coming sections [5]. Demonstrating DDoS attack as a practical case study for implementing deterrence by denial and analysing efficiency of deterrence by denial approach in maximizing cost

of attacking to the attacker. The case here is to assure failure of any DDoS attack attempted by state adversaries correlated directly to maximize lose calculation. Following this model will confirm that the "$LOSE$" will be certainly as a consequence to the state cyber adversary if it is confronted with strong cyber defense. In the situation of attacked state develop its cyber defensive capacity "$LOSE$" going to be bigger than any gain expected by state adversary.

Subsequently, selecting DDoS as a case study for examining raised argument will assist state in measuring success in deterring one threat within the cyber battle. Deterring one threat will reflect both state outcome within the same game. Model developed are based on value of gaining and losing and at the same time gain and lose reflecting collectively strategy of cyber deterrence in total.

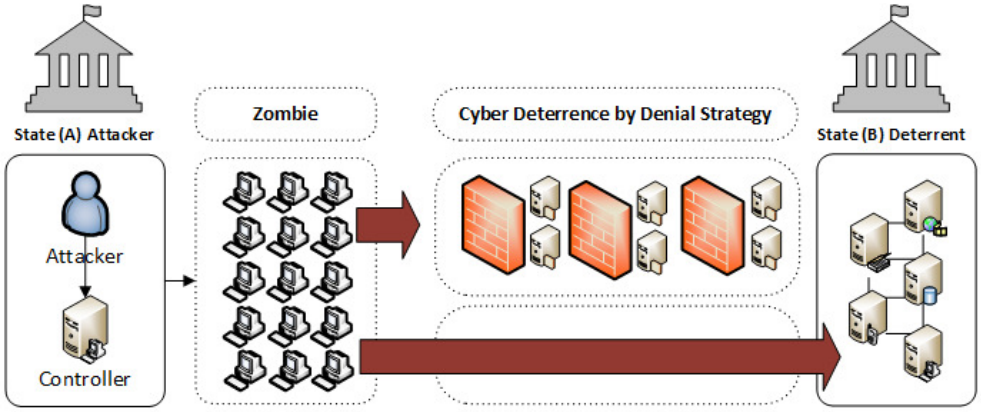

Figure 1: Cyber Deterrence by Denial Strategy

Generalizing deterrence against all cyber threat will not help in measuring progress. There are another argument about complete efficiency of cyber deterrence which means complete or total stop of cyber threat from state adversaries, which seems impossible. So, one of the cyber uniqueness is that both states can recover from the attacks or might fix the attacks consequence and pursue the operations. Comparing cyber to other conflicts domains and assume recovery from nuclear will be similar to cyber is not logically accepted. Cyber has its uniqueness and approaching this uniqueness by measuring deterrence by denial success a solid respond to the assumption of total en-efficiency of deterrence by denial via confirming the efficiency. Assuming there no efficiency is not proof and by align deterrence by denial concept to the practise these assumptions will be more confirmed.

Nominating DDoS as a case study is only as a case or evidence consistent with the outcomes predicted in different scenario. Assuming that this

deterrence by denial model will fit deterring other cyber threats. Deterring selective cyber threats may success unless unable to test directly which of these threats are more reliable for the technical experience. However, we provide suggestive evidence in supporting hardening national strategy for cyber deterrence by denial to reduce cyber conflict heat.

In responding to the deterrence by denial argument and its functionality in cyber space, this research tightening together traditional definition of deterrence by denial via technical practice. This technical and practical case is a sample and can be replicated against many other cyber attacks. DDos attack is well known disruptive cyber attack and has been used within many cyber conflicts

Focus of this paper is to correlate relationship between theoretical concepts of deterrence by denial and it practise and by following this approach in selecting one particular cyber attack for the

4 Cyber Deterrence by Denial Model

Main application for deterrence by denial is to reduce the likelihood of a successful cyber-attack by state adversary. Reducing success likelihood within a repeated cyber interaction will stimulate state adversary believe regarding state immunity against cyber threats. It is because high cost of initiating cyber attack to the attacker exceed the cost of expected gain and this concept are presented within the the Fig.[2].

Model used to examine questions of interest is assuming two states involved in a cyber conflict. Each state trying to advance its strategic mission via utilising cyber space and its threats as a tools to impose its adversaries. Cyber attacks are vary in term of its nature and the attempt here is to model one attack rather than generalizing the model. Deterring all kinds of cyber threats is not a logical approach because not all cyber threats similar in term of its technicality. So, deterrence by denial model analysing the deterrence strategy against one particular cyber attack for the purpose of confirming applicability of the concept to be practised in the cyber space. The advantage from following narrowed approach like this will assist state measuring its strategic achievements in deterring each cyber threat from practical point of view. Deterrence by denial relying more on the attack rather than the attacker. This approach will concentrate on hardening state cyber defence collectively.

In modelling cyber deterrence by denial, we consider two states (A) and (B) with opposed interest regarding cyber attacks and main mission of model analysis is to address chances and conditions that make cyber deterrence

by denial works. State (A) acting as offender who want to change the *Status Quo* situation within the cyber conflict. State (B) is the deterrer whom repeatedly aim to deter state (A) by implementing and optimizing cyber deterrence by denial national strategy. Optimising deterrence by denial strategy might work under very strict context of cyber attack and its detection methodology [7]. In approaching modelling the context, state (A) assumed to initiate DDoS attack against state (B) cyber infrastructure under different motivations [8]. Next, it is (B) to respond and proceed to next sub game and to make the decision. The Fig.(2) drawing the core idea of cyber deterrence by denial in term of hardening (B) cyber defense and the expected outcome from different scenarios. In case State (A) attacking (B) the expected outcome for (A) $E_A = (n)$ is correlated to (B) cyber defense capacity against modeled and assumed cyber attack. For that, scenario where (A) *Attack* (B) and (B) response via defend (A) *Attack* strategy is the outcome expected for (A) in its *Attack* strategy reflecting (B) cyber defense capacity strategy against (A) *Attack*. In this case, its (B) who suppose to optimize its cyber defense against -known- cyber threats that (A) might utilize it against (B) cyber vulnerabilities.

Practically, state (A) either not to cooperate and attack $E_A = (n)$ and simultaneously (B) confront (n) with efficient cyber defense. This scenario certainly will confirm $E_A = Gain > Lose$ unless (B) was not capable either to detect or to response to (A) first attack. Fig.(2) also has explained the second possible strategy for the (A) where it prioritize the cooperation $E_A = (c)$ and not to attack (B). Cooperation with state opponent is not achievable especially between adversaries unless there is sort of incentives might help in stimulating cooperation between.

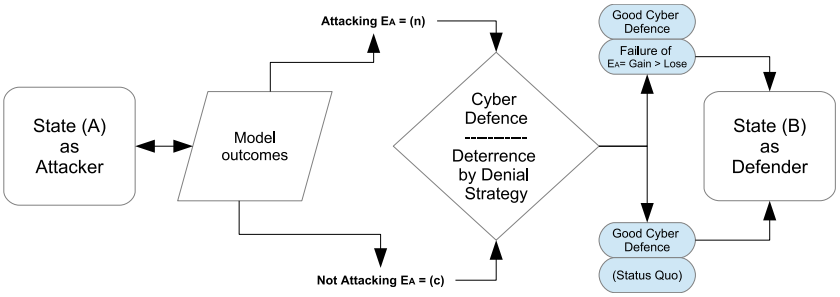

Figure 2: Cyber Deterrence by Denial Model

Strategically, reasons that might stimulate (A) as attacker not to attack (B) could be certainty of failure any DDoS attack against (B) infrastructure. Second, could be the cost of initiating the attack is higher than any expected benefit and within both situation $E_A = Lose > Gain$.

Core difference between nuclear and cyber deterrence model is that deterrence in cyber will work after repeatable cyber interaction due to cyber space uniqueness (attribution, different perceptions) while in nuclear it is working sufficiently within first round within the model. Nuclear threat of retaliation from the state (B) is credible enough to deter state (A) not to attack while in cyber it is not going to work similarly. It might work under model with repeatable cyber interaction that conceptualized in Fig.(3).

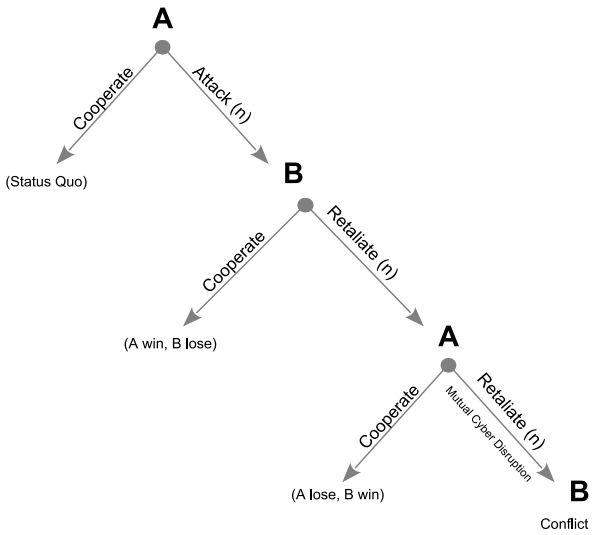

Figure 3: Cyber Deterrence Model

Practicing cyber deterrence by denial, state (B) supposed to defend against state (A) DDoS cyber attacks via maximizing efficiency of its cyber defense repetitively till enforce (A) to give up and not to attack (B) with any DDoS. Success of (B) defense depend on efficiency of (B) cyber defence in detecting and defending against attack. First attack from (A) might not get detected by (B) because it is not a considered as a harmful attack. Second attributed attack from (A), state (B) get stimulated to deter (A) attack by denial approach and should begin by gathering possible technical information about attack and who is standing behind. Repetitively, as fig.(4) If not immediate (B) to prioritize infrastructure with more value compared to less value infrastructure. Point here is that state (B) practise in strengthening cyber space and raise its immunity is correlated to $Maximize$ success of (B) denial approach and $Maximize$ failure of (A) $Attack$ strategy and this approach can be considered as punishment by failing any attempts of state (A) to attack (B) with certain $E_A = (n) = Lose > Gain$.

Traditional deterrence models has focused on the fear of nuclear retalia-

tion strategy and this strategy is not going work similarly in cyber due to different perceptions between adversaries about value of target as well as consequence of cyber attacks [9]. In reducing misperception between adversaries within cyber conflict, state (A) will *Attack* (B) targeting the critical infrastructure using (DDoS) attack and assumed (B) going to protect its critical infrastructure against (DDoS).

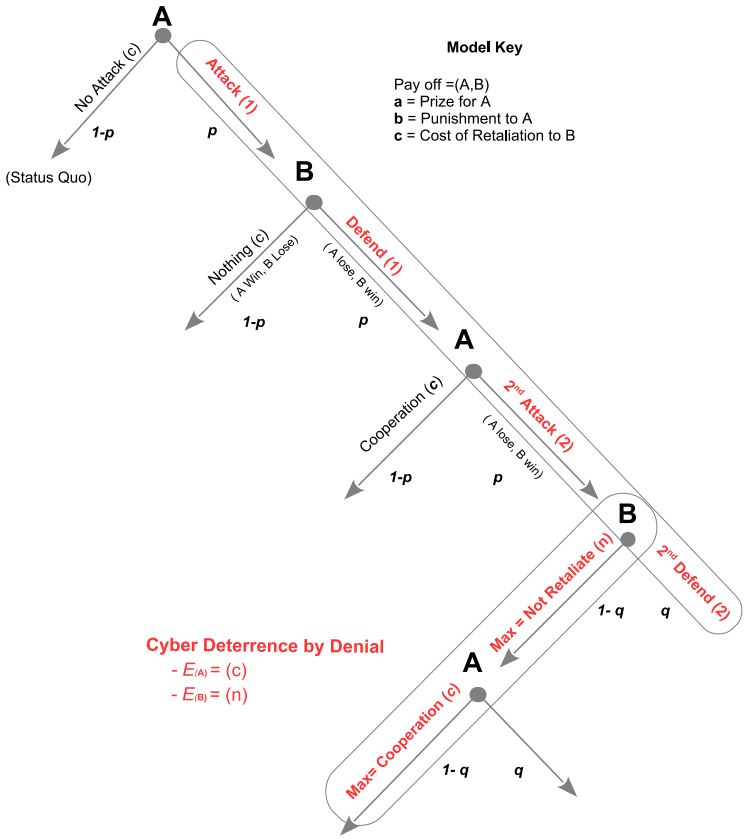

Figure 4: Cyber Deterrence by Denial Model

Repetitive cyber interaction between (A) and (B) going to develop repetitive value during these interactions. Main concern within this model is the accumulative value of ***Lose*** vs to vs expected ***Gain*** from initiating the attack. Ongoing fail of (A) *Attack* strategy is the core of deterrence by denial and it is (B) to maintain it continuously.

4.1 Scenario A :- Successful Deterrence by Denial

At this point, the assumption is that state (A) will select "$Attack(1)$" and state (B) already has the $Defend(1)$ strategy against this particular attack

completely. So, if state (A) initiate 100 cyber attack and state (B) was capable to fail these attack, result will be lose to the state (A). In cyber space state (B) will defend against (A) cyber attacks only if it can detect incoming attacks, which is not always all attacks get detected. Assuming that (B) has detect the attack and the Assume b= Prob (B) will defend against detected (A) attack.

Expected payoff to (A) in sub-game and after ongoing attack (B) is going to result the outcome:

$$E_A = (1-p)a + p(a-b) = a - pb \tag{1}$$

In this case, (A) assumed will be deterred to "Do Nothing" if $a < pb$ repetitively. But, who is believe this will be happen. In cyber, states are not going to give up easily and will repeat the attempts again and again until the state (A) realise that accumulative value for initiating (DDoS) attack against (B) is worthless to spend and better to try another Cyber Attack. This diversion is where the enforcement against (A) to give up and change from utilizing (DDoS) attack against (B). Success of state (B) deterrence by denial strategy under two main conditions. First, when (B) detect incoming (DDoS) attacks using its active cyber defense against particular -(DDoS)- cyber threat. Second, it should be in place within all (B) critical infrastructure and it should be in the same level of efficiency all over state critical infrastructure.

In this case, if (A) repeat the attempts of attacking (B) utilizing same attack against other targets within (B) infrastructure, then (B) supposed has already prepared its critical infrastructure against any (DDoS) attack either from (A) or from any other state and this will deter attacker from utilizing (DDoS) attack. Which means cost of attack to the (A) maximized to a level of assuring failure of any attempts even if *attacker* changing the attack targets. Measuring success of deterrence by denial relying on how much success that state (B) can detect and defend against (A) (DDoS) cyber attacks. Within model case, the scale can be conducted more with instrumental and technical approaches to verify how much state (B) are capable to fail (A) **(DDoS)** cyber attack. It can be approached via By measuring this particular progress will response to answer deterrence by denial progress.

For state (B) as a lesson learned is to maintain its strategy of hardening its cyber defences repetitively allover its critical infrastructures to assure $E_A = Lose > Gain$ persistently. This infinite model of hardening cyber defense is the most possible approach in assuring efficiency of cyber deterrence by denial strategy.

4.2 Scenario B :- Failure Deterrence by Denial

Second scenario, state (A) will attack state (B) utilizing (DDoS) $Attack(1)$ and unfortunately state (B) simply has fail in developing its capacity to detect and defend against incoming (DDoS) attack within its critical infrastructure. In this situation nothing going to prevent (A) from repeating same attack against another targets within (B) infrastructure. Detecting the (DDoS) attack is the first line of deterrence by denial strategy. Strategy should be prepared, implemented and tested against any (A) $Attack(1)$ strategy utilizing (DDoS). In addition, defending against these attacks should tested before the scenario occurring.

Strategically, cyber detection followed by cyber defense is a fundamental step in developing state cyber deterrence by denial strategy. Without these two factors -Detection and Defense- it is difficult to expect any success of the deterrence by denial strategy and with high certainty it will struggle to work technically. The analysis in Fig.(4) has begun with first round of cyber confrontation and it should at least detect the first $Attack(1)$ for the purpose of response to the source of attack. A correlation between maximizing detection of the cyber attack and success of deterrence by denial is a positive relationship.

In equation (1), the a prize for (A) reflecting the expected gain and it should be below the cost of DDoS attack that is targeted (B). Estimates of disruptions caused by the first attack might be within acceptable cost to the (A). For that, (B) in avoiding failure of deterrence by denial strategy, should provides robustness assurance in deterring "known" cyber threats and identify limitations of denial model in deterring "Unknown" threats. Data and modeling approach strengthening over $Maximizing$ [b] outcomes over repeated interaction reflecting either (DDoS) attack or any other cyber attack.

Testing the Relevance of Hypotheses

The biggest concern in modelling cyber deterrence by denial analysis is whether relevant of other cyber attack to this DDoS attack between two adversaries. The response to this argument is that the selected attack is like a case study and it is an example satisfy the scenario where State (B) attempting to deter State (A) particular within cyber space. If this approach worked with (DDoS) assumed to work with other cyber attacks and need more instruments assessments to validate.

Before addressing model conclusion, it is useful to examine the estimated hypotheses and the variable of interest listed in Fig.(4) estimated impact of

strengthening cyber defense within (B) strategies is going to $Maximize$ **b** which reflect punishment to (A) due to fail the attack. So, analysis suggest that an increase in adversary **cost of attack** parallel with increasing in probability of attack failure is positively correlated with (A) self deterrence $E_A = NotAttack(c) > Attack(n)$and not to pursue with failed strategy. while an increase in strengthening state (B) cyber defense is positively correlated with deterrence by denial strategy. The conclusion her is that cyber deterrence is more similar to deterring criminal behaviour and need repeated successful steps that $maximize(c)$ cooperation and similarly and at the same time $minimize(n)$ non cooperation by maintain (A) *attacking* strategy.

So, state (B) deterrence by denial strategy consistently working under the condition and strategies of $E_B = n > c$ and keep cyber defense in ongoing strengthening cycle:

1. $Minimize(a)$: Keep optimising cyber defense repeatably and not to give adversary any chance to success any preemptive -known- cyber attack within cyber space,

2. $Minimize(c)$: Continuously assure to minimize cost of denial -Cyber Defense- strategy. Approaching this can be achieved by assuring efficiency of cyber security control via on going procedure of assuring its efficiency in defending against known cyber threats,

3. $Maximize(p)$: Keep maximizing probability of attacks detection for signaling state adversary about its capacity in detection and attribution,

4. $Maximize(b)$: keep maximizing the retaliation to (A) in ways to detect and defend effectively against -known- cyber threats within state infrastructures which consequence to fail adversary attempts of $maximizing(a)$,

Maximizing probability of failure within adversary attacking strategy is the core of cyber deterrence by denial. It is directly correlated to stimulate adversaries rational calculation to justify amount of lose in comparison to the gain. Overall, state (B) has to focus on two axes: first, strengthening its cyber defenses systems and infrastructure. Second, reducing the percentage of vulnerabilities within its cyberspace systems and infrastructure. These two axes will assist state in maximize its main cyber deterrence strategy via maximizing the cost of attacking to the opponent equation and enforce lose over any expected gain. The question here, will state (A) get deterred and choose -not to attack- (B) as a consequence of (B) successful deterrence by denial strategy?. Best answer for this question is to assume that after repeatable $failed$ cyber attack by (A) and repeatable $successful$ cyber deterrence

by denial in defending against nominated cyber attack, state cyber adversary assumed rationally to give up via $not - to - attack$ state (B) utilizing the same cyber threat.

5 Conclusion

This paper has responded to the argument that cyber deterrence is not working and tried to confirm the opposite and assure deterrence is working but it depends on what kind of deterrence is followed by the state to approach results. if any state want to deter cyber threats following deterrence by denial strategy, it should be narrowed to one particular cyber threat and scope the strategy over it. It is important to mention that the analysis model has its limitations in term of analysing instrumental cyber attack. Instrumental attack reflects the ideal situation where all information about the scenario between both actors are complete and clear within the model. Yes, it might be argued about unknown cyber threats and this model might not be able to deter these kind of cyber threats. For that, it was mentioned from the beginning that this approach is about deterring known cyber threat and this can be measured by strengthening cyber defense to make cost of attacking is higher than the expected gains. In other words, the deterrent need to continuously enhance its cyber defense, which is a fundamental process in success to enforce adversary to reduce (not to attack) strategy. Given the nature of our finding, if state want to deter its opponent, it need to have state of art in cyber defense technologies and it should be implemented as best practices. Further studies are needed to determine the equation that help attacker to decide whether the attack is beneficial or not.

Finally, it is important to reiterate that approaching cyber deterrence by denial via equation of maximizing cost of cyber attacks for state opponents is the core of cyber deterrence by denial approach. Practising this mission in cyber space is mainly by scoping the investment within cyber defense. States need to improve its contextual cyber space by integrating cyber technologies and keep optimising by following approaches like defense on depth or multi-layers of authentications to ensure valuable infrastructures are under sufficient protection.

References

[1] Morgan, P.M., 1977. Deterrence: A conceptual analysis (pp. 25-43). Beverly Hills, CA: Sage Publications.

[2] Ryan, N.J., 2018. Five kinds of cyber deterrence. Philosophy Technology, 31(3), pp.331-338.

[3] Paul, T.V., Morgan, P.M. and Wirtz, J.J. eds., 2009. Complex deterrence: Strategy in the global age. University of Chicago Press.

[4] Freedman, L., 2004. Deterrence. Polity.

[5] Eve Keiser and John Edwards (August 5, 2015) How DoD is making cyberattacks more costly, less successful, Available at:https://www.c4isrnet.com/2015/08/05/how-dod-is-making-cyberattacks-more-costly-less-successful/ (Accessed: 9/12/2019).

[6] Geers, K., 2010. The challenge of cyber attack deterrence. Computer Law Security Review, 26(3), pp.298-303.

[7] Ghanbari, M. and Kinsner, W., 2020. Detecting DDoS Attacks Using Polyscale Analysis and Deep Learning. International Journal of Cognitive Informatics and Natural Intelligence (IJCINI), 14(1), pp.17-34.

[8] Chen, W., Xiao, S., Liu, L., Jiang, X. and Tang, Z., 2020. A DDoS attacks traceback scheme for SDN-based smart city. Computers Electrical Engineering, 81, p.106503.

[9] Al Azwani, N. and Chen, T., 2018. Cyber Deterrence by Punishment: Role of Different Perceptions. Cyberpolitik Journal, 3(5), pp.62-75.