THE EIGHT LEVERS OF COERCIVE CONFLICT

No More, No Less

2021 September 07

William A. Dawson

Center for Global Security Research
LAWRENCE LIVERMORE NATIONAL LABORATORY

The Eight Levers of Coercive Conflict: No More, No Less

William A. Dawson[1]

Lawrence Livermore National Laboratory

Executive Summary

Few concepts are more important to our nation than the principle of deterrence. It is at the very core of our national security strategy. Despite its lasting import to our nation, and the rest of the world, we still lack a complete and explicit formulation of the calculus of deterrence. This has, at times, resulted in failed policies costing the Nation lives and wealth. With the ultimate objective of making the Nation more secure, we establish a complete and explicit formulation of deterrence calculus, which consists of eight levers. As it turns out this formulation also applies to the calculus of compellence, and is thus a unifying model of coercive conflict.

[1] *The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes*

Introduction

Deterrence – the act of instilling doubt or fear to discourage someone from doing something – has been an implicit element of the U.S. national security since its founding and reached it height of import during the Cold War. The principle of deterrence is so basic and simple it surely dates to at least to the time when someone could first raise a fist to their adversary[2]. Additionally, its relevance is widespread, covering the gamut from conflict between child and parent to conflict between nations. Despite this long history and widespread relevance, we still lack a complete, concise, and explicit description of deterrence. The same can be said for the sister concept, compellence – threatening a penalty on an adversary to compel them do something (or stop doing something)[3].

Make no mistake, our understanding and formulation of deterrence and compellence underwent a renaissance during the Cold War that has continued to this day (albeit with short periods of retarded development). Few if any works pushed the field forward in single leaps more than Shelling's[4], which brought a new comprehensive view of the key principle of deterrence, compellence, and the union of the two – coercion – as related to the strategy of conflict. Countless others also deserve credit for driving the field forward. Over the years the basic principle of deterrence by threat of punishment has grown in complexity. For example, not only considering the threat of imposing a cost given an adversary's action, cost(action)[5], but the probability of imposing that cost conditioned on the adversary's action $p(\text{cost}|\text{action})$[6]. Or deterrence by denial, which seeks to deter an adversary by denying their potential benefits of carrying out a hostile action. Or deterrence through encouraging restraint[7], entanglement[8], resilience[9], etc. Given the soft definition to most of these concepts and their interrelation, it is not surprising that it can at times be difficult to understand the relative import of one method of deterrence over the other, or even distinguish between some of the methods[10]. This begs the question, is there a way to unify these concepts into a coherent whole? The answer to this question is all the more relevant with the U.S.'s recent focus on integrated deterrence[11], which should involve some consideration of the right balance across our deterrence toolkit In

[2] Note that by adversary, we simply mean one's opponent in conflict. This could just as well be an ally or enemy, the calculus of coercion is agnostic, just as Schelling notes that "deterrence is as relevant to relations between friends as between potential enemies." (p 11 Schelling, Thomas C. *The Strategy of Conflict*. Cambridge, Mass: Harvard University Press, 1960; hereafter Schelling 1960.)

[3] Whereas the objective of deterrence is for adversary to maintain the status quo regarding a particular action, the objective of compellence it to have the adversary change the status quo regarding a particular action.

[4] Schelling 1960 and Schelling, Thomas C. *Arms and Influence*. Yale University Press, 1966; hereafter Schelling 1966.

[5] We have colorcoded each of the eight levers in an attempt to help the reader distinguish them.

[6] A concept central to the strategy of the threat that leaves something to chance (Schelling, 1960 p187; Schelling 1966 p92).

[7] DoD "Deterrence Operation Joint Operating Concept", Version 2.0, December 2006

[8] Joseph S. Nye Jr, "Deterrence and Dissuasion in Cyberspace," International Security 41, no. 3 (2017): 44-71

[9] Guillaume Lasconjarias, "Deterrence through Resilience - NATO, the Nations and the Challenges of Being Prepared", NATO Eisenhower Paper 7, Research Division - NATO Defense College, Rome May 2017

[10] For example, it is not entirely clear what the distinction between deterrence by denial and resilience are. It appears resilience attempts to deny one's adversary their objective of causing long-term harm to you by being resilient to their attack, which would then make it at most a subcategory of deterrence by denial.

[11] The White House *National Security Strategy*, *National Defense Strategy*, and *Nuclear Posture Review*, October 2022.

response to this question and need, we present the eight fundamental levers of coercive conflict in explicit form[12], to which all coercive methods can be mapped.

[12] There is math in this article which at first will likely evoke a repellent response among many readers. We feel confident in this forecast because we have seen such a response when presenting this material firsthand. We beg the reader to push past this initial impulse. We promise that the math in this article requires you to only consider eight terms and their elementary relation (addition, subtraction, multiplication, and division) in order to extract the bulk of the value. In principle this material is well within the reach of anyone with a high school diploma who is willing to devote an hour of their time.

The Complete Calculus of Deterrence

Given the widespread and lasting import of deterrence it is not surprising that all of the general deterrence concepts necessary to develop a complete and explicit formula exist in one form or another in the vast amount of existing related literature. Our task is simply to combine them in a complete explicit form. Several authors have even expressed the deterrence calculus in explicit form, albeit incomplete and typically relegated to the footnotes[13]. Glaser provides an explicit formulation of the calculus of deterrence being successful if "(Probability of U.S. carrying out threat X Costs if threat carried out) > (Probability of accomplishing the action X Benefits of the action)"[14]. In other words, assuming rational actors, we achieve deterrence when our adversary perceives that their costs associated with their action (cost(action)) times the probability of that cost being imposed ($p(\text{cost}|\text{action})$) is greater than their probable benefits ($p(\text{benefit}|\text{action})$ × benefit(action)), or more compactly:

$$\frac{p(\text{cost}|\text{action}) \times \text{cost}(\text{action})}{p(\text{benefit}|\text{action}) \times \text{benefit}(\text{action})} > 1.$$

Equation 1

Thus, we want to maximize their perceived cost that they will have to pay if they carry out a given action (cost(action)), as well as their perceived probability of having to pay that cost ($p(\text{cost}|\text{action})$). At the same time, we wish to minimize, or deny, the benefit that they expect to receive from carrying out the action (benefit(action)), as well as their estimate of the probability of receiving that benefit ($p(\text{benefit}|\text{action})$).

Note that each of the terms in Equation 1 is a function of the action. In other words, the cost one threatens to impose depends on the action they are deterring. Also note that the adversary's perceived probability of a cost being imposed can vary as a function of both the action and cost[15], and the adversary will often be uncertain about the associated probability function, see for example Figure 1. Whether they are aware of it or not, when one speaks of manipulating 'risk' in deterrence strategies, they mean manipulating these probability distributions and their associated uncertainty. In Appendix A we explore another concept related to these probabilities.

[13] Perhaps one of the earliest is Bruce Russett's "The Calculus of Deterrence, 1963, The Journal of Conflict Resolution Vol. 7, No.2, pp. 97-109", esp. p. 107 footnote 14. We can only guess that no one has formulated these concepts into a complete and explicit form due to the repellence of mathematical notation in the field. We have experienced few things less constant than this response, and also think back to Schelling's preface to the 1980 edition of " The Strategy of Conflict".

[14] Charles L. Glaser, "Analyzing Strategic Nuclear Policy", 1990, Princeton University Press, Princeton New Jersey, p. 20. Note that this explicit formulation is also relegated to the footnotes.

[15] Since $p(\text{cost}|\text{action})$ and $p(\text{benefit}|\text{action})$ are often distributions, technically you should integrate the terms of Equation 1, and similar equations in this paper. For example, $\int p(\text{cost}|\text{action}) \times \text{cost}(\text{action})\, d\text{cost}$. If one is attempting to maximize their expected gains, as is the case in utility or game theory, then the bounds of this integral are $-\infty$ to $+\infty$. If, however, the adversary is risk adverse or risk acceptant it may be more appropriate to integrate over a subset of the cost/benefit space. For notational simplicity, and to avoid unnecessarily complexity that might stand in the way of conveying the core concepts, the integrals are not shown in the equations.

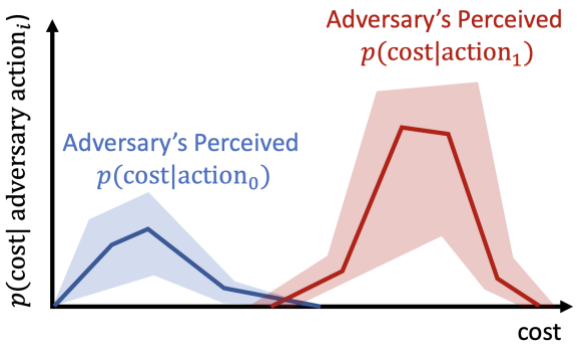


Figure 1: A carton to demonstrate the concepts that the perceived probability of imposing a cost can vary as a function of both the action (red vs blue) and cost (red and blue lines), and the adversary will often be uncertain about the associated probability function (shaded regions). In this cartoon the adversary would perceive that they run less risk by carrying-out action 0 versus 1.

It is sometimes overlooked that from the perspective of one's adversary, cost(action) includes both the threatened cost ($\text{cost}_{threatened}(\text{action})$) and whatever investment cost the adversary must pay in order to carry out the action ($\text{cost}_{investment}(\text{action})$). In other words,

$$\text{cost(action)} = \text{cost}_{\text{threatened}}(\text{action}) + \text{cost}_{\text{investment}}(\text{action}).$$

Equation 2

A pure deterrence by denial strategy will only be successful when the investment cost is not small relative to the potential benefits. Unfortunately for the U.S., this is not the case in the cyber-domain where the investment costs of many cyber actions are much smaller than the potential benefits. This is the reason the U.S. cyber security strategy prior to 2018, which was almost purely based on deterrence by denial, was bound to be ineffective. It could only have been successful had we almost perfectly denied the adversary benefits (either $\text{benefit(action)} \approx 0$, or $p(\text{benefit}|\text{action}) \approx 0$), which is inconceivable in cyber.

While Equation 1 is explicit, and as the cyber example above shows it can be useful, it is not complete. To complete the deterrence calculus formula, we need to incorporate the concept of encouraging restraint[16]. In other words, account for the fact that the rational adversary must simultaneously weigh the potential costs and benefits of not carrying-out the action. In other words, it is possible to encourage adversary restraint by decreasing the probability of a negative cost if they don't take the hostile action ($p(\text{cost}|\sim\text{action}) \times \text{cost}(\sim\text{action})$) or similarly increasing the probability of reward if they don't take the hostile action ($p(\text{benefit}|\sim\text{action}) \times \text{benefit}(\sim\text{action})$), in addition to denying benefits and imposing costs. Combining the concept of encouraging restraint with Equation 1,

$$\frac{p(\text{cost}|\text{action}) \times \text{cost(action)} + p(\text{benefit}|\sim\text{action}) \times \text{benefit}(\sim\text{action})}{p(\text{benefit}|\text{action}) \times \text{benefit(action)} + p(\text{cost}|\sim\text{action}) \times \text{cost}(\sim\text{action})} > 1.$$

Equation 3

[16] See for example the DoD "Joint Operating Concept: Deterrence Operations", Dec. 2006

Regarding a specific action there are only two possibilities at any given time: you can either carry-out that action or not carry-out that action. For each there will be both some possible benefit and cost associated with that specific action[17]. Thus, we know that Equation 3 is the complete form regarding the deterrence of a given action.

Fundamentally the terms of Equation 3 are the eight levers of deterrence. There are no more, there are no less. The game of deterrence reduces to maximizing the numerator relative to the denominator.

Some Properties of the Eight Levers of Deterrence

There are several properties of Equation 3 that are worth noting. Some are inherent in the mathematical structure, while others are a result of how these terms are typically realized and interpreted.

The direct coupling of the cost/benefit terms with their associated probabilities is inherent in the mathematical structure. Given their coupling it often makes sense when designing policy to consider the multiplicative terms together. For example, it may be impractical to devote resources to increasing the ability to impose a cost if the probability (or credibility) of imposing that cost remains low.

One of the more important properties is that $p(\text{cost}|\text{action})$ and $\text{cost}(\text{action})$ are the only levers that might directly lead to escalation; thus, it is most stable if you can change the adversary decision calculus by operating the other levers. That said, there are at times strategies rely on the perception of increased instability.

The $\text{cost}(\sim\text{action})$ is an inherently difficult lever to manipulate and change the deterrence calculus. Primarily because $\text{cost}(\sim\text{action})$ is highly correlated with an adversary's ability to impose cost (i.e., $\text{cost}(\text{action})$) or deny benefits (i.e., decrease $p(\text{benefit}|\text{action}) \times \text{benefit}(\text{action})$). This is at the heart of the security dilemma. For example, nuclear weapons work as a deterrent because they have an incredibly large $\text{cost}(\text{action})$ term in the deterrence calculus. However, assuming a secure nuclear capability, nuclear weapons can impose their cost irrespective of an adversary's action, i.e., $\text{cost}_{NW}(\text{action}) = \text{cost}_{NW}(\sim\text{action})$. Thus, these terms counterbalance each other out in Equation 3. Nuclear weapons work as a deterrent because the probability of launching a nuclear attack on someone if they don't carry-out a hostile action ($p(\text{cost}_{NW}|\sim\text{action})$) is fortunately very small. Perhaps in an ideal world there would be such a thing as perfect and purely defensive capabilities and one could decouple the $\text{cost}(\sim\text{action})$ lever from the others. Ultimately though the offensive-defensive (i.e., dual-capable) nature of much of a nation's power ensures that $\text{cost}(\sim\text{action}) \approx \text{cost}(\text{action})$.

Given the coupling of the cost of action and in-action terms, it becomes all the more important to skillfully increase the $p(\text{cost}|\text{action})$ term and decrease the $p(\text{cost}|\sim\text{action})$ term if one

[17] Although sometimes these can take on a value of zero.

wants to favorably manipulate the overall deterrence calculus. Otherwise, there is potential for the terms in the numerator and denominator to balance each other out and there be no net deterrence effect. However, manipulating these terms in opposite direction is easier said than done, since appearing more threatening to increase $p(\text{cost}|\text{action})$ would seem to be positively correlated with an adversary's perceived $p(\text{cost}|\sim\text{action})$. Especially after carrying-out a prior threat, and especially if that cost imposition may have been made in error. It is easy to imagine that both the $p(\text{cost}|\text{action})$ term and the $p(\text{cost}|\sim\text{action})$ term increased for many countries' perception[18] of the U.S. after the 2003 invasion of Iraq and especially after it was revealed that there were no viable weapons of mass destruction[19], which was the justification for the invasion. If one must carry out actions that may be perceived as threatening to deter a given adversary[20], then it is important that the threat should be perceived as justified to all other observers (or at least the subset of observers whose deterrence calculus you care about). In other words, ensuring that your threats are consistent with relevant laws and norms as well as not making a mistake and imposing a cost when an adversary didn't carry-out the accused action. Similarly, a clear declarative policy can help provide empirical evidence to decrease the uncertainty associated with the two cost imposition probabilities.

In general, it may be beneficial from a purely mathematical deterrence calculus perspective to decrease the $\text{benefit}(\text{action})$ lever, however in practice this is not a practical lever since it is typically directly correlated to a nation's strength. For example, logically you could deter someone from robbing you by giving away all your money but in most circumstances this is counterproductive. That is not to say that this lever is never intentionally manipulated. For example, an army that disperses and flees the battlefield does so because the individuals are trying to change the adversary's decision calculous by decreasing the benefit of continued attack below $\text{cost}_{investment}(\text{continued attack})$. All said, it is often preferable to manipulate the $p(\text{benefit}|\text{action}) \times \text{benefit}(\text{action})$ multiplicative pair by decreasing the $p(\text{benefit}|\text{action})$ term.

[18] Since it is so important a concept it is worth the aside to explicitly state what may be obvious to many. Threats and actions taken to deter one adversary will affect the deterrence calculus of all other observers.

[19] Hoar, Jennifer. "Weapons Found In Iraq Old, Unusable". June 23, 2006. CBS News. Archived from the original on 1 April 2019. Retrieved 02 September 2021.

[20] And it appears that this is sometimes the case, recall the aforementioned discussion about the inefficiency of the pre-2018 U.S. cyber deterrence policy because it lack the credible threat of cost imposition.

The Eight Levers of Coercion

At the outset we promised to provide the eight levers of coercion. So not just the mechanics of deterring an adversary from carrying-out an action, but also the mechanics of compelling an adversary to carry-out a different action. Conveniently the calculus of compellence is the same as Equation 3 just with the inequality reversed. Thus, in the case of compellence the objective is to minimize the numerator of Equation 3 relative to the denominator.

Conclusion

As noted, there are few concepts more important to the security of a nation and peace in this world than the concept of deterrence. It is my hope that by presenting the explicit and complete form of deterrence that nations, states, and the like will be better able to defend themselves. Ironically, as is too often the case, progress with defensive intentions results in simultaneous progress towards offensive capability. In this case we showed that the eight levers of deterrence, and their relation, are the same as those for compellence. Perhaps an ancillary benefit of the explicit deterrence presentation is that it should enable more rapid progress with computational deterrence decision support.

While technically one only needs the deterrence equation to reap the bulk of the benefits of this work, we hope that we added some richness to its interpretation by explaining some of the properties and relations of the various levers. For those readers that still feel this is all a bit too abstract we have included in Appendix B an example of how Equation 3 can be used to think through a possible solution to cyber-deterrence.

Finally, it is important to note that deterrence is dynamic and your adversary's decision calculus levers are inexorably linked to your decision calculus levers[21]. This is probably best formalized in the game theoretic treatment of extensive form games[22]; however, we have included in Appendix C a conceptual example of how this interplay can be important.

[21] Schelling 1960 p21-22, 54.

[22] See for example, Powell, Robert. *Nuclear Deterrence Theory: The Search for Credibility*. Cambridge: Cambridge University Press, 1990 and references therein.

Appendix A: The Probability of Extreme Events

At times it may appear to be a worthwhile exercise to attempt to simply the problem of deterrence calculus by considering just the probability of an extreme cost being imposed (e.g., a nuclear weapons response attack) to a range of actions rather than complicating matters by considering all the possible costs that might be imposed for a set of actions (e.g., Figure 1). This might be a reasonable simplification if such an extreme cost is much larger than all other possible costs. For example, consider Figure 2 which explores the hypothetical probability that the U.S. will respond to an action with a nuclear attack. For simplicity's sake let us assume that the U.S. has adopted a sole purpose policy. Then the probability of the U.S. launching a nuclear response attack may be 100% for a nuclear attack on the U.S. or its allies and zero for any lesser action (dashed blue line). However, the adversary does not trust that the U.S. will actually follow this policy and thus their perceived probability $\mathrm{p}(\text{U.S. nuclear response}|\text{action})$ is non-zero for actions less hostile than a nuclear attack on the U.S. or its allies. The adversary has a fair amount of uncertainty associated with this probability (orange shaded region) such that for any given action (i.e., single location on the x-axis) there is a range of probabilities (e.g., the gray dash-dot line). When performing their decision calculus for taking a given action the adversary might assume the mean of that marginal probability (gray X; $\langle \mathrm{p}(\text{cost}|\text{action}) \rangle = \int_{-\infty}^{\infty} \sigma\big(\mathrm{p}(cost|action)\big)\mathrm{dp}(cost|action)$, where σ is the uncertainty function along the dash-dot line), or if they are conservative they might assume some upper confidence limit probability associated with that action (gray circle), or the lower confidence limit if they are adventurous (gray diamond).

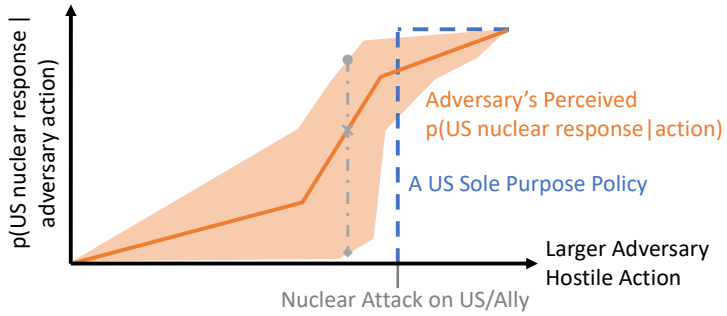


Figure 2: A conceptual cartoon of both the U.S.'s probability of responding to an adversary's hostile action as a function of the hostility of that action (blue dashed curve), and the adversary's uncertain perception of that probability (orange shaded region). For simplicity's sake the U.S. has adopted a sole purpose policy such that the probability of the U.S. launching a nuclear response attack may be100% for a nuclear attack on the U.S. or its allies and zero for any lesser attack.

Appendix B: Comprehensive Batch Response Cyber Deterrence

What follows is primarily an example fit for the purpose of demonstrating how Equation 3 and the eight levers of deterrence can be used as a tool to consider deterrence policy. To burn off some of the fog that may exist surrounding the abstract concepts in the body of the report we suggest a definite cyber-deterrence policy. We do not claim that this is a viable strategy, nor complete in considering the array of adversaries worthy of a tailored deterrence approach.

Past and Current Strategy

As previously noted, U.S. cyber security strategy prior to 2018 was almost purely based on denial. Since self-imposed costs of cyber operations are close to zero (given the low cost of hardware and software needed for cyber-attacks, coupled with automation) such a strategy was bound to fail. As can be seen from Equation 3, if the other terms are zero it is only possible to deter the adversary if you can perfectly deny their benefits (either $\text{benefit}(\text{action}) = 0$, or $p(\text{benefit}|\text{action}) = 0$), which is inconceivable in cyber.

In 2018 the Defense Cyber Strategy[23] outlined the current strategy called “persistent engagement”, which changed from reactive "crisis response" to continual active operations, including a “defend forward” component with operations in adversary networks. This enabled more, but intentionally limited, competition. Simultaneously increasing the probability of imposing a cost on the adversary and the cost, although both were intentionally limited in an effort to reach a state of “agreed competition” to limit escalation. Persistent engagement is a step in the right direction compared to past strategies, and at times been effective (2018 U.S. National Elections). However, the rate and severity of strategic level cyber-attacks are increasing (e.g., the 2019-2020 SolarWinds, 2021 Colonial Pipeline, 2021 JBS, etc.), which is indicative that the limited increase in the cost ($\text{cost}(\text{action})$) and probability of imposing that cost ($p(\text{cost}|\text{action})$) were not enough to chance the adversary calculus for even some large actions, let alone many more less egregious actions. Thus, let us use consider the eight levers of deterrence and consider what policy changes might help.

It seems useful to consider the levers in their multiplicative pairs (e.g., $p(\text{cost}|\text{action}) \times \text{cost}(\text{action})$) since these levers are most strongly coupled. We should also ensure that we consider all eight levers in an effort of not repeating past mistakes of incomplete deterrence policies. Finally, as previously noted, there are six levers of deterrence which do not risk escalation. It would be ideal if these were sufficient to deter the adversary without the need to impose cost, thus we will explore these first and try to determine is there is a potentially non-escalatory solution.

Decreasing Perceived Cost of No-action

$\text{cost}(\sim\text{action})$

This is an inherently difficult lever for the U.S. to manipulate because it is harder for the adversary to estimate a relation between the absence of action (i.e., no action) and effect than

[23] https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

it is between action and effect. More critically though, $\text{cost}(\sim\text{action})$ is highly correlated with a country's ability to impose cost (i.e., increase $\text{cost}(\text{action})$) or deny benefits (i.e., decrease $p(\text{benefit}|\text{action}) \times \text{benefit}(\text{action})$). This is at the heart of the security dilemma. For example, nuclear weapons work as a deterrent because they have an incredibly large $\text{cost}(\text{action})$ term in the deterrence calculus. However, assuming a secure capability, nuclear weapons can impose their cost irrespective of an adversary's action, or $\text{cost}_{NW}(\text{action}) = \text{cost}_{NW}(\sim\text{action})$. Thus, these terms counterbalance each other out in Equation 3. Nuclear weapons work as a deterrent because the probability of launching a nuclear attack on someone if they don't carry-out a hostile action ($p(\text{cost}_{NW}|\sim\text{action})$) is fortunately very small. Perhaps in an ideal world there would be such a thing as perfect and purely defensive capabilities and one could decouple the $\text{cost}(\sim\text{action})$ lever from the others. Ultimately though the offensive-defensive (i.e., dual-capable) nature of much of the U.S.'s power ensures that $\text{cost}(\sim\text{action})$ will remain high.

$p(\text{cost}|\sim\text{action})$

To decrease the perceived probability of the U.S. imposing a cost if our adversaries don't carry-out a hostile action, we should in general not do threatening things to other agents. However, this is diametrically opposed to the cost imposition levers. If we must carry out actions that may be perceived as threatening to deter a given adversary, then it is important that this should be perceived as justified to all other observers. This is difficult given that perceptions will vary widely from observer to observer, especially in cyber where norms and laws have not been established. Ways to decrease our adversary's perception of this probability include: (1) defining laws/norms and holding to them, (2) publishing a clear declarative policy to facilitate discussion before we need to impose cost, and (3) if possible, warn others before imposing costs.

Conclusion: It is important to manage these levers (especially in non-cyber domains), however it is insufficient to change current calculus alone given the inescapable security dilemma.

Increasing Perceived Benefit of No-action (i.e., The Pull of Success)

$p(\text{benefit}|\sim\text{action})$

To increase the perceived benefit of not carrying out a hostile action against the U.S., we need to value non-actors more, or better yet positive actors (but let us not complicate matters by considering compellence in this simple example). To increase their perceived probability of receiving a reward for being a good actor, we could formalize the process of reward distribution. Perhaps this could be done by establishing formal international collaborations, such as NATO CCD COE. Although these may be better structured if they were not tied to regional alliances since cyber does not share the same regional confinements and the targets are often outside of our alliances.

$\text{benefit}(\sim\text{action})$

While it is easy to exercise this lever with our allies (e.g., through information and talent exchanges, or favored trade deals), it is more difficult to exercise with our adversaries due to associated uncertainty that they may later use the benefits against us. That said, it should not be completely written off. There is precedent for incentivizing some hackers to not exploit insecurities they find (e.g., bug bounty programs, or hiring them to work for you legitimately). The DOJ and IC should conduct a study to determine the legality and feasibility of such a

national program. While State and Treasury should consider what state level benefits might be extended.

Conclusion: The potential for win-win scenarios makes this worth exploring further, however there are many cases where it is unlikely to exceed $benefit(action)$ *and still be a cost-effective strategy.*

Decreasing Perceived Benefit of Action

$p(\text{benefit}|\text{action})$

It is the U.S. public and private cyber defense measures that predominately decrease the adversary's perceived probability of receiving some benefit from their hostile action. For the most part, existing policy has already enumerated many of the necessary actions: (1) a focus on securing critical infrastructure and supply chains, (2) better USG partnerships with allies and private industry, (3) better incentivization of best cyber security practices, perhaps through insurance requirements or Cyber Maturity Model Certification for DoD contracts, and (4) more clearly defined responsibility, authority, as well as proportionate resources. Ultimately though, we need to get on the right side of the cost imposition curve and the $p(\text{benefit}|\text{action})$ lever will not get us there.

$\text{benefit}(\text{action})$

In general, this is a difficult lever for the U.S. to manipulate defensively. One potential area is negotiating with cyber criminals. While this may be against most USG policy, it may be a viable tactic for private companies. One could imagine cyber insurance companies managing the negotiations to pursue a smaller payout based on compiled information as well as preassessment of company risks.

Conclusion: While denial is an essential element of deterrence, we need to get on the right side of the 'cost imposition curve' and cyber denial alone will not get us there.

Increasing Perceived Cost of Action

Discussion of the previous levers suggests that it will be very difficult to significantly change the decision calculus of all adversaries without imposing costs, albeit at the risk of escalation.

$p(\text{cost}|\text{action})$

As previously noted, 'defend forward' and 'persistent engagement' are a good start to increasing the adversary's perceived probability of receiving a cost for their actions. However, there are three key limitations which impede our efforts: (1) it is difficult to respond to 'salami tactics' or 'corrosive cyber-attacks', thus for the most part the adversary gains a small benefit at no cost, (2) it is difficult to quickly achieve the necessary accurate and precise attribution to confidently respond to most attacks, and (3) scale is in our adversaries' favor (large attack surface, many adversaries, and many separate attacks). That said this lever can still be increased by: (1) increasing information sharing among USG institutions, allies, and partners, (2) increasing uncertainty associated with $p(\text{cost}|\text{action})$, leveraging human psychological flaws of overestimating the likelihood of rare events, and (3) introduce a new Batch Response Strategy to cost imposition.

$cost_{action}$: Batch Response Strategy to Cost Imposition

We can simultaneously navigate the 'salami tactics', attribution, and scale problems while getting us on the right side of the cost imposition curve by establishing a cyber security policy that responds to cyber-attacks in batch rather than on a case-by-case basis. This begins by keeping track of smaller attacks as best we can and maintaining a cumulative total for each associated suspect. We can overcome the unavoidable uncertainty associated with attribution of individual events by leveraging the statistical property that uncertainty decreases roughly proportional to the square root of number of attacks (the exact scaling can be slightly more complicated). This could be done with existing ATT&CK pattern attribution methods. As part of the strategy, it may be worth communicating this running tally publicly[24]. Eventually, at a time of our choosing, impose a cost on the adversary proportional to the sum of their actions. This is key to getting us on the right side of the cost imposition curve.

There is the added benefit that this approach synergistically increases both the amplitude and uncertainty around perceived $p(\text{cost}|\text{action})$. This approach will be more effective if both the private sector and allies to work with us for an accurate tally[25]. The IC will play the key role maintaining an accurate tally. The approach also requires establishing new norms, tactics, techniques, and procedures, as well as the associated talent. It would also require increased management of risk associated with the intentional escalation.

As previously noted, if we are not careful, any progress we make by imposing larger $\text{cost}(\text{action})$ could be undone by unintentionally increasing the perceived cost of no-action. Thus, we must clearly define both for ourselves and more importantly for our adversaries the $\text{cost}(\text{action})$ we will impose as a function of type and scale of attack. As well as how the cost associated with individual attacks will accumulate. We need to communicate this action both through overt as well as clandestine actions. To maintain credibility, we need an open policy that acknowledges the challenges of imposing costs all the time, but that we will do it when we can. Combined with the batch response strategy, this should stabilize escalation as the level of punishment is communicated and increases incrementally as an adversary continues to attack us (in a sense naturally using finer grained escalation, while ensuring the eventual cost is proportional to the total attacks). In many cases we will likely require cost imposition through domains outside of cyber as the total cost increases beyond that that can be applied through cyber means (especially without cascade collateral effects that might risk unintentional escalation).

Conclusion: There are currently unavoidable limitations to our ability to impose costs on adversaries. A batch response strategy can overcome these limitations, although it will require establishing new norms and increased risk management.

---

[24] This of course requires much further consideration. How much do risk reveling about your capabilities by making some of this information public. Also, if you aren't actually every to impose costs on these actors then it could serve as empirical data that is counterproductive by decreasing $p(\text{cost}|\text{action})$.

[25] At least incompleteness in the tally only decreases the efficiency of the policy and does not unintentionally increase escalation. Note also that there is potential for participants to weaponize the tally, however robust statistics could help mitigate this risk.

Appendix C: The Dynamics of Deterrence

In general, it is important to consider the interplay of yours and your adversary's decision calculus levers. Consider for example the interplay of Red and Blue decision calculus levers of Blue deciding to invest in an anti-ballistic missile (ABM) system, Figure 3. Blue considers paying the investment cost of an ABM system at some initial time (①) realizing that this will decrease Red's perceived benefit from carrying out a nuclear weapon (NW) attack on Blue (②) at a future time, and thus provide an increased benefit to Blue (③). The benefit potentially outweighing the ABM investment cost and making it worthwhile for Blue to take the action of building an ABM system.

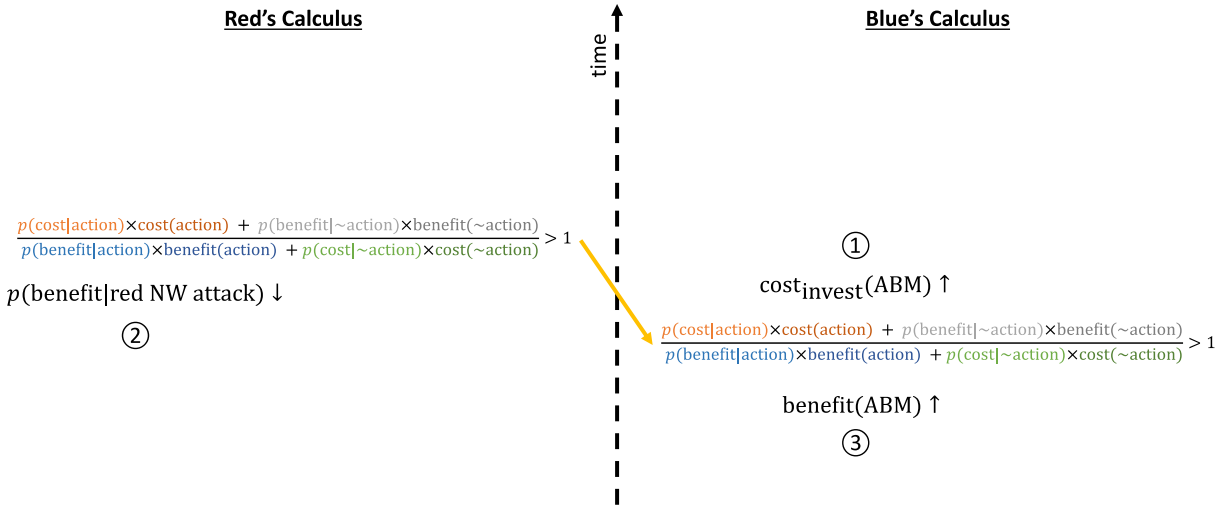


Figure 3: Limited consideration of the decision calculus dynamics of Blue investing in an anti-ballistic missile (ABM) system.

However, as can be seen from Figure 4, Red will look forward in time and realize that Blue's ABM system will decrease Blue's perceived cost of carrying out a nuclear weapon attack at some future time (④) since it will decrease the cost Red is able to impose with a retaliatory strike. This will increase Red's perceived cost of not carrying out a nuclear weapon attack before Blue's ABM system is online (⑤), potentially canceling out Blue's actual benefit of developing an ABM system (⑥). Of course, whether any of these shifts of the levers will flip the deterrence inequality in favor of acting or not will depend on the relative amplitude of the terms. Even without actual values for each of the terms, the decision calculus formalism can help decision makers more comprehensively think through problems and identify key uncertainties that may need to be addressed before making a decision.

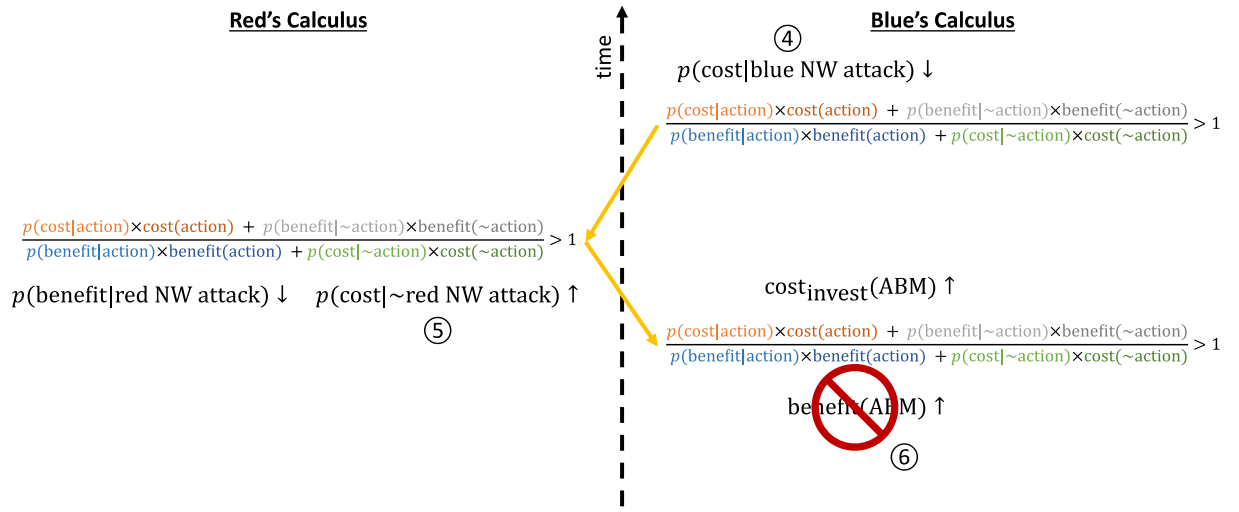
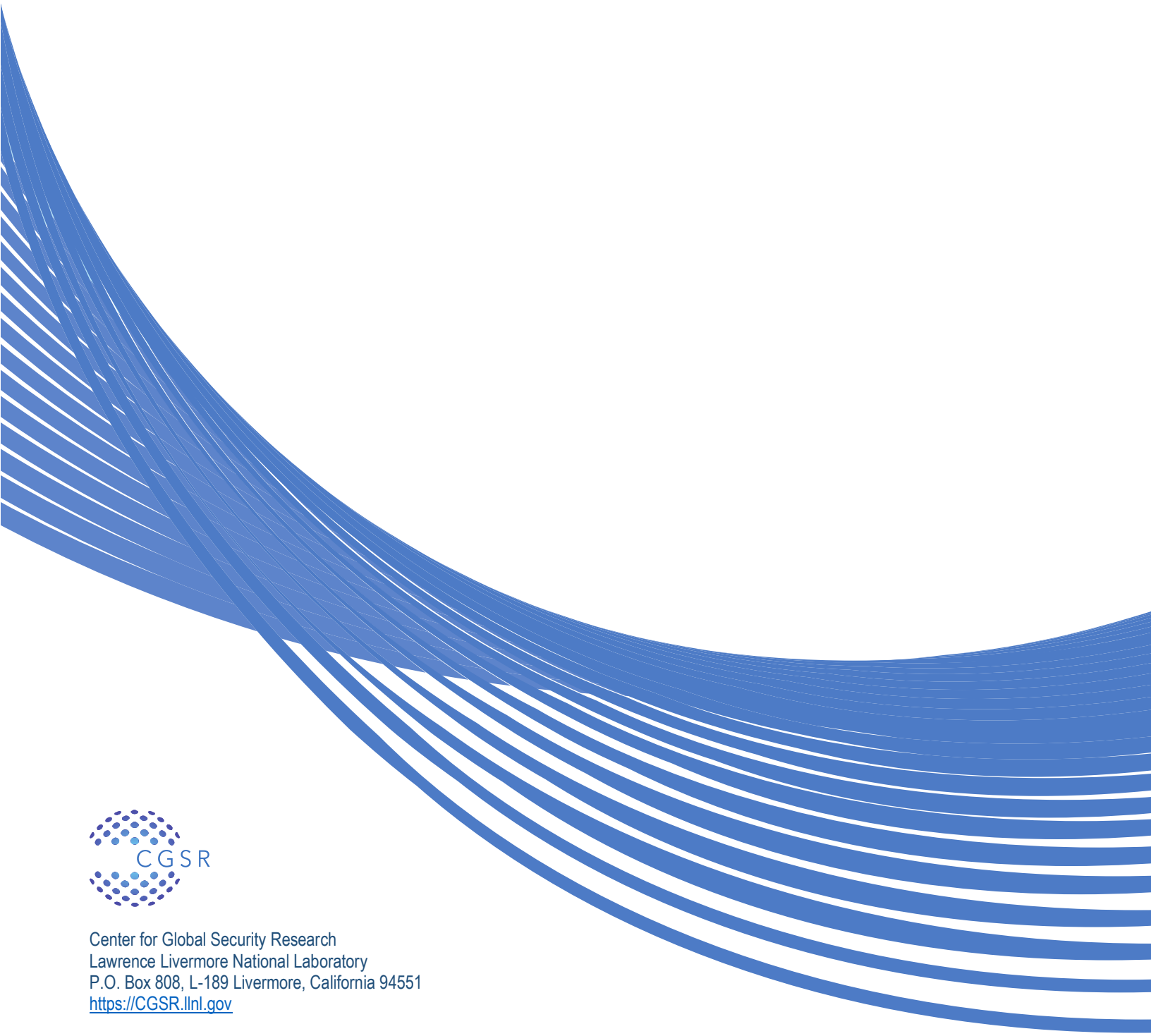


Figure 4: Extended consideration of the decision calculus dynamics of Blue investing in an anti-ballistic missile (ABM) system.



Center for Global Security Research
Lawrence Livermore National Laboratory
P.O. Box 808, L-189 Livermore, California 94551
https://CGSR.llnl.gov

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344. LLNL-TR-843013