future internet

MDPI

Review

A Survey of Game Theoretic Approaches to Modelling Decision-Making in Information Warfare Scenarios

Kathryn Merrick *, Medria Hardhienata, Kamran Shafi and Jiankun Hu

School of Engineering and Information Technology, Australian Defence Force Academy, University of New South Wales Canberra, Northcott Drive, Canberra 2600, Australia; m.hardhienata@adfa.edu.au(M.H.); k.shafi@adfa.edu.au(K.S.); j.hu@adfa.edu.au (J.H.)
* Correspondence: k.merrick@adfa.edu.au; Tel.: +61-2-6268-8023

Academic Editor: Sherali Zeadally
Received: 6 May 2016; Accepted: 1 July 2016; Published: 22 July 2016

Abstract: Our increasing dependence on information technologies and autonomous systems has escalated international concern for information- and cyber-security in the face of politically, socially and religiously motivated cyber-attacks. Information warfare tactics that interfere with the flow of information can challenge the survival of individuals and groups. It is increasingly important that both humans and machines can make decisions that ensure the trustworthiness of information, communication and autonomous systems. Subsequently, an important research direction is concerned with modelling decision-making processes. One approach to this involves modelling decision-making scenarios as games using game theory. This paper presents a survey of information warfare literature, with the purpose of identifying games that model different types of information warfare operations. Our contribution is a systematic identification and classification of information warfare games, as a basis for modelling decision-making by humans and machines in such scenarios. We also present a taxonomy of games that map to information warfare and cyber crime problems as a precursor to future research on decision-making in such scenarios. We identify and discuss open research questions including the role of behavioural game theory in modelling human decision making and the role of machine decision-making in information warfare scenarios.

Keywords: game theory; information warfare; cyber warfare; cyber security

1. Introduction

Game-theory is a mathematical language for describing strategic interactions and their likely outcomes [1]. The application of game-theoretic approaches to information- and cyber-security problems has been of recent interest to capture the nature of information warfare between an attacker (or group of attackers) and a defender [2–4]. Game theoretic techniques are utilised to perform tactical analysis of the options available in response to a cyber-threat. Various games have been developed to illustrate the different requirements for effective strategies in information warfare [2,3]. These games are analysed to establish their equilibrium points and suggest beneficial strategies for players. However, it is increasingly recognised that it is necessary to model players in greater detail, including their intent, objectives and strategies [5] and their motives [6]. This paper presents a taxonomy of games that map to information warfare and cyber crime problems, as a precursor to future research on decision-making in such scenarios.

Information warfare is not a new concept [7]. People and organisations (and even animals) have long been gathering information about their environment and transmitting information to others. However, manifestations of information warfare are changing as information and communication

technologies (ICT) play a steadily greater role in our lives. Our increasing dependence on these technologies has escalated international concern for information- and cyber-security [8,9].

A number of review papers have been written to cover game-theoretic approaches to different categories of information warfare. Table 1 presents a summary of some notable surveys. The columns represent the related areas of information warfare that are included in the current review. The rows highlight the categories of information warfare that each of the ten selected reviews touch upon. As can be seen, most review papers only cover one or two related topics of information warfare. This shows a need for a comprehensive review of game-theoretic approaches across a range of information warfare related topics. This survey aims at addressing this gap and provides a comprehensive coverage of different areas of information warfare where game-theoretic approaches have been proposed. We break these into a number of key sub-categories in Section 2.4, which also cross into the areas of cyber warfare and cyber crime, which have not been a focus in existing surveys. We extend and revise existing taxonomies of information warfare to inform a systematic review of the game theory literature in Section 4.

Table 1. A summary of existing survey papers in the domain(s) of game theory and/or information warfare.

		Information Warfare				
Year of Publication	**Reference**	**Cyber Security**	**Network Security**	**Information Security**	**Wireless Sensor Network**	**Sensor Network Security**
2008	[10]				yes	
2008	[11]			yes		
2009	[12]		yes			yes
2010	[4]	yes				
2010	[3]		yes			
2011	[13]		yes		yes	
2011	[14]				yes	
2012	[15]				yes	
2013	[16]		yes		yes	
2013	[17]		yes			
	This paper	yes	yes	yes	yes	yes

Survey Methodology

In this paper, the identification of existing literature related to game theory and information warfare topics was based on a keyword search. We began our search by entering relevant keywords to common search engines such as Google Scholar. Initially, we entered two main keywords which are most relevant to this study: “game theory” and “information warfare”. To specifically find studies that fall under a particular information warfare category, we entered “game theory" as an input to the search engine and the name of a particular information warfare category. For example “game theory” and “economic warfare”, “game theory” and “psychological warfare”, and so on. To further expand our search, we took other relevant keywords from the definition of each information warfare category. These include the types of operation and actors involved in the game. For example, we considered “game theory”, “espionage”, and “nation” as combined keywords when we searched about intelligent-based warfare and considered “game theory”, “radio jamming”, and “government” when we searched studies that fall under electronic warfare. Other subtopics such as “cyber-warfare”, “cyber-crimes”, “cyber-bullying”, and other related cyber-events were also taken into account as relevant keywords.

In this study, we relied predominantly on sources published in well-established, academic databases such as IEEE Xplore, ACM Digital library, Elsevier, and Springer [18]. As information

warfare covers diverse domains including the military, economic, politics, engineering and computer science, we also identified the literature from journals in a range of disciplines.

To ensure that only relevant and high quality publications were considered, we evaluated the source that we found according to several aspects. These aspects are the reputation of the authors (including their affiliations and the organization they work for), the citation frequencies, the academic database in which the paper/book is published, as well as the date of publication. In addition, we also consider publications which come from military documents/reports that we think are relevant to improving our understanding of these topics.

The remainder of this paper is organised as follows: Section 2 of this paper presents a survey of information warfare literature as a foundation for identifying and discussing such games. Section 3 provides a brief overview of game theory and discusses relevant concepts. Section 4 identifies games that model different types of information warfare operations. We conclude in Section 5 with a discussion of research findings, challenges, and future work in the application of game theory to analysis of information warfare scenarios.

2. Information Warfare

One of the earliest uses of the term "information warfare" in the context of computer networks was by Thomas Rona in 1976 [19]. More recently, information warfare has been defined by the United States Air Force as *"any action to deny, exploit, corrupt or destroy the enemy's information and its functions; protecting ourselves against those actions and exploiting our own military information functions"* [20]. Other authors [21,22] agree that information can be both the target of information warfare attacks and the weapon utilised to perform such attacks.

Kuehl [23] provides another military-oriented definition of information warfare as: *"Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries"*. Information operations are defined as *"Actions taken to affect adversary information and information systems while defending one's own information and information systems"*. More recent military-oriented definitions include information warfare as *"the process of protecting one's own sources of battlefield information and, at the same time, seeking to deny, degrade, corrupt, or destroy the enemy's sources of battlefield information"* [24]. This implies information warfare is a series of offensive and defensive operations. Offensive operations attack information and information systems, while defensive operations defend these targets. This perspective is consistent with the definition given by Denning [21] who views information warfare as a game played between defenders and attackers involved in a direct competition.

While the work above suggests a strong link between information warfare and the military, other sources [9,21,25–27] argue that the context of information warfare can be freed from association with its military underpinnings. The focus of information warfare is primarily on the use of information to make decisions, and on how an adversary influences, denies or disrupts the information that is required in the decision-making process [26]. These processes can occur in non-military contexts including criminal activities and impingement of individual rights.

Technology development has increased significantly compared to when most definitions of information warfare were made. Advances in technology, such as integrated computers, smart mobile phones, smart vehicles, and internet-based industry/home devices, have occurred rapidly in the recent decades. Such technologies have increased risk of becoming targets for information warfare and cyber-attacks. This emphasizes the need to extend the field of information warfare to encompass diverse fields, including in the domains of cyber warfare, cyber-crime, cyber bullying and espionage [26]. This paper thus considers information warfare in these diverse fields.

While information warfare has been studied widely in the past few decades, there is lack of an agreed definition in the literature [28]. The remainder of this section thus considers extended definitions for "information" (Section 2.1), a brief discussion on how related terms in information warfare have been defined (Section 2.2), the goals of information warfare (Section 2.3), types of

information warfare operations (Section 2.4) and the recognised domains and actors in information warfare (Section 2.5). This provides a basis for identifying and classifying information warfare games in Section 4 which is the primary contribution of this paper.

2.1. Information

There are a range of definitions of "information" concerned with its nature, storage and communication [7]. They reveal that information is data, intelligence or news about facts, subjects, people and events. Information can be stored or communicated by either people or machines. With this in mind, the next section discusses various terms in the cyber-security domain that relate to information warfare.

2.2. Information Warfare Related Terms

The term "information warfare" is often used interchangeably with other terms in the cyber security domain. We consider a number of these terms here and their relationship to information warfare: cyber-space, cyber-attack, cyber-warfare, and cyber-crime.

As with the term "information", various definitions of cyberspace have been offered by the research community [29]. One comprehensive definition of cyberspace was offered by Kuehl [29]. He argued that cyberspace includes more than just computer and digital information aspects. Kuehl concluded that cyberspace includes four important aspects: an operational space, a natural domain, information based and interconnected networks [28,29]. To reflect these aspects, Kuehl [29] defines cyberspace as:

> *"A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information communication technologies."*

The difference between information- and cyber-based assets has also been discussed, including a discussion comparing information security and cyber security [30]. Unlike information security, cyber security has also been linked to non-information based assets such as human factors. An example is the case where cyber-bullying occurs. It is argued that being bullied in cyberspace does not constitute a loss of confidentiality, integrity, or availability of information. Rather, the victim of such attacks might be the user him/herself.

Taking the definition of cyberspace [29] into account, Robinson et al. [28] offered a definition of cyber-attack, as: *"An act in cyber space that could reasonably be expected to cause harm."* Harm in the above definition was viewed in a broad context such as from the perspectives of economic, psychological and physical aspects.

To reach a general definition that can describe any related cyber situation, two major components were considered by Robinson et al. [28]: (1) the actor, which is the one launching cyber-attacks; and (2) the intent of their attack. An actor can be a state, an individual, a group of terrorists, and so on. The intent, on the other hand, relates to the purpose of the attack performed by the actor. This component plays a key role in the definition. Some examples of common intents [28] include achieving military objectives (warfare), gaining personal benefit through illegal means (crime), causing psychological distress to another individual (bullying), and influencing a nation's policies through violence and fear (terrorism [31,32]). By considering the two components, the definition extends to any cyber situation. For instance, if the actor is a nation and the intention of launching a cyber-attack is to reach a military objective, than such a situation is considered as cyber warfare. On the other hand, if the actor is an individual who launches a cyber-attack to cause shame, guilt, and depression to other individual, such a situation is likely to be considered as cyber-bullying.

Using the above definition, cyber warfare was defined as: *"The use of cyber attacks with a warfare-like intent"* [28]. This paper adopts the definition of Robinson et al. [28], as it proposes a

methodical approach that can distinguish any cyber events. However, we argue that the intent of cyber-crime may possibly go beyond what was described by Robinson et al. Rather, we adopt a broader view of cyber crime similar to Tekes [33], who defines cyber-crime as: *"any illegal cyber activity or unlawful computer network action."*

By using the above definition, we consider that cyber-crime consists of various activities in the cyberspace that can potentially cause harm and are against the law. Cyber-crime can, therefore, be seen as a broad domain which includes any cyber situations that are unlawful, such as cyber warfare, cyber-bullying, cyber-espionage, and so on. We acknowledge the use of different terms of information warfare and cyber-crimes.

In this paper, we adopt the perspective that information warfare and cyber-crime are two categories that overlap with each other as shown in Figure 1. Such categories are considered in this paper as a basis to search for and classify game theory literature. In Section 4.2 we present games that fall in both of these categories, but use information warfare as a general term. The next section thus considers the goals of information warfare.

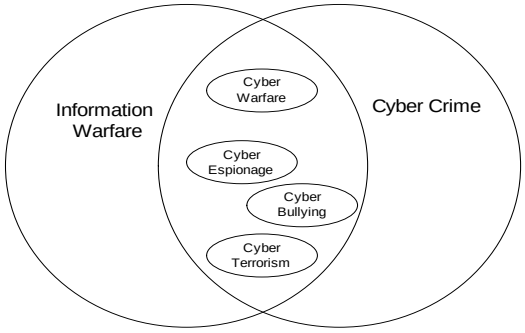

Figure 1. Information warfare as a combination of traditional information warfare and cyber-crime. This view is adopted in this paper.

2.3. Information Warfare Goals

Early work by [9] defines the goals of information warfare attacks as theft, modification or destruction of information, or the destruction of information infrastructure. These primary goals may satisfy secondary goals such as the acquisition of money, power or generation of fear. Offensive and defensive information warfare operations have six goals as follows [21]:

1. To increase the availability of information to an attacker (offensive);
2. To decrease the availability of information to a defender(offensive);
3. To decrease the integrity of information (offensive);
4. To protect information from an attacker (defensive);
5. To protect the availability of information to a defender (defensive);
6. To protect the integrity of information (defensive).

These goals are relevant across various definition of information and cyber-warfare as well as cyber-crime. Several researchers have devised broad lists of strategies for achieving the six goals listed above, including labels such as denial, corruption, deception, degradation and subversion (see [7] for a review). However, this paper focuses on the specific types of information warfare operations, rather than generic strategies. The specific type descriptions give us more detail to work with in identifying corresponding information warfare games in Section 4.

2.4. Types of Information Warfare Operations

There are numerous definitions for types of information warfare operations, including categorisations that group them according to properties such as whether they are offensive or defensive [34], the environment they occur in [25], or the actors in the operation [9]. This section

examines some of these definitions of information warfare operations, and groups them using a selection of common headings. Examples of offensive and defensive information warfare operations are also discussed. These examples provide insight into the core elements of information warfare, and give us a starting point for developing a taxonomy of information warfare games in Section 4 and Figure 2.

Schwartau [9] defines information warfare in a civilian context, describing various attacks against information systems and telecommunications networks. He focuses particularly on offensive information warfare operations. Schwartau [9] specifies three different types of information warfare attack based on the type of target that is attacked: personal, corporate and global information warfare. Schwartau's definitions focus primarily on offensive actions, but he recognises that these actions may occur in both civilian and military domains. Other authors specify more types of information warfare attacks, but focus on a particular attach domain such as the military [20,23]. Fogleman and Widnall [20] detail six types of offensive information warfare attacks for the military. A broader taxonomy [25] divides the information warfare actions by the environment in which they occur. It lists seven types of operations that can be categorised as information warfare. All describe *"conflicts that involve the protection, manipulation, degradation and denial of information"*. However, some attacks may overlap multiple categories. More recent work by Ventre [34] includes a selection of the categories introduced by other researchers, involving both offensive and defensive operations. The following subsections follow Ventre's taxonomy to some extent, with some additions and name changes to reflect other taxonomies and more recent developments in the information warfare literature.

2.4.1. Offensive Operations

Offensive information warfare operations attempt to control the information environment by paralysing, deteriorating, interrupting, destroying or attempting to deceive information and information systems [34]. The following types of offensive information warfare have been discussed in the literature.

Command and Control Warfare

Command and control warfare [25] attacks an opponent's command and communications infrastructure. It aims to degrade the opponent's responses to further military action. The destruction of command facilities disrupts military decision-making. Likewise, the destruction of communications infrastructure disrupts the flow of information between decision-makers and the troops implementing those decisions. Command and control warfare has also been categorised simply as 'physical destruction' [20] or 'physical attacks' [34]. These more general terms once again remind us that information warfare has relevance beyond the military context.

Military Deception

Military deception falsely represents the attacker's capabilities or intentions to the enemy [20]. More specifically, deception is a series of measures that manipulate, deteriorate or falsify evidence to trigger a reaction that is detrimental to the enemy's interests [34]. Deception may involve the employment of physical or electronic means to camouflage one's own force posture [24]. Examples of physical deception include the deployment of dummy aircraft on the tarmac of an air base, or broadcasting radio situation reports from "phantom" (dummy) units [24].

Psychological Warfare

Fogleman and Widnall [20] define psychological warfare as using information to affect the enemy's reasoning and thereby their behaviour. Brumley [7] and Ventre [34] define psychological warfare in a similar way as the use of information against the human mind. Classical psychological warfare techniques include air dropping propaganda leaflets and using airborne loudspeakers that broadcast demands for surrender [24].

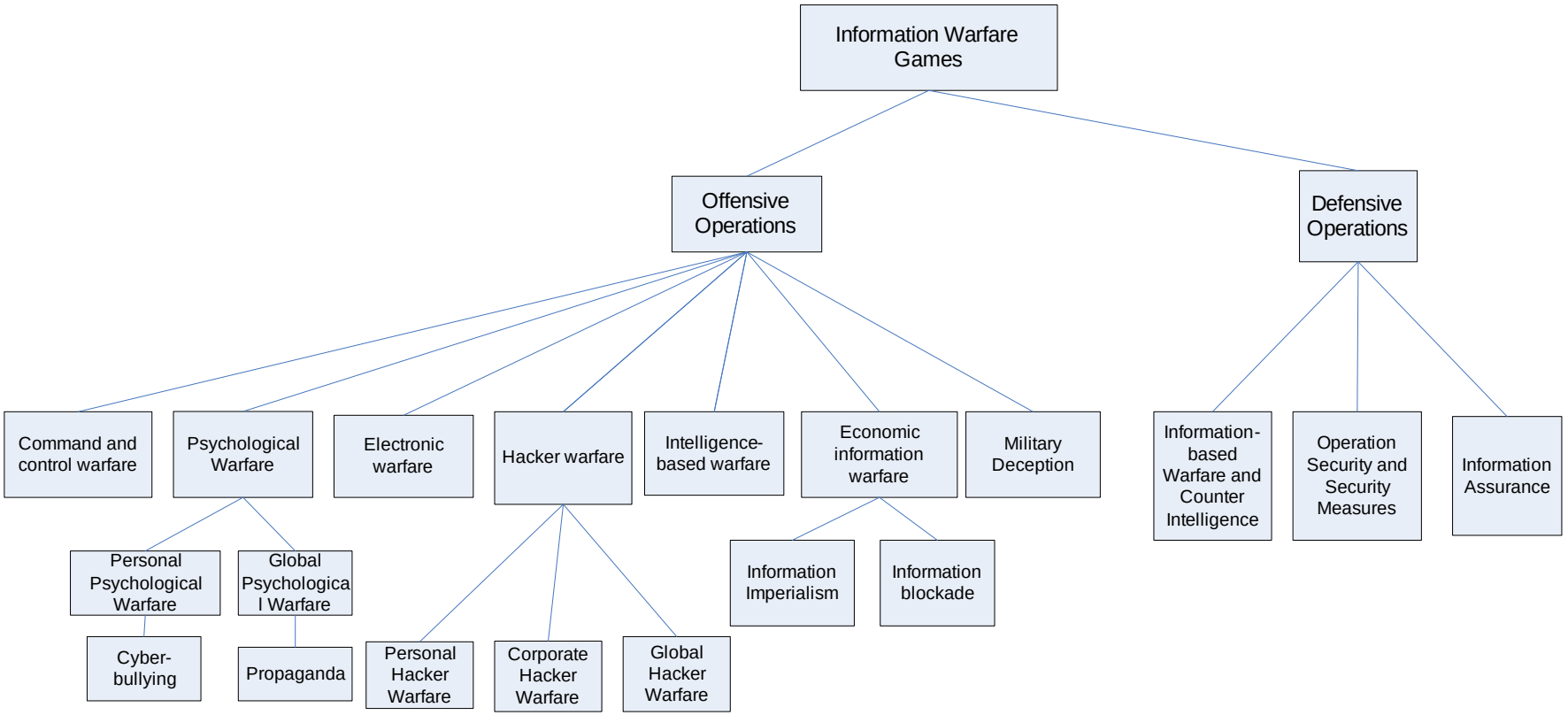

Figure 2. Framework to classify information warfare games.

Libicki [25] divides psychological warfare into four sub-categories based upon its intended target: counter-will operations, cultural conflict, counter-forces attacks and counter-commander operations. Counter-will operations and cultural conflict are aimed at civilian populations. Counter-will operations counter the opponent's national will by transmitting a deceptive message to a population. For example, messages may suggest that present and future military attacks are likely to fail. Cultural conflict targets an opponent's culture. For example, it may attempt to replace their traditions and beliefs with those of the attacker.

In contrast, counter-forces and counter-commander attacks target an opponent's military troops more specifically. Counter-forces attacks aim to convince troops that fighting is against their best interests. Counter-commander operations intend to confuse and disorientate an opponent's military commanders, detrimentally affecting their decision-making abilities.

Many aspects of psychological warfare have a long history, independent of the use of ICT. However, ICT can faciliate wider and faster application of psychological warfare techniques. Cyber-bullying is a recent example of the changing nature of psychological cyber-attacks.

Electronic Warfare

Early definitions of electronic warfare describe it as attempts to degrade the physical basis of an opponent's communications [25,35] and attempts to deny the enemy accurate information from the environment [20]. More recent work describe the goal of electronic warfare as controlling the electromagnetic spectrum [34]. Brumley [7] lists three main targets for such electronic warfare attacks: radar receivers, communication systems or communicated messages. Attack types include electronic attacks (jamming), physical assaults or decryption of sensitive messages [24].

More recently, the focus of electronic warfare has altered to include attacks on services which support physical layer activities [26]. Whilst the military still maintains separate tactical communication systems, many commercial enterprises have opted for increased integration. One example is the use of the Internet for voice communications. Integrated network systems are considered more vulnerable to attack [26]. As integration can be applied across wide area, mobile and ad hoc networks, all such networks have potential vulnerabilities.

Economic Information Warfare

Economic information warfare attempts to control the flow of information between competing nations and societies. Economic information warfare shares some of the characteristics of electronic warfare operations, but has a focus on economic rather than military targets. It also share properties with Schwartau's [9] category of global information warfare, because of its focus on national level conflict. Sub-types of economic information warfare include information blockade and information imperialism. An information blockade attempts to prevent the real-time transfer of information by methods such as jamming and destruction of equipment. Information imperialism occurs when knowledge-intensive industries become geographically concentrated, because this can disadvantage those without access to the region. Silicon Valley is an example of information imperialism according to this definition [25].

Information Attack and Hacker Warfare

Information attack is an action taken to manipulate or destroy enemy information without visibly changing the physical entity on which it resides [34]. Other similar terms include 'computer network attack' and 'hacker warfare'. This category is arguably the fastest growing in today's climate of smart devices.

Nichiporuk [24] defines information attack as involving the use of computer technology to electronically shut down, degrade, corrupt, or destroy an enemy's information systems. Viruses, logic bombs, and sniffers are three of the "information munitions" used in such attacks. Libicki [25]

describes a similar concept of 'semantic attacks', in which computer systems are given seemingly valid information that causes them to produce undetectably incorrect output.

Libicki [25] also describes a concept of hacker warfare. Hacker warfare consists of attacks against civilian computer networks and systems. The non-military target in this case differentiates hacker warfare from command and control warfare. The aims of hacker warfare include the temporary or permanent shut-down of computer systems, the introduction of errors into data, the theft of information or services, and the injection of false message traffic. Attacks on internet and social networking sites are examples of the use of hacking as an information warfare operation to disrupt communications and promote political ideologies. While such operations may not directly impact military operations, their effects on the civilian population may reduce public or political support for military operations. Attacks that lead to economic losses can also undermine a national will or a nation's capability to wage war.

Hacker warfare also includes information warfare types proposed by Schwartau [9], in particular personal and corporate information warfare. Personal information warfare targets individuals' personal details stored in electronic databases. Schwartau [9] refers particularly to data stored by third party companies and government agencies, which individuals cannot directly protect. However, with the increasing use of mobile devices and internet enabled home devices such as televisions and game consoles, there is an increased opportunity for personal information warfare attacks directly on individuals [26]. It is these kinds of attacks that have lead to the definition of new terms such as cyber-crime and cyber-bullying discussed previously.

In corporate information warfare, companies rather than individuals are targeted, typically by their competitors. Schwartau [9] describes industrial espionage, spreading disinformation, leaking confidential information and damaging a company's information systems as examples. Espionage occurs when competitive information gathering crosses the edge of legal and ethical boundaries [26]. Techniques include surveillance and social engineering, which are increasingly supported by novel technological advances. Cyber espionage can extend to terrorist groups as well as military and industrial actors [26].

Hacker warfare may also occur in competitive non-military social environments, including politics or product marketing [7]. In these cases, deception and related forms of information warfare are used to promote a group, an idea, or a product to various people, typically among members of the general public.

An emerging trend in the area of information attack is hacktivism [26,36]. This trend occurs when cyber activism crosses the boundary of legal practice. The focus of hacktivism has been multinational corporations. Hactivism targets, for example, practices in globalization and capitalism and can challenge international relations. Conway [37] suggests that there is a shrinking gap between hacktivism and cyber-terrorism.

2.4.2. Defensive Operations

Defensive information warfare operations are carried out to protect and defend friendly information and information systems [34]. The following types of defensive information warfare have been discussed in the literature.

Information Assurance

The concept of information assurance groups the measures that protect and defend information and information systems by ensuring their availability, integrity, capacity to be authenticated, confidentiality and their non repudiation [34]. Information assurance measures include restoration of information systems by incorporating protection, detection and methods of reaction.

Information-Based Warfare and Counter-Intelligence

Information-based warfare [25] involves collection and use of information when planning and implementing military actions. Techniques include reconnaissance to assess the effectiveness of previous military attacks, or to determine the priority of targets for future strikes. More recently, Williams [26] discusses information-based warfare in relation to intelligence and counter intelligence. Williams writes that it is becoming apparent that more state-based attacks on governments are occurring. She cites numerous major attacks on the US government and defence systems over in recent years, many of which are state-based or supported from China.

Operations Security and Security Measures

Information resources are protected from information warfare attacks by using defensive information warfare operations to achieve operational security [24]. Operations security is a methodology intended to keep an adversary from accessing critical information necessary to correctly evaluate the capabilities and intents of the target. Security programs and security measures are specific steps to conceal an attacker's military capabilities and intentions from the enemy [34].

2.4.3. Future Information Warfare Operations

New kinds of information warfare actions can emerge rapidly. Libicki's [25] final category of 'cyberwarfare' collected a variety of futuristic attacks to emphasise this, some of which have since come to pass. Along with new categories of cyber-crime and cyber-bullying discussed already, an example of an emerging topic in information warfare is the concept of space war [26]. Uncontrolled or malicious satellites or uncontrolled satellite debris have the potential to create chaos in the space environment. Our dependency on satellite technology heightens the threat posed in this respect. Another aspect of space war more in the domain of information warfare is that of incepted and altered satellite signalling, and misuse of anti-satellite weapons technologies.

2.5. Information Warfare Domains and Their Actors

As we have seen, some definitions of information warfare suggest that it is primarily associated the domain of the military [20,23]. However, others [9,25,26] suggest that the domain of information warfare is broader than this. In fact, with the ubiquity of computer networks, information warfare is applicable across a wide variety of domains, in particular domains that offers some competitive advantage to one actor over another [7]. This may include, but not be limited to military warfare, politics, industry or marketing to name a few. The actors in these domains include individuals, organisations and governments. We will use these three categories of actors to classify information warfare games in Section 4. First, however, we give an overview of game theory and its components to support this classification.

3. Game Theory

Denning [21] writes that information warfare requires at least two types of players. These players include an offensive player who attacks an information resource and a defensive player who protects the information resource. Such players may be associated with individuals, organisations or nations. Offensive players include insiders, hackers, criminals, corporations, governments or terrorists. The goal of offensive information warfare operations for the attacker is to increase the availability or integrity of information, while for the defender the goal is to decrease the availability or integrity of information. This has the effect of positive payoff to the attacker and negative payoff to the defender. From this viewpoint, information warfare can be modelled as a game that is played between offensive and defensive players who select strategies with different payoff. Representing information warfare in a game-theoretic manner suggests that information warfare operations can be analysed with game-theoretical methods [2,3,7].

Game theory [1] is a mathematical language for describing multi-person decision-making scenarios. The scenario is described as a game. Decision-makers are called players and their moves are called actions. Players receive payoff based on their own move and the moves of other players.

A key advantage of this is the ability to examine a large numbers of possible threat scenarios that potentially occur in the cyber space [38,39]. Another advantage of game theory is its ability to control future attacks by providing methods for suggesting probable actions with the predicted outcomes [3]. Computers can analyse combinations of parameters to consider large numbers of possible outcomes.

We also acknowledge that there are challenges associated with the application of game theoretic analysis. Hamilton et al. [38], for example, identify seven challenges in applying game theory to the domain of information warfare, including a limited database of relevant games, and the fact that the real-world 'game' may change, meaning that the set of legal moves may change. Despite these challenges, game theory offers us a well defined framework in which to analyse decision-making.

The following sections provide further details defining different types of games, players, actions and payoff.

3.1. A Game

A game is an abstract description of the strategic interaction between players. In this paper, we consider a game to be an abstract representation of an information warfare operation. A game describes the interaction among rational, mutually aware players, where the decisions by some players affect the payoffs of others. A game is described by its players, the actions taken by the players, and the resulting payoffs from each outcome. In sequential games, the game determines the order of moves. A game includes a description of the payoff to each player as a consequence of the actions they both take. A number of different sub-categories of game are possible, and games may fall into more than one category, for example:

3.1.1. Static Games

A static or simultaneous game is one in which all players make decisions without knowledge of the strategies that are being chosen by other players. This may occur because players make decisions simultaneously, or because they make decisions at different points in time, but do not get any information about previous decisions to aid their own.

3.1.2. Sequential Games

A sequential game is a game where the players make decisions in a certain predefined order, and one or more players can observe the moves of the players who preceded them.

3.1.3. Dynamic Games

When players interact by playing a game numerous times, the game is called a dynamic, repeated or iterative game. Unlike static/simultaneous games, players have at least some information about the actions chosen by others and thus may contingent their play on past moves. Evolutionary game theory [40] provides a dynamic framework for analysing repeated interaction.

3.1.4. Perfect Information Games

A perfect information game is a sequential game where each player is assumed to be aware of all the previous moves taken by all other players. In contrast, an imperfect information game is a game where at least one player is not aware of the past moves of at least one other player. According to this definition, all static games can be considered as games with imperfect information.

3.1.5. Complete Information Games

In a complete information game all factors of the game are common knowledge. Specifically, each player is aware of all other players, the timing of the game, and the set of strategies and payoffs for each player, but not necessarily the actions. This term is distinct from perfect information game, by the fact that it does not take into account the actions each player have already taken.

For comparison, incomplete information include one or more players who are unaware of the possible strategies and payoffs of one or more of the other players.

3.1.6. Bayesian Games

A Bayesian game [41] is a game in which information about the strategies and payoff for other players is incomplete and a player assigns a 'type' or 'prior' to other players at the onset of the game. Bayesian analysis is used in predicting the outcome of the game.

3.1.7. Stochastic Games

A stochastic game [42] is a dynamic game with probabilistic transitions through some states. The game begins with a start state. The players receive payoff based on the action that they choose and the current state of the game. At each state of the game, the game transitions into a new state with a probability that is based on the actions that the players choose and the current state.

3.1.8. Cooperative Games

A cooperative game is a game where players are able to make enforceable contracts. Players do not actually have to cooperate, but any cooperation that does occur is enforceable by an outside party such as a judge, a police, etc. In non-cooperative games, on the other hand, contracts must be self-enforcing. A majority of existing game-theoretic research applied to network security falls under the heading of non-cooperative games [3].

3.1.9. Zero-Sum Games

A game in which the interest/intention of each player is directly opposed is defined as a zero-sum game [43]. This definition implies that when a player win the other player has to loose. In other words, the payoff of one player is the negative of its opponent [44]. The game is referred to as "zero-sum" because when the total gains of a player are added and the total losses of its opponent are subtracted from those gains, the total sum will be zero. In contrast, in "a non-zero sum game" the aggregate of the total gains and losses between the players can be greater or less than zero.

3.2. A Player

A player is a decision-making entity in a game. Players choose which actions to take. In this paper, a player may be an individual, an organisation or a nation, depending on the information warfare operation represented by the game being played. Games may have different numbers of players. Two-player and n-player games are to common categories of games studied. In game theory, a player who is logically omniscient and wants to maximize his/her expected utility is referred to as a rational player [45].

3.3. An Action

An action is a move in the given game. In this paper, we consider that actions may represent complex behavioural sequences required to address an information warfare operation. The action itself is simply a decision to execute that particular sequence of behaviours.

3.4. Payoff

Payoff values are rewards or punishments for taking a particular action.

3.5. Strategies

A strategy is a plan of play, outlining which actions a player should take during the game. Strategies can be 'pure' if they specify a unique action to take at all times, or they can be 'mixed' if they specify a probability distribution over all possible actions at any time. A common assumption is that players would like to choose actions such that they cannot achieve greater payoff by switching to another action. When both players do this, a Nash Equilibrium occurs [46]. This kind of analysis can give us insight into the long term outcomes of information warfare scenarios modelled as games. We now present a classification of such games.

4. Games for Representing Information Warfare Operations

In this section, we examine information warfare games according to the types of operation identified in Section 2.4. We first summarises our findings of information warfare operations and relevant games found in the literature in Section 4.1. We then present a taxonomy of information warfare games and provide a discussion of information warfare games in more detail in Section 4.2.

4.1. Common Information Warfare Operations and Relevant Games

We summarise our findings of common information warfare operations and relevant games found in the literature in Table 2. The first column indicates whether an operation is offensive or defensive. The third and fourth columns summarises the actors in the operations, either individuals (I), groups including terrorists (T), corporations/organisations (C), or nations/governments (G). These actors become players in the games in Section 4.2. The fifth column maps the information operation type to six goals of information warfare (labeled 1–6, see Section 2.3 for definitions).

4.2. A Taxonomy of Information Warfare Games

This section describes in detail a number of games according to the types of information warfare operations, and list others for reference. In this paper, we focus less on defensive information warfare as a majority of game theory literature assumes the competitive situation created during an attack.

4.2.1. Command and Control Games

Table 3 summarizes several examples of command and control games found in the literature. An example of a command and control game is the terrorist game. The terrorist game involves two rational players, the terrorists (attacker(s)) and the government (defender). The interaction between the two players is modelled as a static game of complete information. In this scenario, the terrorists capture hostages and force the government to provide their requirements. If their requirements are not accepted by the government, they threaten to explode the hostages and to attack the command, control, communication and intelligence infrastructure. The government, on the other hand, asks the terrorists to surrender to be kept in jail. The players have two strategies. Using the first strategy, the player accepts the suggestion of the other player (i.e., terrorist surrender or the government provides the ransom). Using the second strategy, the player rejects the suggestion of the other player (i.e., the terrorists blow up the hostages or the government refuses to negotiate). Simulation results show that to solve such a conflicting situation, a bold strategy is needed. Such an action will force the enemy to believe that the opponent will not accept the threats.

Table 2. Summary of information warfare operations.

	Operation Type	Offensive Actors	Defensive Actors	Goal(s)	References
Offensive	Command and control warfare	I, T, G	G	2, 3	[7,25]
	Physical destruction	I, T, G	C, G	2, 3	[20]
	Physical attack	I, T, G	C, G	2, 3	[34]
	Phycological warfare	I, T	I	3	[7,20,24,25,34]
	Military deception	G	G	2,3	[20,24,34]
	Electronic warfare	I, T, G	G	1, 2, 3	[7,20,24–26,34,35]
	Economic warfare	I, T, G	G	1, 2, 3	[7,25]
	Information attack	I, T	I, C	3	[7,24,34]
	Semantic attack	I, T	I, C	2, 3	[7,25]
	Hacker warfare	I, T	I, C	1	[7,25]
	Hactivism	I, C	I, C, G	1, 2, 3	[26,36]
	Espionage	C, T	C, G	1	[7,9,26]
	Cyberterrorism	I, T	G	1, 2, 3	[37]
	Personal information warfare	I	I	1, 2, 3	[7,9]
	Corporate information warfare	I, C	C	1, 2, 3	[7,9]
	Global information warfare	T, G	G	1, 2, 3	[7,9]
	Intelligence-based information warfare	I, T, G	G	1	[25]
Defensive	Information assurance	I, C	C, G	6	[34]
	Information-based warfare	T, G	G	4, 5, 6	[7,25]
	Counter Intelligence	T, C, G	C, G	4, 5	[26,34]
	Operation security	T, G	G	4, 5	[24,34]
	Security measures	I, T, G	C, G	4, 5, 6	[34]
	Security programs	I, T	G	4, 5, 6	[34]
	Psychological counter operations	I, T	I	6	[34]
	Counter deception	I, T, G	G	4, 5	[34]
	Electronic protection	I, T, G	G	4, 5, 6	[34]

Table 3. List of Command and Control Games.

References	Information Warfare Properties			Game Theory Properties			
	Actors		Goals	Static (S)/ Dynamic (D)	Complete (M)/ Incomplete Information (IM)	Perfect(P)/ Imperfect Information (IP)	Bayesian (B)/Non-Bayesian (NB)
	Offensive	Defensive					
[2]	I, T, G	G	2, 3	S	M	IP	NB
[47]	G	G	2, 5	D (Stage)	M	IP	NB
[48]	G	G	2, 4, 5	S	IM	IP	B

Another example of a command and control game is presented by Cruz et al. [47]. This paper considers a scenario where two conflicting forces (players), namely 'blue force' and 'red forces', were involved in a military combat. The mission of the blue force is to attack the red force by damaging their weapons and infrastructure. The decision making process is made through a hierarchy of command and control. This command and control hierarchy consists of commanders who need to take a decision at each stage of the game. A non-zero sum dynamic game is used to analyze the best strategies that can be played by the two forces in such a scenario.

The paper by Brynielsson [48] focuses on threat prediction in the command and control domain. This study considers the case where friendly and hostile forces, referred to as blue and red forces, involve in a military combat mission. Within this scenario, the Red force launches an attack by sending tanks and infantry from several directions to the Blue Force's base camp. The commander battalion needs to make a decision regarding this conflicting situation. The scenario possesses several uncertainties which make it suitable to be solved using game theoretic reasoning. One example of such uncertainties is when the Blue Force needs to consider several actions by taking into account whether the tanks of the Red Force have enough fuel. To deal with such an uncertainty, a Bayesian game technique is employed.

4.2.2. Military Deception Games

Hespanha et al. [49] investigate the use of deception by rational players in non-cooperative stochastic games with partial information. In the context of information warfare, this study falls under the category of military deception games. Specifically, this work considers problems that occur in the control of military operations. It is shown that deception can be used to increase player's payoff when one of the player can manipulate the information that is available to the opponents. In the case where the degree of possible manipulation is high, however, deception becomes useless against an intelligent opponent as it can potentially ignore the information that has been manipulated.

The role of deception in game theory and information warfare has also been considered by Greenberg [50]. This study considers the case where the opponent can use deception so that the decision maker might misperceive the likelihood that a particular state was selected. The deception value is represented in terms of the payoff matrix and the misperceived likelihoods. This work considers the case of Normandy invasion in 1994 as an example case study to test the proposed approach.

In general, Zhuang and Bier [51] define deception as disclosing a signal that is different from the hidden action. They consider the specific case of homeland security where deception is considered as displaying a different level of defensive investment to the enemy than what is actually implemented. A game-theoretic approach is used to determine whether and how resource allocation should be disclosed by the first mover. Simulation results show that deception can be employed as equilibrium strategies for the defender.

Table 4. List of Military Deception Games.

References	Information Warfare Properties			Game Theory Properties			
	Actors		Goals	Static (S)/ Dynamic (D)	Complete (M)/ Incomplete Information (IM)	Perfect(P)/ Imperfect Information (IP)	Bayesian (B)/Non-Bayesian (NB)
	Offensive	Defensive					
[49]	I	I	2, 3	D (Sequential)	M	IP	NB
[50]	G	G	2, 3, 5, 6	S	M	IP	NB
[51]	C, T	C, G	1, 2, 4, 5	S	IM	IP	B
[52]	I, T	I, C	1–6	D (Sequential)	M	IP	NB

Table 5. List of Psychological Warfare Games.

References	Information Warfare Properties			Game Theory Properties			
	Actors		Goals	Static (S)/ Dynamic (D)	Complete (M)/ Incomplete Information (IM)	Perfect(P)/ Imperfect Information (IP)	Bayesian (B)/Non-Bayesian (NB)
	Offensive	Defensive					
[53]	T	G	3	S	M	IP	NB (Decision Tree)
[54]	I, T	I	1, 2, 3	D (Stochastic)	IM	IP	NB

Garg and Grosu [52] propose a game theory framework to model deception in honeynets. Honeypot in this study is defined as a host that is left unprotected to the attackers in order to test the vulnerabilities of a system. Honeynets, accordingly, is defined as a set of interconnected honeypots. An example of deception moves in this study includes the strategy to make the attacker believes that the system is a honeypot when actually it is a regular host. The equilibrium solutions of an extensive games of imperfect information are studied in this work. Simulations show that the solutions of such a game can be used to examine the strategies of the attacker and the honeynet system (defender). Other relevant literature exists which investigates deception in a game theoretic setting [55–57].

Table 4 lists game theoretic approaches that fall under military deception category.

4.2.3. Psychological Warfare Games

One example of studies that fall in this category is the work by Johns and Silverman [53]. In their study, a framework that integrates emotion and personality theory into agent decision-making is proposed. The study considers the scenario of a terrorist bombing mission. Simulation results reveal that agents which are embedded with emotion models take better decisions and show more realistic behavior during the game.

Another example of a psychological warfare game is presented by Sallhammar et al. [54]. In this work, the Nash Equilibrium of a stochastic game is employed as a mathematical tool for calculating the expected behavior of attackers. The results of their study show that when the probability of getting caught is known by the attacker, there is always a pure strategy that maximize the expected payoff received by the attacker.

Table 5 summarizes the information warfare and game theory properties of the above studies.

4.2.4. Electronic Warfare Games

The study by Wang et al. [58] is one example of electronic warfare games with a sub-category of anti-radio. This study proposes a stochastic game framework for anti-jamming defense in cognitive radio networks. In particular, a game theory approach is used to model the interaction between the secondary users and the attackers. This study takes into account the spectrum environment

which is time-varying and it also considers the case where the attacker uses an adaptive strategy. The secondary users, on the other hand, can adapt their strategy by observing the availability of the spectrum environment, the quality of the channel, as well as the actions taken by the attackers. The proposed framework in this study is able to model various defense mechanism in several layers of a cognitive radio network.

Another example of electronic warfare games under the anti-radar sub-category is presented by Bachmann et al. [59]. This study addresses the problem of jamming adaptive radar systems where the interaction between a radar and a jammer is investigated. The results of this study indicate that game theory analysis can be used to identify the condition where jamming attack can be effective in platform self-protection. It is also shown that such an analysis can be employed to identify the condition where the radar can effectively detect the attacker.

A game-theoretic approach to dealing with anti-radio jamming in sensor networks is proposed by Zhu and Jian [60]. A non-zero sum game is used to model the interaction between the sensor network and the attacker. The study proves that there is no dominant strategy for the attacker or the sensor network in this game.

Furthermore, the concept of game theory is employed by Holmgren et al. [61] to find the best strategies to protect an electric power system against antagonistic attack. A number of defense strategies to protect the system against attack scenarios are investigated in this study. One of the aims of this study is to investigate whether a dominating defense strategy exist in the considered scenario.

Law et al. [62] use a game theoretic approach to improve protection of power grids from potential threats, such as false data injection. In this study, a risk assessment process is used to measure the consequences of data injection attacks. The quantified risks are then employed as an input to a stochastic (Markov) game. The game provides a framework that can be used by the defender to select the best response strategies against the attackers.

Another work under the electronic warfare category includes the work by Cardenas et al. [63]. One of the problems considered in this work is electric theft detection. A game theory approach is employed in this work to study the interaction between the electric utility and the electricity theft. The objective of the electricity thief is to steal a predefined amount of electricity while minimizing the chance that he/she will be detected by the system. In contrast, the objective of the electricity utility is to maximize the probability of detecting an attack. A number of simulations are conducted to study the Nash Equilibrium of the game.

Table 6 summarizes examples of electronic warfare games.

Table 6. List of Electronic Warfare Games.

References	Information Warfare Properties			Game Theory Properties			
	Actors		Goals	Static (S)/ Dynamic (D)	Complete (M)/ Incomplete Information (IM)	Perfect(P)/ Imperfect Information (IP)	Bayesian (B)/Non-Bayesian (NB)
	Offensive	Defensive					
[58]	I	I	1, 2, 3	D (Stage)	M	IP	NB (Extended Markov Decision Process)
[59]	I	I	1, 2, 3	D (Sequential)	IM	P	B
[60]	I	I	3, 6	S	IM	IP	NB
[61]	I, T, G	I, G	3, 6	S	M	IP	NB
[62]	I	I	1–6	D	M	IP	NB
[63]	I, C	I, C, G	1–6	S	IM	IP	NB

Table 7. List of Economic Information Warfare Games.

References	Information Warfare Properties			Game Theory Properties			
	Actors		Goals	Static (S)/ Dynamic (D)	Complete (M)/ Incomplete Information (IM)	Perfect(P)/ Imperfect Information (IP)	Bayesian (B)/Non-Bayesian (NB)
	Offensive	Defensive					
[2]	I, T	I, C	1, 2, 3	S	M	IP	NB
[64]	I, T	I, C	1, 2, 3	S	M	IP	NB
[5]	I, T	I, C	1, 2, 3	S	IM	IP	B
[65]	I, T	I, C, G	1, 4	S	M	IP	NB
[66]	C, G	C, G	1,2, 4, 5	S	M	IP	NB
[67]	I, T	C	4, 5, 6	S	IM	IP	B
[68]	I, T	C, G	1–6	S	M	IP	NB
[69]	I, T	I, C, G	4, 5, 6	S	M	IP	NB
[70]	I, T	I, C	1–6	D	M	P	NB

4.2.5. Economic Information Warfare Games

Jormakka and Molsa [2] describe a game in which a group of attackers performs long-term information warfare that possibly results in economic losses and delay technical development. They call this the rebel game. In the rebel game, it is shown that excessive damages to a weaker party may cause rebellions. This may result in a large damage for both the dominating and weaker parties. It is therefore suggested that high costs for the weaker party should be avoided in this game. Otherwise, rebellions may emerge from the weaker party, and as a consequence, it leads to substantial costs to the dominating party.

Carin et al. [64] addresses the problem of determining the appropriate investment to protect critical infrastructure property from cyber-attack. To address this problem, they propose a new computational approach to quantitative risk assessment which they refer to as Quantitative Evaluation of Risk for Investment Efficient Strategies (Queries). In this approach, techniques from game theory was employed to construct and evaluate the attack/protect economic model.

Liu et al. [5] modelled attacker intent, objectives and strategies (AIOS) using a general incentive-based method. Techniques from game theory are adopted to infer AIOS. It is shownthat the concept of incentives is able to unify a variety of attacker intents. A number of specific case studies are used to show the feasibility of using attack strategies in real-world attack-defense scenarios.

Vatsa et al. [65] propose a novel game theory approach to model the conflicting motives between an attacker and a detection system. In particular, they focus their study on credit card fraud problem and propose a novel fraud detection using concepts derived from game theory. The proposed approach works by predicting the future move of the fraudster and conducts learning at each step of the game. This approach is new in the domain of information warfare and has shown to improve existing rule-based system.

Brander and Spencer [66] focus their work on export subsidies and international market share rivalry. They conduct an analysis based on imperfect competition to investigate why export subsidies can be attractive policies from a domestic viewpoint. They emphasized that it is beneficial for a country to capture a large share of the production of profit-earning imperfectly competitive industries. The industry in this case is represented as a simple Nash Quantity duopoly.

Cavusoglu et al. [67] provide a model to evaluate Information Technology (IT) security investment using techniques drawn from game theory. In this study, the players of such IT security investment problem are the firm and the hackers. The payoff of the firm from security investment is based on the extent of hacking it is subjected to. On the other hand, the payoff of the hacker is determined based on the likelihood she or he will be detected. A Ggme theoretic approach is used to analysis the strategic interaction among these players.

Hua and Bapna [69] study the impact of cyber-terrorism on economy. They propose a game theoretical model to find the optimal information system security investment and investigate the economic looses caused by terrorism and common hackers. Results of their simulations indicate that organizations should increase investment to protect strategic information systems from cyber terrorists.

Other work [69] investigates the impact of cyber-threats on information systems investment using game theory approach. Specifically, they propose a non-state non-cooperative static 2×2 general-sum game to capture the interaction between an insider and a target. Results of the simulation indicate that the magnitude of optimal investment needed to protect the infrastructure from insiders is higher compared to protecting the system from cyber-threats against external hackers.

Bensoussan et al. [70] study the economic aspects of botnet activity and suggest defensive strategies to deal with botnet herders. In their study, botnets are defined as a number of connected computers infected with malicious software that permit botnet herders to remotely control the infected systems without the knowledge of the owner. Botnet activities are often motivated by economic incentives, such as profit that the herders obtain from their illegal activity. To address this problem, Bensoussan et al. [70] develop a game theory approach that can be used to choose the optimal strategy to deal with botnet herders. In this study, the amount of computers that are infected evolves based on a modified susceptible-infectious-susceptible (SIS) epidemic model. Game theory allows the defender to analyse botnet business equilibrium given available defense strategies.

A summary of economic information warfare games can be found in Table 7.

4.2.6. Information Attack and Hacker Warfare Games

Game theory research in this category has been most prolific. We thus consider three sub-categories for personal, corporate, and global hacker warfare games.

Personal Hacker Warfare Games

The paper of Liu et al. [71] provides an example of a study that falls into this category. This study proposes a game theory approach to study the interaction between an attacker and a defender in wireless ad hoc networks. The game theory is modeled in both static and dynamic scenarios and the Nash equilibrium strategies of the players is investigated. In particular, this study considers the case where the defender is uncertain about the attackers's type, i.e., whether it is malicious or regular. To address this issue, a Bayesian game formulation is used to provide a framework for the defender to choose a strategy based on his belief of the attacker's type. In the static game scenario, results of the simulations show that the defender always assume fixed prior probabilities of his/her opponent's types throughout the game. The dynamic game scenario, on the other hand, permits the defender to observe the attacker actions. This allows the defender to change his/her belief according to the game history.

The use of Stackelberg games to model attacker and defender interaction has been explored [72,73]. The Stackelberg game is a two-player extensive game where a leader can select an action from a set of available options and the follower, informed with the leader selection, chooses his/her strategy accordingly. [73] uses such a game to model the interaction between the attackers and the defenders in a network intrusion game. They conduct a theoretical analysis of the game and derive expected behaviors of rational attackers.

The use of game theory to study the optimal strategies of the players in a network security scenario as also been considered [74]. In particular, this work studies the interaction between attackers and a network administrator and models the interaction as a non-cooperative non-zero-sum dynamic game with incomplete information. Compared to existing network security approaches, the proposed approach has shown to be more efficient and significantly reduces the damage of the network.

Another game theory approach to address problems in computer and communication networks has been proposed [75]. This study considers the case where the players have a lack of knowledge about the opponent's motivation. They also take into account the report of the sensor systems about imperfectness of the operations. Two possible scenarios are taken into account in this study. The first scenario considers the case where the player knows the error probabilities of the sensor system. In such a case, the proposed analysis can be used as a guideline for each player to achieve the Nash Equilibrium point. In contrast, the second scenario considers the case where the players have no knowledge of the error probabilities of the sensor system. In this case, the error probabilities in the observation on the convergence to the Nash Equilibrium point as well as the final outcome of the game are studied.

Sagduyu et al. [76] consider the problem of jamming attack in wireless network. In this study, jamming attack is modeled as a noncooperative game that is played by two types of players, transmitters and jammers. In this context, transmitters are associated with normal users who want to optimize their own performance. In contrast, jammers are associated with attackers who aims to degrade the performance of the transmitters. The focus of this work is primarily on the vulnerability of the system to Denial of Service (DoS) attacks at the Medium Access Control (MAC) layer. The use of basic tools from game theory has shown to improve the understanding the impact of DoS attacks on the performance of the system in wireless networks.

A game theory framework for attack prediction has also been proposed by Liu and Lin [77]. The interaction between the computer system (defender) and the attacker(s) in this study is modeled as a multi-stage games. The aim of the computer system is to optimize its security from cyber-attacks. On the other hand, the attacker aims to maximize his/her attacks on the security. A novel approach is proposed to predict different types of attacks. More specifically, the study provides a model to predict attacks on IDS-protected systems and a model for credit card fraud detection.

Xiaolin et al. [78] propose a novel risk assessment model for the network information system based on Markov game theory. Two players are considered in this study: treat agent (attacker) who launch the attacks and the vulnerability agent who mitigates the risks by repairing the vulnerability of the system. The Markov game method is used in this study to estimate the belief of each cyber-attack pattern and suggest the best response to counter those attacks. Simulation results show the effectiveness of the proposed method.

A number of studies reviewed by Al Skaif et al. [79] fall under the category of personal hacker warfare [80,81]. Based on evolutionary game theory, [80] propose an active defense model to protect wireless sensor nodes from attackers. This study considers the specific scenario where the attackers try to plunder resource from other nodes to extend their lifetime. The proposed defense model allows the wireless sensor nodes to dynamically adjust their defensive strategies based on different strategies of the attackers. Simulation results show that the proposed model improves the performance of the wireless sensor networks and greatly saves energy consumption.

Liu et al. [81] consider the security issues that arise for centralized coordinator nodes in wireless sensor networks. In this study, the attackers are considered to be a kind of malicious nodes which aim to disrupt the performance of the coordinator nodes by strategic jamming attack. To address this problem, a coordinator selection scheme and a stochastic game model for dynamic defense are presented. Simulation results indicate that by selecting a new coordinator node that are not attacked by malicious entity, the lifetime and reliability of the wireless sensor networks can be improved.

Table 8. List of Hacker Warfare Games.

References	Information Warfare Properties			Game Theory Properties			
	Actors		Goals	Static (S)/ Dynamic (D)	Complete (M)/ Incomplete Information (IM)	Perfect(P)/ Imperfect Information (IP)	Bayesian (B)/Non-Bayesian (NB)
	Offensive	Defensive					
Personal							
[71]	I, T	I	1, 2, 3	S, D	IM	IP	B
[72]	I, T	I, C	1, 2, 3	D (Sequential)	M	P	NB
[74]	I, T	I	1–6	D (Stage)	IM	P	NB (Game Tree)
[75]	I	I	1–6	S	IM	P, IP	NB (Binary Channels)
[76]	I	I	1–6	D (Stage)	IM	P	B
[77]	I	I	1–6	S	IM	IP	B
[78]	I	I	1, 2, 3	D	M	P	Markov
[80]	I	I	1, 2, 4, 5	D	M	IP	NB
[81]	I	I	2, 3, 5, 6	D	M	IP	NB
[82]	I	I	1–6	D	M	IP	NB
Corporate							
[83]	I, C	C	4, 5, 6	S	IM	IP	NB
[84]	I, T	I, C	1, 2, 3	S, D	M	IP	NB
[85]	I	I, C, G	4, 5, 6	D (Stochastic)	IM	IP	NB
Global							
[2] (evildoer)	I, T	I, C	1, 2, 3	S	M	IP	NB
[2] (vandal)	I, T	I, C	1, 2, 3	S	M	IP	NB

Zhang et al. [82] handle the problem of how a system of multiple nodes can be protected against stealthy attacks. The interaction between the attacker and the defender is modelled as a two player-non-zero-sum game where both players have limited resources. Specifically, an asymmetric feedback model is considered where the moves of the defender are fully observable while the moves of the attacker are stealthy. This study analyses the optimal strategies for both players and characterizes the Nash Equilibrium of the game.

Table 8 shows a summary of personal hacker warfare games mentioned above.

Corporate Hacker Warfare Games

A vast increase in the use of the internet for business purposes has exposed corporate to face greater risks for cyber-attacks. To better understand the interaction between corporate and attackers, Garcia and Horowitz [83] propose a game theoretic approach which specifically considers economic motivations for investment in internet security. In particular, this study investigate a scenario in which firms/corporates plan for long-term security investment by considering the likelihood of cyber-attacks.

A game theoretic approach to modelling decision-making in information security investment has also been considered [84]. In this study, security investments were modelled in several types of games which cover common practical security situations. In each game, players are able to choose two independent decision parameters. The first parameter is the protection level which relates to

the level of security a player selects for his/her resource. The second parameter, on the other hand, is the self-insurance level which reduces losses when successful attacks occur. The considered games were studied from a rational agent perspective and from a central player's view. The main results of the simulations indicated that the type of game that is chosen determines the difference between the impacts of central planning and the laissez-faire.

In their study, Lye and Wing [85] propose a game-theoretic method for analyzing the security of computer networks. The interaction between an attacker and the system administrator (defender) is viewed as a two-player stochastic game. This study offers an analysis of the best strategy the players can choose from a set of available options in the game. Explanation on how these strategies are realistic and how the administrator can employ the results to improve its network security are presented.

Table 8 shows a list of corporate hacker warfare games.

Global Hacker Warfare Games

Jormakka and Molsa [2] present a hacker warfare game they call the evildoer game. The evildoer game involves two players, an attacker and a victim, which are assumed to be rational. The aim of the attacker is to damage the victim networks and systems. These include harmful actions such as crashing the hosts, installing harmful software, causing loss of service, and so on. To successfully launch such attacks, the attacker needs to carry out a primary attack which can not be directly identified by the system. Each player in the evildoer game has two strategies. The fist strategy of the attacker is to attack the victim by launching many secondary attacks in parallel with the primary attack. This is done to overwhelm the victim so that the primary attack can not be detected. Such an attack may also interrupt the observe-orient-decide-act (OODA)-loop of the victim. The second strategy of the attacker is to only launch the primary attack. The victim has also two strategies to defend his/her networks from such attacks. The first strategy of the victim is to detect and to be alert on all suspicious network traffic. The second strategy of the victim is to detect and block only the most critical attack. Results of the simulations show that the dominative position of the attacker can be reduced by using mixed strategies.

Another game presented by Jormakka and Molsa [2] is the vandal game. This game consists of two types of players which are assumed to be rational. The first player is the vandal who tries to attack the communication network of the victim(s). This can be done, for example, by launching cyber-attacks such as jamming a wireless network or overloading the network of the victim. The second player is the legitimate users of the network. In this study, all users are assumed to be identical. All players in the vandal game have two strategies. The first strategy is to use the network. The second strategy, on the other hand, is to be idle. If the vandal chooses the first strategy, then it is expected that the legitimate users can not use the network as it is overloaded by the attack. Results of the simulations suggest that in the case where there is no cost for launching a Denial of Service (DoS) attack, the network should be overloaded by the attacker only part of the time. Such an action will potentially encourage the defender to continue its network service rather than stopping the network due to the attack.

Table 8 shows a list of global hacker warfare games.

4.2.7. Intelligence-Based Warfare Games

Finally a number of information warfare games that fall in a category called intelligence-based warfare [86–88]. Solan and Yariv [86] focus on games where two players decide their strategies before the beginning of a play. They take into account the case where one of the players has the ability to spy on his opponent's decision. In real world problems, such a situation can be found when an army prepares the strategies to deal with different conflicting situations in the battlefield before the war begins or when the government needs to make a decision/policy before negotiations [86].

Golen et al. [87] consider the scenario of military operations underwater. They focus on the design of a field of passive underwater sensors, to optimize the detection of an intruding adversary (e.g., an enemy submarine). Two rational players are involved in the game, a field designer (labeled as Colin) and the enemy submarine captain (labeled as Rose). The operational areas were divided into four quadrants, each with different acoustics. In this study, game theory is used to derive the probability that an enemy submarine will visit a particular quadrant. The payoff for Colin is computed by calculating the number of times he can expect to identify the enemy submarine. In contrast, the payoff for Rose is the number of times she can expect to be undetected by Colin.

Another example of game theoretic approach in intelligence-based warfare category can be found in the study by Chen et al. [88]. This study develops a data-fusion framework for asymmetric-threat detection and prediction in an urban-warfare scenario. An advanced knowledge infrastructure and stochastic game theory are used as a basic foundation to built the framework.

Some specific properties of the above games are summarized in Table 9.

Table 9. List of Intelligence-based Warfare Games.

References	Information Warfare Properties			Game Theory Properties			
	Actors		Goals	Static (S)/ Dynamic (D)	Complete (M)/ Incomplete Information (IM)	Perfect(P)/ Imperfect Information (IP)	Bayesian (B)/Non-Bayesian (NB)
	Offensive	Defensive					
[86]	I, C, G	I, C, G	1	D (Sequential)	IM	IP	B
[87]	I, G	I, G	1, 4, 5	S	M	IP	NB (Minimax Theorem)
[88]	I, T	I, C	1	D (Sequential)	M	IP	NB (Markov Approach)

4.3. Summary

In Section 4, we have reviewed existing game-theoretic approaches that model the decision making process in information warfare scenarios. We have also included a number of game-theoretic approaches in cyber-security scenarios which are relevant to this context. A diagrammatic version of our framework to classify information warfare games is given in Figure 2.

5. Research Findings, Challenges, and Opportunities

This paper has presented a survey of information warfare literature as a foundation for identifying and discussing games that can model them. Section 4 identified and classified games that model different types of information warfare operations, according to commonly identified types of information warfare. We conclude in this section with a discussion of research findings, challenges and opportunities in the application of game theory to analysis of information warfare scenarios. Specifically, we highlight the gaps in applying game-theoretic modelling to different categories of information warfare presented in Section 2; and refer to some recent advances in behavioural game theory that can be drawn upon to enrich modelling of information warfare scenarios.

5.1. Coverage of Information Warfare Categories

It is clear from the classification in Section 4 that the majority of information warfare games in the current literature falls within the hacker warfare category. This category, as mentioned earlier, consists of attacks on civilian computer networks and systems. The vast development of technology allows people to easily access and share information through these systems. As a consequence, people become more vulnerable to cyber-attacks. We identified, perhaps unsurprisingly, that majority of extant game-theoretic approaches under the information warfare category focus on these issues alone.

Subsequently, there are a number of information warfare related categories where there are either no games or only limited research has been reported.

In the three subcategories of hacker warfare, most of the games we identified fall under the category of personal hacker warfare. Compared to this category, a smaller number of studies have been found within the corporate hacker and global hacker warfare categories. One possible reason for this imbalance could be a fuzzy classification of related warfare categories. Such studies generally involve more than one manifestation of information warfare, and thus, they can be classified into various categories. For example, we found that a number of studies in corporate warfare category can also be classified under economic warfare category as they involve economic objective. It is also identified that studies that fall under global warfare may also involve aspects of command and control warfare, intelligent based warfare and/or electronic warfare. Even though many scenarios in information warfare domain involve a combination of multiple information warfare manifestations, current game theory approaches concentrate mainly on a single manifestation of information warfare. One potential research direction is thus to provide a game theory approach that can possibly be implemented for scenarios with multiple information warfare manifestations.

We also found that in some game theory literature, the actors/players of the game, e.g., whether they refer to individuals, corporate, government, and/or nation are often not clearly specified. Some of the literature in game theory related to information warfare considers players as general attacker(s) and defender(s). In the context of information warfare, however, it is critical to identify the types of entity that carried out the attacks (enemy) and the victim of the attack. This is because different actors may have different intents, behaviors, goals and priorities. Clearly specifying the types of actors and their intent in a game will be useful to correctly map the game into an appropriate information warfare category. This can ease the decision makers to find a game that matches the considered information warfare/cyber-crime scenario.

Furthermore, by specifying the types of actors of the game, there are several critical aspects that can be considered. These include whether the player may have access to critical information resource, whether they have the potential to deceive information, the amount of damage they may potentially cause, and several other characteristics. Such aspects may also affect the belief of the player(s) to choose a certain strategy in the game.

In contrast to hacker warfare category, we found that there is only a few studies conducted in other information warfare categories, particularly in the domain of psychological warfare. Psychological warfare relates to the use of information warfare against the human mind. While a number of computational models drawing upon psychological literature have recently been proposed, their applications to game theory and information warfare domain have not been widely explored. An interesting future research direction in this category includes the use of higher fidelity game players/entities (such as in the areas of motivation and risk preference modelling) to model the actors in information warfare scenarios in a more realistic manner.

We also identified that there remains a paucity of research within the category of command and control warfare. We identified that only a few studies have considered the use of game theory to address the case where the opponent directly attacks the command and control infrastructure. There thus remains a great potential to further develop game theoretic approach for such a scenario.

As discussed in the previous sections, a player in a command and control warfare scenario attacks the command and communications infrastructure of its opponent to avoid further military action. This requires the knowledge of how the opponent communicates. In such a scenario, an enemy can launch a single attack/multiple attacks either simultaneously or sequentially. For future work, such a scenario can be modelled in the form of a non-cooperative static game (when the players act simultaneously) or in a non-cooperative dynamic multi-stage game or sequential game (when it is assumed that the players alternate moves). Another aspect to consider is that the impact after an attack has been launched can be massive (e.g., an attack that completely destroy the flow of information between the decision-makers and the troops). This may results in a change of objective

from the opponent perspective after an attack has been launched. One possible alternative to deal with this problem is to take into account a new evaluation function at some stages of the game [38].

Recent advances in network technology allow information to be shared widely across the network which increases the risks for cyber-attacks not only to the targeted entity but also to other interacting entities in the system. In this context the use of shared decision making to model the cooperation/negotiation between multiple defenders against common enemies is another interesting area open for exploration. Interdependent security (IDS) games [89] are one example of games that model interdependencies between decision makers when dealing with security related investments.

5.2. Alternative Models in Game Theory

The work discussed in Section 4 predominantly uses the traditional game theory assumption that players are rational. However, a number of studies have shown that decision makers in many real situations do not adhere to these assumptions [90]. This has led to an increasing recognition that it is necessary to model players in greater detail, considering their behavioural characteristics including intent, objectives, strategies [5] and motives [6]. A few different branches have emerged in game theory literature that specifically focus on bounding the rationality assumption. One such approach that has recently gained popularity is known as behavioural game theory [91]. Recent research under behavioural game theory has developed game-theoretic frameworks that take into account the subjective rationality of individuals as a result of their intrinsic motivations, modelled as innate preferences for certain kinds of incentives (payoffs) [6]. This research has shown that individuals with different motives can misperceive the payoff matrix of a game, resulting in different play strategies and different equilibriums. Motivational psychologists suggest that motives are influential at both individual and national levels [92]. There are thus multiple levels at which the effects of motivation may influence decision making. Examining the influence of motivation on decision making in information warfare scenarios modelled using a game theoretic framework thus remains an open challenge. This may include examining the game theoretic impact of motivation on decision-making in information warfare scenarios in terms of changed game equilibriums, exploring the impact of changing cost functions on decision making by individuals or groups with different intrinsic motives and developing rules that explain differences in decision-making as a result of motivation, to suggest how individuals with different motives will respond to changing cost functions over time.

Another popular approach that allows relaxing the pure rationality assumption is the evolutionary games [40,93]. Evolutionary games are based on population dynamics and provide a convenient framework to study competitive interactions in a dynamic setting. Different versions of evolutionary games exist including spatial games [94] that allow studying the dynamics on graphs. With an exception of a few different approaches [95,96], the use of evolutionary games is rather a less explored area in the context of information warfare that deserves better attention.

Similar to rationality principle, game-theoretic approaches generally assume players as risk neutral. The risk neutrality assumption is different from the rationality assumption. The latter implies that that agents always choose the action that maximizes their expected payoffs while the former implies that the relationship between utility of agents' preferences over the choice is linear. Similar to rationality principle the observed human behaviour does not conform to risk neutrality assumption. Agent models that incorporate risk preferences in their decisions [97] are thus another important direction that can bring in higher fidelity to game-theoretic modelling of information warfare.

5.3. Trusted Autonomous Systems

Finally, as we enter an age where information systems are becoming more proactive and autonomous, there is an increasing need to design systems that can be 'trusted' [98]. If human users are to embrace proactive, autonomous information systems or robots, there is a requirement for them to first trust those systems. Trust in this context encompasses a spectrum of concepts including reliability, privacy, safety and security. For self-aware autonomous systems to participate in trusting

human-machine relationships, they must be able to model their own security and the perception of their security held by others. Modelling security interactions as games as we propose in this paper is one approach to this issue.

Acknowledgments: This research was funded by the Australian Centre for Cyber Security.

Author Contributions: K.M., K.S. and J.H. conceived and designed the project underlying this review; M.H. and K.M. performed the literature review; K.S. and J.H. contributed to its organisation and content. K.M. and M.H. wrote the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Guillermo, O. *Game Theory*; Academic Press: San Diego, CA, USA, 1995.
2. Jormakka, J.; Mölsä, J.V. Modelling information warfare as a game. *J. Inf. Warf.* **2005**, *4*, 12–25.
3. Roy, S.; Ellis, C.; Shiva, S.; Dasgupta, D.; Shandilya, V.; Wu, Q. A survey of game theory as applied to network security. In Proceedings of the IEEE 43rd Hawaii International Conference on System Sciences, Honolulu, HI, USA, 5–8 January 2010; pp. 1–10.
4. Shiva, S.; Roy, S.; Dasgupta, D. Game theory for cyber security. In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, Oak Ridge, TN, USA, 21–23 April 2010; ACM: New York, NY, USA, 2010; p. 34.
5. Liu, P.; Zang, W.; Yu, M. Incentive-based modeling and inference of attacker intent, objectives, and strategies. *ACM Trans. Inf. Syst. Secur.* **2005**, *8*, 78–118.
6. Merrick, K.E.; Shafi, K. A game theoretic framework for incentive-based models of intrinsic motivation in artificial systems. *Front. Psychol.* **2013**, *4*, doi:10.3389/fpsyg.2013.00791.
7. Brumley, L. Misperception and Its Evolutionary Value. Ph.D. Thesis, Monash University, Clayton, Australia, May 2014.
8. Cornish, P. *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks*; European Parliament Committee on Foreign Affairs: Brussels, Belgium, 2009; p. 17.
9. Schwartau, W. *Information Warfare: Chaos on the Electronic Superhighway*; Thunder's Mouth Press: New York, NY, USA, 1994.
10. Machado, R.; Tekinay, S. A survey of game-theoretic approaches in wireless sensor networks. *Comput. Netw.* **2008**, *52*, 3047–3061.
11. Cavusoglu, H.; Raghunathan, S.; Yue, W.T. Decision-theoretic and game-theoretic approaches to IT security investment. *J. Manag. Inf. Syst.* **2008**, *25*, 281–304.
12. Chen, X.; Makki, K.; Yen, K.; Pissinou, N. Sensor network security: A survey. *IEEE Commun. Surv. Tutor.* **2009**, *11*, 52–73.
13. Shen, S.; Yue, G.; Cao, Q.; Yu, F. A survey of game theory in wireless sensor networks security. *J. Netw.* **2011**, *6*, 521–532.
14. Akkarajitsakul, K.; Hossain, E.; Niyato, D.; Kim, D.I. Game theoretic approaches for multiple access in wireless networks: A survey. *IEEE Commun. Surv. Tutor.* **2011**, *13*, 372–395.
15. Shi, H.Y.; Wang, W.L.; Kwok, N.M.; Chen, S.Y. Game theory for wireless sensor networks: A survey. *Sensors* **2012**, *12*, 9055–9097.
16. Manshaei, M.H.; Zhu, Q.; Alpcan, T.; Bacşar, T.; Hubaux, J.P. Game theory meets network security and privacy. *ACM Comput. Surv. (CSUR)* **2013**, *45*, doi:10.1145/2480741.2480742.
17. Liang, X.; Xiao, Y. Game theory for network security. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 472–486.
18. Jesson, J.; Matheson, L.; Lacey, F.M. *Doing your literature review: Traditional and Systematic Techniques*; Sage: Thousand Oaks, CA, USA, 2011.
19. Berkowitz, B.; Hahn, R.W. Cybersecurity: Who's watching the store? *Issues Sci. Technol.* **2003**, *19*, 55–62.
20. Fogleman, R.R.; Widnall, S.E. *Cornerstones of Information Warfare*; Air Force: Arlington, VA, USA, 1997.
21. Denning, D.E.R. *Information Warfare and Security*; Addison-Wesley Reading: Essex, UK, 1999; Volume 4.
22. Hutchinson, W.; Warren, M. Principles of information warfare. *J. Inf. Warf.* **2001**, *1*, 1–6.
23. Kuehl, D.T. *Strategic Information Warfare: A Concept*; Number 332; Strategic and Defence Studies Centre, Australian National University: Canberra, Australia, 1999.

24. Nichiporuk, B. *US Military Opportunities: Information-Warfare Concepts of Operation*; RAND Corporation Report; RAND: Santa Monica, CA, USA, 1999; pp. 179–216.
25. Libicki, M.C. *What Is Information Warfare*? Technical Report, DTIC Document; US Government Printing Office: Washington, DC, USA, 1995.
26. Williams, P.A. Information Warfare: Time for a redefinition. In Proceedings of the 11th Australian Information Warfare & Security Conference, Perth, Western Australia, 14–17 February 2010; pp. 37–44.
27. Cronin, B.; Crawford, H. Information warfare: Its application in military and civilian contexts. *Inf. Soc.* **1999**, *15*, 257–263.
28. Robinson, M.; Jones, K.; Janicke, H. Cyber warfare: Issues and challenges. *Comput. Secur.* **2015**, *49*, 70–94.
29. Kuehl, D.T. *From Cyberspace to Cyberpower: Defining the Problem*; Cyberpower and National Security: Washington, DC, USA, 2009; pp. 26–28.
30. Von Solms, R.; Van Niekerk, J. From information security to cyber security. *Comput. Secur.* **2013**, *38*, 97–102.
31. Al Mazari, A.; Anjariny, A.; Habib, S.; Nyakwende, E. Cyber Terrorism Taxonomies: Definition, Targets, Patterns, Risk Factors, and Mitigation Strategies. *Int. J. Cyber Warf. Terror.* **2016**, *6*, 1–12.
32. Dillon, L. Cyberterrorism: Using the internet as a weapon of destruction. In *Combating Violent Extremism and Radicalization in the Digital Era*; IGI Global: Hershey, PA, USA, 2016; pp. 426–450.
33. Tekes, R.O. A Common Architecture for Cyber Offences and Assaults-(Organized Advanced Multi- Vector Persistent Attack): Cyber War Cyber Intelligence, Espionage, and Subversion Cyber Crime. Master's Thesis, University of London, London, UK, September 2011.
34. Ventre, D. *Information Warfare*; John Wiley & Sons: Hoboken, NJ, USA, 2012.
35. Frater, M.; Ryan, M. *Electronic Warfare for the Digitized Battlefield*; Artech House, Inc.: Norwood, MA, USA, 2001.
36. Hearn, K.; Mahncke, R.J.; Williams, P.A. Culture jamming: From activism to hactivism. In Proceedings of the Australian Information Warfare and Security Conference, Perth, Western Australia, 1–3 December 2009; p. 3.
37. Conway, M. *Cyberterrorism: Hype and Reality*; Potomac Books, Inc.: Sterling, VA, USA, 2007.
38. Hamilton, S.N.; Miller, W.L.; Ott, A.; Saydjari, O.S. Challenges in applying game theory to the domain of information warfare. In Proceedings of the 4th Information Survivability Workshop (ISW-2001/2002), Vancouver, BC, Canada, 18–20 March 2002.
39. Hamilton, S.N.; Miller, W.L.; Ott, A.; Saydjari, O.S. The role of game theory in information warfare. In Proceedings of the 4th Information sUrvivability Workshop (ISW-2001/2002), Vancouver, BC, Canada, 18–20 March 2002.
40. Smith, J.M. *Evolution and the Theory of Games*; Cambridge University Press: Cambridge, UK, 1982.
41. Harsanyi, J.C. Games with Incomplete Information Played by "Bayesian" Players. Part I. The Basic Model&. *Manag. Sci.* **1967–1968**, *14*, 159–182.
42. Shapley, L.S. Stochastic games. *Proc. Nat. Acad. Sci. USA* **1953**, *39*, 1095–1100.
43. Von Neumann, J.; Morgenstern, O. *Theory Of Games and Economic Behavior*; Princeton University Press: Princeton, NJ, USA, 2007.
44. Fudenberg, D.; Levine, D.K. *The Theory of Learning in Games*; MIT Press: Cambridge, MA, USA, 1998; Volume 2.
45. Jäger, G. Evolutionary game theory and typology: A case study. *Language* **2007**, *83*, 74–109.
46. Nash, J.F. Equilibrium points in n-person games. *Proc. Nat. Acad. Sci. USA* **1950**, *36*, 48–49.
47. Cruz, J.B., Jr.; Simaan, M.; Gacic, A.; Jiang, H.; Letelliier, B.; Li, M.; Liu, Y. Game-theoretic modeling and control of a military air operation. *IEEE Trans. Aerosp. Electron. Syst.* **2001**, *37*, 1393–1405.
48. Brynielsson, J. Using AI and games for decision support in command and control. *Decis. Support Syst.* **2007**, *43*, 1454–1463.
49. Hespanha, J.P.; Ateskan, Y.S.; Kizilocak, H. Deception in non-cooperative games with partial information. In Proceedings of the 2nd DARPA-JFACC Symposium on Advances in Enterprise Control, Minneapolis, MN, USA, 10–11 July 2000.
50. Greenberg, I. The role of deception in decision theory. *J. Confl. Resolut.* **1982**, *26*, 139–156.
51. Zhuang, J.; Bier, V.M. Secrecy and Deception at Equilibrium, With Applications To Anti-Terrorism Resource Allocation. *Def. Peace Econ.* **2011**, *22*, 43–61.

52. Garg, N.; Grosu, D. Deception in honeynets: A game-theoretic analysis. In Proceedings of the IEEE Information Assurance and Security Workshop, West Point, NY, USA, 20–22 June 2007; pp. 107–113.
53. Johns, M.; Silverman, B.G. *How Emotions and Personality Effect the Utility of Alternative Decisions: A Terrorist Target Selection Case Study*; Center for Human Modeling and Simulation: Pensilvania, PA, USA, 2001; p. 10.
54. Sallhammar, K.; Knapskog, S.J.; Helvik, B.E. Using stochastic game theory to compute the expected behavior of attackers. In Proceedings of the IEEE 2005 Symposium on Applications and the Internet Workshops, Trento, Italy, 31 January–4 February 2005; pp. 102–105.
55. Brown, G.; Carlyle, M.; Diehl, D.; Kline, J.; Wood, K. A two-sided optimization for theater ballistic missile defense. *Oper. Res.* **2005**, *53*, 745–763.
56. Brams, S.J. *Superpower Games: Applying Game Theory to Superpower Conflict*; Yale University Press: New Haven, CT, USA, 1985.
57. Brams, S.J.; Zagare, F.C. Deception in simple voting games. *Soc. Sci. Res.* **1977**, *6*, 257–272.
58. Wang, B.; Wu, Y.; Liu, K.; Clancy, T.C. An anti-jamming stochastic game for cognitive radio networks. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 877–889.
59. Bachmann, D.J.; Evans, R.J.; Moran, B. Game theoretic analysis of adaptive radar jamming. *IEEE Trans. Aerosp. Electron. Syst.* **2011**, *47*, 1081–1100.
60. Zhu, Y.; Jian, Y. A game-theoretic approach to anti-jamming in sensor networks. In Proceedings of the IEEE 16th International Conference on Parallel and Distributed Systems, Shanghai, China, 8–10 December 2010; pp. 617–624.
61. Holmgren, Å.J.; Jenelius, E.; Westin, J. Evaluating strategies for defending electric power networks against antagonistic attacks. *IEEE Trans. Power Syst.* **2007**, *22*, 76–84.
62. Law, Y.W.; Alpcan, T.; Palaniswami, M.; Dey, S. Security games and risk minimization for automatic generation control in smart grid. In *Decision and Game Theory for Security*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 281–295.
63. Cardenas, A.; Amin, S.; Schwartz, G.; Dong, R.; Sastry, S. A game theory model for electricity theft detection and privacy-aware control in AMI systems. In Proceedings of the IEEE 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 1–5 October 2012; pp. 1830–1837.
64. Carin, L.; Cybenko, G.; Hughes, J. Cybersecurity strategies: The queries methodology. *Computer* **2008**, *41*, 20–26.
65. Vatsa, V.; Sural, S.; Majumdar, A.K. A game-theoretic approach to credit card fraud detection. In *Information Systems Security*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 263–276.
66. Brander, J.A.; Spencer, B.J. Export subsidies and international market share rivalry. *J. Int. Econ.* **1985**, *18*, 83–100.
67. Cavusoglu, H.; Mishra, B.; Raghunathan, S. A model for evaluating IT security investments. *Commun. ACM* **2004**, *47*, 87–92.
68. Hua, J.; Bapna, S. The economic impact of cyber terrorism. *J. Strateg. Inf. Syst.* **2013**, *22*, 175–186.
69. Hua, J.; Bapna, S. Who Can We Trust?: The Economic Impact of Insider Threats. *J. Glob. Inf. Technol. Manag.* **2013**, *16*, 47–67.
70. Bensoussan, A.; Kantarcioglu, M.; Hoe, S.C. A game-theoretical approach for finding optimal strategies in a botnet defense model. In *Decision and Game Theory for Security*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 135–148.
71. Liu, Y.; Comaniciu, C.; Man, H. A Bayesian game approach for intrusion detection in wireless ad hoc networks. Proceeding from the 2006 Workshop on Game Theory for Communications and Networks, Pisa, Italy, 14 October 2006; p. 4.
72. Osborne, M.J.; Rubinstein, A. *A Course in Game Theory*; MIT Press: Cambridge, MA, USA, 1994.
73. Chen, L.; Leneutre, J. A game theoretical framework on intrusion detection in heterogeneous networks. *IEEE Trans. Inf. Forensics Secur.* **2009**, *4*, 165–178.
74. Luo, Y.; Szidarovszky, F.; Al-Nashif, Y.; Hariri, S. Game theory based network security. *J. Inf. Secur.* **2010**, *1*, 41–44.
75. Nguyen, K.C.; Alpcan, T.; Başar, T. Security games with incomplete information. In Proceedings of the IEEE International Conference on Communications, Dresden, Germany, 14–18 June 2009; pp. 1–6.
76. Sagduyu, Y.E.; Berry, R.; Ephremides, A. Jamming games in wireless networks with incomplete information. *IEEE Commun. Mag.* **2011**, *49*, 112–118.

77. Liu, P.; Li, L. *A Game Theoretic Approach to Attack Prediction*; Technical Report PSU-S2-2002-001; Penn State Cyber Security Group: Baltimore, MD, USA, 2002.
78. Xiaolin, C.; Xiaobin, T.; Yong, Z.; Hongsheng, X. A markov game theory-based risk assessment model for network information system. In Proceedings of the IEEE International Conference on Computer Science and Software Engineering, Wuhan, China, 12–14 December 2008; Volume 3, pp. 1057–1061.
79. AlSkaif, T.; Zapata, M.G.; Bellalta, B. Game theory for energy efficiency in Wireless Sensor Networks: Latest trends. *J. Netw. Comput. Appl.* **2015**, *54*, 33–61.
80. Chen, Z.; Qiao, C.; Qiu, Y.; Xu, L.; Wu, W. Dynamics stability in wireless sensor networks active defense model. *J. Comput. Syst. Sci.* **2014**, *80*, 1534–1548.
81. Liu, J.; Yue, G.; Shen, S.; Shang, H.; Li, H. A game-theoretic response strategy for coordinator attack in wireless sensor networks. *Sci. World J.* **2014**, *2014*, doi:10.1155/2014/950618.
82. Zhang, M.; Zheng, Z.; Shroff, N.B. A Game Theoretic Model for Defending Against Stealthy Attacks with Limited Resources. In *Decision and Game Theory for Security*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 93–112.
83. Garcia, A.; Horowitz, B. The potential for underinvestment in internet security: Implications for regulatory policy. *J. Regul. Econ.* **2007**, *31*, 37–55.
84. Grossklags, J.; Christin, N.; Chuang, J. Secure or insure? A game-theoretic analysis of information security games. In Proceedings of the 17th International Conference on World Wide Web, Beijing, China, 21–25 April 2008; ACM: New York, NY, USA, 2008; pp. 209–218.
85. Lye, K.w.; Wing, J.M. Game strategies in network security. *Int. J. Inf. Secur.* **2005**, *4*, 71–86.
86. Solan, E.; Yariv, L. Games with espionage. *Games Econ. Behav.* **2004**, *47*, 172–199.
87. Golen, E.F.; Shenoy, N.; Incze, B.I. Underwater sensor field design using game theory. In Proceedings of the IEEE Military Communications Conference, Orlando, FL, USA, 29–31 October 2007; pp. 1–7.
88. Chen, G.; Shen, D.; Kwan, C.; Cruz, J.B., Jr.; Kruger, M. Game theoretic approach to threat prediction and situation awareness. In Proceedings of the IEEE 9th International Conference on Information Fusion, Florence, Italy, 10–13 July 2006; pp. 1–8.
89. Kunreuther, H.; Heal, G. Interdependent Security. *J. Risk Uncertain.* **2003**, *26*, 231–249.
90. Colman, A.M. Cooperation, psychological game theory, and limitations of rationality in social interaction. *Behav. Brain Sci.* **2003**, *26*, 139–153.
91. Camerer, C. Behavioral game theory: Predicting human behavior in strategic situations. In *Advances in Behavioral Economics;* Princeton University Press: Princeton, NJ, USA, 2004; pp. 374–392.
92. Heckhausen, J.E.; Heckhausen, H.E. *Motivation And Action*; Cambridge University Press: Cambridge, UK, 2010.
93. Axelrod, R.; Hamilton, W.D. The evolution of cooperation. *Science* **1981**, *211*, 1390–1396.
94. Nowak, M.A.; May, R.M. Evolutionary games and spatial chaos. *Nature* **1992**, *359*, 826–829.
95. Kilner, R.M.; Hinde, C.A. Information warfare and parent—Offspring conflict. *Adv. Study Behav.* **2008**, *38*, 283–336.
96. Shafi, K.; Bender, A.; Zhong, W.; Abbass, H.A. Spatio-temporal dynamics of security investments in an interdependent risk environment. *Phys. A Stat. Mech. Appl.* **2012**, *391*, 5004–5017.
97. Ghoneim, A.; Shafi, K. The effect of risk perceived payoffs in iterated interdependent security games. In Proceedings of the Australian Conference on Artificial Life and Computational Intelligence 2016, Canberra, Australia, 2–5 February 2015; pp. 348–359.
98. Abbass, H.; Petraki, K.; Merrick, K.; Harvey, J.; Barlow, M. Trusted Autonomy and Cognitive Cyber Symbiosis: Open Challenges. *Cognit. Comput.* **2015**, *8*, 1–24.