Operational Decision-Making for Cyber Operations: In Search of a Model

Dr. Max Smeets | JD Work

ABSTRACT

The decision-making behind cyber operations is complex. Dynamics around issues such as cyber arsenal management, target assessment, and the timing of dropping a destructive payload are still ill-understood. Yet, limited published research has thus far explored formal theoretic constructs for better understanding decision-making in cyber operations. Multiple models help to understand and explain the courses of action through which state cyber missions are executed, including conduct or restraint of cyber effects operations against target systems and networks. This paper evaluates four models - surprise model, duelist model, mating-choice model, and the Black-Scholes model. Each model offers specific advantages and suffers characteristic drawbacks. While these models differ in application and complexity, each may provide insights into how the unique nature of cyber operations impacts the decision dynamics of cyber conflict.

Keywords: Cyber operations, timing, decision-making, Black-Scholes, vvulnerability equities, arsenal management

I. INTRODUCTION

Conceptualization of operational art and logistics factors in cyber operations remains immature in published literature.[1] However, these factors are the *sine qua non* of successfully executing strategic intent, sustaining campaigns over time, and managing resource investment in what are ever costlier offensive cyber capabilities in an environment of spiraling complexity. Despite this, the behavior of designers, operators, and decision-makers responsible for the conduct of national cyber missions is largely discussed without a theoretic construct that identifies the choices, tradeoffs, and associated determinants that influence the courses of action that arise during cyber conflict.

At the heart of the contemporary instantiation of much of the problem space is understanding cyber operations' distinct features. Indeed, there has been much writing on how

cyber operations have several features that differentiate them from other warfighting domains. According to a report from the *National Academy of Sciences*, cyber operations come "with high degrees of anonymity and with plausible deniability; [...] more uncertain in the outcomes they produce; [...] [and] involve a much larger range of options and possible outcomes, and may operate on time scales ranging from tenths of seconds to years."[2] Cyber operations are also transitory in nature: they are strongly time dependent in terms of their potential to cause harm to targeted systems.[3] Finally, and perhaps most important, there are close similarities between cyber effects operations and espionage operations, or what in intelligence jargon is called Computer Network Exploitation (CNE) and Computer Network Attack (CNA).[4] Former NSA and CIA director Michael Hayden writes:

> Reconnaissance should come first in the cyber domain too. How else would you know what to hit, how, when—without collateral damage? But here's the difference. In the cyber domain the reconnaissance is usually a more difficult task than the follow-on operation. It is tougher to penetrate a network and live on it undetected while extracting large volumes of data from it than it is to, digitally speaking, kick in the front door and fry a circuit or two. [...] Let me go further. An attack on a network to degrade it or destroy information in it is generally a lesser included case of the technology and operational art needed to spy on that same network.[5]

The purpose of this paper is to help systematize our thinking on how these attributes of cyber operations affect decision making and conflict dynamics. We do this through assessing the potential value of formal modeling—drawing on different fields of research—to cyber conflict dynamics. More specifically, *to what degree can we model how the nature of cyber operations impacts decision-dynamics of cyber conflict?*

The importance of improved systematic thinking in this area has been raised as US government posture has changed over the past several years, moving explicitly towards a vision of cyber capabilities in ongoing employment, rather than as a "fleet in being."[6] Under the concept of persistent engagement, cyber operations will be conducted to demonstrate resolve, counter ongoing intrusion and attack campaigns that directly target sources of national power, and impose friction and cost on the hostile actors orchestrating these malicious activities.[7] Pursuit of this strategic vision requires understanding both of how scarce and often-ephemeral advantage within the domain may best be leveraged for operational purposes, but also how adversary operators, planners and decisionmakers may interpret and respond to actions conducted in the course of options generation and capabilities employment.

Formal modeling and policy have influenced each other since the publication of Neumann and Morgenstern's *The Theory of Games and Economic Behaviour*.[8] While the interaction between the two fields has often been highly constructive, various unsystematic and confusing applications of game theory on policy issues exist.[9] A common misunderstanding of the power of game theory is that it is treated as a descriptive rather than analytical tool. Instead, as

Duncan Snidal indicates, "[t]he real power of game theory, for both empirical and theoretical purposes, emerges when it is used to generate new findings and understandings rather than to reconstruct individual situations."[10] Snidal adds that "while the simplicity of game models leads to a clarity that illuminates social phenomena, the deductive apparatus of game theory allows us to infer new understandings about international politics."[11]

Furthermore, as an analytical tool, many are concerned about whether the lessons learned from formal analysis are mere spurious experimental results.[12] Yet, as Thomas Schelling writes:

> What can one learn [in games]. [...] Is not each game, especially ones that involve much human judgment and imagination and risk taking, a unique story that may never be repeated? [...] The answer is that games are not different from real experience. Anyone who goes through a Bay of Pigs, a Yom Kippur surprise attack, or a battle over the Falklands has had an enormous learning experience. For some it can amount almost to a rebirth. Each such crisis [however] is unique. Few people ever participate in enough of them to compare them or to get a sense of relative proportions. Whether one experienced the event personally or studied it as historian, one must beware of generalizing. The corresponding danger in games is probably no greater than in real experience possible less so because games can be replicated and varied experimentally.[13]

Given the complexity of cyber operations, and the constantly changing character of the domain's technical and tactical features, that a single "unified" theory of planning and decision making may serve to explain or estimate behavior by the varied actors, diverse capabilities sets, and highly heterogenous organizational structures by which task requirements are manned, trained, equipped, and executed. Within this limitation, however, it is expected that some models may have analytic if not predictive value as a lens to explore aspects of the wider problem space. The body of this paper assesses and compares four families of formal and game-theoretic models in their ability to infer new insights regarding the way the nature of cyber operations affects decision dynamics on (cyber) conflict. The next section briefly reviews an existing formal model applied to cyber conflict, that is Robert Axelrod's surprise model, the only published study in the field to date. Section III, in turn, provides a different model on the timing of cyber conflict, the 'Duelist model', which also takes other actors into consideration. The third model, described in Section IV, comes from the field of biology: we show it has a fruitful application for attackers to decide when to drop a destructive payload or continue intelligence gathering. Finally, borrowing from Finance, we discuss the Black-Scholes model in Section V. The model provides a superior understanding of how to model arsenal dynamics for cyber commands and organizations.

The results are summarized in Table 1. Overall, we find that the field of cyber conflict—both scholars and practitioners—can draw significant insights from other disciplines to better capture the dynamics of cyber conflict. We have not yet fully tapped into this potential, but hopefully this paper has provided an initial avenue to do so.

Table 1. Application of Game Theoretic Models to Cyber Conflict

	I	II	III	IV
Models	Surprise	Duelist	Search	Black-Scholes
Field of Origin	Politics / Economics	International Relations	Biology	Finance
Conventional Application	When should a resource be exploited for surprise?	When two duelists approach each other, when should they shoot?	When should an individual stop searching for a mate?	How should I price an option with a potential expiration date?
Cyber Conflict Application, General	Timing of cyber conflict	Timing of cyber conflict	Transition from cyber espionage to destructive attack	Arsenal management
Cyber Conflict Application, specific	When to use a zero day exploit?	i. When to hit a target before a rival actor will hit the same target? ii. When to attack a rival before the rival attacks me?	When should an individual stop searching for a mate?	How to price an option with a potential expiration date?
Complexity	Simple	Simple – Moderately Complex	Moderately Complex	Highly Complex
Utility	- Using both concepts of 'stealth and 'persistence' allows for better discussion of cyber operations Time dynamics. - Only useful if there is a clear overview of what determines an operations transitory nature. - Current application is highly problematic in terms of case study analysis.	- The model's primary weakness lies in the unlikelihood that all three basic assumptions hold. - But the model's strength lies in its wide range of potentially applicability, if the three basic assumptions hold.	- The model's assumptions apply well to cyber conflict - Relatively simple application. - It cannot deal with non-linear processes.	- The model provides a compelling way to capture the patching dynamic of software vulnerabilities. - The assumptions made are not easy to translate to cyber conflict. - The model is not only complex to develop, but will also be difficult to use to justify decision making.

Before turning to the discussion of the models, three caveats are provided. First, the models discussed here have been ordered from least to most complex, however, that increased complexity does not make the model necessarily more useful or accurate. Second, though game theory is referred to as the "mathematical study of strategic interaction,"[14] the discussion here omits the quantitative elements here to the extent possible to focus on the underlying logic behind each model, in order to examine the transferability of this logic to the cyber domain. Third, there are two assumptions underlying all four models: i) states are the most important actors, and ii) states are rational.[15] The rationality assumption implies that states are choosing the best option available to them, from a set of possible options or strategies.

II. MODEL I: RATIONAL TIMING OF CYBER SURPRISE

In 1979, Robert Axelrod published a paper, "The Rational Timing of Surprise".[16] The paper aimed to explore when a resource for surprise should be exploited. The article discusses several situations for which the model is relevant: using information from code breaking or spying, using a new weapon, or giving false information to a double agent. Despite the differences in cases, Axelrod argues that all of them present the same structural problem in determining whether to wait or immediately exploit the resource.

Axelrod develops a model with four parameters:

- **i)** The stakes vary over time; and the greater the stakes, the greater the gains from exploiting a resource.
- **ii)** There are costs to maintaining a resource, which does not necessarily have to be material costs.
- **iii)** Exploitation risks exposure.
- **iv)** Value is discounted over time—the assumption is that if the payoff were the same for exploiting a resource today or waiting until a future opportunity, the choice would be made to exploit it today.

In a later paper, Axelrod and Iliev applied this framework to cyber conflict.[17] The article explicitly states that the model can deal with only one aspect of the problem, "the timing of a cyber conflict, either in the form of espionage or disruption."[18] As the authors state, "[t]he paper takes the point of view of an actor who has a resource to exploit a vulnerability in a target's computer system, and a choice of just when to use that resource."[19]

The main conclusions of their model are straightforward. First, if a cyber resource is likely still useable in the future if not used today, an actor is less likely to use it today. Second, an actor is also less likely to use a cyber resource when there is a low probability of being able to use it again, i.e. where there is a low chance of "resource survival".[20] Third, the authors find that an actor is more likely to hold their fire if there is the expectation that the stakes are high in a rare event happening in the future. Overall, as Axelrod and Iliev state, at "[t]he heart of [the] model is the trade-off between waiting until the states of the present situation are high enough to warrant the use of the resource, but not waiting so long that the vulnerability the resource exploits might be discovered and patched even if the resource is never used."[21]

The work of Iliev and Axelrod is commendable in that the model makes it possible to incorporate a more refined understanding of the transitory nature of resources used during cyber operations. Unlike most earlier studies, in this paper issue is not presented as a binary variable, i.e. the idea that a resource can only be used once ('single-use'), but rather as a continuous variable. Also, the scholars estimate two parameters that determine whether the resource will be available in the next time period; 'stealth' and 'persistence'. In their own words, "[t]he Stealth

of a resource is the probability that if you use it now, it will still be usable in the next time period. The Persistence of a resource is the probability that if you refrain from using it now, it will still be useable in the next time period."[22] This distinction is important as the use of resources during one operation significantly increases the chances of the discovery in the next period.

In addition, the paper usefully distinguishes between different resources in contract to the primitive notion that all cyber resources are similarly transitory in nature. Integrating this more nuanced understanding into their formal model means the scholars reconcile the contrasting views of earlier works discussed above (although they may fail to deliberately recognize this integration). The degree to which the cyber domain incentivizes a use-it-or lose-it dynamic or a waiting-for-the-right-moment dynamic depends on the type of capability and whether the stakes remain constant.

Existing research demonstrates the relevance of the rational timing model, but further development is still needed. Additional case study examples are required to provide further empirical depth. Furthermore, the study of Axelrod and Iliev has a primitive understanding of the requirements of cyber operations. For example, it is unclear if the model applies only to the use of exploits or also implants.

III. MODEL II: DUELING IN CYBERSPACE

The application of game theory to analyze conflict situations blossomed during the Cold War. In light of the progressive development of nuclear weapons and delivery systems, numerous recommendations were made whether a first strike against the Soviet Union was rational.[23] Considering this situation, most scholars provided a simplified model in which each of the two states involved in a conflict have two strategies: first and second strike.[24]

The principle family of models that followed from this analysis (initiated by David Blackwell and other mathematicians in the reports of RAND corporation in 1948-52[25]) are two-person games of timing in an uncertain environment. These models are often referred to as 'duelist models'[26] and are metaphorically seen as two duelists approach each other: the longer one of them waits to fire, the more likely it becomes that the other will fire first therefore striking first (the accuracy function increases with time). On the other hand, the closer the duelists get, the more likely it becomes that the first to fire will hit and disable the other (if a player fires too late, the opponent may hit his target earlier and the game may be terminated as the player has lost the opportunity to engage).

The basic features of this family of models are described by Radzik in a review paper entitled "Results and Problems in Games of Timing." These features are each player has one bullet, which may be fired at any time; accuracy (i.e. the probability that the player hits) increases over time, and; the player who first hits the target is the winner and ends the game.[27]

The duelist models could differ in several ways based on additional assumptions. First, the settlement of payoffs in this game can be arranged in two manners. The first pay-off structure produces a zero-sum game, the latter leads to a nonzero-sum game with various outcomes: The winner receives one 'unit' from his opponent, that is, each player wishes to maximize his expected return (this is in line with the classic duelist model). The winner receives one 'unit' from the umpire of the contest. That is, each player wishes to maximize his winning probability (this is more like a marksmanship contest). Second, there are two information patterns available to players: i) A player is informed of his opponent's action time as soon as it takes place (this action is referred to as 'noisy bullet' or 'noisy action'). ii) Neither player learns when or whether his opponent has acted (i.e. 'silent bullet' or 'silent action').[28]

Third, there are different interpretations as to what 'uncertain environment' could entail. The following accuracy functions have previously been solved: i) When there is imperfect ability to perceive opponent;[29] when duelist have uncertain knowledge about the existence of a bullet fitted to their guns;[30] when the appearance of the object is random and whether or not the players are able to obtain the object is uncertain;[31] when the bullets are only accessible at random times;[32] when one player has one noisy bullet and one silent bullet and is forced to fire the former first, whereas the other player has only a silent bullet.[33]

The value of this model would, like the previous model of Axelrod and Iliev, be in the timing of cyber conflict. However, the specific application of the model is slightly different: if I have a zero day exploit, and I know another actor has the same exploit, when should I use mine?[34] In Axelrod and Iliev's model, the use of your own exploit does not depend on whether the other actor has the same exploit. The chance of independent rediscovery of zero-day exploits is found to be relatively low. A study from RAND Corporation indicates that zero-day exploits have an average life expectancy of almost 7 years.[35] Yet, about 25 percent of exploits will not survive for more than one and a half years, and another 25 percent will survive more than 9.5 years. Based on the data available, the RAND study was unable to provide any predictors on which *stockpiled* vulnerabilities are more or less likely discovered or disclosed.[36] This data may be considered representative of Blue Force inventory, provided by contract acquisition to US and allied programs. One may infer similarities to other actors' capabilities sets, although it may be presumed that zero-day exploits sourced from underground markets would be under greater collision pressure with commensurately shorter viable lifespans on the shelf.

Yet, considering the growth of the zero-day market, and the potential in which two or more actors may source capabilities acquired from the same entity due to opacity in gray and black-market transactions, the duelist model seems to describe a realistic scenario. These dynamics are further exacerbated by recurring features of vulnerability discovery and exploit development research, in which "interesting" operating system, application, and firmware/hardware targets attract similar development approaches across available attack surfaces, particularly where exploit engineers have relatively similar experiences and ongoing access to

earlier vulnerability disclosures from open source publication, private research communities, or the hacker "scene."[37] In this case, vulnerability collision may develop not as an unanticipated factor of common supply chains, but as an emergent feature of contemporaneous exploitation trends—the vulnerability zeitgeist, if you will.

The model's primary weakness lies in the unlikelihood that all three basic assumptions will hold. The model's strength lies in its wide range of potential applicability, if the three basic assumptions hold. The first assumption is that each player has only one bullet. Yet, it is to be expected that in most scenarios a state has more than one cyber option in inventory, or at least, could develop additional options within the actionable timeline of the conflict. The second assumption is that waiting pays off, as you have a higher chance of hitting the target. This model's assumption goes against the assumption Iliev and Axelrod make: if you wait longer there is a higher chance that your exploit will be discovered; hence waiting does not pay off. Using this model in terms of a cyberattack, the value of gathering more info about your target and testing it outweighs the costs of potential discovery of the exploit. Whether or not this is the case is an empirical question and goes beyond the scope of this paper. Yet, one factor to consider is that the trade-off likely depends on how important the actor finds minimizing the undesired impact of offensive cyber operations. If the attacker cares a lot about collateral damage to other systems besides the intended target, the assumption of the duelist model is more likely to hold.[38] The third assumption is that, if you do not strike, the other will strike against you—which also terminates the game.

During the early Cold War period, when the great powers did not yet have a second-strike capability, this assumption was highly applicable to reality. In relation to cyber conflict, however, could a preventive strike be beneficial? And what if this preventive strike could deny the other actor's ability to 'hit' back? This proposition seems unlikely in the macro sense.[39] It is highly unrealistic to expect that one actor could be able to conduct a preventive cyber operation, eliminating any possibility of the rival's ability to retaliate through other cyber means. However, by targeting specific capabilities, employment mechanisms, or command and control infrastructure, that may have been enumerated through intelligence in advance of preventative action, this proposition may valid within specific operational windows for certain planning objectives. Indeed, this is one of the central concepts of cost imposition upon adversary actors through friction within the construct of persistent engagement, where the loss of certain capability options at a given moment of time forces investment in defending other surviving platforms, and regenerating new infrastructure, in order to accomplish espionage objectives and hold-at-risk operational preparation of the environment (OPE) posturing (prior to deployment at threshold of armed conflict.)

Beyond the application of these assumptions, however, this family of models offers a wide range of interesting logics to explore. First, following the above discussion on differences in pay-off structure and type of 'bullet,' the duelist model could serve different applications on the timing of cyber activity. These applications are summarized in table 2.[40]

Table 2: Taxonomy of duelist model application to cyber conflict dynamics

	Noisy	Silent
Zero Sum	**I. CNA against rival** When should actor A conduct a destructive or disruptive cyberattack against actor B, before actor B attacks actor A?	**II. CNE against rival** When should actor A conduct a cyber espionage operations against actor B, when actor B is also interested in conducting the same type of operation against actor A?
Positive Sum	**III. CNA against non-rival** When should actor A conduct a destructive or disruptive cyberattack against a target of interest, when actor A knows that actor B might potentially attack this system too?	**IV. CNE against non-rival** When should actor A conduct a cyber espionage operations against a target of interest, when actor A knows that actor B might potentially attack this system too?

* *This assumes that CNA activities are immediately discovered (i.e. noisy bullet) and espionage operations not (i.e. silent bullet).*

** *Rival actor means an actor which is also able to conduct a cyberattack against you. A non-rival concerns an actor you may want to conduct a cyberattack against, but is unable to attack you*

Conventional application of the model could potentially be fruitfully applied to offensive cyber operations (i.e. imperfect perception of the opponent) in multiple ways. First, there are many situations in which the attacker has incomplete knowledge of the computer systems and networks of the target. Second, there may also be uncertainty about the potential undesired impact of a cyber operation (i.e. uncertain knowledge of the bullet). Third, as was stated above, CNA activities tend to follow after CNE activities. This means that a potential application of the 'noisy and silent bullet' is possible too, though the game set up must be reversed: first comes the silent bullet, and after that, the noisy bullet.

IV. MODEL III: SEARCH THEORY AND MATE CHOICE

The third potential model to consider is less conventional and comes from an application in the field of biology. Ever since Charles Darwin introduced his ideas on sexual selection in 1871, there has been an interest in understanding evolutionary change. The possibility of evolutionary change rests upon the notion that over time desired qualities in a species are more frequently passed on to each generation. In 1990, biologist Leslie Real wrote an influential evolutionary biology paper, "Search Theory and Mate Choice."[41] Real set up a model with the aim to resolve four questions: [42] i) How do individuals find the best potential mates? ii) For how long should individuals search for mates for accepting a potential mate? iii) how are the critical values of acceptable mates determined? iv) What are the implications of increased mate competition, environmental uncertainty, variables survival, and/or mating costs for the decision-making process?[43]

Real built her analysis upon the assumptions made by Janetos' earlier model on what may constitute an optimal policy for mate choice.[44] The following five assumptions underlie Janetos' model(s): i) Individuals mate only once at any time, meaning that the model is implicitly restricted to monogamous or serially monogamous mating systems. ii) Mates are dispersed

in space such that they are encountered randomly with respect to fitness. iii) Only one of the sexes is discriminating. iv) The probability of a mate having a charitable fitness is based on a cumulative-probability density function (with a certain mean and standard deviation). The probability of an individual's mating depends only on its inherent, W, and the response of the actively searching mate.

Real argues that Janetos neglected a key feature of the problem, which led to significant biases in the model: the cost of searching and sampling.[45] This radically changes the relative performance of the different strategies. In Janetos' model, with no search costs, a best-of-n is the best strategy: the searcher should sample all potential mates in the population before making a decision. In the case of Real's model, there is a growing cost for the mate to continue the search. As Real shows, this means that now a sequential-search model will always dominate.[46] Also note that increased search costs reduce the threshold critical value for mate acceptability.

At first sight, it seems that the situation of evolutionary biology is very different compared to offensive cyber operations. However, the search model could have several fruitful applications for cyber conflict decision making. Whereas the search model in biology imagines an individual who must decide to accept or reject a mate on the basis of the sequence of encounters and a knowledge of the distribution of mates' qualities, in conducting cyber operations we can imagine an attacker who must decide to either deliver a destructive payload or continue intelligence gathering on the basis of the sequence of systems it has gained access to and the knowledge of the distribution of other system's importance.

The key point is that, if an attacker decides to only conduct espionage activities the chances of discovery are low. In cases where the attacker uses a zero-day exploit to access the system, it may be able to re-use this exploit for a prolonged period.[47] Yet, if it decides to drop a destructive payload the chances of discovery are suddenly vastly higher. This leads to an important trade-off: when to move from espionage to disruptive or destructive activities (or from CNE to CNA)?[48]

The search model provides an excellent framework to analyze this question. First, the key decision value in this respect is not 'mate quality' but the value an actor gains from dropping a destructive payload. Second, like searching for a mate, there are also costs in terms of continuing cyber espionage operations. There are the costs of the conducting the early phases of a cyber operation—reconnaissance, intrusion, privilege escalation, and lateral movement—to compromise a new system and / or network. There may also be costs to remaining stealthy in case an actor wants to maintain access to a certain system. In addition, potential other costs concern the potential patching of an exploit by the vendor or other change in the operating environment. Third, in the search model, the individual must consider what the expected fitness would be from sampling an additional 'passive mate'. In turn, an actor conducting a cyber operation must consider the expected value from intruding an additional computer system or network (i.e. what is the chance that there will be another system out there which is more valuable to intrude and drop a destructive payload?)

Table 3: Overview key parameters search model: Mate choice vs. cyber attacks

Variable	Mate Choice	Cyber Operation
Wcrit	Decision variable: the minimally acceptable mate quality	Decision variable: the minimally acceptable strategic value gained of dropping a destructive payload
c	Cost of searching	Cost of continuing cyber espionage activities
F(w)	The expected fitness gain from sampling one additional passive mate	The expected value from intruding an additional computer system or network

* *For a more comprehensive overview of the equation and variables see: Real, p. 384.*

** *The cumulative costs in the case of cyber-attacks could be negative, i.e. value from searching. For example, if the attacker gains knowledge of the system which is in and of itself valuable. For example, let us imagine an actor aims to attack an oil refinery. If the espionage activity itself provides valuable information regarding the process of refinery, which the actor can use, it can offset the costs of dropping a destructive payload.*

A key weakness of the search model of Real is that it ignores mutual mate choice in which both sexes are choosy; there are only 'passive mates' in this environment. Although this assumption is problematic in her model, this assumption is more likely to hold for cyber-attacks; after all, no target generally wants to be attacked (honeypot and other deception systems excepted).

However, "choosiness" may be observed in real world action at differing points in more sophisticated offensive operations. Payload deployment choices may be constrained by temporal characteristics where the intended effect is not merely simple destructive execution (i.e. rm -rf like commands in simplified expression), but rather more complex degradation of functionality, particularly in ways that are less detectable or traceable. Such effects—including manipulation of system, application, sensor, and/or data integrity—are often highly sensitive to target configuration, workload factors, and other features. These may influence the "best match" option at varying points in time throughout the course of an operation or longer campaign. An easily considered example of such a case might be given based on business continuity processes, in which destructive or integrity-degrading effects offer variable impacts depending on time between back-up cycles. More sophisticated modeling may be required across heterogenous target sets, as may be encountered within an Integrated Air Defense System (IADS) network composed of equipment acquired across multiple generations and knit together with architectures of differing original design and retrofit modification. Likewise, there is much variability in destructive payload effects, and further effects beyond simple destruction, which may provide differing complexities for analysis under this model.

V. MODEL IV: CAPABILITIES OPTION "PRICING" AND THE BLACK-SCHOLES MODEL

The final model is from modern option pricing (i.e. a form of hedging) in finance.[49] The notion of options is centuries old. In the 16th century, grain dealers in Amsterdam were said to use options. A century later, Joseph de la Vega provided the first heuristic method to price and deal with exposure. And more sophisticated techniques emerged in the 19th century as

the financial markets developed in London, Paris, and New York. Charles Castelli was the first to provide a theory of hedging in 1877.[50] Bachalier followed with a theory of speculation in 1900.[51] Modern option pricing was reborn in the 1950s. In 1955, Paul Samuelson famously published his work on Brownian Motion in the stock market. Black and Scholes in 1973 provide a new method to price options and corporate liabilities.[52]

Following this work, the Black-Scholes equation is the main tool used to price options in today's market. Buying an option means buying the right to engage in a particular transaction, yet the buyer has no obligation to follow through on the transaction.[53] There are three types of options: a European option may be exercised only at the expiration date of the option, an American option may be exercised at any point before the expiration date of the option, and a Bermudan option may be exercises only on pre-determined dates before the expiration date of the option, typically a month.

To price an option, one tries to find a way to value its 'dynamic hedge,' that is, mirror the option's payout using the underlying asset. When one initially creates a riskless delta hedge, it is only riskless at the instant it is created.[53] Hence, it needs to be continuously rebalanced. This requires a 'dynamic' hedge. The Black-Scholes has (at least) five pricing inputs: i) spot price of underlying asset, ii) options strike price; iii) risk free rate, iv) volatility returns of the underlying asset, and v) time-to-expiry.

It rests on the following assumptions: i) presence of constant risk-free rate; ii) efficient market hypothesis holds; iii) securities are infinitely divisible (i.e. it is possible to buy any fraction of a stock); iv) no restrictions on short selling; v) no opportunity for arbitrage; vi) the price of the underlying follows a log-normal distribution; and vii) the return of the underlying follows a normal-distribution. These assumptions are subject to much criticism, and there are methods available to relax some of them, however the initial model shall suffice for this analytic purpose.

Conventional weapons' aging is generally modeled as a gradual (log-linear) deterioration. Yet, this typical type of function does not hold up for cyber operations. The malleability of cyberspace offers, in the words of Bruce Schneier, a unique "window of exposure" for cyber-attacks to be effective.[54] The life-cycle of a vulnerability normally follows the following stages: vulnerability introduction, vulnerability discovery, creation of exploit for vulnerability, awareness vulnerability by the vendor, vulnerability is publicly reported, and release of the patch. The procedure of these stages is not a (log)linear process. Instead, the ability to use an exploit damage remains constant for a certain period of time, but rapidly declines the moment the vendor discovers the exploit, or a third party with visibility into the exploit informs the vendor.[55] Indeed, the decay function of an exploit is characterized by 'random crashes.'

The Black-Scholes model might provide a way to model this dynamic of this life cycle. The use of an exploit is similar to an 'American option' (i.e. it can terminate at any time). The value of using an exploit could be modeled as a 'Brownian motion' with random crashes. These random crashes may be caused by cases when other actors have used the same exploit, or when the vendor becomes aware of the vulnerability without an actor having used it in the past. Such instances may result from independent vulnerability rediscovery, or from visibility derived from detection through defensive countermeasures or through counter-cyber operations against other similar capabilities deployed from equivalent resource inventories held by other actors. The model assumes that the capability price fluctuates with constant drift and volatility, which leads to a geometric Brownian motion model for the price path.

Exploit inventory value crashes may also result from vulnerability discovery occurring based on identification of similar exploit chain components in other uses, including both primitives as well as weaponized exploitation in the wild. This, too, may have an underlying "physics-like" modeling property based on the fundamental characteristics of formal mathematical proof of exploitability (or more likely unexploitability), in which multiple pathways may be found to reach the same "weird machine" state of unintended code behavior.[56]

Overall, unlike the model of Iliev and Axelrod, or other more primitive models, when applied to cyber-attacks, this model does not assume that the loss of an exploit's value is a linear or log linear function. Instead, if one incorporates a model with 'random crashes' it provides a much closer representation of reality. In that sense, setting up this type of model could help government institutions to obtain a better cost estimate of arsenal maintenance.[57]

VI. CONCLUSION

This paper assesses to what degree (and which) formal models help to explain strategic choice and behavior in relation to cyber conflict. To this end, this paper discussed four models: one model already previously discussed by Axelrod and Iliev and three new models in relation to cyber conflict. All four models are potentially useful in explaining certain cyber conflict dynamics, although they have different strengths and weaknesses. It was never the aim of this paper to be comprehensive; there will be many deserving models and issues that are not covered or cited here. Instead, it is hoped that the models discussed here will serve as a useful doorway into a more structured understanding of cyber conflict dynamics.

Modeling the range of the future decision space under a variety of potential scenarios finds new relevance as offensive cyber operations (OCO) and counter-cyber operations (CCO) activities are considered beyond the episodic events which surface as major headlines from time to time, but instead are more deeply considered as the product of sustained organizational and individual efforts by military, intelligence, and proxy forces in pursuit of competitive objectives below the threshold of armed conflict, in preparation for future conflict, or seeking advantage in ongoing disputes that push gray zone thresholds.[58] There is an underlying logic that dictates the course, pace, and evolution of such operations by rational actors with differing interests, balancing differing equities. To date, these logics have been understood only dimly through analogy to other warfighting domains, and through inherited conceptual frameworks. The argument has been made that offensive cyber capabilities are perhaps the first military innovation to emerge directly from the intelligence community.[59] If one accepts this well-supported hypothesis, it is understandable then that cyber operations to date have followed the logic of intelligence operations.[60]

However, as emerging capabilities are coupled ever more tightly with conventional national security strategies, and across military globally integrated operations concepts, extant logics may well be changing. At the very least, new players and new priorities are likely to alter considerations of equities balancing, and perceptions of constraints, restraint or the lack thereof will likely differ as new audiences consider what were previously decisions taken in more rarefied and classified environments. The different mechanisms for signaling, public disclosure, parliamentary oversight, as well as generating and sustaining the public support that accompany military operations may also play key roles in influencing decision-making.

Thus, much additional work is needed to capture the complexity, variability, and path-dependence of offensive decision-making in cyberspace. This work may also be further enriched by more detailed insight into adversary specific strategic cultures (to the extent that such cultures may or may not be observed to exist), organizational influences, and operational experiences. Likewise, much of the decision space in which such logic is exercised is heavily influenced by the intelligence picture available to leadership, and where lacunae exist due to collection gaps, analytic failures, or deliberate deception impacts, the potential for misperception creates as yet unexplored strategic and operational risks.[61]

Beyond theoretic constructs, it is almost certain that the rapidly accelerating pace of current events shall see the employment of capabilities and response by other states, many times over across ongoing crisis flashpoints. It is expected that a robust body of case examples will result from these events, which may offer unique insights for future analysis and modeling.

Author Bios

Dr. Max Smeets

Dr. Max Smeets is a senior researcher at the Center for Security Studies (CSS). He is also an Affiliate at Stanford University Center for International Security and Cooperation and Research Associate at the Centre for Technology and Global Affairs, University of Oxford. Max was previously a postdoctoral fellow and lecturer at Stanford University CISAC and a College Lecturer at Keble College, University of Oxford. He has also held research and fellowship positions at New America, Columbia University SIPA, Sciences Po CERI, and NATO CCD COE. Before his academic career, Max worked in finance in London and Amsterdam. He received a BA in Economics, Politics and Statistics summa cum laude from University College Roosevelt, Utrecht University and an M.Phil (Brasenose College) and DPhil (St. John's College) in International Relations from the University of Oxford.

JD Work

JD Work serves as the Bren Chair for Cyber Conflict and Security at the Marine Corps University, leading efforts developing the theory, practice, and operational art of the cyber warfighting function, and to explore the wider role of the cyber instrument in national security strategy and the future defense competition, and stability problem space. Mr. Work has over two decades experience working in cyber intelligence and operations roles for the private sector and U.S. Government. He previously directed multiple international research programs to provide insight into the emerging strategic issues, economic consequences, and technology implications created by hostilities in the information environment, in order to support early warning, crisis management, and crisis prevention in and through cyberspace. Mr. Work also holds appointments with Columbia University School of International and Public Affairs, Saltzman Institute of War and Peace Studies, as well as the George Washington University Elliot School of International Affairs. He further serves as a senior advisor to the U.S. Cyberspace Solarium Commission.

NOTES

1. Application of game theory constructs to strategic and functional future cyber operational planning is known to have been conducted in nonpublic communities of interest associated with major national capabilities since at least 2008, building on related prior work examining the similar challenges regarding signals intelligence decision-making.
2. William A. Owens, Kenneth W. Dam and Herbert S. Lin (eds.), "Excerpts from Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities", National Research Council, (2009); S-1, Section 1.4 and 2.1.
3. Max Smeets, "On the Transitory Nature of Cyber Weapons," Journal of Strategic Studies, (2017)1:28
4. Matthew Monte, *Network Attacks and Exploitation*, (Wiley, 2015)
5. Hayden also writes: "I can think of no other family of weapons so anchored in the espionage services for their development (except perhaps armed drones)." Michael Hayden, Playing to the Edge: American Intelligence in the Age of Terror, New York, Penguin Random House, 2016, 137.
6. John B. Hattendorf. "The Idea of a 'Fleet in Being' in Historical Perspective." *Naval War College Review*, 67:1 (2014).
7. Paul M. Nakasone. "A Cyber Force for Persistent Operations. Joint Force Quarterly. 92: 1st Quarter 2019.; Michael P. Fischerkeller, Richard J. Harknett. "Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation," Institute for Defense Analyses, Alexandria, VA, May 2018; For review of strategy's potential impact also see: Max W.E. and Herbert Lin, "4 A Strategic Assessment of the U.S. Cyber Command Vision," in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, Herbert Lin and Amy Zegart (eds.) (Brookings Institution Press: 2018).
8. Neumann and Morgenstern's work is usually considered to be the first systematic and extensive formal analysis of social interaction. See: John von Neumann and Oskar Morgenstern, Theory of Games and Economic Behaviour, Princeton University Press: Princeton, 1944; Also see: Jacob Marschak, "Neumann's and Morgenstern's New Approach to Static Economics", Journal of Political Economy 54 (1946), 97–115.
9. This is hardly surprising as the subject matter of international relations is often seen as the study of the interactions themselves. See Lake, David H. and Powell, Robert (eds.), Strategic Choice and International Relations, Princeton University Press: Princeton, 1997.
10. Duncan Snidal, "The Game Theory of International Politics," World Politics, 38-1(1985), 25-57.
11. Ibid, 28.
12. Paul K. Davis, "Studying First-Strike Stability with Knowledge Based Models of Human Decision making," Washington DC., RAND, 1989.
13. Thomas C. Schelling, "The Role of War Games and Exercises," in Carter et. al. (Eds.), Managing Nuclear Operations, The Brookings Institution, Washington, D.C., 1987, 439-440.
14. Andrew Kydd, International Relations Theory: The Game-Theoretic Approach, Cambridge: Cambridge University Press: 2015.
15. While discussion of these models may be usefully extended in the context of nonstate actors, further work is required to explore these dynamics in other contexts.
16. Robert Axelrod, "The Rational Timing of Surprise," World Politics, 31:2, (1979), 228-246.
17. Robert Axelrod and Rumen Iliev, "Timing of cyber conflict," PNAS, 111:4 (2014), 1298–1303.
18. Ibid.
19. Ibid.
20. Ibid.
21. Ibid.
22. Ibid.
23. William Poundstone, Prisoners' Dilemma, Anchor Books: New York, NY, 1993, 141.
24. Alan D. Taylor, Mathematics and Politics: Strategy, Voting, Power and Proof, Springer Verlag: New York, 1995, 166.
25. David Blackwell, The noisy duel, one bullet each, arbitrary accuracy, The RAND Corporation: 1949; David Blackwell and A. Girshick, "A loud duel with equal accuracy where each duelist has only a probability of possessing a bullet", The RAND Corporation: 1949, David Blackwell and A. Girshick, Theory of Games and Statistical Decisions, John Wiley, New York: 1979; for an excellent review see: Tadeusz Radzik, "Results and Problems in Games of Timing, Statistics, Probability, and Game Theory," IMS Lecture Notes Monograph Series, 30, (1996).

NOTES

26. See Ken Binmore, Fun and Games: A Text on Game Theory, D. C. Heath and Co: Lexington, 1992; Melvin Dresher, The Mathematics of Games of Strategy: Theory and Applications, Dover Publications Inc.: New York, 1981.
27. Radzik, "Results and Problems in Games of Timing".
28. Yoshinobu Teraoka, "Two-Person Game of Timing with Random Termination," *Journal of Optimization Theory and Applications*, 40: 3 (1983).
29. Calvin W. Sweat, "A single shot noisy duel with detection uncertainty," Operation Research, 19 (1971), 170-185.
30. Yoshinobu Teraoka, "Noisy Duel with Uncertain Existence of the Shot," International Journal of Game Theory, 5 (1976), 239-249, 1976; Yoshinobu Teraoka, "Silent-Noisy Duel with Uncertain Existence of the Shot," Bulletin of Mathematical Statistics, 18 (1981), 43-52.
31. Teraoka, "Two-Person Game of Timing with Random Termination."
32. S. Styszyiqski, "A Silent-Silent Duel with Bullets Accessible at Random Moments," Politechniki Wroclawskiej, Instytut Matematyki, Research Report, No. 40 (1979).
33. T, Kurisu, "On a Noisy - Silent versus Silent Duel with Equal Accuracy Functions," *Journal of Optimization Theory and Applications*, 39 (1983), 215-235.
34. The model could potentially account for adding a *probability* that the other actor has the same exploit.
35. Lillian Ablon and Andy Bogart, "Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits," RAND Corporation: 2017.
36. Ibid.
37. Discussion with vulnerability researchers under Chatham House rule, Marine Corps University, June 2019.
38. For a lengthier discussion on this point see: David Raymond, Greg Conti, Tom Cross, and Robert Fanelli, "A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons". 2013 5th International Conference on Cyber Conflict K. Podins, J. Stinissen, M. Maybaum (Eds.) 2013 © NATO CCD COE Publications, Tallinn https://ccdcoe.org/uploads/2018/10/8_dlr2s6_raymond.pdf, http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=67E851l4AA1D5C3942296FA224578088?doi=10.1.1.385.7204&rep=repl&type=pdf.
39. Also see: Max Smeets, " The Strategic Promise of Offensive Cyber Operations," *Strategic Studies Quarterly*, Fall 2018, 90-113; Max Smeets and Herbert S. LIn, "Offensive Cyber Capabilities: To What Ends?" 2018 10th International Conference on Cyber Conflict, CyCon X: Maximising Effects, T. Minárik, R. Jakschis, L. Lindström (Eds.) 2018, NATO CCD COE Publications, Tallinn.
40. For a discussion on similar trade-offs see: Aaron F. Brantly, The Decision to Attack : Military and Intelligence Cyber Decision-Making, University of Georgia Press, 2016, 79 – 89; Brantly, "Aesop's Wolves: The Deceptive Appearance of Espionage and Attacks in Cyberspace." Intelligence and National Security 31, no. 5 (2015), 674-85, https://doi.org/10.1080/02684527.2015.1077620.
41. Leslie Real, "Search Theory and Mate Choice. I. Models of Single-Sex Discrimination", *The American Naturalist*, 136-3(1990):376-405; also see: Leslie Real, "Search theory and mate choice: II. Mutual interaction, assortative mating, and equilibrium variation in male and female fitness," *American Naturalist*, 138:(1991) 901–917; Russell Bonduriansky, "The evolution of male mate choice in insects: a synthesis of ideas and evidence," Biological Reviews , 76-3(2001), 305-339.
42. This model does not explicitly deal with the behavior of rivals in a game theoretical Sense, i.e., the strategy of other actors is not considered, merely a modeling term is added that considers the risk of waiting.
43. Ibid, 377.
44 Anthony C. Janetos, "Strategies of female choice: a theoretical analysis," *Behavioral Ecology and Sociobiology,* 7 (1980), 107-112.
45. Real divides the costs of sampling into two forms. First, there are 'direct costs' which concerns aspects such as expenditures of time and energy through added search, directed aggression from other competing searchers, risk of predation, or death. Second, there are 'indirect costs' (or opportunity costs) which includes aspects such as loss of previously encountered mates due to death, emigration, or loss of mating status.
46. According to Leslie Real, "the problem is formally analogous to a variety of classic sequential-search models discussed in the literature of both economics and statistics. The problem, variously known as the secretary problem, marriage problem, and job-search problem, imagines an agent who must decide to accept or reject candidates based on the sequence of encounters and a knowledge of the distribution of candidate qualities." Real, "Search Theory and Mate Choice."

NOTES

47. However, the use of zero-day exploits is much less common than some would think. See: Rob Joyce, "Disrupting Nation State Hackers," *USENIX Enigma 2016*, retrieved from: https://www.usenix.org/sites/default/files/conference/protected-files/engima2016_transcript_joyce_v2.pdf.
48. Also see: Max Smeets, "Organizational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks", in Henry Roigas, Raik Jakschis, Lauri Lindstrom, and Tomáš Minarik (Eds), 9th International Conference on Cyber Conflict, Tallinn, NATO CCD COE Publications: 2017; Max Smeets, "Integrating offensive cyber capabilities: meaning, dilemmas, and assessment," D*efence Studies*, 18:4 (2018), 395-410.
49. In the market there are two ways to think about hedging; i) loss mitigation for an asset, and ii) the creation of a diskless portfolio. Option pricing uses the second of these definitions.
50. Charles Castelli, The Theory of Options in Stocks and Shares, London: F. C. Mathieson: 1877.
51. Bachalier, "The Theory of Speculation", Annales sceintifiques de l'Ecole Normale Superieure, 3:17 (1990), 21-36 (Translated by May) retrieved from: http://www.radio.goldseek.com/bachelier-thesis-theory-of-speculation-en.pdf.
52. Fischer Black and Myron Scholes, "The pricing of options and corporate liabilities," *The Journal of Political Economy*, 81:3 (1973), 637–654.
53. Jacob Abernethy, Rafael M. Frongillo, and Andre Wibisono, "Minimax Option Pricing Meets Black-Scholes in the Limit," STOC'12, (May 19–22, 2012, New York, USA).
54. Bruce Schneier, "Crypto-Gram,"(2000), hxxps://www.schneier.com/crypto-gram/archives/2000/ 0915.html.
55. Smeets, "A Matter of Time."
56. For further exploration of the concepts of formal proof in exploitation, see the unique work of Thomas Dullien. "Weird machines, exploitability, and provable unexploitability." IEEE Transactions on Emerging Topics in Computing. December 2017. DOI: 10.1109/TETC.2017.2785299.
57. Again, note that the use of exploits is only one small part of the military cyber arsenal.
58. Also see: Florian Egloff, "Cybersecurity and Non-State Actors: A Historical Analogy with Mercantile Companies, Privateers, and Pirates." DPhil Thesis, University of Oxford, 2018.
59. Craig J. Wiener, *Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as A Major Military Innovation*, George Mason University, 2016.
60. Discussion under Chatham House rule at Strategic Competition in Cyberspace: Challenges and Implications. Center for Global Security Research. Lawrence Livermore National Laboratory, July 10-11, 2019.
61. The seminal work in this area of course remains Robert Jervis. *Perception and Misperception in International Politics*, Princeton, NJ: Princeton University Press, 1976; additional consideration specific within this new domain seems of value.