Cybered Competition, Cooperation, and Conflict in a Game of Imperfect Information

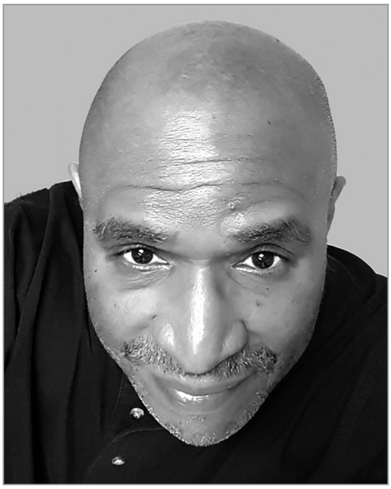
Hiram Henderson

ABSTRACT

This article proposes that "the strategy of conflict," or game theory, can enhance joint planning processes applied to cybersecurity operations. Game theory could perhaps prove most useful during operational design for understanding actors, tendencies, and potentials actions inherent in cooperation, competition, and conflict situations. A canonical anti-coordination game, Hawk-Dove, is employed to explore equilibrium evolutionary game strategies and deterrence outcomes applicable to cyberspace operations. Tractable extensions to the Hawk-Dove game are introduced to understand mechanisms for signaling, reputation, norms, and ambiguity in deterrence. Game parameters are transferred to a model of Surprise-Attack for comparison. Advantages and disadvantages for incorporating games in the joint planning process are considered.

The Strategy of Conflict

Thomas Schelling's *The Strategy of Conflict*[1] is a collection of essays that presents a "vision of game theory as a unifying framework for the social sciences."[2] The Nobel laureate proposed calling this framework the study of "the strategy of conflict."[3] He regarded many conflict situations as bargaining problems with elements of opposed and common interests. For this reason, he argued the analysis of non-cooperative games was essential for understanding the theory of deterrence in international security, and more broadly for the study of "rational, conscious and artful" conflict behavior.



Hiram Henderson is a Senior Plans Analyst assigned to the U.S. Cyber Command (USCYBERCOM) in the J5 (Plans and Policy) directorate. His prior civilian assignment was at Joint Force Component Command-Network Warfare (JFCC-NW). As a Navy Reserve officer, he has several long-term assignments supporting information operations at the former U.S. Space Command, U.S. Strategic Command, and U.S. Special Operations Command. He studied economics at the University of Illinois, Chicago (B.S.), and University of Chicago (M.A.) and has a diploma from the Air War College. He is currently pursuing graduate study in international affairs at King's College London. He is an advocate for the wider use of games in joint planning and operational design.

In game theory, a strategy is a complete plan of actions across all possible contingencies. In a military context, a strategy is the application of military power to attain political objectives, specifically "the theory and practice of use, and the threat of use, of organized force for political purposes."[4] A broader definition regards strategy as "a plan of action designed in order to achieve some end; a purpose together with some system of measures for its accomplishment."[5]

In most of this article, strategy is used in the narrower game-theoretic sense. However, before exploring games and their application to "cybered conflict"[6] and competition, it is helpful to review the contours of DoD cyber strategy in place, as well as mechanisms of deterrence. This will assist in ascertaining whether some game forms appear to fit stylized facts for competition or cyberspace.

Strategies in Cyberspace

The unclassified version of the *DoD Cyber Strategy 2018* prioritizes deterrence and competition in cyberspace and commits to an operating posture of "persistent engagement" and "defending forward" in cyberspace. Key passages in this regard are the following:

1) Deter malicious cyber activities: The United States seeks to use all instruments of national power to deter adversaries from conducting malicious cyberspace activity that would threaten U.S. national interests, our allies, or our partners.[7]

2) Persistently contest malicious cyber activity in day-to-day competition: The Department will counter cyber campaigns threatening U.S. military advantage by defending forward to intercept and halt cyber threats and by strengthening the cybersecurity of systems and networks that support DoD missions.[8]

In game logic, the *DoD Cyberspace Strategy 2018* represents a commitment to protect national security interests in cyberspace. It is executed through defensive cyberspace operations missions as authorized in forward and/or friendly cyberspace to contest, deny and defeat malign adversary campaigns in cyberspace. In a wider sense, the strategy also serves to set conditions for deterrence and shape norms for responsible behavior in cyberspace.[9]

Deterrence Approaches

Deterrence is the process of influencing the cost-benefit calculus of actors from taking unwanted actions. The fundamental strategies for deterrence are punishment and denial; both involve dissuasion by threats to impose costs and/or deny benefits. However, a wider view of deterrence also considers dissuasion involving reassurances or other inducements to encourage adversary restraint.[10]

In the Age of Enlightenment, legal thinkers reasoned that it was "better to prevent crimes than to punish them" for the benefit of society. The effectiveness of deterrence by punishment was said to depend on the severity, certainty, and celerity of punishments.[11] Such beliefs derived from utilitarian philosophy, which maintained that rational, self-interested individuals seek to maximize well-being or advantage.[12]

Deterrence by punishment can be specific (to individuals) or general (to populations). Deterrence is absolute when an actor completely avoids a prohibited action and is restrictive when actors restrain prohibited actions to reduce the risk or severity of punishment.[13] In the Cold War, nuclear "deterrence was specific and absolute."[14] However, general and restrictive forms of deterrence are the norm for crimes and political violence.[15]

Deterrence by denial seeks to deter unwanted action by "making it infeasible or unlikely to succeed," and by reducing an actor's confidence of success in reaching his goals.[16] Deterrence by denial involves commitment to the defense of vital interests.[17]

Deterrence in cyberspace will not be absolute and lower-level malign actions can never be prevented entirely. The wide array of threat actors to include nation-states, proxies and criminal organizations, requires that deterrence in cyberspace is tailored. It can be specific or general. The Deterrence Operations Joint Concept is the framework for decisively influencing the adversary's decision-making calculus in order to "prevent hostile actions against US vital interests."[18] The concept developed out of the need for a modernized deterrence framework applicable to a "broader range of adversaries and situations" in an evolving security environment[19]

The concept frames the three primary elements of deterrence decision calculus as:

- The benefits of a course of action
- The costs of a course of action
- The consequences of restraint (of not taking the course of action we seek to deter)[20]

Using these elements, the concept describes deterrence operations as:

> Deterrence operations convince adversaries not to take actions that threaten US vital interests by means of decisive influence over their decision-making. Decisive influence is achieved by credibly threatening to deny benefits and/or impose costs while encouraging restraint by convincing the actor that restraint will result in an acceptable outcome.[21]

Viewed through the deterrence joint concept, persistent engagement and defending forward in cyberspace can be characterized as strategies of deterrence through denial. They create frictions (or resistance costs) on malicious cyber activities from threat actors, while preserving space for diplomatic, informational, or economic responses.[22] The game constructs used here will assume unitary actors for decision-making and will abstract from internal political-bureaucratic considerations, as well as from "audience costs,"[23] that would otherwise affect strategy choices.

Many political economy models of war and deterrence are constructed as stage games, initially featuring periods of bargaining that transition to conflict when there is a failure to reach a diplomatic agreement.[24] However, the canonical models used here will have elements of cooperation and conflict, and hence bargaining in a sense is built in. We also assume participation constraints are met, which means playing the game leaves actors at least as well off as from abstaining from the game.

The Hawk-Dove Game

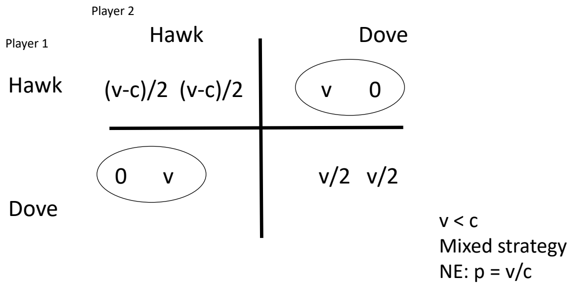
The canonical Hawk-Dove game represents a classic model of competition and conflict in game theory. The framework was developed in biology literature to describe evolutionary strategies within a species.[25] In this game, opponents fight over a resource, which is rival in consumption and has some value *(v)*. Fighting for this resource involves a cost *(c)* that represents the damage arising from conflict.

In normal form, Hawk-Dove is a simultaneous-move game of imperfect and complete information. Imperfect information means a player is unaware of strategies other players have chosen.[26] Complete information means that there is "common knowledge" of player types, payoffs, preferences, and strategies known by all players, and all players know that it is known by all players.[27]

In this game, hawkish strategies broadly are non-cooperative actions involving aggression or fighting. As applied to cyberspace, non-cooperative strategies will involve the projection of power. This includes cyberspace attack—actions that create denial and/or manipulation effects, as well as forms of cyberspace exploitation, which include intelligence, maneuver, information collection, attack-specific preparations, as well as other enabling actions that prepare for future operations.[28]

In contrast, cooperative actions will involve the absence of fighting in cyberspace, with greater emphasis on protection. This includes cyberspace security measures or actions to prevent unauthorized access, exploitation, or damage from general threats, as well as cyberspace defense actions to defeat specific threats that have breached, or are threatening to breach, cyberspace security measures.[29]

We consider cyberspace as a network good that grows in value as its use and connectivity expands. We will further suppose the value of cyberspace is common knowledge as is the cost of fighting. Players contest each other for advantage in this interconnected domain, competing for access, position, and control to support their informational or military objectives in the wider operational environment. This is represented in the abstract by attaining a greater share (or control) of *(v)*.



Player 1 \ Player 2	Hawk	Dove
Hawk	(v-c)/2 (v-c)/2	v 0
Dove	0 v	v/2 v/2

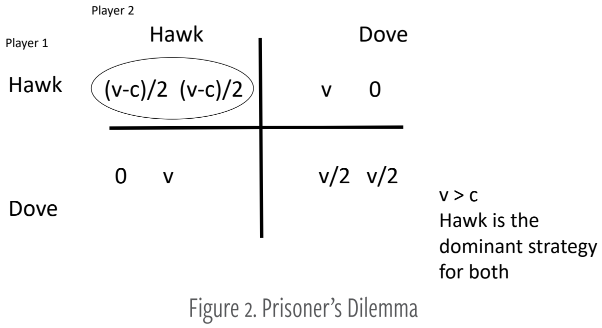
v < c
Mixed strategy
NE: p = v/c

Figure 1. Hawk vs. Dove

Payoffs in the Hawk-Dove game are displayed in Figure 1 and arranged within a 2x2 matrix as follows:

$$\text{hh } [\frac{(v-c)}{2}, \frac{(v-c)}{2}]\text{; hd } [v, 0]\text{; dh } [0, v]\text{; and dd } [\frac{v}{2}, \frac{v}{2}]$$

Nash equilibrium is a core solution concept in non-zero-sum games and represents the best responses of players to the best responses of all other players.[30] To fully enumerate equilibrium outcomes, we will consider two variants of the game with respect to the relationship of value to cost.



Player 1 \ Player 2	Hawk	Dove
Hawk	(v-c)/2 (v-c)/2	v 0
Dove	0 v	v/2 v/2

v > c
Hawk is the
dominant strategy
for both

Figure 2. Prisoner's Dilemma

When *v* > *c,* the game reduces to a Prisoner's Dilemma in Figure 2. This variant of the game has a single Nash equilibrium, where both players find it optimal to pursue non-cooperative (Hawk) strategies in cyberspace. As long as *v* > *c,* an increase in cost or reduction in value will not change the equilibrium outcome. This is because Hawk is a dominant strategy; i.e., it is the best strategy regardless of any action the other player takes. This outcome may correspond to cyberspace exploitation actions well below conflict threshold. High values along with low costs/consequences might explain why exploitation actions are so pervasive in cyberspace in equilibrium.

When $v < c$, the game becomes Chicken, and fighting becomes much more costly for the players. This variant of the game has two pure strategy Nash equilibria (where one player plays Hawk and the opponent, Dove), and one mixed strategy equilibrium, where players randomize between playing Hawk or Dove strategies. Absent prior coordination, play will not likely arrive at the pure strategy outcomes.[31] The mixed (randomizing) strategy equilibrium is:

$$p = \frac{v}{c}$$

In equilibrium, mixing toward fighting increases with value and declines with cost.[32] This variant of the game involves higher cost/consequence Hawk actions in cyberspace, with some scaling to a use of force. In a mixed strategy equilibrium, the frequency of fighting increases when (Hawk) actions have lower costs/consequences, and decreases when (Hawk) actions have higher costs/consequences.[33] This may explain why lower-level cyberspace attacks are more commonplace than damaging attacks at conflict thresholds.

As players randomize, another way to see the inverse relationship between fighting and costs is in the expected value (EV) of the game, which is given by:

$$\mathrm{EV} = \left(1 - \frac{v}{c}\right) \frac{v}{2}$$

The value of the game increases in costs because there are fewer fights.

In equilibrium, players mix to make their opponent indifferent between playing Hawk or Dove in terms of expected payoffs. Mixing is like game play in tennis, if the strategy space is limited to forehand and backhand shots. If a player becomes more proficient at her backhand, the opponent mixes in a fashion to neutralize that advantage, forcing her to play more forehand.

If there is asymmetry between players where $v > c$ for Player 1 and $v < c$ for Player 2, then fighting is more costly for Player 2. A pure strategy Nash equilibrium results where Player 1 always plays Hawk and Player 2 plays Dove. This situation involves imbalances in power and capacity. Although outside the strategy space of the game, the weaker player could find it advantageous to form alliances.

Hawk-Dove in Sequential Games

Schelling noted that a paradox arises in bargaining situations where the "power to constrain an adversary may depend on the power to bind oneself."[34] A player who can commit to an "irreversible sacrifice of freedom of choice" can obtain a better outcome.[35] To win the game of

Chicken, Schelling claimed, you need to rip off your steering wheel and wave it visibly in the air for your opponent to see.

In sequential form games, moves convey information. To illustrate credible deterrence commitments in Hawk-Dove, we take game payoffs and convert them to a simple, sequential (two-stage), extended-form game of perfect information. “A game is said to have perfect information if, throughout its play, all rules, possible choices, and past history of play by any player are known to all participants.”[36]

The extended-form game is represented in Figure 3 depicting a tree comprised of decision nodes, end nodes, and edges. A subgame begins at a decision node and includes all nodes that follow in the game tree. However, subgames cannot begin at the very first decision node of a game.

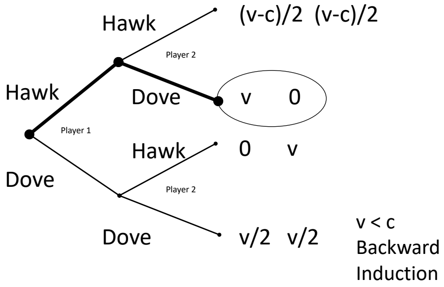


Figure 3. Hawk vs. Dove

In sequential games of complete information, the solution concept is subgame perfection. A Nash equilibrium is subgame perfect if it induces a Nash equilibrium in every subgame.[37] Through backward induction, the subgame perfect equilibrium path of play is that Player 1 plays Hawk and Player 2 plays Dove. Here Player 1 has a first-mover advantage. However, moving first does not always confer advantage under perfect information, for example, the hand game of Rock-Paper-Scissors.

If Player 2 could irreversibly commit to play Hawk if Player 1 plays Hawk, and signal this intent, she could deter Player 1 from aggression. Player 2 may do this by reducing her options (breaking off edges) on the game tree. The subgame perfect equilibrium path becomes Dove, Dove. The off the path equilibrium, where Player 1 would play Hawk with no signal from Player 2, is not reached. See Figure 4.

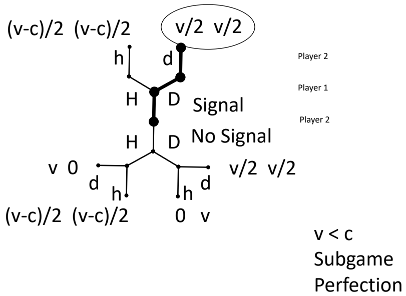


Figure 4. Hawk vs. Dove

Sequential games require trust that others play best responses, and that threats are believed. While situations involving complete and perfect information are unlikely to be encountered in cyberspace, signaling credible commitments enhances deterrence by presenting an adversary with clear choices.

Hawk-Dove with Incomplete Information

In games of incomplete information, or Bayesian games, players will not have common knowledge about other players, and may not know their types, actions, nor payoffs. Consequently, they may not believe other players' signals.

Assume Player 1 is the uninformed player who has a probability distribution of beliefs in an information set, where *(q)* is the probability (belief) of encountering a commit-type Player 2, when there is a threat signal, and *(r)* is the probability (belief) of encountering a commit-type Player 2 without a threat signal. Assume Nature *(N)* makes the first move, establishing informed Player 2 types.

The commit-type Player 2 will carry out threats to retaliate if Player 1 ignores the deterrence signal. The non-commit, or normal-type Player 2 will not honor promises or threats, and always plays a best response. This situation illustrates commitment problems that often arise in game forms.[38]

Both Player 2 types benefit from sending the same deterrence signal. The commit-type Player 2 will always send a deterrence signal, since not signaling is a dominated strategy, hence. The normal-type Player 2 also stands to gain if Player 1 is deterred, or plays Dove. Beliefs should be determined in accordance with Bayes' Rule; however for tractability, we will consider limiting cases involving beliefs.

Suppose Player 1 does not believe the signal *(q = 0)* and acts on that belief by playing Hawk. The normal Player 2 reveals her type by playing Dove. The commit Player 2 retaliates by playing Hawk, producing a situation in which deterrence breaks down. If Player 2 types were equally encountered in nature, this would seem an unreasonable belief, and perhaps very costly where c is sufficiently high.[39]

Alternatively, suppose Player 1 believes the signal *(q = 1)* and plays Dove. The normal Player 2 again reveals her type by playing Hawk, (see Figure 5). The commit Player 2 type plays Dove. In this case, deterrence holds.[40] This "pooling" is an example of the "threat that leaves something to chance."[41]

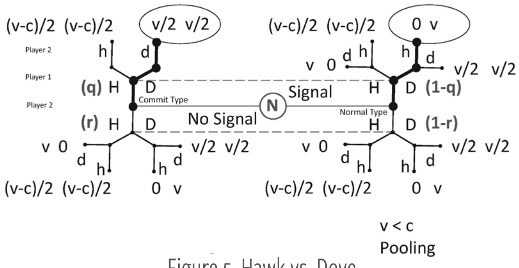


Figure 5. Hawk vs. Dove

Since Player 2's are unsure of Player 1's response, suppose Player 2's could also threaten to let things "slip out of hand." Albeit stylized, further suppose the normal Player 2 type presents Player 1 with the simultaneous-move Hawk-Dove as a continuation game, regardless of a deterrence signal.

Play in mixed strategies again yields an expected value of:

$$\text{EV} \quad = \quad \left(1 - \frac{v}{c}\right) \, \frac{v}{2}$$

which is less than

$$\frac{v}{2}$$

from the cooperative path.

In the restyled game, this enhancement has the effect of strengthening deterrence and assurances, since signaling is equilibrium and message dominated for the commit-type Player 2, and the normal-type Player 2 is now indifferent to sending a deterrence signal.

Applying the Intuitive Criterion,"[42] the commit-type Player 2 could send a signal and announce, "Seeing this signal should convince you that I am the commit Player type, since believing otherwise would not improve outcomes for other Player type, nor for yourself." If this speech is believed, Player 1 could reasonably set her belief to (q = 1), resulting in a separating equilibrium, see Figure 6.

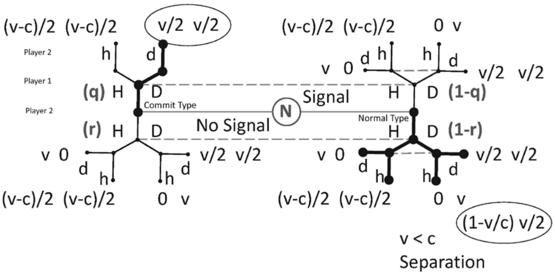


Figure 6. Hawk vs. Dove

In this restyled game, threats that leave something to chance along with credible signals can enhance deterrence in equilibrium.[43] When player interests align, signals are more informative, and when interests diverge, signals are less informative.[44]

In practice, decision-makers do not face black boxes as adversaries. They will have gained insights from past experiences to better understand their opponents and improve their outcomes.[45] Knowledge isn't perfect and information asymmetries are sources of fog and friction in deterrence.[46] If players had common knowledge of each other's beliefs, they could not agree to disagree.[47] Errors regarding an opponent's beliefs (or intentions) explain in many cases why deterrence fails.

Hawk-Dove in an Infinite Game

Many interactions are naturally recurring. For repeated interactions, threats to eliminate future opportunities help make agreements enforceable, especially if their long-term value outweighs the gain from cheating.[48] To explore this, we can play Hawk-Dove as a repeated stage game of imperfect information and having an infinite time horizon with a discount factor (d), where d is between 0 and 1 and represents the probability that the game continues.[49]

The value of trying to win today through playing Hawk is balanced against rewards and punishments in the future that are discounted by d. The reward is to play the Dove strategy forever with payoffs of :

$$[\frac{v}{2}, \frac{v}{2}]$$

at each stage. However, a player can only threaten credible punishments that the other will accept, which are Nash equilibria.

Consider the Grim-Trigger strategy, where deviations from Dove are punished forever with non-cooperative (Hawk) responses. When $v < c$, which is the chicken game, the highest punishment the other is willing to accept is to play Dove with a payoff of 0, resulting in equilibrium discount factors of the following:[50]

$$d > \frac{1}{2}$$

In equilibrium, the punished player is willing to accept an uneven distribution more than half of the time. This suggests the potential for an unstable long-run outcome. And one that could likely be renegotiated if disaffected audiences connected to this player found that distribution unacceptable.

A player could also threaten a lesser punishment by mixing forever resulting in:[51]

$$d > \frac{c}{v+c}$$

When players are mixing, higher costs increase the equilibrium discount factor (deterrence), and there are fewer fights.

If $v > c$, which is the Prisoner's Dilemma game, the highest punishment the other would be willing to accept is to play Hawk with a payoff of:

$$\frac{(v-c)}{2}$$

resulting in equilibrium discount factors:[52]

$$d > \frac{v}{v+c}$$

In this instance, since Hawk is a dominant strategy for both players, higher costs reduce the punishment payoff, which decreases equilibrium discount factors and lowers deterrence.

If there were payoff asymmetries between opponents ($v > c$ for Player 1 and $v < c$ for Player 2), there is no other Nash equilibrium, that Player 1 could accept as a punishment, and she could not be deterred from playing Hawk.

In infinite-horizon games, there are multiplicities of subgame perfect equilibria for sufficiently patient players. This structural problem is captured in variants of the Folk Theorem. Repeated games are also stateless games, and they would not be useful for situations where environments are changing and when strategy spaces are in transition.

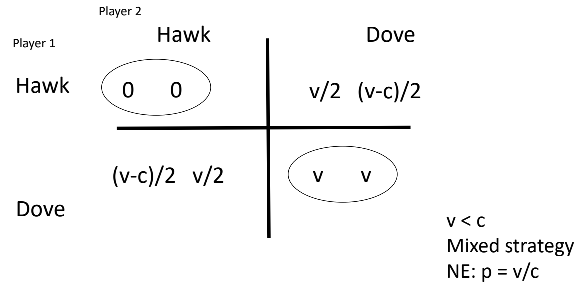
Rewards and trigger punishments can induce cooperation where relationships are valued and there are patient players. However, cooperation is less sustainable when there are impatient players. A similar logic with respect to time applies to reputations and norms, since both have long-term value. When reputations are lost and norms have atrophied, both can be very costly to restore.

Comparisons to Surprise-Attack

The translation of Hawk-Dove payoffs into the simultaneous-move game of "Surprise-Attack"[53] in matrix form appears in Figure 7 as:

$$\text{hh } [0,\, 0];\ \text{hd } [\frac{v}{2},\, \frac{(v-c)}{2}];\ \text{dh } [\frac{(v-c)}{2},\, \frac{v}{2}];\ \text{and dd } [v,\, v].$$

This game represents a model of nuclear deterrence. There are two pure strategy Nash equilibria in the upper left and lower right corners, i.e., (Hawk, Hawk) and (Dove, Dove).



Player 1 \ Player 2	Hawk	Dove
Hawk	0 0	v/2 (v-c)/2
Dove	(v-c)/2 v/2	v v

v < c
Mixed strategy
NE: p = v/c

Figure 7. Hawk vs. Dove

They include what can be considered the costly outcome with payoffs *[0, 0],* and a Pareto-dominant outcome with payoffs *[v, v].* As before $v < c$, and in some cases, c could be considered very large. Off the equilibrium path, a player experiencing a surprise attack suffers a loss of:

$$\frac{(v-c)}{2}$$

The mixed strategy equilibrium is the following:[54]

$$p = \frac{v}{c}$$

However, p is very low if c is considered very high. The probability that at least one player plays Hawk is very low, again if c is considered to be very high:[55]

$$1 - \left(1 - \frac{v}{c}\right)^2$$

With imperfect information, deterrence against surprise attack appears more a matter of degree than kind in mixed strategies. However, in this game, there are strong incentives not to suffer from a surprise attack, and to respond in kind to attacks. When there is incomplete information, players will be unsure what risks the other is willing to take.[56]

In an infinite game, where the reward payoffs are the Pareto-dominant outcome *[v, v]*, the maximum punishment the other player would accept would be *[0, 0]*. In this situation, any discount factor *[0 <d< 1]* suffices. No matter how impatient players are, conducting a surprise attack is inefficient in the long run. The same applies to the lesser grim trigger punishment strategy of mixing.[57]

Suppose equilibrium rewards in an infinite game are in mixed strategies. The maximum punishment the other player would accept are *[0, 0]* payoffs. Under a grim trigger strategy, the equilibrium discount factor is the following:[58]

$$d > \frac{v}{c}$$

which is very low, if c is very high.

In this situation, there is somewhat greater temptation for surprise attack, and trigger equilibria require less patience as costs increase. Where c is low, trigger equilibria require exceptional patience. However, where c is very high. trigger equilibria would fail only under exceptional circumstances, such as players who only lived for the present, or if fighting was a near certainty.[59]

Reflections

While the canonical models and their extensions presented here are abstractions about competition and conflict, they fit stylized facts in connection with the pervasiveness of cyberspace exploitation, propensities for various scales of cyberspace attack as well as surprise attack. They also suggest deterrence in cyberspace is possible through “threats that leave something to chance.”

Cyberspace exploitation involves clandestine maneuvers that are generally unobserved.[60] However, cyberspace attacks create denial effects that are eventually observed.[61] Active deterrence in cyberspace is thought to require attribution, credibility, and signaling,[62] all of which underline the importance of information or intelligence in strategy.

In cyberspace, deterrence is complicated by the complexities of technical and/or political attribution to machines, tradecraft, and agency. However, for various reasons, including the growth of private cybersecurity companies, threat actors cannot presume they will enjoy complete sanctuary from attribution, and this allows for deterrence in cyberspace.[63]

In tacit bargaining situations,[64] where communication is impossible or incomplete, and distrust is high, norms of behavior in cyberspace may be emerging, such as agreed competition.[65] These evolving norms are thought to be enabled by persistent engagement and defending forward, and this bears some semblance to mixed strategies in Hawk-Dove.

While inspired by evolutionary models, this analysis did not explore evolutionarily stable strategies (ESS), which are hard-wired in players. ESS are Nash equilibria that cannot be invaded or changed. In the Prisoner's Dilemma variant of Hawk-Dove, non-cooperation is the evolutionarily stable strategy. In the Chicken variant of Hawk-Dove, mixed strategies are evolutionary stable. In the Surprise- Attack game, the pure cooperative and non-cooperative strategies are evolutionarily stable.

Games contain elements of common and conflicting interests spanning the continuum of cooperation, competition, and conflict. They are bargaining situations for time or positional advantages, that do not always entail pure conflict. Games also remind us of the interdependence among relevant actors in an equilibrium. This can help planners understand the range of best responses.

Unfortunately, game theory is largely unfamiliar to planning staffs. Some models are quite complex and may not readily correspond to planning problems at hand, or could distort them.[66] Still, some game forms might be usefully explored during operational design, where the focus is on understanding actors, tendencies, and potentials.

Games such as Stag-Hunt can help in understanding security cooperation situations. The underlying structure and strategy spaces of the Stag-Hunt coordination game mirror that of Surprise-Attack, though they involve different situations. When played against the long shadow of the future, the canonical games considered here suggest much could be gained from strengthening norms, conventions, and partnerships to deter or contain threats in cyberspace.[67]

DISCLAIMER

The views expressed in this work are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

NOTES

1. Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960).
2. Robert J. Aumann and Thomas C. Schelling, "Contributions to Game Theory: Analyses of Conflict and Cooperation," Information on the Bank of Sweden Prize Economic Sciences in Memory of Alfred Nobel (Stockholm: Royal Swedish Academy of Science, 2005), 2.
3. Thomas C. Schelling, "The Retarded Science of International Strategy," *Midwest Journal of Political Science*, 4 (2),1960: 107-137, https://doi.org/10.2307/2108704.
4. The quotation was the author's description of his book. However, it also provides a succinct and classical definition of strategy. See Colin S. Gray, *Modern Strategy* (London: Oxford University Press, 1999), 1.
5. RDML J.C. Wylie, *Military Strategy: A General Theory of Power Control* (Annapolis, MD: Naval Institute Press, 2014), 14.
6. Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens, GA: University of Georgia Press, 2011).
7. Department of Defense, "Summary Department of Defense Cyber Strategy 2018" (Washington, DC: Government Printing Office, 2018), 2.
8. Ibid.
9. A case study of a norms construction through deterrence can be found in: Thomas Rid, "Deterrence Beyond the State: The Israeli Experience," *Contemporary Security Policy* 33 (1), 2012: 124-147, 2012, https://doi.org/10.1080/13523260.2012.659593.
10. This summarizes perspectives from Michael Mazarr in Michael J. Mazarr, "Understanding Deterrence" (Santa Monica, CA: RAND Corporation, 2018), https://doi.org/10.7249/PE295.
11. The seminal work on legal theory is Cesare Beccarria, "Beccaria: 'On Crimes and Punishments' and Other Writings," (original work published 1764), edited by Richard Davies (Cambridge, UK: Cambridge University Press, 1995), 103.
12. Sally S. Simpson, *Corporate Crime, Law, and Social Control* (Cambridge, UK: Cambridge University Press, 2002), 9.
13. Thomas Rid is adapting these definitions from Gibbs; see: Jack P. Gibbs, Crime, Punishment, and Deterrence (Amsterdam: Elsevier, 1975), 34.
14. Thomas Rid, "Deterrence Beyond the State: The Israeli Experience," *Contemporary Security Policy* 33 (1), 2012: https://doi.org/10.1080/13523260.2012.659593, 127.
15. Ibid.
16. Michael J. Mazzarr, "Understanding Deterrence." (Santa Monica, CA: RAND, 2018), https://doi.org/10.7249/PE295, 2.
17. Ibid.
18. Joint Chiefs of Staff, "Deterrence Operations Joint Operating Concept" (Washington, DC: Government Printing Office, 2006), 5.
19. Ibid., 7.
20. Ibid., 5.
21. Ibid., 8.
22. Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 41 (3), 2017: 44-71, https://doi.org/10.1162/ISEC.
23. James D. Fearon, "Domestic Political Audiences and the Escalation of International Disputes," *American Political Science Review* 88 (3), 1995: 577-592.
24. James D. Fearon, "Rationalist Explanations for War," *International Organization* 49 (3), 1995: 379-414, https://doi.org/10.1017/S0020818300033324.
25. John M. Smith and Geoff A Parker, "The Logic of Asymmetric Contests." *Animal Behaviour* 24 (1), 1976: 159-175. https://doi.org/10.1016/S0003-3472(76)80110-8.
26. Robert S. Gibbons, *Game Theory for Applied Economists* (Princeton, NJ: Princeton University Press, 1992).
27. Robert J. Aumann, "Agreeing to Disagree," *The Annals of Statistics*, Vol. 4, 1976, https://doi.org/doi:10.1214/aos/1176343654.
28. Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations" (Washington, DC: Government Printing Office, 2018).
29. Ibid.
30. John F. Nash, "Non-Cooperative Games," Annals of Mathematics 54 (2); 1951: 286-295. https://doi.org/10.2307/1969529.

NOTES

31. Robert J. Aumann and Thomas C Schelling, “Contributions to Game Theory: Analyses of Conflict and Cooperation,” Information on the Bank of Sweden Prize Economic Sciences in Memory of Alfred Nobel (Stockholm: Royal Swedish Academy of Science, 2005), 5.
32. To find the mixed strategy Nash equilibrium, a player mixes with probability (p) such that the opponent is indifferent between the two strategies. Since the game is symmetric:

$$\begin{aligned} \text{Value from playing Hawk} &= \text{Value from playing Dove} \\ p\,\frac{(v-c)}{2} + (1-p)\,v &= p\,0 + (1-p)\,\frac{v}{2} \\ \text{which solves for} & \\ p &= \frac{v}{c} \end{aligned}$$

Substituting this value on the right-hand side gives the expected value (EV) of the game:

$$\text{EV} = \left(1-\frac{v}{c}\right)\frac{v}{2}$$

33. The proposition is potentially testable. Taking a logarithmic transformation of mixed strategy equilibrium gives:

$$ln(p)=ln(v) - ln(c)$$

which is a log-linear equation that could be estimated using suitable proxies.
34. Thomas C. Schelling, “An Essay on Bargaining,” *The American Economic Review* 46 (3), 1956: 281-306, https://www.jstor.org/stable/1805498.
35. Ibid.
36. Saul I. Gass, “What Is Game Theory and What Are Some of Its Applications?” *Scientific American*, June 2, 2003, 2.
37. Reinhard Selten, “Spieltheoretische Behandlung Eines Oligopolmodells Mit Nachfragetr¨agheit – Teil I Bestimmung Des Dynamischen Preisgleichgewichts (Game-Theoretical Treatment of an Oligopoly Model with Sluggish Demand: Part I: Determination of the Dynamic Price Balance),” Preisgleichgewichts,’ Zeitschrift Fu¨r Die Gesamte Staatswissenschaft Journal of Institutional and Theoretical Economics 121 (2), 1965: 301-324.
38. Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960), 188.
39. There is no requirement for Player 1 necessarily has to hold reasonable beliefs. However, play must be consistent with beliefs. Hawk strategy is sequentially rational (i.e., optimal, given her beliefs and strategies) if:

$$\begin{aligned} \text{Value from playing Hawk} &> \text{Value from playing Dove} \\ q\,\frac{(v-c)}{2} + (1-q)\,v &> q\,\frac{v}{2} + (1-q)\,0 \end{aligned}$$

Since c > v > 0, a hawk strategy is sequentially rational when the retaliation threat is not believed in the limiting case (q = 0) as this requires v > 0. The hawk strategy is not sequentially rational when the retaliation threat is believed (q = 1) as this requires:

$$\frac{(v-c)}{2} > \frac{v}{2}$$

which cannot happen.
40. A pooling equilibrium in messages and actions among player 2 types occurs if player 1 mostly believes retaliation threats *(q ≥ .5)* and plays Dove. For the Dove strategy, sequential rationality for player 1 requires:

$$\begin{aligned} \text{Value from playing Hawk} &< \text{Value from playing Dove} \\ q\,\frac{(v-c)}{2} + (1-q)\,v &< q\,\frac{v}{2} + (1-q)\,0 \end{aligned}$$

Since c > v > 0, a dove strategy is sequentially rational when the retaliation threat is believed in the limiting case (q = 1) as this requires

$$\frac{(v-c)}{2} < \frac{v}{2}$$

The Dove strategy is not sequentially rational when the retaliation threat is not believed (q = 0) as this implies

$$v < 0$$

which cannot happen.

NOTES

41. Thomas C. Schelling, *The Strategy of Conflict,* 187.

42. The Intuitive Criterion is a refinement that enables elimination of equilibria involving unreasonable beliefs for deviations off the equilibrium path, and where deviations in question would be a bad idea for a particular type. David Marc Kreps and In-Koo Cho, "Signaling Games and Stable Equilibria," *The Quarterly Journal of Economics* 102 (2), 1987: 179-221, https://doi.org/10.2307/1885060.

43. In The Strategy of Conflict, Schelling mainly applied "threats that leave something to chance" to incomplete information situations and sometimes to situations involving imperfect information.

44. Vincent P. Crawford and Joel Sobel, "Strategic Information Transmission," *Econometrica: Journal of the Econometric Society* 50 (6) 1982: 1431-1451.

45. Hal Brands, "The Lost Art of Long-Term Competition," *The Washington Quarterly* 41 (4), 2018: 31-51, https://doi.org/10.1080/0163660X.2018.1556559.

46. Colin S. Gray, "Maintaining Effective Deterrence," edited by Strategic Studies Institute (Carlisle, PA: U.S. Army War College, 2003), 24-25.

47. Aumann, "Agreeing to Disagree," *The* Annals *of Statistics,* Vol. 4. https://doi.org/doi:10.1214/aos/1176343654.

48. Schelling, "An Essay on Bargaining," *The American Economic Review* 46 (3), 1956: 281-306, https://www.jstor.org/stable/1805498.

49. James W. Friedman, "A Non-Cooperative Equilibrium for Supergames," *The Review of Economic Studies* 38 (1), 1971: 1, https://doi.org/10.2307/2296617.

50. The solution for an equilibrium discount factor in an infinite game uses the properties of a geometric series. For some amount (a) discounted infinitely by factor (d) giving a value of x, then x is computed by:

$$\begin{aligned} x &= a + ad + ad^2 + ad^3 + ad^4 + \ldots \\ xd &= ad + ad^2 + ad^3 + ad^4 + ad^5 + \ldots \\ x - xd &= a \\ x &= \frac{a}{(1-d)} \end{aligned}$$

To find the equilibrium discount factor for the grim trigger strategy we set:

$$\begin{aligned} \text{Rewards Forever} &> \text{Gain Today} + \text{Punishments Forever } * \\ * \ \ \text{(Starting Tomorrow)} & \\ \frac{v}{2}\frac{1}{(1-d)} &> v + 0\,\frac{d}{(1-d)} \\ \text{which solves for} & \\ d &> \frac{1}{2} \end{aligned}$$

51. Using the more lenient punishment, to find the equilibrium discount factor we set:

$$\begin{aligned} \text{Rewards Forever} &> \text{Gain Today} + \text{Punishments Forever } * \\ * \ \ \text{(Starting Tomorrow)} & \\ \frac{v}{2}\frac{1}{(1-d)} &> v + \left(1 - \frac{v}{c}\right)\frac{v}{2}\frac{d}{(1-d)} \\ \text{which solves for} & \\ d &> \frac{c}{(c+v)} \end{aligned}$$

52. To find the equilibrium discount factor for the grim trigger strategy we set:

$$\begin{aligned} \text{Rewards Forever} &> \text{Gain Today} + \text{Punishments Forever } * \\ * \ \ \text{(Starting Tomorrow)} & \\ \frac{v}{2}\frac{1}{(1-d)} &> v + \frac{(v-c)}{2}\frac{d}{(1-d)} \\ \text{which solves for} & \\ d &> \frac{v}{(c+v)} \end{aligned}$$

53. Schelling, "The Reciprocal Fear of Surprise Attack" (Santa Monica CA: RAND, 1958), https://www.rand.org/pubs/papers/P1342.html.

NOTES

54. To find the mixed strategy Nash equilibrium, a player mixes with probability (p) such that her opponent is indifferent between the two strategies. Since the game is symmetric:

$$\begin{aligned}\text{Value from playing Hawk} &= \text{Value from playing Dove}\\ p\,0 + (1-p)\,\frac{v}{2} &= p\,\frac{(v-c)}{2} + (1-p)\,v\\ \text{which solves for}&\\ p &= \frac{v}{c}\end{aligned}$$

Substituting this value on the right-hand side gives the expected value (EV) of the game

$$\text{EV} = \left(1-\frac{v}{c}\right)\,\frac{v}{2}$$

55. The probability that both will not fire missiles is (1 – p)   (1 – p) or

$$\left(1-\frac{v}{c}\right)^2$$

Consequently, the probability that at least one res missiles becomes:

$$1-\left(1-\frac{v}{c}\right)^2$$

56. Another nuclear deterrence game that illustrates this point is reported in:

Oliver Roeder, 2017, "How To Win A Nuclear Standoff." FiveThirtyEight, September 6, 2017, https://fivethirtyeight.com/features/how-to-win-a-nuclear-standoff/.

57. An allocation is Pareto optimal and efficient if there is no other distribution that can make some players better off without making others worse off.

58. To find the equilibrium discount factor for the grim trigger strategy we set:

$$\begin{aligned}\text{Rewards Forever} &> \text{Gain Today} + \text{Punishments Forever *}\\ \text{* (Starting Tomorrow)}&\\ \left(1-\frac{v}{c}\right)\,\frac{v}{2}\,\frac{1}{(1-d)} &> \frac{v}{2} + 0\,\frac{d}{(1-d)}\\ \text{which solves for}&\end{aligned}$$

59. An allocation is Pareto dominated if another distribution exists that can make some players better off without making others worse off.

60. Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations," (Washington, DC: Government Printing Office, 2018), II-7.

61. Ibid.

62. Clorinda Trujillo, "The Limits of Cyberspace Deterrence." *Joint Force Quarterly* 75 (Q4), 2014: 43-52.

63. Herbert Lin, "Attribution of Malicious Cyber Incidents." 1607. Aegis Paper Series (Palo Alto, CA: Hoover Institution, Stanford University, 2016), 43.

64. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960), 53.

65. Agreed competition amounts to "continuous strategic competition in cyberspace that does not reach the level of armed conflict." See Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," Institute for Defense Analysis, 2019, 1.

66. Schelling, *The Strategy of Conflict*, 4.

67. Robert M. Axelrod, *The Evolution of Cooperation* (New York: Basic Books, 1984).