Chapter 1
Cyber War Games: Strategic Jostling Among Traditional Adversaries

Sanjay Goel and Yuan Hong

Abstract Cyber warfare has been simmering for a long time and has gradually morphed into a key strategic weapon in international conflicts. Doctrines of several countries consider cyber warfare capability as essential to gain strategic superiority or as a counterbalance to military inferiority. Countries are attempting to reach consensus on confidence building measures in cyber space while racing with each other to acquire cyber weaponry. These attempts are strongly influenced by the problem of clear attribution of cyber incidents as well as political imperatives. Game theory has been used in the past for such problems in international relations where players compete with each other and the actions of the players are interdependent. Problems in cyber warfare can benefit from similar game theoretic concepts. We discuss in this book chapter the state of cyber warfare, the key imperatives for the countries, and articulate how countries are jostling with each other in the cyber domain especially in the context of poor attribution and verification in the cyber domain. We present game theoretic models for a few representative problems in the cyber warfare domain.

1.1 Introduction

Cyber warfare started as a low intensity activity among nations and was initially used for nuisance attacks such as website defacement and denial of service attacks but it has developed into a fierce cyber arms race among countries. Cyber warfare now figures prominently in doctrines of major military superpowers and terrorist organizations. There have been cyber warfare incidents in the past where attacks were launched on Estonia and Georgia in context of political conflicts with Russia. There have also been attacks on South Korea and Japan related to regional political conflicts involving similar modes of attacks. Aside from these overt attacks, there have been several covert attacks involving espionage across different countries where both the

S. Goel (✉) · Y. Hong
University at Albany, State University of New York, New York, USA
e-mail: goel@albany.edu

Y. Hong
e-mail: hong@albany.edu

S. Jajodia et al. (eds.), *Cyber Warfare,* Advances in Information Security 56,
DOI 10.1007/978-3-319-14039-1_1

military and civilian infrastructure is targeted. There are suspicions that countries are attempting to intrude into the critical infrastructure of other countries to gain a strategic lever during conflict. There is also an apprehension that the Internet could be used to change national ideological and cultural values; along these same lines, a strong concern is that social media could be used to cause upheaval and overthrow governments. Countries are blaming each other for attacks and espionage while at the same time planning their own cyber warfare strategy. Mutual distrust among nations is driving them to invest in cyber warfare capabilities in order to gain strategic leverage over other countries while at the same time lobbying for slowing down the other countries. A big fear is cyber attack launched from a country by groups outside of government control could trigger a kinetic response.

There have been attempts at creating international treaties and laws related to cyber crime and cyber warfare but these are moving at a very slow pace while traditional military rivals jockey with each other to gain their own strategic advantage. A key impediment to building consensus on cyber warfare treaties is the inherent anonymity of the Internet that can camouflage the identity of the perpetrators and make it attribution of attacks to any specific individual, group, or nation uncertain. Attacks launched by actors who are not in direct control of the state can trigger a misdirected counter attack at a nation state. There is an additional problem of misdirection where attackers can deliberately leave a trail to implicate other parties for their activities. Countries are thus reluctant to sign any legal document that will hold them responsible for activities that can get misattributed to them through subterfuge and deceit of other countries.

Realizing the futility of attempting to forge a broad consensus on enforceable international treaties on cyber warfare and the urgency to cool down the torrid cyber arms race. There have been attempts at confidence building measures as a prelude to eventual signing of treaties. Efforts to create confidence-building measures to reduce the threat of cyber warfare are active in several international bodies including the United Nations (UN) and the Organization for Security and Cooperation in Europe (OSCE). States are attempting (or pretending) to cooperate with each other while at the same time competing with one another in the cyber arms race.

Game theory is well suited for analyzing relationships among multiple actors, who in this case include, nation states, non-state actors (terrorists, hacktivists, etc.), and supranational organizations (e.g., UN, OSCE, etc.). Since the seminal work of Von Neumann and Morgenstern (1944, 1994) "The Theory of Games and Economic Behavior", game theory has been used extensively for studying international relations. There are several areas where game theoretic models are suitable including security, economics, education, environment, human rights, and international law. In this chapter we focus on the security issues related to cyber warfare and formulate problems in the cyber warfare domain using game theoretical models. The chapter does not contain a deep mathematical development in this field but rather focuses on demonstrating the modeling of game theoretic concepts for cyber warfare.

The rest of the chapter is organized as follows: Sect. 1.2 provides a background of the problem including the adversaries (players), their strategic positions (options), and the key objectives (optimization function) to achieve. Sect. 1.3 discusses fundamental game theoretic concepts and some recent work on cyber warfare that includes game theoretic models. Sect. 1.4 discusses the models in details followed by a succinct conclusion.

1.2 Cyber Warfare

Definition of cyber attacks is contextual: depending on the actors, motivation, targets, and actions, they can be called cyber terrorism, cyber crime, cyber activism, etc. There are several distinct modes of conflicts related to cyber warfare. Understanding the relationships between actors, their behavior, and their motivations is essential in order to understand cyber warfare better and to reduce chances of a serious cyber conflict. We use game theoretic models to look at positions of the key players on each of these conflicts to understand the dynamics among the players in these conflicts. We select four modes of cyber conflict that are dominating international cyber politics for further analysis including: (1) social media wars that influences a country's internal politics often with a goal of fomenting social uprisings that can result in political change; (2) strategic war aimed at causing damage for the adversary as well as pillaging resources (e.g., industrial espionage); for this, countries are acquiring resources to conduct both espionage and develop tools that can be used to disable the adversarial activities occurring in critical infrastructure including power, communication, media, Internet, etc.; (3) ideological battle where fundamentalist organizations use the Internet to spew their ideology and to recruit members in other countries for their cause; (4) citizen-initiated war where a country's civilians directly attack another country's citizens and institutions as a part of larger conflict (ideological or kinetic).

Foreign intervention through social media has become a significant fear for countries leading to aggressive monitoring if not outright controlling of social media content. Some countries have already invested in censorship and control of the Internet mainly driven by intention to decrease political unrest or ideological and religion polluting. Social media-facilitated revolutions have driven some countries to the point of paranoia regarding control of online activity. If this type of distrust keeps growing, there is only one logical conclusion: separation of the Internet across country borders. A separated Internet could have severe consequences with negative impacts from the individual to national level from social relationships, educational pursuits, commerce, and tourism. In a lot of the authoritarian and corrupt regimes the conditions on the ground are ripe for popular revolutions. In the past, they have been kept in check through censorship and coercion. Social media has provided a forum for organizing large scale protests—which countries are prone to such attacks and which countries have incentives to sponsor such attacks.

The strategic war of targeting the resources has each country building up their cyber arsenals quietly while publicly denouncing similar activities by others. Each country considers cyberspace a natural place for gaining strategic military advantage. This is causing serious misgivings between different countries. For instance, the

United States is very concerned about Chinese reconnaissance into the power grid and at the same time attempting to gather intelligence from foreign networks. Similarly, businesses are constantly claiming intrusion by the Chinese for corporate espionage or stealing data. These illicit activities have been widely publicized by the media resulting in civilian unease and condemnation from the U.S. government. However, at the same time, it has been revealed that the U.S. ran one of the largest spying operations around the world sparing neither friend nor foe.

Terrorism fits naturally with game theory since when it is reduced to its simplest level, many terrorist events can be summed up to simple or complex strategic interactions. It can be examined both at a micro-level dealing with individual attack decisions and at a macro-level that involves overall strategy of the attacker (terrorist group) and defender (nation states). Each country seems to have their own terrorist problem; inciting such anti-national activities in other countries can backfire. Each country has their own terrorist foes that they are concerned with, e.g., Russia about Chechnya-based jihadi elements, the U.S. about Al Qaeda, India about Pakistan-based terrorist organizations, E.U. about jihadi elements from the Middle East, and China about Tibetan activities. While countries are being victims of terrorism, they are supporting terrorism in other countries. The link between sponsors and the victims can be established in order to formulate a strategy to counter cyber terrorism. Consider for instance a country has a chance to sponsor terrorism against a rival country. The choices are two fold i.e. sponsor or not to sponsor. The country against which it is targeted can either negotiate or retaliate. This creates a game theoretic problem.

There have been many incidents of citizen-initiated attacks against other countries either through tacit government support or through support of non-state actors. Examples of these types of incidents include hacker group activities in India and Pakistan. Similarly, there have been attacks by Russian citizens on Estonia and Georgia during conflicts. Citizen-initiated war typically starts with a strong rhetoric in the media and then takes a life of its own often outside of governmental control. Citizen-initiated attacks provide leverage to governments since they can absolve themselves at least partly in participating in an act of war but they may get out of control and lead to unanticipated disproportionate retaliation.

A key concerns for strategists is to prevent unexpected and unwarranted escalation of the war. The escalation can come from political reasons when the attacked nation is forced to have a forceful response to cater to public perception. Countries can deliberately force a response from other countries looking for an excuse for conflict. Non-state actors who launch attacks masquerading as a nation state can cause dangerous escalation in tension by launching cyber attacks purportedly from one nation state to another. This becomes especially potent since attribution is hard and distinguishing between an attack by a proxy representing the state and a non-state actor can be difficult. Given the shared security doctrines that exist among countries this conflict to escalate into a multi-county conflict. At some point a cyber attack will lead to a kinetic attack if tensions escalate sufficiently or phony cyber attacks will be used as a ruse to launch a kinetic attack. Attacks on the critical infrastructure have already escalated cyber warfare to the next level there have been mutual incriminations about surveillance and penetration into critical infrastructure networks among countries. Stuxnet worm that was used to launch attack on the centrifuges in the Iranian nuclear program has demonstrated the potency of critical infrastructure attacks leading each country to build their defensive capability and at the same time invest in offensive capabilities for deterrence.

Escalation of the social media war and information censorship may also escalate compelling countries to isolate them on the Internet leading to the fragmentation of the Internet that is also undesirable. Countries that consider the freedom of Internet a threat to the political structure and social fabric of society will start separating from the Internet. China has already insulated their citizens from the "objectionable content" of global Internet through stringent laws on admissible content on the Internet and aggressive censorship where they filter Internet traffic, block specific IP-addresses, and aggressively monitor the content on the Internet. Several other countries such as Russia, Iran, and Germany are making attempts to insulate their networks or data from other countries albeit for different reasons.

We formulate game theoretic problems related to some of these dynamic scenarios to better understand the dynamics and to determine optimum strategy. The overall goal of the endeavor is to support the creation of international treaties based on optimum strategies for each of the key player.

1.3 Game Theory

Game theory involves the formulation of a decision-making problem as a game in which two or more players make decisions such that the decisions of one player has an impact on the decision of the other player. The game is defined as a set of *strategies* and *payoffs* for each player. The players are assumed to be rational and their goal is to maximize their payoffs (utility) from participating in the game. All players also expect other players to be rational. Generally, rationality assumes perfect and complete information among players about the strategies and payoffs of each other. Complete information refers to the recognition of the identity of other players involved and the payoff for their particular strategies, whereas perfect information refers to the ability to observe the actions of other players. In the context of incomplete information, where players do not know their opponent's strategies, a Bayesian game based on a probability distribution of actions in the strategy set may be modelled (Harsanyi 1967).

There are three types of payoff functions: zero-sum; constant-sum; and non-zero sum. In zero-sum games the gains of one player are directly opposite to the losses of another. What one player wins, the other must lose. This assumes that opponent's evaluation functions are opposite. In constant-sum games, only one player will have a non-zero payoff at any one time, and in non-zero sum games no restrictions are applied to the payoff structure (Aumann and Maschler 1995). Hamilton et al. (2002) suggests that zero-sum assumptions are not reasonable in cyber warfare as state actors have different goals and priorities. Burke (1999) suggests a non-zero sum model is most realistic in the context of this type of information warfare.

The goal of the game is to find an equilibrium solution, i.e. the best outcome or payoff for the players considering the decisions of all other players. In classical optimization terms this is a local optima solution to the problem for a player. One of the most basic solution for a game is the minimax solution that minimizes a players' maximum expected loss. Nash Equilibrium, is achieved when a unique, optimal strategy for each player corresponding to every move of the opponent is available (Gibbons 1992). A strategy is said to be *pure* if the probability that the strategy will be chosen is 1 for a given scenario. In many cases, however, opponents do not have complete information or are uncertain about the structure of the game and a pure strategy is not evident. In this case, a stochastic model called the *mixed strategy* is used in which a probability associated with specific strategies are defined.

Games can be cooperative and non-cooperative. Cooperative games are usually modeled when mechanisms are available to enforce particular sets of behavior (source). Although we may assume cooperative strategies in cyber warfare (for example, cooperation among NSA and GCHQ), in this chapter we model non-cooperative games. We make policy recommendations to reduce problems of cyber warfare based on the conclusions derived from our non-cooperative models. Perfect information also involves the concept of *perfect recall*, or knowledge of the history of strategies chosen by each player. We expect the cyber warfare confidence building and treaty process to have perfect recall while cyber war strategy games to deploy offensive and defensive capabilities to have incomplete information. In the cases we model, however we make a simplification assumption of perfect information.

In general, games are either *static* or *dynamic.* In static games, decisions by all players are made simultaneously without knowledge of the decisions that other players have actually carried out. Dynamic games involve a series of games where the strategies can be re-evaluated based on previously made choices by the players involved. In the context of cyber warfare *dynamic* games may be present when intrusion tactics involve multiple steps and trials. At the same time, defense mechanisms may allow the recognition of previous attacks and influence future behavior in order to protect the systems. Sequence in time is thus an important component of cyber warfare (e.g. see Libicki 1997). It is also reasonable to assume static games, however, as many cyber attacks happen unbeknownst to those being attack. We create static models for several games.

1.3.1 Game Theory in International Relations

One of the key assumptions in game theory is that actors are non-altruistic and are purely driven by their own goals. The field of international relations is a quintessential representation of this assumption where nation-states are motivated only by their interests and are not guided by ethical or humanitarian concerns but are only concerned about maximizing their utility function (Evans and Newnham 1998; Hollis and Smith 1990). There are two areas of International Relations that can greatly improve the understanding of cyber warfare deterrence and arms race as well as international diplomacy. International relations scholars (Gleditsch 1990; Intriligator and Brito 1990; Bolks and Stoll 2000; Reuveny and Maxwell 1998) have extensively studied deterrence and arms races using game theoretic models. In its simplest form deterrence between two nation states can be studied where each threatens to retaliate to a potential attack by the other to prevent the other from launching the attack in the first place. The objective of the nation-states is to prevent destruction or domination by the other and each would feel more secure if it acquires weapons for protection. The acquisition of the weapons, albeit for defensive purposes, trigger the adversary into acquiring more weapons especially if the weapons are dual use leading to an arms race. This phenomenon where actions by a state to heighten its security can lead other states to respond with similar measures thereby escalating dangers of conflict rather than reducing them even though no one desires it is called the security dilemma and can be studied using game theoretic concepts. This phenomenon is studied extensively using the Prisoner's Dilemma game (Brams 1975; Clemens 1998; Dixit and Skeath 1999; Hamburger 1979; Powell 1999; Taylor 1995), which often results in a less than desirable outcome for each player. There has been very little research on the use of Game Theory for cyber warfare and cyber terrorism.

Matusitz (2009) suggests that game theory is particularly important and useful to apply to cyberterrorism. Jormakka and Mölsä (2005) present 4 distinct scenarios in which game theory may be applied in the context of information warfare. The first example includes a terrorist group (T) with certain requirements, holding hostages and threatening to cause destructive damage; and a government (G) wanting the terrorists to surrender. This game is modelled as a two-player static game of complete information, where each player has two strategies (e.g., accepting or rejecting the other's). Initially, this game ends with two Nash equilibriums with no unique solution as is typical in asymmetric warfare. If the game is repeated, and each player adopts a "bold" or single strategy, a dominated outcome can be obtained (i.e. outcome other than equilibrium). They also show that using a mixed strategy can prove effective against a dominative attack strategy. Finally they demonstrate an n-person game where an attacker is perpetrating a DoS attack on a network and each player has two strategies i.e. using the network or being idle. There is one attacker who wants to overload the network, and a number of other users who want to maintain the network functioning. This situation results in a payoff that is 0 for all players. After initial shutdown of the network, users will find another network in which to operate. Making this assumption the attacker ("vandal") cannot win. However, if the game is modeled as a dynamic game, and the vandal only overloads the network 50 % of the time, he can have some gain. Ma et al. (2011) develop a game theoretic model for interaction between government agencies and firms that are faced with cyber threats. They use the Crawford and Sobel (1982) "cheap talk" model. A similar model can be used to understand the interactions between the hacker groups and the Chinese government.

1.4 Problem Formulation

The basic game theory problem is that each country wants to deescalate cyber tension however they cannot trust the other adversaries and thus need to invest in cyber arsenals to catch up with the adversaries leading to the arms race where each party incurs a heavy loss. This can be explained by using the classical Prisoner's Dilemma problem—a two-person game. In this game both players have two strategies either to cooperate or to defect. If both players cooperate with each other they receive a low cost i.e. go to prison for 1 year. If one of them cooperates and the other defects, the prisoner who defects gets no cost i.e. goes free and the prisoner who cooperates gets a high cost i.e. 5 year prison term. If both of them defect then they both get a moderate cost of 3 years of prison term. Given the assumption that each player is only interested in self-gain and there is no trust with the other player the minimax strategy is to defect for both player (Table 1.1).

Table 1.1 Basic formulation for Prisoner's Dilemma

	Prisoner B stays silent (cooperates)	Prisoner B betrays (defects)
Prisoner A stays silent (cooperates)	Each serves 1 year	Prisoner A: 5 years Prisoner B: goes free
Prisoner A betrays (defects)	Prisoner A: goes free Prisoner B: 5 years	Each serves 3 years

In cyber arm race, if two nation states cooperate they have no cost (building a cyber arsenal). If both states defect i.e. they both have to build cyber arsenals, they have a moderate cost (building an arsenal). However if one cooperates (does not build an arsenal) and the other defects (builds an arsenal) the defecting state will have a low cost but the cooperating state will have a high cost (loss during conflict). Consequently, both states will choose to build an arsenal.

For instance, the U.S. and China may have been hacking and spying on each other for a long time (from traditional manners to computer based tactics), and try to gain the strategic military advantage in cyberspace. To build the cyber arsenal for the above purpose, increasing military expenditure becomes indispensable, however such military expense increase clearly affects their economics by appropriating the spending allocated for other areas such as construction, education and healthcare. Each of these two countries have two strategies: (1) reducing the military expenditure (cooperate), and (2) increasing expenditure to build up cyber arsenal (defect). Essentially, the rational strategy for them is to reduce cyber warfare expenditure for both countries by establishing a treaty (cooperate), then both of them are able to at least maintain the allocated expenditure in other areas—a win-win situation. However, countries may betray the treaty and privately increases the expenditure to build up cyber arsenal, and thus attempt to win the strategic military advantage in the cyber warfare. If the U.S. cooperates and China defects, the U.S. could easily win the advantage, and vice-versa. In reality, due to mutual lack of trust (each country is fear of the covert cyber activities from the other country), the cyber deterrence would indeed lead to an irrational result for the participated countries—both countries are strongly inclined to covertly increase its expenditure on building up the cyber arsenal (defect). Therefore, both countries have to invest considerable amount of expenditure on cyber warfare. Compared to the case of cooperation, both countries lose their payoff to some extent. (Table 1.2)

Table 1.2 Payoff matrix of "Prisoner's Dilemma" in cyber warfare

		United States	
		Reduces military expenditure (Cooperates)	Increases expenditure to build up cyber arsenal (Defects)
China	Reduces military expenditure (Cooperates)	Both countries can cut the expense on cyber arsenal, and thus save military expenditure	United State wins the strategic military advantage in cyberspace
	Increases expenditure to build up cyber arsenal (Defects)	China wins the strategic military advantage in cyberspace	Both countries spend considerable amount of money on cyber arsenal, and thus reduce expenditure on education, healthcare, construction, etc

Based on the "Prisoner's Dilemma", Nadiya Kostyuk (2013) studied another cyber conflict case between two powerful countries, e.g., the U.S. and China in cyber espionage that can hurt trade between the two. They are not likely to cooperate with each other, even though cooperation could bring mutual benefits to both countries. (Table 1.3) Please refer to the payoff matrix as below:

In the same article, Kostyuk (2013) showed that prisoner's dilemma can be also applied to the cyber warfare case between one powerful country and one less powerful country i.e Russia and Estonia. These two countries are also highly likely to choose "Do not cooperate", which is evidently a worsen case than both cooperate. (Table 1.4) Please refer to the payoff matrix given as below:

Besides the "Prisoner's Dilemma", we present another class model applicable to cyber warfare—zero-sum game. In zero-sum games, a player's gain (or losses) of utility is exactly balanced by the other player's utility losses (or gain). Hence, the total sum of gain and losses is equal to zero. For any two-player zero-sum game, if mixed strategy is allowed, the Nash Equilibrium can be found using linear programming (LP). As a key form of cyber warfare, anti-national cyber terrorism activities in a country are usually supported by another country, then the utility loss caused in the activities may lead to the activity supporter's payoff gain. Assuming that the payoff loss of one country equals the payoff gain of the other country, per the minimax theorem, the Nash Equilibrium—optimal (mixed) strategies for both countries on the international cyber terrorism activities can be derived by solving an LP problem.

For instance, each of two conflicting countries in cyber warfare have four different strategies regarding the support of cyber terrorism activities in the other country (attack) and counter cyber terrorism activities/mechanisms for itself (anti). The payoff for each combination of the players' strategies is balanced (an example is given in Table 1.5).

Each country aims at developing a cost-effective strategy to decide whether to spend money on overseas cyber terrorism activities and/or to establish its own counter

Table 1.3 Payoff matrix of "Digital Prisoner's Dilemma" (Two powerful nations). (Kostyuk (2013))

		United States	
		Cooperates	Does not cooperate
China	Cooperates	Likely Scenario:	Highly Unlikely Scenario:
		(1) individual hackers are punished	(1) U.S. denies responsibility
		(2) trade between the two nations continues	(2) U.S.—China relations worsen
			(3) Trade declines causing severe economic losses in the States
			(4) The number of cyber attacks coming from both countries increases
	Does not cooperate	Unlikely Scenario:	*Highly Likely Scenario:*
		(1) the U.S. continues experiencing losses in its intellectual property	(1) The attacks escalate
		(2) the U.S. could try applying sanctions against China	(2) U.S. relies on its adept domestic and international law enforcement arms
		(3) Mutual Legal Assistance Treaty is worthless	(3) China appears incapable of policing its cyberspace, making it vulnerable to internal attacks and eventually is forced to cooperate with the States

Table 1.4 Payoff matrix of "Digital Prisoner's Dilemma" (One powerful nation and one less powerful nation). (Kostyuk (2013))

		Estonia	
		Cooperates	Does not cooperate
Russia	Cooperates	Unlikely Scenario:	Highly Unlikely Scenario:
		(1) individual hackers are punished	(1) Russia denies responsibility
		(2) future hacks are deterred	(2) Russo—Estonian relations worsen
	Does not cooperate	Likely Scenario:	*Highly Likely Scenario:*
		(1) Estonia seeks help from Russia	(1) The attacks escalate
		(2) Mutual Legal Assistance Treaty is worthless	(2) Countries are incapable of policing its cyberspace—stepping stone nations for future attacks by third parties
			(3) Estonia seeks help from NATO or EU

cyber terrorism activities/mechanisms. Thus, we can formulate a zero-sum game for the cyber terrorism activities between two countries, where an optimal mixed strategy

Table 1.5 An example of zero-sum game in cyber warfare

	Attack and anti	Attack and no anti	No attack and anti	No attack and no anti
Attack and anti	(0, 0)	(50, – 50)	(– 10, 10)	(40, – 40)
Attack and no anti	(– 50, 50)	(0, 0)	(– 10, 10)	(40, – 40)
No attack and anti	(10, – 10)	(10, – 10)	(0, 0)	(0, 0)
No attack and no anti	(– 40, 40)	(– 40, 40)	(0, 0)	(0, 0)

in the Nash Equilibrium can be derived from the LP problem to facilitate the above decision-making. Furthermore, let us consider the dynamics between countries that have ability to sponsor cyber terrorism through non-state actors versus countries that are victims of such terrorism. The sponsoring country has three choices i.e. actively sponsor, control terror groups, do nothing. The defending country has three options prevent the attack, retaliate, and negotiate. The best scenario for the sponsoring nation is to bring the attacked country to a negotiating table without having to do anything. The best thing for the defending country is for cyber terrorism to not occur. There are different payoff's associated with each of the strategies of the defender and attacker. (Table 1.6) The matrix is shown below:

Table 1.6 State sponsorship of terrorism

		Defending nation		
		Prevent	Retaliate	Negotiate
Sponsoring nation	Sponsor non-state actors	(– 5, – 5)	(– 20, – 10)	(5, – 20)
	Control non-state actors	(– 5, 0)	(– 5, 0)	(4, – 20)
	Do nothing	(– 10, – 5)	(– 10, – 10)	(10, – 20)

1.5 Conclusion

Cyber warfare is becoming increasingly prevalent with multiple actors with several decision-making issues where they are interdependent on each other including, cyber arms race, agreeing to treaties, and dealing with cyber espionage and terrorism. In this chapter we draw from the field of international relations and terrorism to show examples of game theoretic models for cyber warfare. Game theory is well suited for this domain. We create models based on the prisoner's dilemma game. There are other game theoretic techniques that will work as well including stochastic games and multi-step games.

References

Aumann, Robert and Maschler (1995), Michael, “Repeated Games with Incomplete Information”, MIT Press.

Brams, Steven J. (1975) “Game Theory and Politics”, The Free Press: New York, NY.

Bolks, Sean and Stoll, Richard (2000), “The Arms Acquisition Process The Effect of Internal and External Constraints on Arms Race Dynamics”, Journal of Conflict Resolution, Vol 44(5), pp. 580–603, Sage Publications.

Burke, Jonathan (1999), “Robustness of Optimal Equilibrium Among Overlapping Generations”, Economic Theory, Vol. 14, pp. 311–330, 1999.

Clemens, Walter C. (1998) “Dynamics of International Relations: Conflict and Mutual Gain in an Age of Global Interdependence”, Rowman & Littlefield Publishers: Lanham, MD.

Crawford, Vincent and Sobel, Joel, (1982), “Strategic Information Transmission”, Econometrica, Vol 50(6), pp. 1431–1451.

Dixit, Avinash, and Skeath, Susan (1999) “Games of Strategy”, W. W. Norton & Co.: New York, NY.

Evans, Graham, and Newnham, Jeffrey (1998) “Dictionary of International Relations”, Penguin Putnam Inc.: New York, NY.

Gleditsch, Nils P. (1990) “Research on Arms Races”, in Gleditsch, Nils P. and Njolstad, Olav (eds.), Arms Races: Technological and Political Dynamics, Sage Publications: Newbury Park, CA.

Gibbons, Robert (1992), “Game Theory for Applied Economists”, Princeton University Press.

Hamburger, Henry (1979) “Games as Models of Social Phenomena”, W. H. Freeman and Co.: New York, NY.

Hamilton, S. N., Miller, W. L., Ott, A., & Saydjari, O. S. (2002). The role of game theory in information warfare. *4th Information survivability workshop* (*ISW-2001/2002*). Vancouver, Canada.

Harsanyi, John (1967), “Games with Incomplete Information Played by “Bayesian” Players, I-III, Part I, the Basic Model”, Management Science, Vol 14(3), pp. 159–182.

Hollis, Martin, and Smith, Steve (1990). “Explaining and Understanding International Relations”, Oxford University Press: New York, NY.

Intriligator, Michael D. and Brito, Dogobert L. (1990). “Arms Race Modeling: A Reconsideration”, in Gleditsch, Nils P. and Njolstad, Olav (eds.), Arms Races: Technological and Political Dynamics, Sage Publications: Newbury Park, CA.

Jormakka, J., and Mölsä, J. V. (2005). Modelling information warfare as a game. *Journal of Information Warfare*, *4*(2), 12–25.

Kostyuk, Nadiya (2013). “The Digital Prisoner’s Dilemma: Challenges and Opportunities for Cooperation”, published online at http://cybersummit.info/sites/cybersummit.info/files/The%20Digital%20Prisoner’s%20Dilemma-Challenges%20and%20Opportunities%20for%20Cooperation_Nadiya%20Kostyuk%20.pdf.

Libicki, Martin (1997), “Defending Cyberspace, and Other Metaphors”, National Defense University.

Ma Z. (Sam), Chen H. (Daisy), Zhang J., Krings A., & Sheldon F. (2011). Has the Cyber Warfare Threat Been Overstated?: A Cheap Talk Game-theoretic Analysis on the Google-hacking Claim? In *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research* (pp. 42:1–42:1). New York, NY, USA.

Matusitz, J. (2009). A Postmodern Theory of Cyberterrorism: Game Theory. *Information Security Journal: A Global Perspective*, *18*(6), 273–281. doi:10.1080/19393550903200474.

Powell, Robert (1999), "In the Shadow of Power", Princeton University Press.

Reuveny, Rafael and Maxwell, John (1998). “Free Trade and Arms Races”, The Journal of Conflict Resolution, 42: 771–803.

Taylor, Alan D. (1995). “Mathematics and Politics: Strategy, Voting, Power and Proof”, Springer-Verlag: New York, NY.

Von Neumann, John and Morgenstern, Oskar (1944). Theory of Games and Economic Behavior, Princeton University Press: Princestone.

Von Neumann, John and Morgenstern, Oskar (1994). “Theory of Games and Economic Behavior”, John Wiley & Sons, Inc.:New York, NY.