Military Cyber Affairs

Volume 5
Issue 1 *HammerCon 2022 Special Issue*

Article 5

May 2022

Hypergaming for Cyber: Strategy for Gaming a Wicked Problem

Joshua A. Sipper
Air University

Hypergaming for Cyber: Strategy for Gaming a Wicked Problem

Cover Page Footnote

Kopp, C. (2003). Shannon, Hypergames and Information Warfare, Journal of Information Warfare, Vol. 2, No. 2 (2003), pp. 108-118. Papamichail, K., Alves, G., French, S., Yang, J., and Snowdon, R. (2007). Facilitation Practices in Decision Workshops, The Journal of the Operational Research Society, Vol. 58, No. 5, Special Issue:Problem Structuring Methods II (May, 2007), pp. 614-632. Jaitner, M. and Kantola, H. (2016). Applying Principles of Reflexive Control in Information and Cyber Operations, Journal of Information Warfare, Vol. 15, No. 4 (Fall 2016), pp. 27-38. Kopp, C. (2003). Shannon, Hypergames and Information Warfare, Journal of Information Warfare, Vol. 2, No. 2 (2003), pp. 108-118. Ibid. Zwicker, W. (1987). Playing Games with Games: The Hypergame Paradox, The American Mathematical Monthly, Vol. 94, No. 6 (Jun. - Jul., 1987), pp. 507-514. Said, A. and Hartley, D. (1982). A Hypergame Approach to Crisis Decision-Making: The 1973 Middle East War, The Journal of the Operational Research Society, Vol. 33, No. 10 (Oct., 1982), pp.937-948. Perry, W. and Gordon, J. (2008). Analytic Support to Intelligence in Counterinsurgencies, RAND Corp. pp. 25-49. Papamichail, K., Alves, G., French, S., Yang, J., and Snowdon, R. (2007). Facilitation Practices in Decision Workshops, The Journal of the Operational Research Society, Vol. 58, No. 5, Special Issue:Problem Structuring Methods II (May, 2007), pp. 614-632. Bennett, P. (1985). On Linking Approaches to Decision-Aiding: Issues and Prospects, The Journal of the Operational Research Society, Vol. 36, No. 8 (Aug., 1985), pp.659-669. Ibid. Bennett, P. (1995). Modelling Decisions in International Relations: Game Theory and Beyond, Mershon International Studies Review, Vol. 39, No. 1 (Apr., 1995), pp. 19-52. Bennett, P. (1991). Modelling Complex Conflicts: Formalism or Expertise?, Review of International Studies, Vol. 17, No. 4 (Oct., 1991), pp. 349-364. Bryant, J. (1984). Modelling Alternative Realities in Conflict and Negotiation, The Journal of the Operational Research Society, Vol. 35, No. 11 (Nov., 1984), pp. 985-993. Fraser, N. and Hipel, K. (1983). Dynamic Modelling of the Cuban Missile Crisis, Conflict Management and Peace Science, Vol. 6, No. 2 (Spring 1982-83), pp. 1-18. Bennet, P. and Huxham, C. (1982). Hypergames and What They Do: A 'Soft O.R.' Approach, The Journal of the Operational Research Society, Vol. 33, No. 1 (Jan., 1982), pp.41-50. Ibid. O'Brien, F. (2015). On the roles of OR/MS practitioners in supporting strategy, The Journal of the Operational Research Society, Vol. 66, No. 2 (FEBRUARY 2015),pp. 202-218. Mateski, M., Mazzuchi, T., and Sarkani, S. (2010). The Hypergame Perception Model: A Diagrammatic Approach to Modeling Perception, Misperception, and Deception, Military Operations Research, Vol. 15, No. 2 (2010), pp. 21-37. Bennett, P., Dando, M., and Sharp, R. (1980). Using Hypergames to Model Difficult Social Issues: An Approach to the Case of Soccer Hooliganism, The Journal of the Operational Research Society, Vol. 31, No. 7 (Jul., 1980), pp.621-635. Bracken, J. and Darilek, R. (1998). Information Superiority and Game Theory: The Value of Information in Four Games, Phalanx, Vol. 31, No. 4 (December 1998), pp. 6-7, 33-34. Jormaka, J. and Molsa, J. (2005). Modelling Information Warfare as a Game, Journal of Information Warfare, Vol. 4, No. 2 (2005), pp. 12-25. Jaitner, M. and Kantola, H. (2016). Applying Principles of Reflexive Control in Information and Cyber Operations, Journal of Information Warfare, Vol. 15, No. 4 (Fall 2016), pp. 27-38. Ibid. Kopp, C. (2004). Reflections on Information Age Air Warfare, Journal of Information Warfare, Vol. 3, No. 3 (2004), pp. 11-28. Ibid. Ibid. Ibid. Kopp, C. (2003). Shannon, Hypergames and Information Warfare, Journal of Information Warfare, Vol. 2, No. 2 (2003), pp. 108-118. Ibid.

Hypergaming for Cyber: Strategy for Gaming a Wicked Problem

Joshua Sipper

Abstract

Cyber as a domain and battlespace coincides with the defined attributes of a "wicked problem" with complexity and inter-domain interactions to spare. Since its elevation to domain status, cyber has continued to defy many attempts to explain its reach, importance, and fundamental definition. Corresponding to these intricacies, cyber also presents many interlaced attributes with other information related capabilities (IRCs), namely electromagnetic warfare (EW), information operations (IO), and intelligence, surveillance, and reconnaissance (ISR), within an information warfare (IW) construct that serves to add to its multifaceted nature. In this cyber analysis, the concept of hypergaming will be defined and discussed in reference to its potential as a way to examine cyber as a discipline and domain, and to explore how hypergaming can address cyber's "wicked" nature from the perspectives of decision making, modeling, operational research (OR), IO, and finally IW. Finally, a cyber-centric hypergame model (CHM) will be presented.

Introduction

Hypergaming analysis as a tool for examining conflicts, situations, and constructs has been used liberally throughout numerous environments for decades. Its flexibility and applicability in military, government, business, education, and virtually all other organizational settings has made hypergaming a tool that some find indispensable. This is mostly due to the immersive and complex landscape of hypergames.

> "Hypergames are games in which the respective adversaries (players) may not be fully aware of the nature of the engagement they are participating in, or indeed that they are actually participating in an engagement." [i]

The blind locale of hypergaming sets the stage for meta-cognition in ways that other game theory associated analysis tools cannot. This is due to the broaching of numerous unknown realities and meta-realities present within the hypergame construct. It is especially useful in gaming for disciplines like cyber since there are so many meta-realities and situations in the cyber domain where the unknown is the reality. Attribution is one such unknown in which cyber has conceptual and practical shortfalls. This being said, the shortfall in this instance is not just a side issue, but a fundamentally "wicked problem" since it falls directly center of the heart of Sun Tzu's admonition to "know your enemy." Several other such problems

exist in cyber as well such as sovereignty, influence, deterrence, and a plethora of others that can benefit from hypergame analysis.

Within the scope of this discussion, several areas attuned to hypergame analysis for cyber will be examined. Decision making is an area not specific to the cyber discipline, however, many very complicated and confusing problems arise within cyber operations and warfare that require making decisions that are not always completely positive or negative. Such dilemmas are common in cyber, especially when attribution and deterrence are involved. Modeling is another tool often used to analyze diverse problems in an array of organizations. Modeling for cyber can be useful, especially when coupled with hypergaming. The combined effectuality of modeling through the use of hypergames creates a deep and richly textured canvas of opportunity for problem discovery, analysis, and resolution. Operational research (OR) uses gaming and specifically hypergaming to peer into the far reaches of the seemingly infinite matrix of operational problems extant across military and government organizations. Cyber operations are well suited to receive similar analytical rigor as they are characterized by fluid and elaborate situations. Information operations (IO) is a discipline conjoined to cyber within the IW framework. Its closeness and relationship as an IRC makes IO a prime candidate for analytical expression through hypergaming. Analysis of IO within the cyber scaffold will give a deeper look into how the same principles can be applied to cyber and within greater cyber/IO influence and psychological operations. Information Warfare (IW) has been examined multiple times using various types of gaming constructs. However, hypergame analysis offers a profound and multidimensional method for delving into IW in ways inexpressible through other games.

Prior to the individual perspectives concerning hypergaming for cyber, hypergaming itself will be examined and defined in relation to cyber. The purpose of this explanatory section is to prepare the reader and potential user of hypergaming for cyber with knowledge pertaining to how hypergaming works, some basic principles and theory, and how cyber as a discipline and domain might benefit from hypergame analysis. Following the hypergaming for cyber exploration, each section will expand upon this concept and purport a cyber-centric methodology for hypergaming, presented as a model in the final section.

Hypergaming for Cyber

Cyber as a discipline has its roots spread out in many directions between information technology, information assurance, network security, information operations, and many other areas involving the use of technology for offensive cyber operations (OCO), defensive cyber operations (DCO), and cyber network exploitation (CNE). However, the common rhizome among all of cyber's capillary reach is the concept of guiding, vectoring, and manipulating information to create effects. The cyber concept originates in the Greek term *kybernete* associated with piloting, governing, or steering a boat. This term was later adapted and used to coin the term "cybernetics" which is the practice of piloting or steering information through systems. Papamichail, et. al., reference cybernetics when discussing

decision making in their paper regarding problem structuring methods (PSM), an area of direct applicability to the cyber discipline, especially in relation to hypergaming analysis[ii]. Cyber as an information piloting discipline contains innate, vast complexity such that simple models of gaming only graze the surface of its ultimate operational potential. This makes hypergaming a potentially good fit for analyzing cyber and seeking out its prolific extensions into every domain and construct in the modern world.

> "[T]here is an advantage to using cognitive operations together with cyber operations. Actions taken in the spheres of cognitive and cyber operations have to be well planned, prepared, and coordinated." [iii]

This crossing of disciplines within only a binary construct presents complex alternative capabilities and decisions that outstrip many analytical tools. However, through the use of hypergaming, these potentialities may be identified, planned, prepared, and coordinated.

Hypergaming for cyber is, in practical terms, an analysis of the various problems encountered within the overarching cyber meta-reality; a reality about realities. The accompanying and pervasive layers of information and systems associated with the cyber domain require a multi-layered and consistently scalable analysis methodology.

> "In practical terms, players in hypergames have perceptions of the engagement which may not reflect the true nature of the engagement, resulting in decisions and outcomes which may not reflect the interests or indeed intent of the players." [iv]

The multilayered and organic growth of situational play within cyber hypergames allows for exploration of the unknowns and generates situations that must be handled through judgment and decision making that is more realistic and exploratory. In general, many other game types such as exercises might create situations through scenarios and vignettes that point to making one or two decisions regarding one or two problems. The ultimate point of the cyber hypergame construct, however, is to force players to recognize not just what they can know, but what they do *not* know, leading to a deeper cognitive understanding of decision making and creative, constructive thinking. One might liken hypergaming to the popular board game Clue™ (although this game is technically considered a game with incomplete information), wherein players know only a few bits of information about what the game is and who the players are, but they are missing the pertinent information concerning how to actually win the game. The object then is to discover what you as a player do *not* know.

This is further described in four tenets of hypergaming:

> "1. Players may have false perceptions of the intent or aims of the other players; 2. Players may not understand the choices available to other players; 3. Players may not know who other players in the game may be; 4. A player may be subject to one or more of the previous misperceptions of the game." [v]

Thus, hypergaming is like Clue™, but without knowing it is a murder mystery game, the characters, the murder weapons, the locations, or even the fact that you are playing a game against other players at all or even who the other players may be!

Interestingly, Zwicker in his analysis of the nature of hypergaming came to an enlightening conclusion about what hypergaming really is, or is not. Zwicker discovered what he terms the "Hypergame Paradox" which led him to determine that hypergames actually are not games at all. He determined this by applying a definition of what a game is connoted by five criteria:

> "(1) Two players, I and II, move alternately, I going first. Each has complete knowledge of the other's moves. (2) There is no chance involved. (3) There are no ties (when a play of G is complete, there is one winner). (4) Every play ends after finitely many moves. (5) At any point in a play of G, there are but finitely many legal possibilities for the next move." [vi]

However, Zwicker found that number five in the list could not be satisfied by the hypergame construct and therefore hypergames could not be games. The most interesting piece of this discussion isn't really whether or not hypergames are games, but the fact that Zwicker established a mathematical proof for infinite "legal" moves within any given hypergame; a compelling corollary for cyber operations and cyber warfare in the current environment of at least apparent infinite cyber possibilities.

Regardless of its status as a game by any definition, hypergaming appears to suit cyber domain analysis well in that cyber presents numerous problems, intractable through traditional gaming methodologies. This is not to say that other gaming, exercises, or analysis methods are of no value. Quite the contrary, there are many advantages to examining components of the cyber domain and cyber operations and warfare. However, if one wishes to see a full spectrum, holistic view of cyber through a multilayered and organic lens, hypergaming is potentially a better fit, especially considering the power held in computer modeling, artificial intelligence (AI), and machine learning (ML).

Cyber Hypergaming and Decision Making

Cyber, as any complex discipline, includes multiple situations in which a dizzying array of decision paths are available. Decision making is a common, difficult

occurrence within cyber that carries with it the potential to create untold second and third order effects. Therefore, courses of action (COA) must be considered carefully. But, it is vitally important to understand that COAs cannot be made or taken in a vacuum. In fact, many information sources pour into the development of COAs including cyber, ISR, IO, and EW, not to mention considerations from other domains of warfare. With this rich and often overwhelming flow of data, developing a COA can be daunting, if not impossible.

> "In game-theoretic analyses it is usually supposed that all participants are well-informed of the game being played, i.e. of each other's aims and options. This is clearly an invalid supposition for most interesting real-world conflicts and even for games… in which players are presented with a common game matrix. The fact that decision makers may have radically differing views of the world has been shown to crucially affect the decisions." [vii]

This is where hypergaming can bridge the supposition and assumption gap to assist decision makers in understanding a much wider array of possibilities. Fictionalized or even real-world scenarios, dilemmas, and case studies can only go so far, however with the augmentation of hypergaming, unexpected situations and unknowns can inject a real-world caste that would otherwise be missing.

> "The use of game theory to analyze military operations is not new… [I]t is only natural that we examine its applicability to…friendly-enemy interaction analysis. One advantage of using game theory is that the mental process involved in determining the payoffs forces us to assess enemy objectives." [viii]

Enemy objectives, obvious or obscured, are always difficult to follow to their end. While hypergames might not discover every possibility, they do offer a way to explore more possibilities within a cyber medium of understanding than if only a few aspects were considered.

Another area to keep in mind in reference to decision making for cyber while implementing hypergame analysis is the characterization of cyber as a "wicked problem."

> "In today's competitive environments, managers are increasingly faced with 'wicked' problems or messes… Solving wicked problems may cause or worsen other inter- connected problems." [ix]

Hypergames present another advantage in light of the "wicked problem" difficulty in that hypergames do not necessarily seek to "fix" the problem, but to analyze the problem, thus sidestepping potential second and third order effects

caused by disconnecting as a result of procedural, pedagogical, or philosophical displacement.

Hypergaming also coincides with the problem solving and decision-making process of hypermapping. "[The] concept of a hypermap provides a novel way of linking elements of cognitive maps and hypergames." [x] Cognitive mapping is a technique used in numerous fields of study and institutions to present patterns of thought for processes, problem resolution, and reasoning. Hypermapping plays the cognitive mapping method alongside hypergaming to give participants a way to generate possible actions and reactions in the process of playing the game.

> "[T]here is a set of modelling methods with a good deal of theoretical basis in common hypergame analysis, also developed from game theory. Apart from hypergame analysis itself, this conceptual 'stream' includes the *analysis of options* methodology." [xi]

Through analyzing the various COAs possible through hypermapping, players can get a much richer experience and better feel for how cyber operations might actually develop in a real world circumstance.

Modeling for Cyber Hypergames

Modeling has deep roots in military and cyber science applications as this method has been proven as a useful tool for virtually experiencing surprising and unexpected situations within a controlled experimental environment. Modelling is extremely useful when examining the potential conflicts that will invariably arise as cyber operations and warfare progress between two or more entities.

> "Game models are intended to provide an analytical guide through this maze. There are various ways of representing a game, perhaps the most intuitive being as a tree of moves, in which each branch, or move, is under the control of a particular player, and the moves available at any point may depend on those already made. One can visualize the game of chess, for example, as a fantastically-complicated tree of possible moves." [xii]

The *extensive form* model depicted by the complex tree view is just one of many possible ways to look at a hypergame model, although there is likely no model in existence that could fully contain the potentially infinite possibilities of the hypergame construct.

Hypergame models invariably take on a life of their own, growing and branching in many unexpected directions with decision trees taking on the resemblance of a forest. While this tendency can serve to overwhelm many players within a cyber hypergame, the point is not to apply stress and go for a resolution as it is to learn and grow through the hypergame. A cyber hypergame can metastasize

in various ways, "including the existence of 'games within games.' Such problem-structuring is not incorporated into formal analysis, but form a general backdrop against which analysis of specific interactions can proceed."[xiii] The cyber hypergame is then a proscenium stage, set within the vignettes of numerous cyber-related interactions such as OCO, DCO, CNE, ISR, EW, IO, and a host of other operations, security, political, and social climes. In any event, hypergames are iterative and tend to sprout into new and different shoots of possibility.

> "In terms of the games being played… any subsequent hypergame analysis must be able to handle a network of games rather than those occurring in isolation." [xiv]

This again is where the cyber strengths of computer modeling and processing with AI and ML are of great utility.

One final modeling technique that potentially finds purchase in cyber hypergaming is *dynamic modeling*.

> "It is necessary to use a dynamic model for games where there are constraints on players' actions as time passes. The state transition form takes the results … and incorporates them into a structure which permits the inclusion of new information relating dynamic constraints." [xv]

The use of dynamic modeling not only serves to delimit the game so as to now allow too much information travel or time lapse. This can be very helpful in classroom environments or other areas where time may be a factor. Overall, the concept of modeling for cyber hypergames generates a formula for control and bordering that assists in guiding the flow of the hypergame, allowing players to make more reasoned decisions.

Operational Research and Cyber Hypergames

The field of operational research (OR) has long been a mainstay of innovation as relates to understanding how information morphs and flows through organizations and systems. Within the cyber domain, operational research is of paramount importance for the obvious fact that information is the guiding and primary trade. Of course, where there is information there are also many different interpretations and views of that information that must be explored. While this can be a problem if conflicts are allowed to fester, the use of hypergame analysis can be of great help from an operational analysis perspective.

> "Many decision problems involve conflicts of interest between different participants. An effort has been made to develop hypergame analysis as one way of modelling such situations. Specifically this approach is designed to allow for the fact that the various parties may have quite different beliefs about

> the situation-including different models of each other." [xvi]

As decisions within a cyber operational construct become more and more complex, divergent views of everything from strategic purpose to fine-grained tactical choices can become problematic. Through the use of hypergame analysis, conflicts and different interpretations of information can be explored and mitigated within an experimental framework.

> "Examination of conflicts … in warfare, reveals a host of cases in which the parties appear to have quite disparate ideas of what the situation is, what the real issues are, and what each other's aims and possible actions may be. Hypergame analysis was conceived as a possible means of exploring and analyzing this sort of situation." [xvii]

As disparate interactions flow through the hypergame analysis, perceptions and flex points become more visible and open to discussion and optimization. This is the crux of hypergame analysis for cyber.

OR can be particularly constructive in areas where massive amounts of data are matriculated. This is a common problem within the cyber domain since so much information is available, indeed usually too much. In these cases, information databases and aids can be of enormous practical assistance for sorting, binning, and further analyzing massive amounts of information regarding the cyber information environment (IE).

> "Such varied use of IT is perhaps a good reflection of current practice, where there is evidence of web-based decision support systems, the use of organizational databases and systems, the use of specialist software such as [specialist] software through to instances of low-IT use, for example, in the workshop environment." [xviii]

Fortunately, a great deal of technological aids exist to assist in computer modeling for hypergames as well as parsing and organizing the results of analysis, which can sometimes be quite prodigious.

Information Operations and Cyber Hypergaming

Information operations (IO) like cyber is considered an IRC; one with astonishing reach and influence. In fact, IO is one of four IRCs considered to be a discipline within the IW construct along with cyber, ISR, and EW. This fact along with the inborn nature of IO as an information rich discipline gives further impetus to the benefits it might harvest from hypergame analysis. Cyber hypergaming conjoined with IO exponentially increases the benefits of the analysis endpoints as areas inherent to both disciplines can be examined and exploited. "[R]esearchers and analysts have noted the ability of hypergame analysis to model deception and

surprise." [xix] The use of information to influence and mold adversary responses is a key methodology within IO and cyber. Whoever controls the information, controls the battlespace. This is useful not only for ongoing operations, but for influence outside the boundaries of conflict.

> "Hypergame analysis seems to provide one reasonably efficient method of generating and exploring different hypotheses about the reasons for other peoples' behavior, the predictions of which can then be compared." [xx]

The author goes on to specify deterrence as an example; an area of particular interest within cyber, IO, and IW. The overriding concept is that hypergame analysis is a valuable tool for understanding and predicting adversary behavior, which is the pinnacle of power in IO.

Another important aspect of cyber and IO information theory revolves around the concept of information superiority. On the battlefield, the one who has the most information is the one who will most likely prevail. This is a tenet of warfare known from ancient times and has not changed since. As hypergame analysis deals with information, how that information is perceived and used, and how to better construct understandings of information, this exercise has great potential in making way toward information superiority. Bracken and Darilek, in their paper regarding information superiority and game theory, propose the following analysis,

> "To address the question of how much information might be required for US forces to achieve superiority, we have drawn upon game theory as a methodology that looks to be directly relevant to such questions." [xxi]

In their game model, they find that the "payoff" for either side in the game is highly sensitive to the information of both sides. That is to say, as each participant gains more knowledge of the information pertaining to the other participant, the game itself, and the reactions of the other participant, the more power and influence they garner. This works well with the concept of information theory to be explored later. The end analysis comes down to the apparent ability of one to claim and hold superiority within the cyber and IO battlespace based on the available and controlled information at their disposal.

Information Warfare and Cyber Hypergaming

Information warfare (IW) has surged of late as an important and all-encompassing strategy encapsulating the cyber IO, EW, and ISR disciplines and with this corralling of capabilities bringing great complexity. With this convolution comes the need to analyze information and its flow and intricacies. Hypergaming offers a structure for analysis that allows many differing vistas, potentially disaggregating the information river into tributaries. "In information warfare the

fundamental weapon and target is information, while the main goal is information superiority." [xxii] Information is key to the discussion and operations of IW, but it also can be a barrier to understanding as it is often an avalanche of sometimes disparate, singular bits.

A large portion of IW is focused on controlling information and using it to influence other players within the IE. In cyber and IW hypergaming, this method of control is often used in producing COAs.

> "COAs are, for the most part, based on intelligence and information provided by various Situational Awareness (SA) systems, weapons systems, and the like. Thus, decision-making processes rely heavily on collection of data that is purposeful, correct, and timely." [xxiii]

This information and the associated decision-making processes are related directly to what is referred to as reflexive control (RC), a method of using information to manipulate adversaries and other participants in IW and cyber conflicts as well as daily operations.

> "RC can be defined as 'a means of conveying to a partner or an adversary specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action' (Thomas 2004). The essence of a 'reflexive game' … is found in the mutual attempts of the adversaries to impose RC over one another." [xxiv]

The "reflexive game" is related to cyber hypergaming in that cyber is often used within the IW construct to guide and pilot information such that the adversary makes movements and decisions in favor of US and allied interests. Also, both groups attempt to apply RC and are often unaware that this is what is happening, further relating to the hypergame philosophy of unknown and incomplete information.

> "Information age warfare is characterized by rapid evolution, and all indications at this stage are that the capacity for lateral evolution will prove by far more important than the capacity for linear evolution. Opponents faced with overwhelming technological superiority which they cannot beat in a head-to-head contest of engineering and scientific skills will devise new and different ways of competing." [xxv]

This reality has been borne out with countries like Russia and NGOs such as ISIS developing low-cost, high-impact methods for manipulating information that has imposed costs on the US and its allies at many turns economically, politically, and societally. Cyber hypergaming can reach into this issue by modeling

and analyzing the possibilities of adversaries' attempts to find ways of imposing costs that were not intuitively obvious. Explorations in the power of social media to manipulate and degrade information such that integral, cultural and societal values such as elections are disrupted are just one example of adversaries imposing costs through IW. This type of information control and degradation happens often and in interesting ways within the cyber battlespace.

> "Denial of information or degradation strategies offer a large payoff in that the opponent is denied both warning and targeting information, significantly complicating any attempt to mount a defense." [xxvi]

The opportunity to discover these types of denial, degradation, and destruction methodologies within the safe and controlled space of cyber hypergaming offers a way to see the many and varied possibilities a cyber warrior might encounter within the interconnected and complex IW sphere.

Probably the best example of modeling IW with hypergaming was established by Kopp (2003) in his application of Shannon's Information Theory concept to hypergaming. Claude Shannon developed his mathematical theory of information in 1948, drawing on the concept of binary logic which developed eventually into computer programming logic, earning Shannon the title of "Father of Information Theory." His concepts are directly applicable to many concepts within cyber and EW specifically as he looked at how information is transferred across a channel where interference (i.e.., noise) was present, building on the physical waveform experience of signal-to-noise ratio (SNR). Kopp took this concept and further extended it into four canonical offensive IW strategies: "Denial of Information ('Degradation or Destruction' per US DoD), Deception and Mimicry ('Corruption' per US DoD), Disruption and Destruction ('Denial - Form 1' per US DoD), and Subversion ('Denial - Form 2' per US DoD)"[xxvii]. With this concept firmly established, hypergaming was applied and a model was fashioned to depict how these four IW strategies could be analyze within the hypergame construct. In the following section, the same model will be applied to introduce a model of cyber hypergaming, building from Shannon's and Kopp's concepts of information theory and hypergaming.

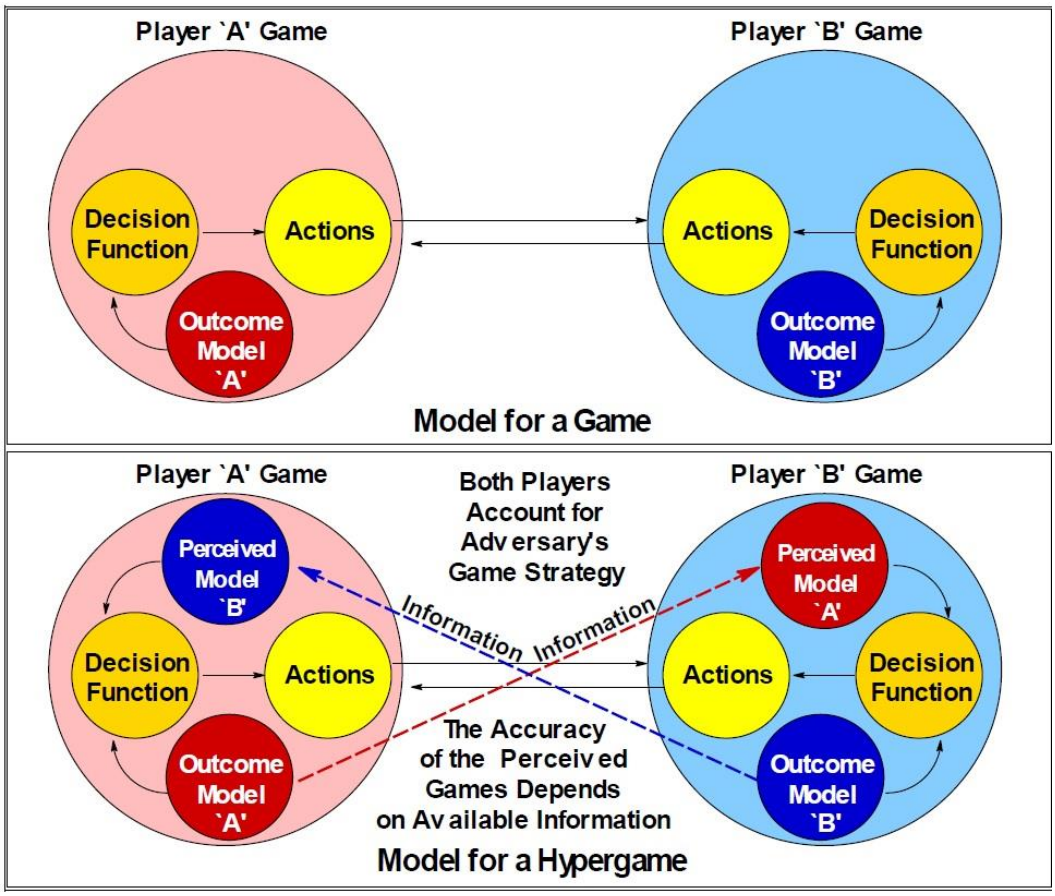
The Cyber Hypergame Model (CHM)

Before a model for cyber hypergames based on the four canonical IW strategies can be laid down, a general understanding of hypergaming as a construct must be presented. In Figure 1, a simple model is presented showing the difference between a game and hypergame. As Kopp explains:

> "In a hypergame the players perceive their opponents' games. How accurate that perception might be depends on the information available to respective players. Inaccurate information leads to a misperception of the game state and may lead to

actions which do not gain the player an advantage."[xxviii]

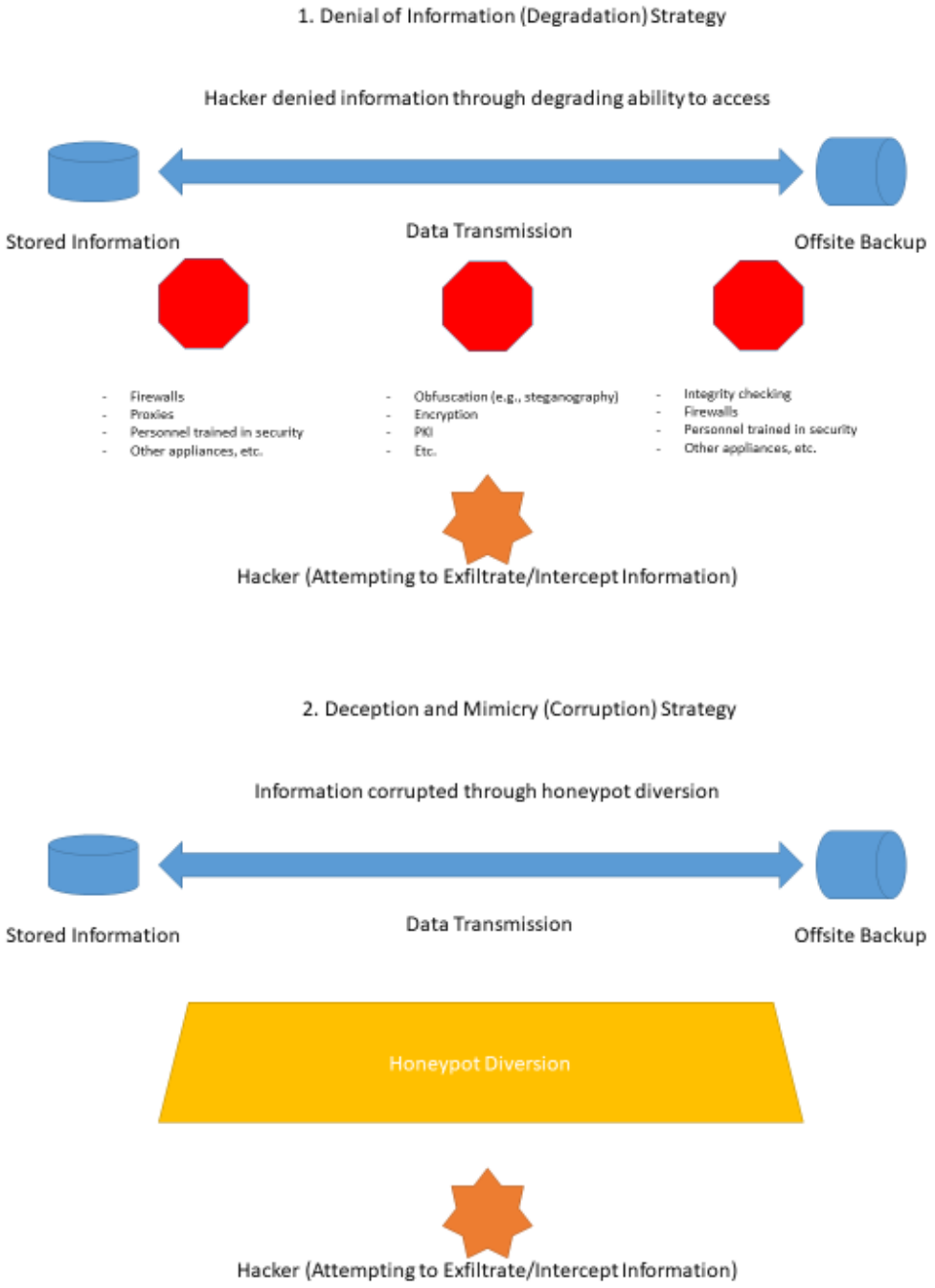
Figure 1. Hypergame General Model (Kopp, 2003)

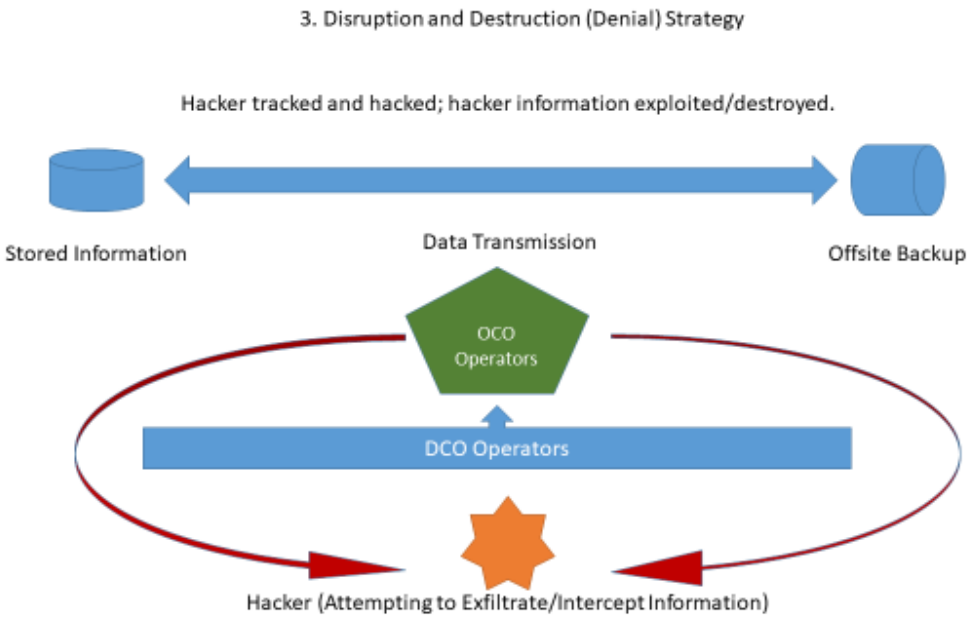


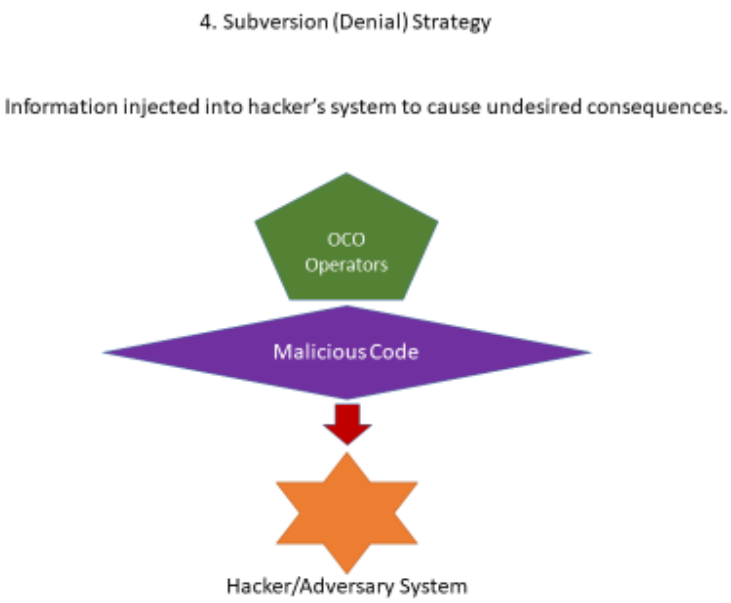
This is where the methods of cyber and IW methods begin to emerge, with denial, deception, degradation, and destruction being used through RC and other IW techniques.

For the examples of the four cyber strategies within the cyber domain, Figure 2 depicts scenarios in which a denial of information, deception and mimicry, disruption and destruction, or subversion might occur.

Figure 2. Contemporary examples of the four canonical offensive Information Warfare strategies in the Cyber domain

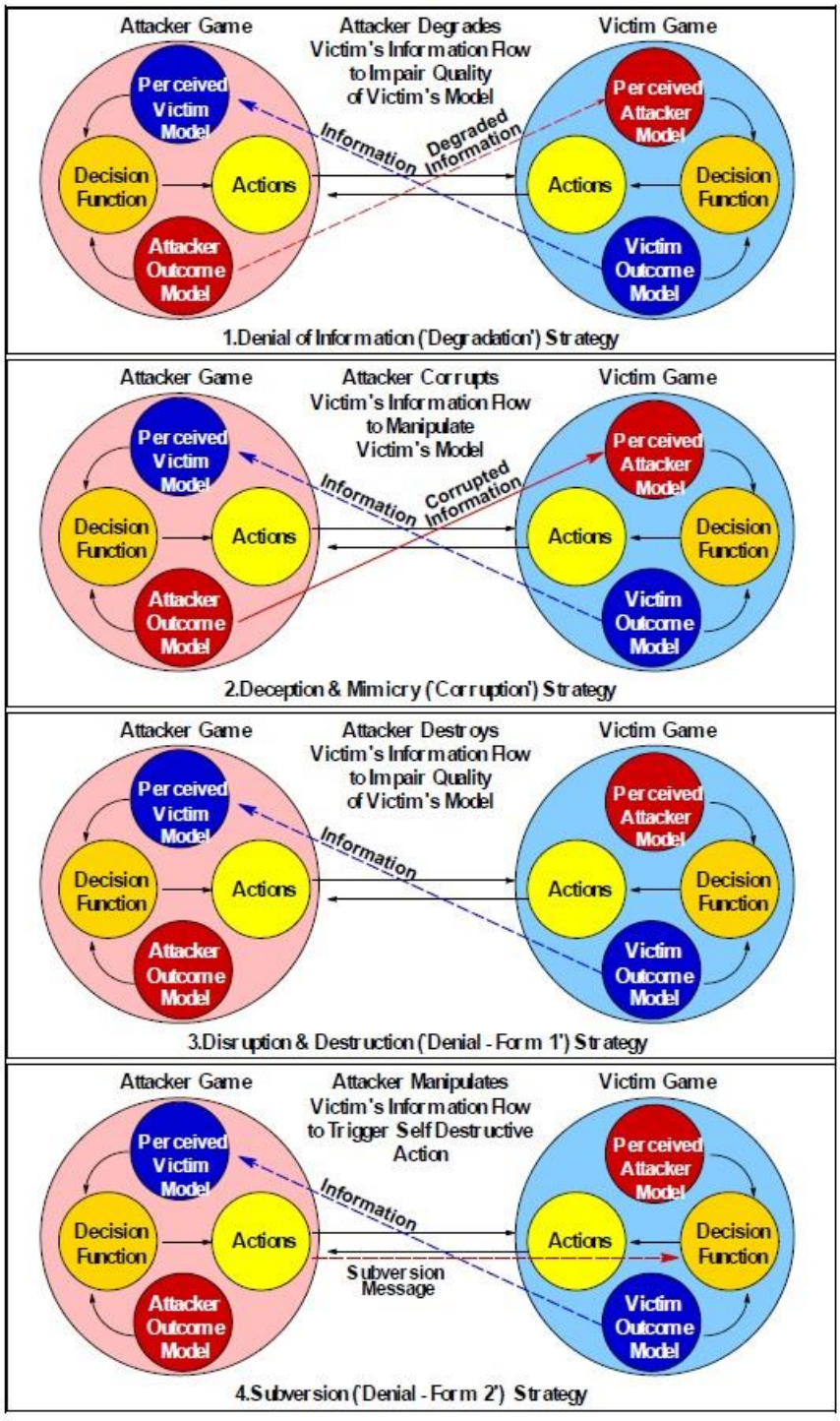






In the above examples, information is manipulated and obscured such that the adversary in the game cannot control the information. Through control of the data and information, the four canonical IW strategies are demonstrated for a cyber hypergame construct. Now this concept must be applied to the prosecution of a game using the four strategies, shown in Figure 3.

Figure 3. Hypergame models for the four canonical Information Warfare strategies, (Kopp, 2003).



The four strategies are depicted using the information flow concept to indicate how information is denied, degraded, disrupted, or destroyed within each

strategic construct. The full complement of the cyber hypergame concept can be used to great effect for analysis of numerous types of cyber operations. This analysis focuses primarily on the OCO aspect with some DCO and CNE augmentations. However, the concept can be applied using information theory across the full spectrum of cyber and IW.

Conclusion

The cyber domain is one of extreme complexity and interconnections due to its role as a central IRC, sustaining the flow of information for every other domain of warfare as well as the other IRCs associated within the IW construct. As a result, virtually infinite decisions can be made, multiplying possible COAs and complicating operations within cyber, IW, and multi-domain operations (MDO). All of this incredibly fluid and constant movement of information, requirements, and operational shuffle call for a methodology for analysis that could be assisted through the use of hypergaming. Hypergame analysis is a powerful tool, capable of allowing its players to see intricacies and unexpected possibilities they might not perceive otherwise. Through the use of the Cyber Hypergaming Model, cyber warriors have the opportunity to delve more deeply into the understanding of the IE and how to more accurately and specifically construct COAs for use in the cyber domain, IW, and MDO.

Endnotes

[i] Kopp, C. (2003). Shannon, Hypergames and Information Warfare, *Journal of Information Warfare*, Vol. 2, No. 2 (2003), pp. 108-118.
[ii] Papamichail, K., Alves, G., French, S., Yang, J., and Snowdon, R. (2007). Facilitation Practices in Decision Workshops, *The Journal of the Operational Research Society*, Vol. 58, No. 5, Special Issue:Problem Structuring Methods II (May, 2007), pp. 614-632.
[iii] Jaitner, M. and Kantola, H. (2016). Applying Principles of Reflexive Control in Information and Cyber Operations, *Journal of Information Warfare*, Vol. 15, No. 4 (Fall 2016), pp. 27-38.
[iv] Kopp, C. (2003). Shannon, Hypergames and Information Warfare, *Journal of Information Warfare*, Vol. 2, No. 2 (2003), pp. 108-118.
[v] Ibid.
[vi] Zwicker, W. (1987). Playing Games with Games: The Hypergame Paradox, *The American Mathematical Monthly*, Vol. 94, No. 6 (Jun. - Jul., 1987), pp. 507-514.
[vii] Said, A. and Hartley, D. (1982). A Hypergame Approach to Crisis Decision-Making: The 1973 Middle East War, *The Journal of the Operational Research Society*, Vol. 33, No. 10 (Oct., 1982), pp.937-948.
[viii] Perry, W. and Gordon, J. (2008). Analytic Support to Intelligence in Counterinsurgencies, RAND Corp. pp. 25-49.
[ix] Papamichail, K., Alves, G., French, S., Yang, J., and Snowdon, R. (2007). Facilitation Practices in Decision Workshops, *The Journal of the Operational Research Society*, Vol. 58, No. 5, Special Issue:Problem Structuring Methods II (May, 2007), pp. 614-632.
[x] Bennett, P. (1985). On Linking Approaches to Decision-Aiding: Issues and Prospects, *The Journal of the Operational Research Society*, Vol. 36, No. 8 (Aug., 1985), pp.659-669.
[xi] Ibid.

[xii] Bennett, P. (1995). Modelling Decisions in International Relations: Game Theory and Beyond, Mershon International Studies Review, Vol. 39, No. 1 (Apr., 1995), pp. 19-52.
[xiii] Bennett, P. (1991). Modelling Complex Conflicts: Formalism or Expertise?, *Review of International Studies*, Vol. 17, No. 4 (Oct., 1991), pp. 349-364.
[xiv] Bryant, J. (1984). Modelling Alternative Realities in Conflict and Negotiation, *The Journal of the Operational Research Society*, Vol. 35, No. 11 (Nov., 1984), pp. 985-993.
[xv] Fraser, N. and Hipel, K. (1983). Dynamic Modelling of the Cuban Missile Crisis, *Conflict Management and Peace Science*, Vol. 6, No. 2 (Spring 1982-83), pp. 1-18.
[xvi] Bennet, P. and Huxham, C. (1982). Hypergames and What They Do: A 'Soft O.R.' Approach, The Journal of the Operational Research Society, Vol. 33, No. 1 (Jan., 1982), pp.41-50.
[xvii] Ibid.
[xviii] O'Brien, F. (2015). On the roles of OR/MS practitioners in supporting strategy, *The Journal of the Operational Research Society*, Vol. 66, No. 2 (Feb., 2015),pp. 202-218.
[xix] Mateski, M., Mazzuchi, T., and Sarkani, S. (2010). The Hypergame Perception Model: A Diagrammatic Approach to Modeling Perception, Misperception, and Deception, Military Operations Research, Vol. 15, No. 2 (2010), pp. 21-37.
[xx] Bennett, P., Dando, M., and Sharp, R. (1980). Using Hypergames to Model Difficult Social Issues: An Approach to the Case of Soccer Hooliganism, *The Journal of the Operational Research Society*, Vol. 31, No. 7 (Jul., 1980), pp.621-635.
[xxi] Bracken, J. and Darilek, R. (1998). Information Superiority and Game Theory: The Value of Information in Four Games, Phalanx, Vol. 31, No. 4 (Dec., 1998), pp. 6-7, 33-34.
[xxii] Jormaka, J. and Molsa, J. (2005). Modelling Information Warfare as a Game, *Journal of Information Warfare*, Vol. 4, No. 2 (2005), pp. 12-25.
[xxiii] Jaitner, M. and Kantola, H. (2016). Applying Principles of Reflexive Control in Information and Cyber Operations, *Journal of Information Warfare*, Vol. 15, No. 4 (Fall 2016), pp. 27-38.
[xxiv] Ibid.

[xxv] Kopp, C. (2004). Reflections on Information Age Air Warfare, Journal of Information Warfare, Vol. 3, No. 3 (2004), pp. 11-28.
[xxvi]Ibid.
[xxvii] Ibid.
[xxviii] Ibid.