Representing Botnet-enabled Cyber-attacks and Botnet-takedowns using Club Theory

Olukayode Adegboyega

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements for the degree of

Master of Applied Science

in

Technology Innovation Management

Faculty of Engineering and Design

Carleton University

Copyright © May 2015, Olukayode Adegboyega

ABSTRACT

The literature on botnet-enabled cyber-attacks and the literature on botnet takedowns have progressed independently from each other. In this research, these two literature streams are brought together. Botnet-enabled cyber-attacks and botnet takedowns are conceptualized as collective actions carried out by individuals, groups, and organizations that are linked by the Internet and club theory is used to examine the inner workings of these collective actions.

This research examines five scenarios of botnet-enabled cyber-attacks and five scenarios of botnet takedowns to develop a representation of cyber-attacks and infer capabilities of four club types: Attacker, Defender, Botnet beheader, and Botnet operator.

The representation developed identifies the dimensions of the three constructs of club theory: club membership size; size of the facility that club members share; and arrangements to operate, purchase/rent and grow the shared facility. Club capabilities were organized into five types: relationships, attack infrastructure, skills, learning, and others.

The results of applying club theory suggest that two club types, Attacker and Botnet operator have the ability to massively scale; whereas, for the other two club types, Defender and Botnet beheader, scalability is not evident. The implication is that clubs that fit the Attacker and Botnet operator types can bring significantly more technical resources to achieve their goals than the clubs that fit the Defender and Botnet beheader types. Increasingly, cyber-security researchers are recommending adaptive and autonomous responses to cyber-attacks. Defender and Botnet beheader may need to act, though under different ethical regimes, in a manner analogous to the

Attacker and Botnet operator. Perhaps, to an extent, there should be a drive towards capability convergence of the clubs.

ACKNOWLEDGEMENTS

My gratitude goes to the Most High God for His grace, mercy and faithfulness.

I am deeply grateful to my supervisor Professor Tony Bailetti for his dedication, tireless guidance and support throughout the process of preparing the thesis. You are such a wonderful mentor.

I would like to express my sincere appreciation to Dan Craigen for his support and ideas for improvement of this research study.

Finally, I would like to thank my wife Shileola and my children ‘Damilola, ‘Damilare, and Eniade for their love, understanding and continuous support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

1. INTRODUCTION

1.1 Motivation

This research conceptualizes botnet-enabled cyber-attacks and botnet takedowns as the activities of clubs that are linked by the Internet.

A cyber-attack is a malicious attempt by a group or an individual to compromise or gain unauthorized access to an institution's systems and technology (Gallagher, et al., 2014). A botnet takedown is a process used to identify and disrupt the botnet's command-and-control (C&C) infrastructure.

Three observations motivated the author to carry out this research. The first observation was that cyber-attacks and botnet takedowns are the result of collective actions[1] of individuals, groups, and organizations linked by the Internet. The second observation was that club theory is a useful perspective to examine the inner workings of collective action in private and public settings (Crosson et al., 2004; Medin et al., 2010). The third observation was that club theory has not been used to examine botnet-enabled cyber-attacks and botnet takedowns.

Extant literature on cyber-attacks and botnet takedowns has highlighted the increased emphasis on cyber-attacks and botnet takedowns as actions of individuals, groups or organizations linked by the Internet (Whitehouse, 2014). A botnet[2] provides the infrastructure for individuals, groups and organizations to share strategies and tools, and combine forces to launch coordinated attacks.

Efforts geared towards botnet takedown recently have demonstrated the potential role for public private partnerships in locating and mitigating botnets (Lerner, 2014).

1.2 Goal, research question and objectives

The goal of the research is to apply the theory of club goods to examine two collective actions: botnet-enabled cyber-attacks, and botnet takedowns. The research question is: What is the unified representation of the actions of groups organized for the purpose of carrying out or preventing cyber-attacks and botnet takedowns?

A unified representation of cyber-attacks and botnet takedowns is important because it: i) highlights higher fidelity of collective actions on the Internet; ii) enables collaboration among agents; iii) reduces the learning required to deal with cyber-attacks; and iv) identifies relationships between different layers of abstractions.

Although, the principal responsibilities of the clubs highlighted in section 3.2.3 (Table 2) suggests the existence of rivalry among the clubs represented on the Internet, however, discussion on such rivalry is intentionally left out of this thesis as it doesn't form part of the scope of this research.

The first objective of this research is to develop a representation of botnet-enabled cyber-attacks and botnet takedown initiatives in terms of the dimensions of the three constructs used in club theory to explain collective action:

i. Club membership size

ii. Size of the facility club members shared

iii. Arrangement to operate, purchase and grow the shared facility

The second objective of this research is to use the dimensions and their values identified from the scenarios to infer capabilities[3] of the clubs engaged in cyber-attacks.

1.3 Relevance

This research will be of particular interest to law enforcement agencies, security firms, critical infrastructure providers, Internet service providers, and researchers working to cost-effectively respond to botnet-enabled cyber-attacks and effectively initiate botnet takedowns.

The thesis will benefit personnel in technical, legal and management functions of heterogeneous organizations interested in improving the quality of their communications and accelerating decision making. Also, entrepreneurs who wish to launch and grown cyber security ventures can leverage on the results of this research to provide solutions to botnet and malware problems.

1.4 Contributions

This research brings together three literature streams that have advanced independently from each other: cyber-attacks, botnet takedowns, and club theory.

The first contribution that this research makes is an application of club theory to cyber-attacks. Club theory has found its application in different fields. However, this research is believed to be the first application of club theory to examine cyber-attacks.

The second contribution that this research makes is a unified representation of cyber-attacks and botnet takedowns. The representation conceptualizes four clubs on the Internet and identifies nine dimensions associated with the three constructs from club theory.

The third contribution of this research is the identification of capability types that may provide advantages to each of the four clubs.

1.5 Organization

The remainder of this thesis is organized into five chapters. Chapter 2 provides a review of the literature and the lessons learned from it. Chapter 3 describes the method used in the research. Chapters 4 and 5 provide the results of the research and a discussion of these results. Finally, Chapter 6 provides the conclusions of the research, identifies the limitations, and suggests further research.

---

[1] Collective action refers to actions undertaken by individuals or groups for a collective purpose, such as the advancement of a particular ideology or idea, or the political struggle with another group (Postmes & Brunsting, 2002).

[2] A botnet is a network of hundreds or thousands of infected computers which are remotely controlled through a command and control infrastructure (Kok & Kurz, 2011; Rajab et al., 2006). A more detailed on botnet is given in section 2.1.2.

[3] By capabilities the research meant the conditions or circumstances that may place one club in a favourable or superior position relative to the other clubs. A more detailed on capability is given in section 3.2.8.

2 LITERATURE REVIEW

Chapter 2 provides a literature review of cyber-attacks, botnet takedown and theory of club goods. This chapter is organized into five sections. Section 2.1 examines the literature on botnet-enabled cyber-attacks. Section 2.2 examines the literature on cyber-attacks carried out to takedown botnets. In section 2.3, the literature on botnet-enabled cyber-attacks and botnet takedowns as collective actions is reviewed. Section 2.4 examines the literature on club goods. Finally, Section 2.5 provides the lessons learned from the literature review.

2.1 Cyber-attacks

2.1.1 Definition of cyber-attacks

The definition of cyber-attack is a subject of debate. Cyber-attack has been defined as: i) the malicious attempt by a group or an individual to compromise or gain unauthorized access to an institution's systems and technology (Gallagher, et al., 2014); ii) a deliberate action to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information transiting such systems or networks (Owens et al., 2009); iii) an exploitation of cyberspace for the purpose of accessing unauthorized or secure information, spying, disabling of networks, and stealing both data and money (Uma & Padmavathi, 2013); iv) an effort to alter, disrupt, or destroy computer systems or networks or the information or programs on them (Waxman, 2011); v) action taken to undermine the functions of a computer network for a political or national security purpose (Hathaway et al., 2012); and vi) hostile acts using computer or related networks

or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions (US Joint Chiefs of Staff, 2010).

2.1.2 Botnet-enabled cyber-attacks

Botnets are considered one of the most prevalent and dangerous threats to connected devices on the Internet today. Over the years, botnets have evolved from being a network of few remote control computers for administrative tasks to several thousands of compromised computers with complex structure and many functions, which are quite difficult to detect, trace and take down (Lerner, 2014; Czosseck et al., 2011; APEC, 2008).

Malware is the tool used by botnet operators to conduct malicious activities on victims' computers and to provide remote control capabilities. Each computer compromised by malware that contacts a command and control (C&C) domain is a bot and the bots sharing the same malware and C&Cs are part of a botnet (Thompson, 2009; Sully & Thompson, 2010). To evade detection, the botnet operator can optionally employ a number of proxy machines, called stepping-stones. The proxy server would operate between the C&C server and the compromised computers (Khattak et al., 2014).

Extant literature on botnet and botnet-enabled cyber-attacks includes studies on botnet economics (Li et al., 2009); botnet size (Rajab et al., 2007; Rajab et al., 2006); botnet life cycle (Kok & Kurz, 2011; Khattak et al., 2014); measuring botnet effectiveness (Dagon et al., 2007);

botnet types (Czosseck et al., 2011; Naseem et al., 2010), and cost of hiring a botnet (Schmidt, 2012; Lerner, 2014).

Khattak et al. (2014) conceptualize the botnet life cycle as being comprised of five stages: i) propagation; ii) rallying mechanism; iii) C&C; iv) purpose; and v) evasion. Botnets employ propagation mechanisms such as scanning, drive-by download, infected media and social engineering to explore the vulnerabilities in computer networks to gain access to a victim's machine. Botnets employ rallying mechanisms like IP addresses and domain names to ensure that the bots are able to discover their C&C servers.

To receive or pass commands, the individual bots need to communicate with one another as well as the C&C servers. The method by which the communication among the bots and the C&C servers takes place determines the topology of the botnet. Methods identified are: i) centralized topology with few C&C servers; ii) de-centralized topology based on peer-to-peer (P2P) protocols; and iii) semi-flexible topologies realized by fluxy domain registration (Czosseck et al., 2011; Khattak et al., 2014; Riccardi et al., 2009; Ahmad & Kamal, 2013). Implementing the botnet gives botnet operators two advantages: i) operators are hard to trace because the actual attacks are launched by the bots, which are distributed both on the network and geographically and ii) the distributed network of bots permits the master to instigate large scale attacks (Lerner, 2014; Whitehouse, 2014).

Over the years, botnets have grown to become weapons used to carry out malicious activities that can cause devastating effects to individuals and organizations. Such malicious activities include

distributed denial-of-service attacks (DDoS), Simple Mail Transfer Protocol (SMTP) mail relays for spam (Spambot), ad click fraud, the theft of application serial numbers, login IDs, and financial information such as credit card numbers and bank accounts (Li et al., 2009; Riccardi et al., 2009; Khattak et al., 2014).

Botnet kits are available for sale and designed with user-friendliness in mind. The entire cyber-attack process can take only a few clicks of the mouse. Configuration is accomplished easily by adapting existing configuration files or purchasing ready-made ones (Czosseck et al., 2011).

2.1.2.1 Characteristics of cyber-attacks

The review of literature on cyber-attacks identified three dominant characteristics of cyber-attacks. First, a cyber-attack can be delivered across borders and can be initiated from any part of the world. Therefore, it is difficult to detect the source of cyber-attacks and then cost-effectively prosecute those responsible for them. By enlisting unsuspecting computers from around the world, botnets spin a web of anonymity around the attacker or attackers, making accurate attribution uniquely difficult (Hathaway et al., 2012).

Second, cyber-attacks are relatively inexpensive. The underlying technology for carrying out many types of cyber-attacks is widely available, inexpensive, and easy to obtain. An attacker can compromise computers belonging to otherwise uninvolved parties to take part in an attack activity; use automation to increase the amount of damage that can be done per person attacking, increase the speed at which the damage is done, and decrease the required knowledge and skill

level of the operator of the system; and even steal the financial assets of an adversary to use for its own ends (Owen et al., 2009).

Third, an attacker needs to find a single vulnerability while the defender must try to eliminate all vulnerabilities. Therefore it is much easier to carry out a cyber-attack than to defend from it (Hathaway et al., 2012).

2.1.2.2 Social engineering attacks

Social engineering provides an effective means to attack information systems. Social engineering is the art of getting users to compromise information systems. Instead of technical attacks on systems, social engineers target humans with access to information, manipulating them into divulging confidential information or even into carrying out their malicious attacks through influence and persuasion (Krombholz et al., 2014).

There are two dominant types of social engineering attacks: physical approaches and social approaches. In the physical approach, the attacker performs some form of physical action in order to gather information on a future victim. This can range from personal information (such as social security number, date of birth) to valid credentials for a computer system. In the social approach, the attackers rely on socio-psychological techniques to manipulate their victims. This approach has been successfully used in spear-phishing and baiting attacks. In order to increase the chances of success of such attacks, the perpetrators often try to develop a relationship with their future victims (Krombholz et al., 2014; Manske, 2000).

The risks related to social engineering to an organization can be significant because the effects of the attacks can be far-reaching. Social engineering attacks target the most vulnerable point in any information security architecture, people. Successful social engineering attacks give the attacker the means to bypass millions of dollars an organization invests in technical and nontechnical protection mechanisms and consulting. Social engineering can nullify security investment. Firewalls, secure routers, PKI, e-mail, VPN, door locks, consulting dollars, and security guards may all go down the drain (Manske, 2000).

2.2 Botnet takedown initiatives

In recent years, government and private sectors have launched aggressive enforcement actions to disrupt and disable botnets. Efforts geared towards reducing the threats of botnet have been described by the word "Behead," "Takedown," "Takeover," or "Eradication" (Dittrich, 2012; Sully & Thompson, 2010; Nadji et al., 2013; Lerner, 2014).

The techniques used to takedown botnets are as varied as the botnets themselves. Exploring the structure of a botnet is often the first step for finding starting points for possible countermeasures. An inherent property of all botnets is that they have to allow new machines, which run on untrusted platforms, to join the network (Leder et al., 2009).

Taking down a botnet entails identifying weaknesses in the botnet structure and disrupting the botnet's command-and-control (C&C) infrastructure (Nadji et al., 2013; Dittrich 2012).

A database of botnet takedown initiatives shows effort to takedown the following botnets: Bamital: 2013; Blackshades: 2014; Bredolab: 2010; Coreflood: 2011; Citadel: 2013; Cutwail: 2009; GameOver Zeus: 2014; Mariposa: 2009; Rustock: 2008; and ZeroAccess: 2013 (Whitehouse, 2014; Dittrich, 2012). Many of the botnet takedown initiatives employed the use of the court system to obtain injunctions to initiate a takedown. While many takedowns initiatives have been successful, some have not.

Czosseck et al. (2011) describe two approaches to take down a botnet: classical countermeasures and proactive countermeasures.

Classical countermeasures

In classical countermeasures, a central weak point in the botnet infrastructure that can be manipulated, disrupted or blocked is spotted. This includes taking down the C&C servers, and deregistration of DNS domains. Effective countermeasures require the identification of the C&C server or the location of the DNS domains, and the cooperation of the DNS registrars as well as the provider hosting the C&C server (Leder et al., 2009; Czosseck et al., 2011). A challenge to the classical countermeasure approach is found in the newer botnets which are not solely relying on a centralized structure anymore. Instead they use peer-to-peer (P2P) functionality or multi-proxy structures to hide their central origin identification of C&C server or the location of the DNS domains (Leder et al., 2009).

Proactive countermeasures

Proactive countermeasures approach includes response DDoS, hack back, infiltration or manipulation from within, and Border Gateway Protocol black-holing (Czosseck et al., 2011).

In response DDoS process, the locations of the C&C endpoints are known and it is possible to launch a counter-DDoS attack to disable these endpoints. However, this process is only possible if there is a single or limit number of C&C servers and would not work in a botnet relying on P2P infrastructure (Czosseck et al., 2011).

Hack-Back process involves identifying the existence of a flaw in the C&C infrastructure which can be exploited, penetrating the C&C server, and taking down the botnet from within (Czosseck et al., 2011).

Botnet infiltration is one of the ways to learn several aspects of a botnet's activity by joining the command and control channel with the aim of manipulating or disabling the botnet from within. Botnet infiltration provides valuable information that can be used for in-depth analysis of several facets of botnets, including inferring their membership by directly counting the bots observed on individual command and control channels (Rajab et al., 2007; Czosseck et al., 2011).

In BGP blackholing, botnet-related traffic is redirected in a process called "sinkholing". The redirected traffic can be analyzed further to gather more information about infected machines. (Whitehouse, 2014; Dittrich, 2012). Sinkholes record malicious traffic, analyze it and afterwards drop it such that it cannot reach the original target it is meant for (Leder et al., 1009). However,

this process is limited in a botnet where there is existence of backup channels for C&C processes (Czosseck et al., 2011).

2.3 Cyber-attacks and botnet takedowns as collective actions

Collective action refers to actions undertaken by individuals or groups for a collective purpose, such as the advancement of a particular ideology or idea, or the political struggle with another group (Postmes & Brunsting, 2002).

While some cyber-attacks are committed by individuals acting alone, a significant amount are accomplished by groups and organizations that vary significantly in terms of their structures and goals, the criminal activities in which they engage, and their organizational life courses. Activities of groups like "Wonderland", "Anonymous", "Drink or Die", "The Ukranian ZeuS", "Dark Market", "Operation Olympic Games", "Ghost Net" and "PLA Unit 61398" have highlighted the collective actions of groups and organizations linked on the Internet (Grabosky, 2014).

The literature on defense against botnet-enabled cyber-attacks highlights the importance of leveraging the diverse skill sets and legal mechanisms available to corporate entities and law enforcement in the form of public-private partnership.

The North Atlantic Treaty Organization (NATO) new cyber defense policy considers cyber-attacks that threaten any member of the alliance as an attack on all which may provoke collective defense from the alliance's 28 members (Cheng, 2014).

In 2009, a collective action from Defence Intelligence, Panda Security, Neustar, Directi, Georgia Tech Information Security Center and some security researchers to form "Mariposa Working Group" led to the takedown of the Mariposa botnet (Sully & Thompson, 2010). Also, in 2013, Symantec in conjunction with Microsoft obtained a court injunction to dismantle the ZeroAccess botnet. In 2014, a group of more than 30 international organizations comprised of law enforcement, the security industry, academia, researchers, and ISPs all cooperated to identify the criminal element and technical infrastructure, develop tools, and craft messaging for users in order to collectively and aggressively disrupt the GameOver Zeus botnet (Whitehouse, 2014).

2.4 Club goods

2.4.1 Club

Club theory researchers have offered various definitions for 'club'. These definitions have been offered in line with the scope of the authors and the justifications for club formation such as taste for association, and cost reduction derived from team production. A club has been defined as a group of consumers sharing a common facility, where each consumer's willingness to pay for admission depends on the facility size, the number of other users, and the characteristics of other users (Glazer et al., 1997); a group of persons who share in the consumption of a good which is not purely private, nor wholly divisible among persons (Pauly, 1970); a consumption ownership-membership arrangement' justified for its members by the economies of sharing production costs

of a desirable good (Buchanan, 1965); and a voluntary group of individuals who derive mutual benefit from sharing one or more of the following: production costs, the members' characteristics, or a good characterized by excludable benefits (Cornes and Sandler, 1996).

The various definitions indicate that a club is a sharing group.

2.4.2 Club goods

A club good has two major characteristics: i) partially-rivalrous and ii) excludability.

A club good has been defined as a good produced and consumed by a group of individuals, whose consumption unit is greater than one but less than infinity (Pauly, 1970); goods that are partially rivalrous and excludable (Sandler and Tschirhart, 1980); resources from which outsiders can be excluded, for which "the optimal sharing group is more than one person or family but smaller than an infinitely large number" (Strahilevitz, 2006); and goods whose benefits and costs of provision are shared between members of a given sharing arrangement or association (Buchanan, 1965).

A good is partially rivalrous in consumption when one person‘s consumption of a unit of the good detracts, to some extent, the consumption opportunities of another person (Sandler and Tschirhart, 1980).

Examples of club goods include hospitals, health clubs, trauma clinics, libraries, universities, movie theaters, telephone systems, and public transport (Sandler and Tschirhart, 1997).

2.4.3 Theory of club goods

The theory of club goods is concerned with how groups (clubs) form to provide themselves with goods that are available to their membership, but from which others (non-members) can be excluded. In short, the theory of clubs accommodates the fact that some goods can be simultaneously available to a defined and finite population and subject to explicit exclusion (Crosson et al., 2004).

Based on Buchanan's (1965) model on club goods, the theory of club goods dwells on three assumptions: i) optimal size of products, ii) optimal membership size, and iii) sharing arrangements.

Size is a central characteristic of organizations which is typically measured by the number of employees, members, or total revenues. The optimal size of a group is the size at which members derive benefits from the consumption of the shared resource. According to Buchanan (1965), for a given size of the facility, there exists some optimal size of the club. Sandler and Tschirhart (1980) explain that the optimal size of a product depends positively on its provision level. The greater the value of provision level, the greater the size or number of goods available for consumption.

Sandler and Tschirhart (1997) define the optimal membership size as a membership condition, which dictates that new members may be added to the club until the net benefit from membership is equal to the additional congestion costs associated with expanding the club's size.

According to Pauly (1970), the total net benefit depends only on the absolute number of members of the club. This makes the characteristics of various clubs depend only on their sizes, and not on the characteristics of their members. The optimal club is the club for which the net benefit per member, or average benefit, is at the maximum. The payoff to any club member then depends not only on the number of members in the club, but also on the composition, over groups, of the membership.

Sandler and Tschirhart (1997) highlight that for every sharing group; there is a utilization condition, which ensures that the shared resource is used efficiently. The consumption-sharing arrangement of a sharing group assumes equal sharing of costs and benefits when deriving the utility function for the individual consuming club goods. This means that the provisional decisions of the good are based on the contribution of the club members as members who contribute more enjoy larger share of the club goods (Buchanan, 1965). For the advantage of every member, it is expected that the sharing gain to every member be greater than or equal to the congestion losses.

Sharing gains include: reduction in the learning required to deal with a problem, holistic assessment of a problem, and effective response to, and remediation of a problem. However, sharing poses a disadvantage of loss of privacy to all the members of the sharing group (Whitehouse, 2014).

The sharing arrangements may or may not call for equal consumption on the part of each member, and the peculiar manner of sharing will clearly affect the ways in which the variable enters the utility function (Buchanan, 1965).

2.4.4 Applications of club theory

Non-Internet applications

Club theory has been applied in different fields. In the field of economics of transportation, club theory has been applied to study the congestion function on the highway, highway pricing, provision, and financing (Glazer et al., 1997; Bergias & Pines, 1981). In the analysis of grids, it has been applied to determine optimum number of users and amount of each resource by regarding grid services and resources as club goods (Shi et al., 2006). In the analysis of telephone systems, club theory has been applied to examine the cost-benefit effect enjoyed by both telephone subscribers and non-subscribers (Artle & Averous, 1973).

Also, club theory has found its application in variety of public settings. Club theory has been applied to examine the problem of a simultaneous deepening and enlargement due to different national policy objectives, economic structures and potentials, financial constraints, and societal preferences and to provide an economical approach to geographical indications in the European Union (Ahrens et al., 2005; Thiedig & Sylvander 2000).

Club theory has been used to analyse the rationale behind governmental support for international organizations (Medin et al., 2010). In the field of economics of religion it has been used to study the optimal size of a religious congregation (Zaleski and Zech, 1995).

Internet application

Extant literature on club theory has mostly focused on its non-Internet applications. However, literature on Internet applications of club theory includes the application of club theory to examine Interest-based self-organizing peer-to-peer networks (Asvanund et al., 2004). Others includes the works of Raymond (2013) that suggested that Internet can be considered as set of "nested clubs", and Hofmokl (2010) who suggested that Internet goods like broadband Internet access, proprietary software, and closed databases can be categorized as club goods because they are non-rivalrous in consumption and excludable.

2.5 Lesson learned

Ten lessons were learned from the literature review. First, club theory has been applied as a solution for exploring the inner workings of collective action (Crosson et al., 2004; Medin et al., 2010).

Second, justification for the partitioning of heterogeneous population into set of clubs includes taste for association and cost reduction as an outcome of team production.

Third, in the context of cyber-security, representations of at least four clubs linked by the Internet can be identified. These clubs are: i) club that uses botnets to carry out malicious activities (Li et al., 2009; Riccardi et al., 2009); ii) club that defends against botnet-enabled cyber-attacks (Khattak et al., 2014); iii) club that carries out botnet takedown initiatives (Whitehouse, 2014; Dittrich, 2012; Sully & Thompson, 2010); and iv) club that defends against botnet takedowns (Sully & Thompson, 2010).

Fourth, originally a botnet was designed to accomplish positive tasks (e.g., chatting) and some botnets continue to serve mankind well. For example, SETI@home is the website of a scientific experiment that uses Internet-connected computers in the Search for Extraterrestrial Intelligence (SETI). Unfortunately, some botnets evolved to become highly efficient and controllable cyber-attack platforms, which are frequently used by hackers (APEC, 2008).

Fifth, a botnet provides its operators at least two advantages: i) the operator is hard to trace because the actual attacks are launched by the bots, which are distributed both on the network and geographically and ii) the distributed network of bots permits the master to instigate large scale attacks (Lerner, 2014).

Sixth, those who use botnets to cause harm have increased in number and sophistication. Botnet users have evolved from being a group of disenfranchised elite hackers to strategic actors comprised of governments and criminal organizations (Dagon et al., 2007; Whitehouse, 2014; Lerner, 2014).

Seventh, the economic benefits offered by botnets have positioned botnets as a profitable industry for botnet owners and individuals who use the botnets for subversive or illegal purposes. In addition to the increased funding, botnet masters also benefit from being more agile than those trying to impede their work (Lerner, 2014).

Eighth, botnet rental has grown in the past couple of years, making repetitive attacks over short periods more effective and less expensive (NSFOCUS, 2013).

Ninth, the number of public-private partnership initiatives to reduce the threat of botnets has increased significantly recently. The intent of these initiatives is to dismantle botnets used to leverage cyber-attacks and arrest the perpetrators (Lerner, 2014).

Tenth, not all the botnet takedown initiatives are successful. This could be due to insufficient knowledge of the botnet, insufficient planning, or (more likely) because not all attacker-controlled assets were eradicated during a previous attempt to behead the botnet (Dittrich, 2012).

3 RESEARCH METHOD

This chapter describes the method used to carry out the research. Chapter 3 is organized into three sections. Section 3.1 describes the objectives of the research and the approach used. In section 3.2, the research method used to carry out the research is described. Section 3.3 provides a summary of the chapter.

3.1 Objectives and approach

3.1.1 Research question and objectives

The research question is: What is the unified representation of the actions of groups organized for the purpose of carrying out or preventing cyber-attacks and botnet takedowns?

The first objective of this research is to develop a representation of botnet-enabled cyber-attacks and botnet takedown initiatives in terms of the dimensions of the three constructs used in club theory to explain collective action:

i. Club membership size
ii. Size of the facility club members shared
iii. Arrangement to operate, purchase and grow the shared facility

The second objective of this research is to use the dimensions and their values identified from the scenarios to infer capabilities of the clubs engaged in cyber-attacks.

3.1.2 Approach

This research uses the inductive reasoning approach because the study of cyber-attacks and botnet takedowns is at an early stage and a dominant theoretical perspective does not exist.

The inductive reasoning approach was believed to be most suitable to achieve the objective of this research. The inductive reasoning approach is a systematic procedure for analysing qualitative data where the analysis is guided by specific objectives (Thomas, 2006). The inductive reasoning approach of theory building has been found to allow the researcher to use observation, categorization, and association to provide constructs, frameworks, and models (Christensen, 2006).

The goals of the inductive reasoning approach are to: i) condense extensive and varied raw text data into a brief, summary format; ii) establish clear links between the research objectives and the summary findings derived from the raw data and ensure these links are both transparent and defensible; and iii) develop model or theory about the underlying structure of experiences or processes which are evident in the text (Thomas, 2006).

The research uses publicly available information on 10 scenarios developed using information collected from the Internet. Qualitative content analysis using the interpretative approach was used to examine data used to develop the scenarios.

Content analysis is defined as a research method for the subjective interpretation of the content of text data through the systematic identification of themes or patterns. Qualitative content

analysis is one of numerous research methods used to analyze text data. Research using qualitative content analysis focuses on making replicable and valid inferences from data to their context, with the purpose of providing knowledge, new insights, a unified representation of facts and a practical guide to action. The aim is to attain a condensed and broad description of the phenomenon, and the outcome of the analysis is concepts or categories describing the phenomenon (Hsieh & Shannon, 2005; Elo & Kyngäs, 2008; Krippendorff, 2012).

Qualitative content analysis is comprised of three phases: preparation, organizing, and reporting (Elo & Kyngäs, 2008).

The preparation phase starts with selecting the unit of analysis for the research which can be a word, theme, letter, or sentence and it depends on the research question (Elo & Kyngäs, 2008).

The organizing phase includes open coding, categorization, and abstraction. In open coding, notes and headings are written in the text while reading it. In categorization, data are being classified as 'belonging' to a particular group and this implies a comparison between these data and other observations that do not belong to the same category. The purpose of creating categories is to provide a means of describing the phenomenon, to increase understanding and to generate knowledge. When formulating categories by inductive content analysis, the researcher comes to a decision, through interpretation, as to which things to put in the same category (Dey 1993; Elo & Kyngäs, 2008). In abstraction, a general description of the research topic through generating categories is formulated (Elo & Kyngäs, 2008).

The organizing phase brings the qualitative content analysis approach to the overall purpose of the research which is usually to build up a model, conceptual system, conceptual map or categories (Elo & Kyngäs, 2008).

3.2 Research method

Table 1 identifies the eight steps used to carry out the research.

Table 1. Steps used to carry out the research

Step	Dominant activities	Output
1	Select a sample comprised of 10 scenarios; 5 for botnet-enabled cyber-attacks and 5 for botnet-takedowns	List of 10 scenarios
2	Collect information on the Internet for each of the 10 scenarios in sample	For each scenario, a list of links to sources of information deemed relevant
3	Produce spreadsheets with the information required to identify the	3 spreadsheets, one for each construct

	conformity to the 3 constructs from club theory	
4	Produce a set of dimensions by using interpretative approach of content analysis in step 3	Set of dimensions
5	Adjust set of dimensions produced in step 4 to eliminate ambiguities and inconsistencies, and identify the ones essential to a unified representation of cyber-attacks and botnet takedowns	Final set of dimensions
6	Use final set of dimensions to represent the results of content analysis	A representation of results of content analysis
7	Identify values for dimensions and make comparison among the 4 conceptualized clubs	Values for dimensions and set of comparisons
8	Deduce the dominant capabilities (i.e., conditions and circumstances) that may	Set of club capabilities

	place one club in a favourable or superior position relative to the other clubs	

3.2.1 List of 10 scenarios

Ten scenarios that contain information relevant to the goal of this research were selected. At the request of the supervisor of this thesis, a security expert validated the list of the 10 cyber-attacks that were examined in this research. The security expert has 25 years of experience, most of which was spent protecting the critical infrastructure of the Federal Government of Canada.

The supervisor requested that the security expert provide a sample that met the following criteria:

i. Information about the scenario in sample published on the internet by media and security firms deemed to be reliable from January 1st, 2009 to December 31, 2014
ii. Information about the scenario in sample is relevant to the goal and objective of the research.

The following sources of information were deemed to provide information that was reliable:

- News organizations such as New York Times, CNN, BBC and New York Times which are reputable news media
- Articles, books or research papers examined and reviewed by academics

- Security reports published from well-established security companies such as Kaspersky, Symantec and Hewlett-Packard
- Well-established magazine outlets such as Times, Forbes, Foreign Policy is considered to be reliable
- Government documents such as those published by Defence Intelligence.

3.2.2 List of links to sources of information deemed relevant to each of the 10 scenarios

The author of this research used the Goggle search utility to find information on the 10 scenarios in the sample. Key words and phrases such as "cyber-attack," "botnet," "behead botnet," "takedown," "collective action," and the names of the botnets, organizations that were attacked, or names for which the attacks were known into the Google search utility.

For each scenario, a list of links to the information used to develop the scenario was assembled.

3.2.3 Three spreadsheets, one for each construct

The author produced three spreadsheets, one for each construct. Each spreadsheet captured the potential dimensions and values collected for the 10 scenarios in the sample. Each scenario had two clubs. Data was also organized by club.

Based on the lessons learned from reviewing the literature, four clubs were conceptualized: Club 1 Attacker, Club 2 Defender, Club 3 Botnet beheader and Club 4 Botnet operator.

Table 2 differentiates the four clubs. Club 1 Attacker and Club 2 Defender were rivals in the five scenarios in which botnets were used to enable cyber-attacks. Club 3 Botnet beheader and Club 4 Botnet operator were rivals in the five scenarios in which botnets were being taken down.

Table 2 makes it clear that Club 1 Attacker and Club 3 Botnet beheader act to impose non-owners' rights and that Club 2 Defender and Club 4 Botnet operator act to enforce owners' rights. Moreover, an organization such as Microsoft or a state such as China can be members of each of the four clubs.

Table 2. Clubs' principal responsibilities

Initiatives	**Club**	**Responsibilities**	
		Enforcing owners' rights	**Imposing non-owners' rights**
Botnet-enabled cyber-attacks	Club 1 Attacker		✓
	Club 2 Defender	✓	
Botnet takedowns	Club 3 Botnet beheader		✓

	Club 4 Botnet operator	✓	

In the botnet-enabled cyber-attacks initiative, Club 1 Attacker aims at imposing the rights that were not intended by their owners on systems, assets, data and capabilities while Club 2 Defender aims at enforcing the rights that were intended by their owners on systems, assets, data and capabilities. In the botnet takedown initiatives, Club 3 Botnet beheader aims at imposing the rights that were not intended by their owners on systems, assets, data and capabilities while Club 4 Botnet operator aims at enforcing the rights that were intended by their owners on systems, assets, data and capabilities.

3.2.4 Set of dimensions

Using interpretative approach of qualitative content analysis of the ten scenarios included in the sample, a set of dimensions to measure the three constructs of club theory was identified.

3.2.5 Final set of dimensions

The supervisor of the research in conjunction with the security expert validated that the final set of dimensions of the three constructs represented the ten scenarios in the sample.

3.2.6 Representation of results of content analysis

The research presents a representation of results of the content analysis that captures the four clubs, the 3 constructs from club theory and the identified dimensions for measuring the constructs and the values observed in each scenario.

3.2.7 Values for dimensions and set of comparisons

The research uses the information captured in the spreadsheets in section 3.2.3 to determine the values for the dimensions and makes comparison of the four clubs.

3.2.8 Club capabilities

Bhatt and Grover (2005) argued that by identifying specific types of capabilities we can contribute to a better understanding of the sources of IT-based competitive advantage. The same argument is made in this research: by identifying the capabilities of each of the four clubs we can derive a better understanding of the sources of competitive advantages of each club.

Using the dimensions and the values for the dimensions the researcher inferred the capabilities of each of the four clubs. By capability the research meant the conditions or circumstances that may place one club in a favourable or superior position relative to the other clubs.

Capabilities identified were organized using five capability types: learning, attack infrastructure, relationships, expertise, and other. The first four capability types used in this research follow those tested empirically by Bhatt and Grover (2005).

The fifth capability type, other, was a type designed to catch-all that did not fit the four capabilities identified by Bhatt and Grover (2005).

For the purpose of this research, the five capability types were defined as follows:

Learning capability: Conditions and circumstances a club uses to accumulate, share, and apply knowledge.

Expertise capability in X: Conditions and circumstance a club uses to understand X.

Relationship capability: Conditions and circumstances a club uses to connect members and objects.

Attack infrastructure capability: Conditions and circumstances a club uses to grow the basic physical infrastructure required to execute cyber attacks

Other: Conditions and circumstances other than those related to learning, experience, relationship, and attack infrastructure capabilities.

3.3 Summary

Chapter 3 provides the research method that was used to attain the two objectives: i) provide a unified representation of botnet-enabled cyber-attacks and botnet takedowns and ii) infer capabilities of four clubs.

The research uses the interpretative approach of content analysis to examine information published in the literature, and publicly available information on ten scenarios to: i) identify dimensions that can be used to measure the three constructs from club theory and provide examples of the values for each dimension; and ii) deduce or conclude the capabilities of each of the four clubs from the evidence provided by the data collected for the 10 scenarios and reasoning.

4 RESULTS

Chapter 4 provides the results of the research. The chapter is organized into six sections. Section 4.1 identifies the sample. In section 4.2, the results of the analysis on the content collected for the ten scenarios are presented. Section 4.3 provides a representation of the results of content analysis. Section 4.4 compares the four clubs: Club 1 Attacker; Club 2 Defender; Club 3 Botnet beheader; and Club 4 Botnet operator. The capabilities of each of the four clubs that were inferred by the researcher are presented in section 4.5. Finally, section 4.6 provides the summary of chapter 4.

4.1 Scenarios in the sample

Table 3 identifies the scenarios include in the sample and a short answer to the question: What is unique about the scenario?

Table 3. Scenarios in the sample

	Scenario	**What is unique about the scenario?**
1	Attack on US banks	• Largest volume of DDoS attack on financial institutions. Throughput of attack was estimated to be 100+ gigabytes

		per second and resulted into delay of several online bank transactions
2	Attack on Spamhaus	• Largest DDoS attack in history. Throughput of the attack was estimated to peak at 300 gigabits/second • Millions of Internet users were delayed
3	Attack on MasterCard	• MasterCard lost millions of pounds as a result of the online financial service disruption
4	Attack on Target	• Data of 110 million customers stolen as a result of the attack
5	Attack on NY Times	• Largest espionage attack on one media company
6	Mariposa botnet takedown	• Botnet is comprised of 15.5 million bots • Botnet was rented to third parties
7	BredoLab botnet takedown	• Botnet is comprised of 30 million bots • Lease parts of botnets to enable fraudulent activities of others

8	Citadel botnet takedown	• Botnet is comprised of about 11 million bots and estimated to have logged keystrokes of over five million users in ninety different countries, leading to more than $500 million in losses
9	Blackshades botnet takedown	• Botnet is composed of 500+ thousand computers in 100 countries • Botnet was reported to have generated over $350,000 in sales
10	Gameover Zeus botnet takedown	• Botnet was built on a decentralized C&C infrastructure which make it difficult to detect and dismantle • Botnet was responsible for theft of millions of dollars from businesses and consumers around world

Note: Appendix A provides the links to the webpages where information for each scenario was extracted.

4.2 Results of content analysis

This section provides the results of the qualitative content analysis. This analysis used the interpretative approach of information collected from the Internet and reproduces it in written text for analysis. A subjective interpretation of the content of text data of the ten scenarios was performed for the purpose of identifying the dimensions of the three constructs of club theory and collecting values for each dimension. The researcher's interpretation of the results was based on the three constructs of club theory (i.e., membership size, facility size, and sharing arrangements) and the conceptualization of the four clubs provided in Chapter 3.

The results of the content analysis suggest that nine dimensions can be used to measure the three constructs. Of the nine dimensions, five had data values for all four club types. Table 4 identifies the nine dimensions. The "Minimum number" dimension is divided into two: Individuals and Organizations. Four diversity types were identified: Role diversity, Organization diversity, Sector diversity, and Country diversity.

Table 4 also shows that the researcher observed data values for five dimensions for the four clubs. These dimensions were: i) number of compromised or end user devices; ii) number of downloaded malware or antimalware; iii) arrangement to rent and/or purchase facility and customised services; iv) arrangement to grow facility; and v) arrangement to take order from authority.

Table 4. Dimensions by club where data value was observed

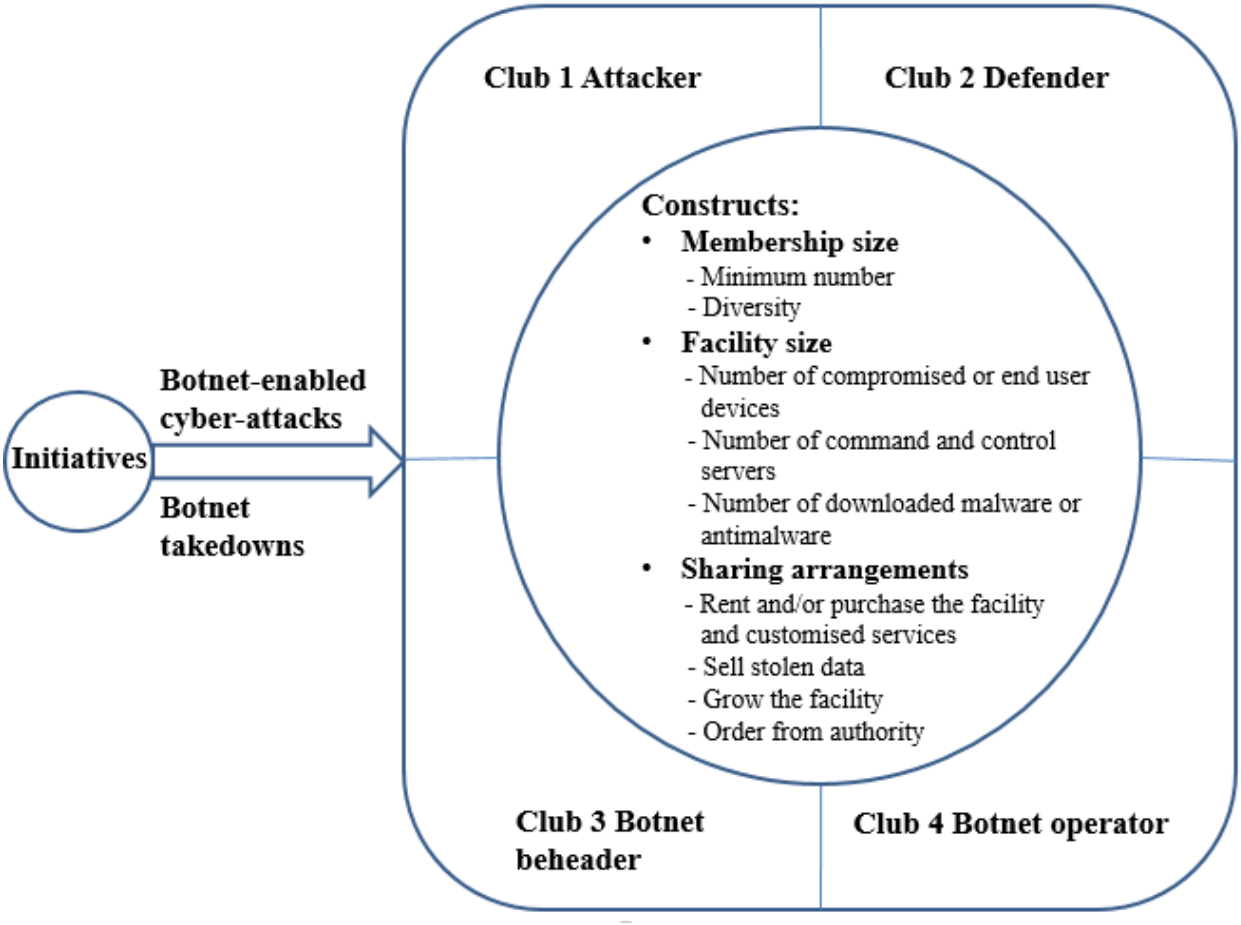
Dimensions		Club 1 Attacker	Club 2 Defender	Club 3 Botnet beheader	Club 4 Botnet operator	Dimensions with data for the four clubs
1. Minimum number	Individuals	✓			✓	
	Organizations		✓	✓		
2. Diversity	Role	✓			✓	
	Organization			✓		
	Sector		✓	✓		
	Country		✓	✓		
3. Number of compromised or end user devices		✓	✓	✓	✓	Yes
4. Number of command and control servers		✓		✓	✓	
5. Number of downloaded malware or antimalware		✓	✓	✓	✓	Yes

6. Arrangement to rent and/or purchase facility and customised services	✓	✓	✓	✓	Yes
7. Arrangement to sell stolen data	✓				
8. Arrangement to grow facility	✓	✓	✓	✓	Yes
9. Arrangement to take order from authority	✓	✓	✓	✓	Yes

4.3 Representation of results of content analysis

Figure 1 provides a representation of the results of the content analysis. Figure 1 includes four clubs, three constructs, and nine dimensions for the two initiatives under consideration: botnet enabled cyber-attacks and botnet takedowns. Figure 1 includes all nine dimensions, even though data values for all four clubs were observed in only five of the nine dimensions.

Figure 1. Representation of the results of the content analysis



4.3.1 Description of nine dimensions

This section describes the nine dimensions associated with the three constructs shown in Figure 1.

4.3.1.1 Membership size construct

The construct "Membership size" has two dimensions: minimum number and diversity. The dimension "Minimum number" is divided into two: minimum number of individuals (MNI), and minimum number of organizations. Minimum number of individuals (MNI) refers to the fewest possible number of people responsible for carrying out or defending against cyber-attacks. The principle of MNI was defined by White (1952) and has been used in forensic anthropology and other disciplines. Minimum number of organizations refers to the fewest possible number of organization responsible for carrying out or defending against cyber-attacks.

Diversity

The dimension "Diversity" is a measure of the uniqueness of the entities responsible for carrying out or defending against cyber-attacks. Four diversity types were identified: role diversity, organization diversity, sector diversity, and country diversity.

Table 5 provide the syntheses of the data for the "Membership size" construct provided in row 6 of Table B.1 and row 6 of Table B.2 included in Appendix B. Table 5 shows that for Clubs 1 and 4, membership size refers to number of individuals while for Clubs 2 and 3 membership size refers to number of organizations. The results suggest that the minimum number of individuals for Club 1 Attacker is 5 and for Club 4 Botnet operator is 1. Moreover, the minimum number of organizations for Club 2 Defender is 8 and for Club 3 Botnet beheader is 3.

Table 5 shows that the dimension "Diversity" refers to role diversity for Clubs 1 and 4; sector and/or organizational diversity for Club 2; and organizational, sector and/or country diversity for Club 3.

Table 5. Summary: Results of the two dimensions of the "Membership size" construct

Initiatives	**Clubs**	**1. Minimum number**		**2. Diversity**			
		Individuals	**Organizations**	**Role**	**Organizations**	**Sector**	**Country**
Botnet-enabled cyber-attack	Club 1 Attacker	5	None	Developer operator, marketer and accomplices	None	None	None
	Club 2 Defender	None	8	None	None	Multiple sectors	Multiple countries
Botnet-takedown	Club 3 Botnet beheader	None	3	None	Multiple private, academic and government organizations	Multiple sectors	Multiple countries

	Club 4 Botnet operator	1	None	Operator	None	None	None

4.3.1.2 Facility size construct

The construct "Facility size" refers to the size of infrastructure (tangible or intangible) used to carry out or defend against cyber-attacks. Examination of the ten scenarios suggests that the construct "Facility size" has three dimensions: Number of compromised or end user devices, Number of C&C servers, and Number of downloadable malware or anti-malware.

Table 6 combines the syntheses of the information collected from row 6 of Table B.3 and row 6 of Table B.4 for the three dimensions of the "Facility size" construct.

The dimension "Number of compromised or end user devices" refers to the number of devices leveraged to carry out or defend against cyber-attacks with or without their owners' consent.

The results shown in Table 6 suggest that Club 1 Attacker and Club 4 Botnet operator may have access to millions of compromised or end user devices. The results also show that Club 2 Defender and Club 3 Botnet beheader have access to a smaller number of compromised or end user devices relative to those of Club 1 Attacker and Club 4 Botnet operator.

The dimension “Number of command and control server” refers to the number of servers used to issue commands to the computers that are part of the botnet and to accept reports back from the compromised computers. Three of the four Clubs made use of C & C servers. Club 1 Attacker and Club 4 Botnet operator made use of C&C servers to have absolute authority over the compromised or end user devices. Club 3 Botnet beheader makes use of C&C servers for “sinkholing,” a botnet takedown process whereby traffic from the compromised devices is routed to servers controlled by those responsible for taking down the botnets. Information on the number of command and control servers for Club 2 Defender was not disclosed in the scenarios that referred to Club 2 Defender.

The dimension “Number of downloadable malware or antimalware” refers to the number of software applications and resources used to exploit or defend against vulnerabilities in computer systems. Table 6 shows that Club 1 Attacker and Club 4 Botnet operator have access to many (50 to millions) of downloadable malware or anti-malware resources.

Table 6 suggests that Club 2 Defender and Club 3 Botnet beheader have access to a small number (10 - 15+) of downloadable malware or anti-malware resources.

Table 6. Summary: Results of the three dimensions of the "Facility size" construct

Initiative	Club	1. Number of compromised or end user devices	2. Number of command and control servers	3. Number of downloaded malware or antimalware
Botnet-enabled cyber-attack	Club 1 Attacker	50 - millions	1 - 2+	50 - millions
	Club 2 Defender	10 - 50+	None	10 - 15+
Botnet-takedown	Club 3 Botnet beheader	15 - 25+	3 - 5+	10 - 15+
	Club 4 Botnet operator	500,000 - millions	1+	600,000 - millions

4.3.1.3 Sharing arrangements construct

The construct "Sharing arrangements" has four dimensions: Arrangements to rent and/or purchase facility and customised services, Arrangements to sell stolen data, Arrangements to grow the facility, and Arrangements to take order from authority.

The dimension “Arrangement to rent and/or purchase facility and customised services” refers to agreements to derive financial benefits from the use of attack or defense infrastructures. Not much is known about these agreements.

The information in Table 7 suggests that there are at least two types of arrangements to rent and or purchase shared facility and customised services: i) de-centralised web market (Club 1 Attacker and Club 4 Botnet operator); and ii) contractual agreements (Club 2 Defender and Club 3 Botnet beheader). Club 2 Defender makes use of contractual agreement to sell products and customised services and Club 3 Botnet beheader makes use of contractual agreements for the purpose of sharing information carrying out botnet takedowns.

The dimension “Sell stolen data” refers to the arrangement to exchange stolen data for money.

The results of the content analysis shown in Table 7 suggest that information on the sale of stolen goods is only relevant to Club 1 Attacker. The information available is for only one type of arrangement, the use of a de-centralised web market to cash out on stolen goods.

The dimension “Grow the facility” refers to the arrangement to expand attack or defense infrastructures. Table 6 shows that there are at least four types of arrangements to grow the facility: i) affordable, customised, easy-to use and multiple variants malwares that ensures each malware can address multiple needs at affordable prices and require the use of less specialized skills (Club 1 Attacker); ii) network capacity upgrades in form of hardware and software upgrades (Club 2 Defender); iii) use of web market and R&D for information capturing (Club 3

Botnet beheader); and iv) use of mixture of centralised and de-centralised C&C network topologies that make total botnet takedown difficult (Club 4 Botnet operator).

The dimensions "Order from authority" refers to the arrangements made with a legal authority to carry out botnet takedowns and arrest the culprits. This dimension was included because all five scenarios on botnet takedown leverage the use of legal mechanisms. Club 2 Defender and Club 3 Botnet beheader had "Order from authority" arrangements to carry out botnet takedown and or arrest and prosecute the culprit of cyber-attack. The "Order from authority" arrangement that Club 1 Attacker and Club 4 Botnet operator had is to remain anonymous to evade arrest.

Table 7 combines the syntheses of the information collected from row 6 of Table B.5 and row 6 of Table B.6 for the four dimensions of the "Sharing arrangements" construct.

Table 7. Summary: Result of the four dimensions of the "Sharing arrangements" construct

Initiative	**Club**	**1. Rent and/or purchase facility and customised services**	**2. Sell stolen data**	**3. Grow facility**	**4. Order from authority**
Botnet-enabled cyber-attack	Club 1 Attacker	De-centralised web market	De-centralised web market	Affordable, customised, easy – to use and multiple variants	Anonymous to evade arrest

	Club 2 Defender	Contractual agreement for product and or service	Not Applicable	Network capacity upgrade	Order to arrest and prosecute culprit
Botnet-takedown	Club 3 Botnet beheader	Contractual agreement for information sharing and botnet takedown	Not Applicable	- Web market for information capturing - R&D	Order to takedown botnet, arrest and prosecute culprit
	Club 4 Botnet operator	De-centralised web market	Not Applicable	Mixture of centralised and de-centralised C&C network topologies	Anonymous to evade arrest

4.4 Comparing clubs

Table 8 provides the results presented as Tables 5, 6 and 7 by Construct and Club. The purpose of providing Table 8 showing the information provided in Tables 5, 6 and 7 is to facilitate comparing the four clubs in terms of the dimensions of the three constructs.

The results in Table 8 suggest that Club 1 Attacker has a minimum of five individuals carrying out attacks who assume at least four roles. This club may have access to millions of compromised devices and downloadable malware, uses a minimum of one C&C server, remain

anonymous to evade arrest, uses web markets to sell products and services and cash out stolen goods. Club 1 grows its facility through access to low cost customised and multiple malware variants.

Club 2 Defender has a minimum of eight organizations engaged in defending against a cyber-attack. These organizations operate in different sectors and countries, establish contractual agreement for product and service sales, grow their facility using hardware and software upgrades, and actively engage legal authorities.

Club 3 Botnet beheader is comprised of a minimum of three organizations that are diverse in terms of operations, sectors, and countries. Club 3 has tens of compromised devices and at least three C&C servers. Members of Club 3 engage in legal and contractual agreements for information sharing and carrying out botnet takedowns. Club 3 grows via R&D and capturing information from web markets.

Club 4 Botnet operator has access to at least 500,000 compromised devices, 600,000 downloadable malware, and at least one C&C server. Club 4 relies on web markets for products and services sales. Club 4 grows using centralised, de-centralised C&C network topologies designed to make botnet takedown difficult and remain anonymous to evade arrest (Table 8, column 6).

Table 8. Comparing the four clubs in terms of the nine dimensions

Construct	**Dimensions**		**Club 1 Attacker**	**Club 2 Defender**	**Club 3 Botnet beheader**	**Club 4 Botnet operator**
Membership size	Minimum number	Individuals	5			1
		Organizations		8	3	
	Diversity	Role	Developer operator, marketer, and accomplices			Operator
		Organization			Multiple private, academic and government organizations	

		Sector		Multiple sectors	Multiple sectors	
		Country		Multiple countries	Multiple countries	
Facility size	Number of compromised or end user devices		50 – millions	Tens	Tens	500,000 – millions
	Number of command and control servers		1 – 2+		3 – 5+	1+
	Number of downloaded malware or antimalware		50 – millions	Tens	Tens	600,000 – millions
Sharing arrangements	Rent and/or purchase facility and customised services		Web market for product and service sales	Contractual and legal agreement for products and services	Contractual and legal agreement for information sharing and botnet takedown	Web market for product and service sales

	Sell stolen data	Web market for cash-out			
	Grow facility	Affordable and customised malware	Hardware and software capacity upgrade	Web market and R&D for information capturing	Mixture of centralised and de-centralised C&C network topologies
	Order from authority	Anonymous to evade arrest	Order to arrest and prosecute culprit	Order to takedown botnet, arrest and prosecute culprit	Anonymous to evade arrest

4.5 Club capabilities

This section infers the capabilities of each of the four clubs based on the information presented in Tables 5, 6 and 7. These capabilities were organized into the five capability types defined in

section 3.2.8 included in Chapter 3. The five capability types are: learning, expertise, relationships, attack infrastructure, and other.

The results shown in Table 9 suggest that Club 1 Attacker has three capability types: Relationship, Attack infrastructure, and Expertise in facility growth and monetising. Members of Club 1 enjoys a relationship that may allow flexibility to act individually or jointly and controls time spent delivering attacks; an attack infrastructure that may allow botnet operators to have authority and direction over compromised devices and malware while members of the club may deliver large scale attacks; and an expertise in facility growth and monetising that may allow the botnet operators to make financial gain and grow botnet infrastructure exponentially, and convert stolen goods into money.

Table 9 provides the Club 1 capabilities inferred from the information provided in Tables 5, 6 and 7.

Table 9. Capabilities of Club 1 Attacker

	Capability	**Table where capability is identified**	**Capability type**	**Reason that capability may deliver advantages**
1	Distributed arrangement	Table 5	Relationship	Club member has flexibility to act individually or jointly and

		Table 7		controls time spent delivering attacks
2	Access tens to millions of compromised devices and downloadable malware	Table 6	Attack infrastructure	Actors can deliver large scale attacks
3	Small number of servers	Table 6	Attack infrastructure	Botnet operators have authority and direction over compromised devices and malware
4	Access to low cost customised and multiple variants of products and services via web markets	Table 7	Expertise in facility growth and monetising	Botnet operators make financial gain and grow botnet infrastructure exponentially
5	Access to cash-out markets	Table 7	Expertise in monetising	Botnet operators have opportunity of converting stolen goods into money

The results in Table 10 suggest that Club 2 Defender has three capability types: Relationship, Attack infrastructure, and Expertise in legal mechanisms. Club 2 has a relationship that allow members to have access to diverse skill sets across countries and sectors; an attack infrastructure that promotes pro-active defense approach especially against a DDoS attack; and an expertise in legal mechanisms that facilitates access to legal required frameworks to apprehend and prosecute culprits of cyber-attacks.

Table 10 provides Club 2 capabilities inferred from the information provided in Tables 5, 6 and 7.

Table 10. Capabilities of Club 2 Defender

	Capability	**Table where capability is identified**	**Capability type**	**Reason that capability may deliver advantages**
1	Joint effort of many organizations across countries and sectors	Table 5	Relationship	Organizations have access to diverse skill sets and legal devices for effective defense, investigation and

				apprehension of culprits
2	Network capacity	Table 7	Attack infrastructure	A pro-active defense approach especially against a DDoS attack
3	Order from authority	Table 7	Expertise in legal mechanisms	Access to legal framework to arrest and prosecute culprits

The results shown in Table 11 suggest that Club 3 Botnet beheader has three capability types: Learning, Relationship, and Expertise in legal mechanisms. Club 3 has a relationship that allow members to have access to diverse skill sets through private-public partnership; a learning through R&D and information gathering from underground markets that provide access to relevant information for effective takedown; and an expertise in legal mechanisms that facilitates access to legal frameworks to carry out botnet takedown, arrest and prosecute culprits.

Table 11 provides Club 3 capabilities inferred from the information provided in Tables 5, 6 and 7.

Table 11. Capabilities of Club 3 Botnet beheader

	Capability	**Table where capability is identified**	**Capability type**	**Reason that capability may deliver advantages**
1	Information gathering from underground markets, and R&D	Table 7	Learning	Access to relevant information for carry out takedown
2	Joint efforts of private and public organizations	Table 5	Relationship	Access to diverse skill sets and legal devices
3	Order from authority	Table 7	Expertise in legal mechanism	Access to legal framework to carry out takedown, arrest and prosecute culprits

The results shown in Table 12 suggest that Club 4 Botnet operator has two capability types: Attack infrastructure, and Relationship. Club 4 has an attack infrastructure built on de-centralized C&C network topology and access to many compromised devices that makes botnet takedown difficult and allows members to instigate large scale attacks as well as ensure botnet

recovers after takedown; and a relationship built on small number of individuals to allows botnet operators conceal their identities and evade arrest for a long time.

Table 12 provides Club 4 capabilities inferred from the information provided in Tables 5, 6 and 7.

Table 12. Capabilities of Club 4 Botnet operator

	Capability	**Table where capability is identified**	**Capability type**	**Reason that capability may deliver advantages**
1	De-centralised C&C network topology	Table 7	Attack infrastructure	To make botnet takedown difficult
2	Access thousands to millions of compromised devices	Table 5	Attack infrastructure	Botnet operators can instigate large scale attacks as well as ensure botnet recovers after takedown
3	Small number of individuals	Table 5	Relationship	Botnet operators can conceal their identities and evade arrest for a long time

Table 13 provides the hierarchical order of terms used in this research.

Table 13. Hierarchical order of terms used in this research

	Level	Definition	Results	Number
1	**Construct**	A single theoretical concept that represents one or several dimensions	1. Membership size 2. Facility size 3. Sharing arrangements	3
2	**Dimension**	A magnitude that, independently or in conjunction with other magnitudes, serves to define, represent or constitute a construct	1. Membership size 1.1. Minimum number 1.1.1.Individuals 1.1.2.Organizations 1.2. Diversity 1.2.1.Role 1.2.2.Organization 1.2.3.Sector 1.2.4.Country 2. Facility size 2.1. Number of compromised or end user devices 2.2. Number of C&C servers	9 (1 with two objects, 1 with 4 objects)

			2.3. Number of downloaded malware or antimalware 3. Sharing arrangements to 3.1. Rent and/or purchase facility and customized services 3.2. Sell stolen data 3.3. Grow facility 3.4. Take orders from authority	
3	**Value**	An amount measured in a dimension	Real number	Varied based dimension

Source: Edwards (2001)

4.6 Summary

Chapter 4 provides the results of the research. The results include: i) a list of the scenarios in the sample; ii) results of content analysis of the ten scenarios; ii) a representation of the results of content analysis; iv) comparisons of the four clubs; and v) capabilities of the four clubs inferred from the data collected.

The representation that was developed unified the collective actions of groups responsible for carrying out or preventing botnet-enabled cyber-attacks and botnet takedowns in terms of: i) four

clubs conceptualization, and ii) the nine dimensions identified for the three constructs from club theory. Data values for the nine dimensions obtained from examining ten scenarios were used to compare the clubs and to infer the capabilities that may lead to club advantages.

.

5 DISCUSSION OF RESULTS

Chapter 5 is a discussion of the results provided in Chapter 4. Chapter 5 is organized into six sections. Section 5.1 discusses insights gained from using the club theory perspective to simultaneously examine cyber-attacks and botnet takedowns. Section 5.2 discusses the constituents of capability types. Section 5.3 is a discussion on the fidelity the results of the research add to the existing literature. Section 5.4 discusses the types of multidimensional constructs used in this research. Finally, section 5.5 provides the summary of Chapter 5.

5.1 Insights from using club theory perspective

According to club theory, members of a heterogeneous population partition themselves into set of clubs that best suits their taste for association (Schelling, 1969), and cost reduction derived from team production (McGuire, 1972). Based on the review of the literature the existence of four clubs engaged in the botnet-enabled cyber-attacks and botnet takedowns initiatives was conceptualized. The results of the research characterize the four clubs in terms of nine dimensions.

The results in Table 4 (column 2) suggests that Club 1 Attacker leverages on all the nine dimensions to carry out its activities. The dominance of individual activities is highlighted by the existence of minimum number of individuals and role diversity. Also, this club's response to legal mechanisms is to remain anonymous to evade arrest.

Club 2 Defender has data for eight dimensions (Table 4, column 3). Dominance of organization activities is highlighted by the data for minimum number of organization and diversity of sectors and countries. Club 2 makes use of order from authority to harness legal mechanisms from multiple countries to carry out the arrest and prosecution of actors responsible for botnet-enabled cyber-attacks.

Club 3 Botnet beheader has data for eight dimensions (Table 4, column 4). Dominance of organization activities is highlighted by the data for minimum number of organization. Club 3 is differentiated from Club 2 by leveraging on the diversity of organizations, sectors and countries. Also, order from authority in Club 3 is to leverage on legal mechanisms to carry out botnet takedown, arrest and prosecute culprits of botnet-enabled cyber-attacks.

Club 4 Botnet operator has data for 8 dimensions (Table 4, column 5). The dominance of individual activities is highlighted by the existence of minimum number of individuals and role diversity. Also, this club's response to legal mechanisms is to remain anonymous to evade arrest.

The data values observed for three dimensions for the four clubs (Table 4, rows 5, 6, 8) can be explained by two dominant justifications for club formation found in the literature: i) taste for association (Schelling, 1969), and ii) cost reduction from team production (McGuire, 1972). An argument can be made that the justification for the dominance of dimension "Number of downloaded malware or antimalware" (Table 4, row 5) is related to the taste of the members of the four clubs. Also, argument can be made that the justification for the dominance of dimensions "Arrangement to rent and or purchase facility and customized services" (Table 4,

row 6) and “Arrangement to grow facility” (Table 4, row 8) refers to the cost reduction from team production.

The researcher cannot link the dominance of dimensions “Number of compromised or end user devices” (Table 4, row 3) and “Arrangement to take order from authority” (Table 4, row 9) in the four clubs to an exact justification(s) for club formation available in the literature. The researcher surmises that club formation can leverage on these two dimensions to ensure that club activities are carried out in an economical manner.

5.2 Club advantages

The researcher inferred the capabilities of the four clubs and identified them in section 4.5.

A capability model is proposed to enable diverse individuals working in heterogeneous organizations to understand botnet-enabled cyber-attacks and botnet takedowns. The capability model summarized in Figure 2 is made up of two parts.

The first part of the model conceptualizes how the four capabilities (i.e., learning, expertise, relationship, and attack infrastructure) may be influenced by the dimensions of the three constructs: membership size, facility size, and sharing arrangements.

The second part of the model examines how the four capabilities may provide advantages for each of the clubs. An argument can be made that the relationships that provide advantages to a club are those that are based on distributed arrangements (Table 9, row 1), attract the joint effort

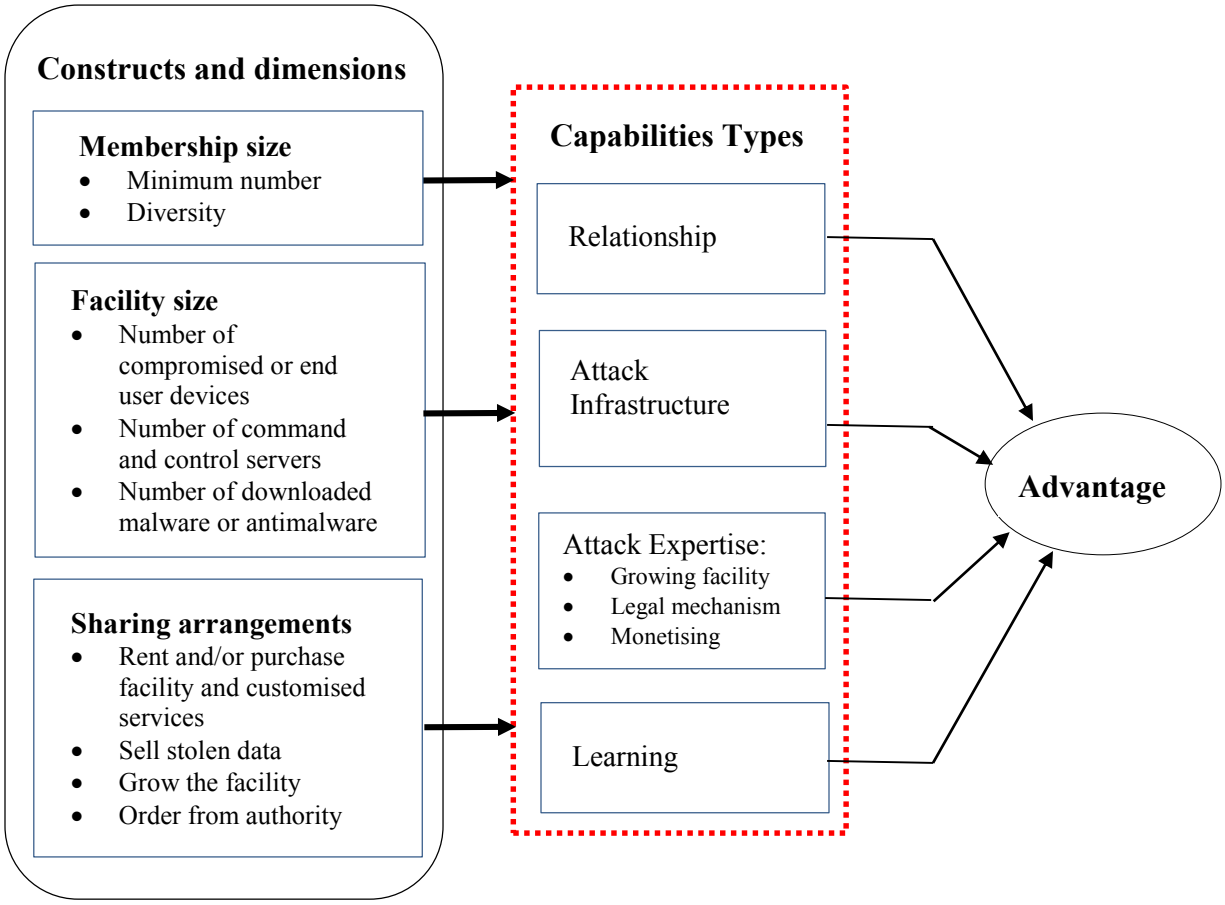
of many organizations across sectors and countries (Table 10, row 1 and Table 11, row 2), and allow anonymity (Table 12, row 3).

Similarly, an argument can be made that the attack infrastructures that provide advantages to clubs are those that allow access to many resources and applications (Table 9, row 2 and Table 12, row 2), require a small number of C&C servers (Table 9, row 3), have high network capacity (Table 10, row 2), and use a decentralized C&C network topology (Table 12, row 1).

Three types of expertise were identified: Expertise in facility growth, Expertise in monetising, and Expertise in legal mechanisms. An argument can be made that the attack expertise that provides advantages are those that promote access to low cost customised and multiple variants of products and services via de-centralised web markets (Table 9, row 4), provide opportunities to convert stolen goods into money (Table 9, row 5), and leverage several legal frameworks (Table 10, row 3 and Table 11, row 3).

Finally, the learning that provides advantages are those that promote acquisition of required knowledge or skills through information gathering from underground markets, and R&D (Table 11, row 1).

Figure 2. Capability model



5.3 Linking results to the lessons learned from reviewing the literature

The results suggest that the club that has a better and/or larger size of capabilities may have an advantage. This suggestion lends support to the lesson learned from the review of the literature that the advantage the botnet operator enjoys is the large distributed network of bots that permit the master to instigate large scale attacks (Lerner, 2014).

There are at least two explanations to the inclusion of dimension "Number of C&C servers". First, a small number of C&C servers provide botnet operators control over the compromised devices as well as attack anonymity. This is evident from examining the results for Club 1 Attacker and Club 4 Botnet operator. Attack anonymity feature supports the observation made in Hathaway et al., (2012) that a botnet provides anonymity.

Second, Club 3 uses C&C for the purpose of operating a "sinkholing" process whereby traffic from the compromised devices communicate with the botnet beheader's servers instead of the attackers' C&C servers. This supports the findings on botnet takedowns made by Whitehouse (2014) and Dittrich (2012).

5.4 Types of multidimensional constructs

The information presented as Table 13 shows the hierarchical order of terms used in this research. There are three level of abstraction: i) Construct, ii) Dimension, and iii) Value. Table 13 (column 3) highlights the use of multidimensional constructs.

Edwards (2001) proposes two major types of multidimensional constructs: superordinate, and aggregate.

When the relationships flow from the construct to its dimensions, the construct may be termed superordinate because it represents a general concept that is manifested by specific dimensions. Superordinate construct is a general concept that is manifested by its dimensions, commonly

used in research on personality, and often operationalized by summing scores on their dimensions (Edwards, 2001).

In aggregate type multidimensional construct, the relationships flow from the dimensions to the construct. The construct may be termed aggregate because it combines or aggregates specific dimensions into a general concept. The dimensions of an aggregate construct are themselves constructs conceived as specific components of the general construct they collectively constitute (Edwards, 2001).

The researcher argues that "Membership size" and "Sharing arrangements" constructs are examples of superordinate type multidimensional construct and "Facility size" construct is an example of aggregate type multidimensional construct.

The researcher argues that this research is better of measuring constructs rather than dimension because of its strengths identified by Edwards (2001) which includes: provision of holistic representations of complex phenomena, allows researchers to match broad predictors with broad outcomes, increases explained variance, and has higher criterion-related validity.

5.5 Summary

The purpose of this chapter is to discuss the results. The research developed a representation of the results of content analysis on ten scenarios. The representation includes four clubs, three constructs from club theory and eleven dimensions.

Using the representation that was developed, four capability types that may turn to advantages were inferred. The relationship centers around a distributed membership arrangement that promotes individual flexibility and allows anonymity, and the joint efforts of many organizations that provide opportunity to leverage on diverse skill sets and legal devices. Attack infrastructures provide access to many resources and applications and high network capacity, and decentralized C&C network topology. Attack expertise is represented as expertise in facility growth, expertise in monetising, and expertise in legal mechanisms. Learning promotes acquisition of required knowledge or skills through information gathering from underground markets, and R&D.

6 CONCLUSIONS, LIMITATIONS, AND SUGGESTIONS FOR FURTHER RESEARCH

Chapter 6 is organized into three sections. Section 6.1 provides the conclusions of this research. Section 6.2 identifies the limitations of the research. Section 6.3 provides suggestions for future research.

6.1 Conclusion

This research applies club theory to develop a representation of the collective actions of individuals and groups organized for the purpose of carrying out or preventing botnet-enabled cyber-attacks and botnet takedowns.

The representation developed identifies four club types that are linked on the Internet (i.e., Attacker, Defender, Botnet beheader, and Botnet operator) and nine dimensions of the three constructs of club theory: club membership size; size of the facility that club members share; and arrangements to operate, purchase/rent and grow the shared facility.

By applying club theory, inner workings of the clubs were uncovered. By understanding these inner workings, we gain enhanced understanding of the capabilities of the clubs and, therefore, can use our understanding to act more decisively and efficiently in mitigating botnet impacts. Hence, the significance of the thesis is that it successfully demonstrates the application of club theory and paves the way for decisive and efficient botnet mitigation approaches.

The capability model proposed is to enable diverse individuals working in heterogeneous organizations to understand botnet-enabled cyber-attacks and botnet takedowns.

6.2 Limitations of the research

The research has at least four limitations. The first limitation is that our understanding of the cyber-attack domain is low. Theories that could shed light on the domain do not exist. What the researcher did was to take a theoretical perspective developed for economics and apply it to examine the domain of cyber-attacks.

The second limitation is the small number of scenarios used. Ideally, the researcher would have liked to carry out a massive study consisting of thousands of cyber-attacks observed from a number of conditions. Practically, this could not happen at this time. The small sample size used does not allow the identification of trends and patterns or generalize results to the population.

The third limitation is that the amount and detail of information for Club 2 Defender and Club 3 Botnet beheader found on the Internet was much greater than the information found for Club 1 Attacker and Club 4 Botnet operator. This resulted in an undesirable asymmetry among the characterizations of the four clubs.

The fourth limitation is that since mass media are typically owned and run by American corporations, most of available data which can be found on-line are pivoting around attacks on American organizations; this is why most studies may reflect a pro-America bias.

6.3 Suggestions for future research

Two areas for future research are suggested. First, is to provide a metric to measure information based on reputation of source that provides it. It would be desirable to find a metric to measure the quality of information used in the research based on the source.

Second, develop hypotheses of what are the sources of competitive advantage for each of the clubs and test them.

REFERENCES

Ahrens J., Hoen. H.W., & Ohr R. 2005. Deepening Integration in an Enlarged EU: A club theoretical perspective. *Journal of European Integration*, 27(4): 417–439.

Ahmad, M.Y., & Kamal, M.A. 2013. Botnet and Botnet Detection Survey. *Journal of Comp. & Math's , 10(1)*: 79-89.

APEC (Asia-Pacific Economic Cooperation) 2008. "Guide on Policy and Technical Approaches against Botnet".

http://www.mtc.gob.pe/portal/apectel38/spsg/08_tel38_spsg_012rev1_botnet-guide-version6-4.pdf

Artle, R. & Averous, C. 1973. The telephone system as a public good: static and dynamic aspects. *Bell Journal of Economics and Management Science, 4(1)*: 89-100.

Asvanund, A., Krishnan, R., Smith, M. D., & Telang, R. 2004. Interest-Based self-organizing peer-to-peer networks: A club economics approach. Available at SSRN 585345.

Bergias, D., & Pines, D. 1981. Clubs, Local Public Goods and Transportation Models. *Journal of Public Economics*, 15: l4l-162.

Bhatt, G.D. & Grover, V. 2005. Types of information technology capabilities and their role in competitive advantage: An empirical study. *Journal of Management Information Systems*, 22 (2): 253-277.

Buchanan, J. M. 1965. An Economic Theory of Clubs. *Economica*, 32(125): 1-14.

Cheng, J. 2014. Raising the stakes: NATO says a cyber-attack on one is an attack on all.

http://defensesystems.com/Articles/2014/09/08/NATO-cyber-attack-collective-response.aspx

Christensen, C. M. 2006. The ongoing process of building a theory of disruption. *Journal of Product Innovation Management*, 23: 39-55.

Crosson, S., Orbell, J., & Arrow, H. 2004. 'Social Poker': A Laboratory Test of Predictions From Club Theory. *Rationality and Society*, 16(2): 225–248.

Czosseck, C., Klein, G., & Leder, F. 2011. On the arms race around botnets-Setting up and taking down botnets. In *Cyber Conflict (ICCC),* 2011 3rd International Conference on (pp. 1-14). IEEE.

Dagon, D., Gu, G., Lee, C. P., & Lee, W. 2007. A taxonomy of botnet structures. In *Computer Security Applications Conference*. ACSAC 2007. Twenty-Third Annual, 325-339.

Dey I. 1993. Qualitative Data Analysis. A User-Friendly Guide for Social Scientists. *Routledge, London*.

Dittrich, D. 2012. So you want to take over a botnet. In *Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats*, 6-6. USENIX Association.

Edwards, J. R. 2001. Multidimensional Constructs in Organizational Behavior Research: An Integrative Analytical Framework. *Organizational Research Methods*, 4(2): 144-192.

Elo, S., & Kyngäs, H. 2008. The qualitative content analysis process. *Journal of advanced nursing*, 62(1): 107-115.

Forman, J., & Damschroder, L. 2008. Qualitative content analysis. Empirical Research for Bioethics: A Primer. Oxford, UK: *Elsevier Publishing*, 39-62.

Gallagher, H., McMahon, W., & Morrow, R. 2014. Cyber Security: Protecting the Resilience of Canada's Financial System.

http://www.bankofcanada.ca/wp-content/uploads/2014/12/fsr-december14-morrow.pdf

Glazer, A., Niskanem, E., & Scotchmer, S. 1997. On the uses of club theory: Preface to the club theory. *Journal of Public Economics*, 65(1997): 3-7.

Grabosky, P. 2014. Organized Crime and National Security. RegNet Working Paper, No. 40, Regulatory Institutions Network.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J.

2012. The Law of Cyber-Attack. *California Law Review*. 100(4): 817-885.

http://www.californialawreview.org/articles/the-law-of-cyber-attack

Hsieh, H. F., & Shannon, S.E. 2005. Three approaches to qualitative content analysis.

Qualitative Health Research, 15(9): 1277-1288.

Hofmokl, J. 2010. The Internet commons: towards an eclectic theoretical framework. *International Journal of the Commons*, 4(1): 226-250.

Khattak, S., Ramay, N. R., Khan, K. R., Syed, A. A., & Khayam, S. A. 2014. A Taxonomy of Botnet Behavior, Detection, and Defense. *Journal of IEEE Communications Surveys & Tutorials*, 16(2): 898-924.

Kok, J., & Kurz, B. 2011. Analysis of the botnet ecosystem. In *Telecommunication, Media and Internet Techno-Economics (CTTE), 10th Conference of*, 1-10.

Krippendorff, K. 2012. Content analysis: An introduction to its methodology. Sage.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. 2014. Advanced social engineering attacks. *Journal of Information Security and Applications.*

Kshetri, N. 2005. Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management*, 11 (2005): 541–562.

Leder, F., Werner, T., & Martini, P. 2009. Proactive botnet countermeasures: an offensive approach. The Virtual Battlefield: *Perspectives on Cyber Warfare*, 3: 211-225.

Lerner, Z. 2014. Microsoft the Botnet Hunter: The Role of Public-Private Partnerships In Mitigating Botnets. *Harvard Journal of Law & Technology*, 28(1): 237-261.

http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech237.pdf

Li, Z., Liao, Q., & Striegel, A. 2009. Botnet economics: uncertainty matters. In *Managing Information Risk and the Economics of Security*, 245-267.

Manske, K. 2000. An Introduction to Social Engineering, Information Systems Security, 9(5): 1-7.

http://www.tandfonline.com/doi/pdf/10.1201/1086/43312.9.5.20001112/31378.10

Max-Neef, M. A. 2005. Foundations of Transdisciplinarity. *Ecological Economics*, 53(1): 5-16. http://www.sciencedirect.com/science/article/pii/S0921800905000273

McGuire, M. 1972. Private good clubs and public good clubs: Economic models of group formation. *The Swedish journal of economics*, 74(1): 84-99.

Medin, F., Andres, J., Antonio, G. L., & Jesus, L. R. 2010. International Organizations and the Theory of Clubs. *Economica*, 9: 17-27.

Nadji, Y., Antonakakis, M., Perdisci, R., Dagon, D., Lee, W. 2013. Beheading hydras: performing effective botnet takedowns. CCS '13 Proceedings of the 2013 ACM SIGSAC *Conference on Computer & Communications Security*: 121-132. http://dl.acm.org/citation.cfm?id=2516749

Naseem, F., Shafqat, M., Sabir, U., & Shahzad, A. 2010. A Survey of Botnet Technology and Detection. *International Journal of Video& Image Processing and Network Security*, 10(1): 9-12.

NSFOCUS technologies Ltd., NS FOCUS Mid-year DDOS threat report 2013.

http://www.nsfocus.com/SecurityReport/2013%20NSFOCUS%20Mid-Year%20DDoS%20Threat%20Report.pdf

Owens, W. A., Dam, K.W., & Lin, H.S. 2009. Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber-attack Capabilities. *National Academy of Sciences*: 1-391.

Pauly, M. V.1970. Cores and Clubs. *Public Choice*, 9(1):53 -65.

Postmes, T. & Brunsting, S. 2002. Collective action in the age of the Internet: Mass communication and online mobilization. *Social Science Computer Review*, 20: 290–301.

http://www.nslg.net/class/Collective%20Action.pdf

Rajab, M. A., Zarfoss, J., Monrose, F., & Terzis, A. 2006. A multifaceted approach to understanding the botnet phenomenon. In *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement,* 41-52.

Rajab, M. A., Zarfoss, J., Monrose, F & Terzis, A. 2007. My botnet is Bigger than Yours (Maybe, Better than Yours): why size estimates remain challenging. *Proceedings of the first conference on First Workshop on Hot Topics in Understanding botnets*

Raymond, M. 2013. Puncturing the Myth of the Internet as a Commons. *Georgetown Journal International Affairs*. International Engagement on Cyber III State Building on a New Frontier Special Issue: 53-64.

Cremonini, M., & Riccardi, M. 2009. The Dorothy project: an open botnet analysis framework for automatic tracking and activity visualization. In *Computer Network Defense (EC2ND), 2009 European Conference on* (pp. 52-54). IEEE.

Shi, Y., Lau, F.C.M., Tse, S.S.H., Du, Z., Tang, R., & Li, S. 2006. Club theory of the Grid. *Concurrency Computat*, 18:1759–1773.

Sandler, T., & Tschirhart, J. T. 1980. The Economic Theory of Clubs: An Evaluative Survey. *Journal of Economic Literature*, 18(4):1481-1521.

Sandler, T., & Tschirhart, J. T. 1997. Club theory: Thirty years later. *Public Choice*, 93: 335–355.

Schelling, T. C. 1969. Models of segregation. The American Economic Review, 59(2): 488-493.

Schmidt, A. 2013. The Estonian cyber-attacks. In J. Healey (Ed.), the fierce domain–conflicts in cyberspace 1986–2012 (pp. 1986–2012). Washington, D.C.: Atlantic Council.

Strahilevitz, L. J.2006, Exclusionary Amenities in Residential Communities, 92(437): 446-47.

Sully, M., & Thompson, M. 2010. The deconstruction of the Mariposa botnet. *Defence Intelligence. Retrieved September*, 16, 2012.

Thiedig, F. & Sylvander, B. 2000. Welcome to the club? - An economical approach to geographical indications in the European Union, *Agrarwirtschaft*, 49(12): 428-437.

Thomas, D. R. 2006. A general inductive approach for analyzing qualitative evaluation data. *American journal of evaluation*, 27(2): 237-246.

Thompson, M. 2009. Mariposa botnet analysis. Technical report, *Defence Intelligence*.

Uma, M., & Padmavathi, G. 2013. A Survey on Various Cyber Attacks and their Classification. *International Journal of Network Security*, 15(5): 390-396.

United States Joint Chiefs of Staff. 2010. Memorandum: Joint Terminology for

Cyberspace Operations. Washington, DC: United States Department of Defense.

Waxman, M. C. 2011. Cyber-attacks and the Use of Force: Back to the Future of Article

2(4). *Yale Journal of International Law*, 36(2): 421-458.

http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf

White, T. E. 1952. Observations on the butchering technique of some aboriginal peoples: I. *American Antiquity*, 337-338.

Whitehouse, S. 2014. Opening Statement. Judiciary Subcommittee on Crime and Terrorism Hearing on: "Taking Down botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks." July 15.

https://www.hsdl.org/?view&did=756247

Zaleski, P., & Zech, C. 1995. The Optimal Size of a Religious Congregation: An Economic Theory of Clubs Analysis. *American Journal of Economics and Sociology*, 54(4): 439-453.

Appendices

Appendix A. Narratives of ten scenarios in the sample

Appendix A includes narratives of the ten scenarios examined in the thesis. The two initiatives examined include: Botnet-enabled cyber-attacks and Botnet takedowns. Five scenarios were included in each of the two initiatives.

Table A.1 identifies the 10 scenarios organized by initiative.

Table A.1. Scenarios in the sample organized by initiative

	Initiative	**Scenario**
1	Botnet-enabled cyber-attacks	Attack on US banks
2		Attack on Spamhaus
3		Attack on MasterCard
4		Attack on Target
5		Attack on NY Times

6	Botnet takedowns	Mariposa botnet
7		BredoLab botnet
8		Citadel botnet
9		Blackshades botnet
10		Gameover Zeus botnet

1. Attack on US banks

In September 2012, there was a distributed denial of service (DDoS) attack targeted at the largest banks in America which include Bank of America, Citigroup, JP Morgan & Chase, and Wells Fargo (Matai, 2012).

The approached used was a DDoS amplification that choked up internet bandwidth thereby disrupting online banking services of the affected US banks. The attack with the estimated throughput of above 100 gigabytes per second was the largest DDoS attack against a financial institution (Matai, 2012; NJ.com 2012).

A group with strong connection to Iran claimed responsibility for the attack claiming that it was in retaliation for cyber-attacks originating from the west and economic sanctions from U.S. and its Arab allies (Zhou, 2012; Matai, 2012).

The attack was reported to have been generated from more than two virtual private web servers and more than a hundred of thousands of computers, many of which were likely owned by sympathizers of the attackers recruited through websites and social networks (Gonslaves, 2012; Zhou, 2012).

The developer of the malware used for the attack was unknown. The attack was reported to have been carried out by a de-centralized criminal gang in the Middle East known as "Cyber Fighter." Files containing the malware for the attack were reported to have originated from an individual traced to a Facebook account "Marzi Mahdavi II". It was reported that more than four individuals collaborated with "Marzi Mahdavi II" to propagate the online recruitment campaigns across multiple Web sites (Danchev, 2012; Chris, 2013; Pastebin, 2012).

The attackers leveraged the anonymity of the Internet. They used affordable and customized malware that was downloadable by more than three thousands users (Danchev, 2012; Gonslaves, 2012).

The team that collaborated to defend against the attack was comprised of at least twelve organizations from different sectors and countries including the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), financial regulator, U.S. Bancorp,

Prolexic Technologies, Akamai, FireEye, Whitehat Security, Anitian Enterprise Security, and Symantec (NSFOCUS, 2012; Gonslaves, 2012; Zhou, 2012; NJ.com 2012).

To defend against the attack, the team upgraded the core network nodes and redirected traffic to dedicated core nodes so as to reduce the capacity of the DDoS attack.

References:

Chris, 2013. Deconstructing the Al-Qassam Cyber Fighters Assault on US Banks.

https://www.recordedfuture.com/deconstructing-the-al-qassam-cyber-fighters-assault-on-us-banks/

Danchev, D. 2012. Dissecting 'Operation Ababil' - an OSINT Analysis

http://ddanchev.blogspot.ca/2012/09/dissecting-operation-ababil-osint.html

Gonsalves, A. 2012. Bank attackers more sophisticated than typical hacktivists, expert says

http://www.csoonline.com/article/2132319/malware-cybercrime/bank-attackers-more-sophisticated-than-typical-hacktivists--expert-says.html

Matai, D.K. 2012. Red Alert-Cyber Attacks on Banks of 100+ Billion Bytes per Second Escalate-Fears of ‘Cyber-Pearl-Harbor’ Mount. October 22.

http://dkmatai.tumblr.com/post/34061092899/red-alert-cyber-attacks-on-banks-of-100-billion

NJ.com 2012. Cyber-attacks on U.S. banks shows sector's vulnerability, experts say. September 28.

http://www.nj.com/business/index.ssf/2012/09/cyber_attacks_on_us_banking_se.html

NSFOCUS technologies Ltd., NS FOCUS Mid-year DDOS threat report 2013.

http://www.nsfocus.com/SecurityReport/2013%20NSFOCUS%20Mid-Year%20DDoS%20Threat%20Report.pdf

Pastebin.com. 2012: http://pastebin.com/E4f7fmB5

Zhou, D. 2012. Iran wages Cyber War against US Banks and Arab Energy Firms. October 2012.

http://www.mic.com/articles/16555/iran-wages-cyber-war-against-us-banks-and-arab-energy-firms

2. Attack on Spamhaus

Spamhaus Project is an international organisation, based in both London and Geneva, founded to track email spammers and spam-related activity.

The DDoS attack on Spamhaus started on March 18, 2013 and lasted for two weeks. The attack with estimated throughput of 300 gigabits per second was deemed to be the largest ever DDoS attack in history (Olson, 2013).

The attack was suspected to have been carried out by CyberBunker, an acclaimed Internet service provider in Eastern Europe which was reported to be providing a host for spammers, botnet command-and-control servers, malware, and online scams at affordable prices. CyberBunker was reported to have more than one million users on its network (Riley et al., 2013).

The attacker leveraged the anonymity of the Internet and used more than one C&C server. CyberBunker was reported to have launched a DDoS attack on Spamhaus from more than one million users on its network. The attack was to retaliate for the loss of business due to Spamhaus including CyberBunker in its black list of spammers (Acohido, 2013; Riley et al., 2013).

In April 2013, a 16-year-old southwest Londoner who was the developer of the malware used for the attack was arrested in connection with the cyber-attacks (Fanner & O'Brien, 2013; Bentham, 2013). However, Spamhaus believes that five additional individuals were also responsible for the attack. These individuals are suspected to live in the U.S., Russia and China (Softpedia.com).

More than eight organizations from different sectors and countries collaborated to defend Spamhaus against the cyber-attack. These organizations included the Dutch Public Prosecution Service, U.K. National Crime Agency, Dutch National High Tech Crime Unit of the Dutch Police Services Agency, Dutch Public Ministry, Spanish National Police, FBI, Sophos and CloudFlare (Goodin, 2013; Linford, 2013; Olson, 2013; Krebs, 2014).

The approach used to get Spamhaus back online was a network capacity upgrade through a process called "Anycast" a routing technique that distributes the same IP address across 23 data centers across the world. Anycast allows the geographically dispersed junk traffic from the DDoS attack to be downloaded by dozens of individual centers, where each packet is then inspected (Goodin, 2013).

References:

Acohido, B. (2013) Attacks on Spamhaus shows good guys making gains. USA Today April 2. http://www.usatoday.com/story/tech/2013/04/02/denial-of-service-spamhaus-good-guys-gain/2046883/

Bentham, M. 2013. London schoolboy secretly arrested over 'world's biggest cyber-attack'. Yahoo News, September 2013.

http://www.standard.co.uk/news/crime/london-schoolboy-secretly-arrested-over-worlds-biggest-cyber-attack-8840766.html

CyberBunker http://en.wikipedia.org/wiki/CyberBunker

Fanner, E. P., & O'Brien, K.J.2013. Provocateur comes into view after cyber-attack. The New York Times. March 29.

http://www.nytimes.com/2013/03/30/business/global/after-cyberattack-sven-olaf-kamphuis-is-at-heart-of-investigation.html?adxnnl=1&adxnnlx=1395516210-pOF8eyFiBRkzFaRclt+5aQ

Goodin, D. 2013. How whitehats stopped the DDoS attack that knocked Spamhaus offline: Someday, operators will secure their networks. Until then, there's Anycast. Ars Technica. March 21.

http://arstechnica.com/security/2013/03/how-whitehats-stopped-the-ddos-attack-that-knocked-spamhaus-offline/

Krebs, B. 2014. SpamHaus, CloudFlare Attacker Pleads Guilty. KrebsonSecurity.

http://krebsonsecurity.com/tag/stophaus/

Linford, S. 2013 An arrest in response to March DDoS attacks on Spamhaus, Spanhaus News. April 26

http://www.spamhaus.org/news/article/698/an-arrest-in-response-to-march-ddos-attacks-on-spamhaus

Olson, P. 2013. ‘Biggest Cyber Attack In History' Could Have Been Carried Out With Just A Laptop. Forbes, March 27

http://www.forbes.com/sites/parmyolson/2013/03/27/biggest-cyber-attack-in-history-could-have-been-carried-out-with-just-a-laptop/

Riley, M., Matlack, C., & Levine, R. 2013. CyberBunker: Hacking as Performance Art

http://www.bloomberg.com/bw/articles/2013-04-04/cyberbunker-hacking-as-performance-art

Softpedia.com. Spamhaus Waiting for Charging of Other Stophaus Members.

http://news.softpedia.com/news/Spamhaus-Waiting-for-Charges-of-Other-Stophaus-Members-449992.shtml

The Spamhaus Project: http://en.wikipedia.org/wiki/The_Spamhaus_Project

3. Attack on MasterCard

MasterCard Incorporated is an American multinational financial services corporation that specializes in processing payments between i) the merchants’ banks and ii) the card issuing banks or credit unions of the purchasers who use the "MasterCard" brand debit and credit cards.

In December 2010, MasterCard blocked all payments to WikiLeaks due to claims that they were engaged in illegal activity (McCullagh, 2010). In response to the action of MasterCard against WikiLeaks, a group of online activist known as "Anonymous" organized an attack on MasterCard. This attack compromised over three millions credit card users in an operation termed "Operation Payback". The Anonymous group is comprised of de-centralised online activists that leverage on anonymity on the Internet to advance their cause, recruit members, and offer their customised attack tool kits at affordable prices (Addley & Halliday, 2010).

In September 2011, Scotland Yard arrested Christopher Weatherhead and co-conspirator 26-year-old Ashley Rhodes for computer-related crimes linked to the "Operation Payback" attack. In addition, a federal grand jury charged more than four men for participating in the "Operation Payback" attack (Schwartz, 2013; Schwartz, 2013; Mlot, 2012).

The defence against the attack on MasterCard was a collaboration of organizations from more than eight organizations from different sectors and countries including the FBI, USA Secret Services, U.K. investigators, Scotland Yard's Police Central eCrime Unit, London's Metropolitan Police Service, U.S. prosecutors, Symantec and FireEye. The approach used to restore MasterCard online services was a mixture of network analysis to identify the security breaches, and hardware and software capacity upgrades (Schwartz, 2013; Mlot, 2012).

References:

Addley, E, & Halliday, J. 2010. "WikiLeaks supporters disrupt Visa and MasterCard sites in 'Operation Payback'".

http://www.theguardian.com/world/2010/dec/08/wikileaks-visa-mastercard-operation-payback

MasterCard Deemed Unsafe? 'Anonymous' WikiLeaks Supporters Claim Privacy Breach.

http://www.huffingtonpost.com/2010/12/08/mastercard-deemed-unsafe-_n_794164.html

McCullagh, D. 2010. MasterCard pulls plug on WikiLeaks payments | Privacy Inc.

http://www.cnet.com/news/mastercard-pulls-plug-on-wikileaks-payments/

Mlot, S. 2012. 22-year-old anonymous hacker convicted.

http://www.pcmag.com/article2/0,2817,2412952,00.asp

Schwartz, M. J. 2013. Operation Payback: Feds Charge 13 On Anonymous Attacks

http://www.darkreading.com/attacks-and-breaches/operation-payback-feds-charge-13-on-anonymous-attacks/d/d-id/1111819?

Schwartz, M. J. 2012. How U.K. Police Busted Anonymous Suspect

http://www.darkreading.com/attacks-and-breaches/how-uk-police-busted-anonymous-suspect/d/d-id/1107835?

4. Attack on Target

The Target data breach started in November 18, 2013 and lasted for 22 days. The attacker used the phishing approach to steal a supplier's credentials and then used them to infiltrate the Target system. The attacker installed memory scraping malware (BLACK POS) in point-of-sale systems at Target's POS machines that were installed at checkout counters. It was estimated that the attacker stole data of 110 million Target's customers (Jamieson & McClam, 2013; Gumuchian & Goldman, 2014).

The malware used for the attack was reported to have been developed by a 17-year-old Russian man who leveraged on anonymity provided by the online underground markets. The developer sold the multi-variant malware (more than 40 variants) to more than 60 customers in Eastern Europe and other parts of the world at affordable prices (Hay-Newman, 2014; Krebs, 2013).

The attack was made possible through a retailer's network (Fazio Mechanical Services). Data compromised was reported to be transferred to more than one server located outside of U.S (Krebs, 2014). Shortly after the Target breach, thieves were able to sell information from these cards via online black market forums known as "card shops." These websites list card information including the card type, expiration date, track data (account information stored on a

card's magnetic stripe), country of origin, issuing bank, and successful use rate for card batches over time (Krebs, 2013; IntelCrawler, 2013; Gumuchian & Goldman, 2014).

Millions of the malware was reported to have been downloaded. This resulted in the compromise of credit card information of Target customers (Jamieson & McClam, 2013; Gumuchian & Goldman, 2014).

The defense against the attack was a collaborative efforts from more than ten organizations from government, financial and IT sectors including FBI, U.S. Secret Service, IntelCrawler, McAfee, FireEye, iSight Partners, Visa, MasterCard, National bank, and Green bank (Krebs, 2013; IntelCrawler, 2013; Kirk, 2014).

Combination of hardware and software network upgrade on more than fifteen network and online payment devices was employed to restore Target online payment system (Krebs, 2013; IntelCrawler, 2013; Kirk, 2014; Kassner, 2015). Although the main actors of the attacks have not been apprehended, two Mexicans trying to enter the U.S. in McAllen, Texas were arrested with 90 fraudulent credit cards believed to have been compromised as a result of the Target data breach (Hsu, 2014).

References:

Greenberg, A. 2014. Banks file class-action against Target and Trustwave over maasive breach. SC Magazine. March 25

http://www.scmagazine.com/banks-file-class-action-against-target-and-trustwave-over-massive-breach/article/339760/

Gumuchian, M.L. and D. Goldman (2014) Security firm traces Target malware to Russia. CNN U.S. January 21.

http://www.cnn.com/2014/01/20/us/money-target-breach

Hay-Newman, L. 2014. A 17-Year-Old Was Behind the Target, Neiman Marcus Credit Card Hacks. Future Tense. January 20.

http://www.slate.com/blogs/future_tense/2014/01/20/target_neiman_marcus_credit_card_number_hacks_were_caused_by_a_17_year_old.html

Hsu, T. 2014. 2 arrested in connection with Target hack

http://www.latimes.com/business/la-fi-target-arrests-20140121-story.html

IntelCrawler. 2013. Target Breach perks underground activities of PIN decryption?

http://intelcrawler.com/news-7

Isidore, C. 2014. Target: Hacking hit up to 110 million customers

http://money.cnn.com/2014/01/10/news/companies/target-hacking/

Kassner, M. 2015. Anatomy of the Target data breach: Missed opportunities and lessons learned

http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

Kirk, J. 2014. Six more U.S. retailers hit by Target-like hacks. Computerworld. January 17. http://www.computerworld.com/s/article/9245531/Six_more_U.S._retailers_hit_by_Target_like_hacks

Krebs, B. 2013. Cards Stolen in Target Breach Flood Underground Markets. KrebsonSecurity

http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/

Krebs, B. 2014. Target Hackers Broke in Via HVAC Company. KrebsonSecurity.

https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

5. Attack on New York Times

The attack on the New York Times (NY Times) started on September 13, 2012 and lasted for 123 days. The phishing attack targeted selected employees of the NY Times and it was followed by the installation of a custom built malware that affected employees' computer systems.

The attack was targeted at stealing corporate passwords of New York Times' employees, for the purpose of learning how information about Chinese leaders was being collected. Computers of 50 employees of the NY Times who downloaded the malwares were compromised during the attack (Perlroth, 2013).

The developer and operator of the malware used were believed to be Chinese. To remain anonymous, the attackers routed their attacks through intermediary computers at universities in North Carolina, Arizona, Wisconsin and New Mexico, as well as at small companies and internet service providers (Zetter, 2013; Ward, 2013).

The defence team against the attack was comprised of more than eight organizations from different sectors and countries including the FBI, US Secret Service, AT&T, Mandiant, Symantec, Sophos, FireEye and the New York Times, (Perlroth, 2013; Ward, 2013).

The approach used by the IT security expert (Mandiant) was to download more than fifteen samples of the malware in order to study the patterns of the attack and help erect better hardware and software defenses. Also, the NY Times replaced more than fifty machines compromised by the attack with new ones (Zetter, 2013; Ward, 2013; BBC.com 2013).

The NY Times beefed up its defences, blocked access from other compromised machines that had been used to get into its network and found and removed every back door into the newspaper's network (Ward, 2013).

References:

BBC.com 2013. New York Times 'hit by hackers from China'.

http://www.bbc.com/news/world-asia-china-21271849

Perlroth, N. 2013. Hackers in China Attacked the Times for Last 4 Months, The New York Times, January.

http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=0

Ward, M. 2013. How the New York Times cleaned house after its hack attack. BBC News.

http://www.bbc.com/news/technology-21273617

Zetter, K. 2013. New York Times Hacked Again, This Time Allegedly By Chinese.

http://www.wired.com/2013/01/new-york-times-hacked/

6. Mariposa botnet takedown

Mariposa is a collection of compromised computers that are directly under the control of a single malicious entity. Defence Intelligence was the first to identify Mariposa as an emerging botnet in May 2009. The botnet later grew to become a network of 13 million compromised machines (bots) in 190 countries in homes, government agencies, schools, more than half of the world's 1,000 largest companies and at least 40 big financial institutions (Finkle, J. 2010).

The operator of Mariposa grew the botnet through a centralised network arrangement consisting of more than one command and control server that enabled more than one million five hundred thousand executable programs to be downloaded daily. This way the botnet operator could extend the functionality of the malicious software beyond what is implemented during the initial compromise and malware can be updated on command, effectively reducing or eliminating the detection rates of traditional host detection methods (Sully & Thompson, 2010).

Mariposa malware was developed by Matjaz Skorjanc (aka Iserdo), a 26 years old who was later arrested in Slovenia. The Mariposa botnet was operated by three individuals identified as "netkairo," aged 31; "jonyloleante," aged 30; and "ostiator," aged 25 (Zerdin, A. 2010; Bustamante, 2010).

A de-centralised underground market (e.g., bfsecurity.net) provided a forum for the sale of mariposa malware packages at affordable prices as well as well as capability to cash-out using stolen goods (Sully & Thompson, 2010).

The Mariposa Working Group (MWG) carried out the takedown of the Mariposa botnet. MWG was an informal group comprised of more than eight organizations from different countries including Defence Intelligence of Canada, the Georgia Tech Information Security Center of USA, Neustar of USA, Panda Security of Spain; FBI; Guardia Civil of Spain; Directi of India, Prevx and F-Secure (Sully & Thompson, 2010).

The takedown initiative combined both technical and legal approaches. The technical approach involved the use of RND and web market for information capturing to carry out forensic analysis and a process known as "sinkholing." The sinkholing process allows traffic from the compromised devices to be directed to C&C servers of the botnet beheader instead of to the C&C server operated by the botnet operator. More than five servers were used to implement the "sinkholing" process and the forensic analysis.

The botnet takedown effort included using the court system to takedown the botnet as well as to apprehend and prosecute the culprits (Sully & Thompson, 2010; Dittrich, 2012).

References:

Bustamante, P. 2010. Butterfly and Mariposa Shutdown and Arrests: Panda Security Virus Bulletin Vancouver 2010.

https://www.virusbtn.com/pdf/conference_slides/2010/Bustamante-VB2010.pdf

Dittrich, D. 2012. So you want to take over a botnet. In *Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats*, 6-6. USENIX Association.

Finkle, J. 2010. UPDATE 1-Spain busts ring accused of infecting 13 mln PCs.

http://www.reuters.com/article/2010/03/02/crime-hackers-idUSN0218881320100302

Sully, M., & Thompson, M. (2010, February). The deconstruction of the Mariposa botnet. Defence Intelligence. Retrieved September 16, 2012, from http://defintel.com/docs/Mariposa_White_Paper.pdf.

Zerdin, A. 2010. Cyber mastermind arrested, questioned in Slovenia.

http://www.washingtontimes.com/news/2010/jul/28/cyber-mastermind-arrested-questioned-in-slovenia/#ixzz3KaCtkmxm

7. BredoLab botnet takedown

Anti-virus companies were the first to report about the BredoLab exploits in May 2009. BredoLab was a complex online downloading platform designed to facilitate malware to spread on a massive, large-scale. The operators used a fee-based service for installing malware to third-parties customers who could use infected machines (bots) to commit various cybercriminal activities (Dittrich, 2012). BredoLab was estimated to infect at least three million machines

through the use of a de-centralised underground forum and more than one C&C server (de Graaf et al., 2013).

To spread malware, BredoLab used a de-centralised network arrangement whereby commands are requested (pulled) by potential computers to be infected using Hypertext Transfer Protocol (HTTP) requests (Dittrich, 2012). The Bredolab botnet was reported to be responsible for generating more than three millions spam e-mails per month (Kirk, 2010).

More than six organizations were involved in the takedown of the BredoLab botnet. These included the National High Tech Crime Unit of the Netherlands' Police Agency (NHTCU), the Dutch High Tech Crime Team, Dutch Forensic Institute, Govcert.nl, the Dutch computer emergency response team, Fox IT, Leaseweb (a hosting provider); and Abuse.ch, a non-profit organization (Dittrich, 2012; de Graaf, 2013; Kirk, 2010).

The BredoLab botnet takedown combined both technical and legal processes. The technical process involved three stages: forensic acquisition of more than fifteen malware resources of the BredoLab botnet, forensic evidence and data extraction of acquired forensic images and communication networks, and analysis of malware samples found in botnet resources. The investigation team leveraged on web market for information capturing, more than three servers, and more than twenty five end user devices for the three technical processes (de Graaf, 2013).

After the forensic analysis and investigation, the bot-herder was identified. The NHTCU issues an international arrest warrant, through which the suspected operator of the botnet was arrested at the airport of Yerevan, Armenia (de Graaf, 2013; Kirk, J. 2010).

References:

De Graaf, D., Shosha, A. F., & Gladyshev, P. 2013. BREDOLAB: shopping in the cybercrime underworld. In Digital Forensics and Cyber Crime (pp. 302-313). Springer Berlin Heidelberg.

http://digitalfire.ucd.ie/wp-content/uploads/2012/10/BREDOLAB-Shopping-in-the-Cybercrime-Underworld.pdf

Dittrich, D. 2012. So you want to take over a botnet. *In Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats, 6-6.* USENIX Association.

Kirk, J. 2010. Dutch team up with Armenia for Bredolab botnet take down

http://www.computerworld.com/article/2513676/government-it/dutch-team-up-with-armenia-for-bredolab-botnet-take-down.html

8. Citadel botnet takedown

Citadel is one of the largest botnets. Citadel installed key-logging software onto zombie computers, giving the master the ability to track everything that the infected user typed. Citadel

was estimated to have logged the keystrokes and steal online banking credentials, credit card information, and other personally identifiable information of users in ninety different countries especially North America, Western Europe, Hong Kong, India and Australia. This to losses estimated to be more than $500 million (Lerner, 2014; Whitehouse, 2014).

Though the developer and operators of the botnet were unknown, the operator of the Citadel botnet was reported to have leveraged on a de-centralised network topology consisting of more than one C&C server to compromise over 11 million victim computers worldwide (Whitehouse, 2014; Lerner, 2014).

The Citadel botnet made use of web market to sell software packs for the botnet and to cash out on stolen goods. The botnet operator grew the botnet by sending about one million twelve hundred thousand phishing messages per week using Facebook and e-mail (Whitehouse, 2014; Lerner, 2014).

The Citadel botnet takedown was carried out in June 2013 through a public-private partnership comprised of more than three organizations from different countries and sectors. These organizations included the Microsoft Corp., Financial Services Information Sharing and Analysis Center (FS-ISAC), the Electronic Payments Association (NACHA), the American Bankers Association (ABA), FBI and other technology industry partners (Redmond, 2013; Lerner, Z. 2014).

The takedown initiative was a combination of legal and technical approaches. The legal approach included using the legal systems to take order to carry out the takedown. The technical approach used was to leverage on web market for information capturing and to wrest C&C servers from cyber criminals' control, prevent infected computers from communicating with the botnet command and control infrastructure by pointing them to more than three servers operated by Microsoft in a process called "sinkholing". More than 1.2 million unique IP addresses were reported to connect to the sinkhole servers in one week (Whitehouse, 2014).

References:

Lerner, Z. 2014. Microsoft the Botnet hunter: The Role of Public-Private Partnerships in mitigating Botnets. Harvard Journal of Law & Technology, 28(1): 237-261.

Redmond, W. 2013. Microsoft, financial services and others join forces to combat massive cybercrime ring.

http://news.microsoft.com/2013/06/05/microsoft-financial-services-and-others-join-forces-to-combat-massive-cybercrime-ring/

Whitehouse, S. 2014. Opening Statement. Judiciary Subcommittee on Crime and Terrorism Hearing on: "Taking Down botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks." July 15.

https://www.hsdl.org/?view&did=756247

9. Blackshades botnet takedown

The Blackshades botnet was built on the Remote Access Tool (RAT), a sophisticated piece of malware that enabled cybercriminals to secretly and remotely gain control over a victim's computer. The RAT featured a graphical user interface which allowed users to easily view the victim's information such as IP address, the computer's name, the computer's operating system, the country in which the computer was located, and whether or not the computer had a web camera (USDJ, 2014).

The operator was reported to have leveraged a centralised network arrangement consisting of more than one C&C server to sell and distribute sophisticated Blackshades Remote Access Tool (RAT). This way the operator was able to infect more than half a million computers in more than 100 countries (Wallace, 2014; Whitehouse, 2014).

In May 2014, an individual who bought the malware and then unleashed it upon unsuspecting computer users was arrested and charged in the U.S. (FBI, 2014; Whitehouse, 2014).

Symantec worked closely with the FBI, Europol and Microsoft in the takedown effort. Symantec shared information that could allow the agency to track down those suspected of involvement. The takedown activity leveraged the web market to capture information required for the takedown (Whitehouse, 2014).

References:

FBI, 2014. International Blackshades Malware Takedown.

http://www.fbi.gov/news/stories/2014/may/international-blackshades-malware-takedown/international-blackshades-malware-takedown

Symantec.com. 2014 Blackshades – Coordinated Takedown Leads to Multiple Arrests

http://www.symantec.com/connect/blogs/blackshades-coordinated-takedown-leads-multiple-arrests

United States Department of Justice. 2014. Manhattan U.S. Attorney And FBI Assistant Director-In-Charge Announce Charges In Connection With Blackshades Malicious Software That Enabled Users Around The World To Secretly And Remotely Control Victims' Computers.

http://www.justice.gov/usao/nys/pressreleases/May14/BlackshadesPR.php

Wallace, C. 2014. A Study in Bots: BlackShades Net

http://blog.cylance.com/a-study-in-bots-blackshades-net

Whitehouse, S. 2014. Opening Statement. Judiciary Subcommittee on Crime and Terrorism Hearing on: “Taking Down botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks." July 15.

https://www.hsdl.org/?view&did=756247

10. Gameover Zeus botnet takedown

Gameover Zeus botnet was widely regarded as the most sophisticated criminal botnet in existence. The GameOver Zeus botnet is made up of a de-centralized network arrangement consisting of more than one C&C server (peer-to-peer command and control) rather than centralized points of origin. This means that instructions to the infected computers can come from more than one C&C server (Krebs, 2014; Stone-Gross, 2012).

The operator of Gameover Zeus leveraged a marketplace provided by the underground economy for cybercriminals to buy and sell their customised products and services at affordable prices (Stone-Gross, 2012).

From September 2011 through May 2014, it was estimated that Gameover Zeus had infected between 500,000 and 1 million computers and was responsible for 678,205 malware download (Whitehouse, 2014; Krebs, 2014).

A grand jury in Pittsburgh convicted Evgeniy Mikhailovich Bogachev for operating the botnet. At least two other individuals also operated the botnet (Krebs, 2014; Gross, 2014; fbi.gov 2014).

A group of more than four international organizations comprised of law enforcement agencies and security industry leveraged R&D and information captured by web market to takedown the botnet in June 2014. The organizations engaged in the botnet takedown included the FBI, Computer Emergency Readiness Teams (CERTs), Europol, the UK's National Crime Agency, security firms CrowdStrike, Dell SecureWorks, Symantec, Trend Micro and McAfee; and Microsoft. These organizations cooperated to identify the criminal element and technical infrastructure, develop tools, and craft messages for users in order to collectively and aggressively disrupt this botnet (Whitehouse, 2014; Krebs, 2014).

In a consolidated legal filing, Microsoft received court approval to seize several servers used to control dozens of the bots. Microsoft used the court approval to take control of more than fifteen domains that were used to download more than ten samples of Gameover Zeus malware for forensic analysis and eventual takedown (Krebs, 2014; Gross, 2014).

References:

FBI.gov. 2014 GameOver Zeus Botnet Disrupted Collaborative Effort among International Partners

http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted

Gross, G. 2014. Law enforcement agencies disrupt Gameover Zeus botnet

http://www.pcworld.com/article/2357820/law-enforcement-agencies-disrupt-gamover-zeus-botnet.html

Krebs, B. 2014. "'Operation Tovar' Targets 'Gameover' ZeuS Botnet, CryptoLocker Scourge". Krebs on Security.

http://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/

Stone-Gross, B. 2012. The Lifecycle of Peer-to-Peer (Gameover) ZeuS. Dell SecureWorks Counter Threat Unit(TM) Threat Intelligence.

http://www.secureworks.com/cyber-threat-intelligence/threats/The_Lifecycle_of_Peer_to_Peer_Gameover_ZeuS/

Appendix B. Constructs and dimensions used to produce a unified representation of cyber-attacks and botnet takedowns

Table B.1. Value of the two dimensions of the "Membership size" construct for scenarios on botnet-enabled cyber-attacks

	Scenarios	Club 1 Attacker						Club 2 Defender					
		Minimum number		Diversity				Minimum number		Diversity			
		Individual	Organization	Role	Organization	Sector	Country	Individual	Organization	Role	Organization	Sector	Country
1	US banks	5+		Operator and few accomplices					9+			Financial institutions (e.g. Bank of America, Citigroup, JP Morgan & Chase, and Wells Fargo)	Governments agencies (FBI, Secret Service),
2	Spamhaus	5+		Developer, operator and few accomplices					8+			IT companies (e.g. Sophos and CloudFlare)	Dutch Public Prosecution Service, Dutch National High Tech Crime Unit of the Dutch Police Services Agency, Spanish National Police
3	MasterCard	6+		Operator and few accomplices					8+			IT companies (e.g. Symantec and FireEye)	Governments agencies (FBI, Secret Service)
4	Target	62+		Developer, marketer and few accomplices					10+			Financial institutions (e.g. Visa, MasterCard, National bank, Green Bank). TI companies (e.g. IntelCrawler, McAfee, FireEye, iSight Partners)	Governments agencies (FBI, Secret Service
5	NY Times	Exact number not		Unknown					8+			IT companies (e.g. AT&T, Mandiant, Symantec, Sophos, FireEye)	FBI, US Secret Service etc.

		availab le											
6	**Summary**	**Minim um value = 5**	**None**	**Role diversity: Developer, operator, marketer, and accomplice s**	**Non e**	**Non e**	**Non e**	**Non e**	**Minimum value = 8**	**Non e**	**Non e**	**Multiple sectors**	**Multiple countries**

Table B.2. Value of the two dimensions of the "Membership size" construct for scenarios on botnet takedown

		Club 3 Botnet beheader						**Club 4 Botnet operator**					
		Minimum number		**Diversity**				**Minimum number**		**Diversity**			
	Scenarios	**Indivi dual**	**Organi zation**	**Role**	**Organization**	**Sector**	**Country**	**Indi vidu al**	**Org aniz ation**	**Role**	**Org aniz ation**	**Sect or**	**Count ry**
1	Mariposa botnet		8+		Defence Intelligence of Canada, Neustar of USA, Panda Security of Spain, Georgia Tech Information Security Center of USA, Guardia Civil of Spain, Directi of India etc.	IT companies (e.g. Prevx and F-Secure)	FBI	3+		Operators			
2	BredoLab botnet		6+		Dutch High Tech Crime team	IT companies (e.g. Fox IT, Leaseweb)		1+		Operator			
3	Citadel botnet		3+		Microsoft, FS-ISAC, NACHA, ABA		FBI	Unk now n		Unknown			
4	Blackshade s botnet		3+		Microsoft	IT companies (e.g. Symantec)	FBI, Europol	1+		Operator			
5	Gameover Zeus botnet		4+		Microsoft	IT companies (e.g. CrowdStrik e, Dell SecureWor ks, Symantec, Trend Micro and McAfee)	FBI, CERT, Europol,	2+		Operator			
6	**Summary**	**None**	**3**	**None**	**Private, public and academic organizations**	**Multiple sectors**	**Multiple countries**	**1**	**Non e**	**Operato r**	**Non e**	**Non e**	**None**

Table B.3. Value of the three dimensions of the "Facility size" construct for scenarios on botnet-enabled cyber-attacks

	Scenarios	Club 1 Attacker			Club 2 Defender		
		No of compromised or end user devices	**No of command and control servers**	**No of downloaded malware or antimalware**	**No of compromised or end user devices**	**No of command and control servers**	**No of downloaded malware or antimalware**
1	US banks	100,000+	2+	3,000+	Unknown	Not applicable	Unknown
2	Spamhaus	1+ million	1+	Unknown	10+	Not applicable	10+
3	MasterCard	2.5+ million	Unknown	Unknown	Unknown	Not applicable	Unknown
4	Target	Unknown	1+	110 millions	15+	Not applicable	Unknown
5	NY Times	50+	Unknown	50	50+	Not applicable	15+
6	**Summary**	**Values: 50 - millions**	**Value: 1 – 2+**	**Value: 50 - millions**	**Value: 10 - 50+**	**None**	**Value: 10 - 15+**

Table B.4. Value of the three dimensions of the "Facility size" construct for scenarios on botnet takedowns

	Scenarios	Club 3 Botnet beheader			Club 4 4 Botnet operator		
		No of compromised or end user devices	**No of command and control servers**	**No of downloaded malware or antimalware**	**No of compromised or end user devices**	**No of command and control servers**	**No of downloaded malware or antimalware**
1	Mariposa botnet	Unknown	5+.	Unknown	13+ millions	1+	1.5 million per day
2	BredoLab botnet	25+	3+	15+	Millions	1+	3.6 million infectious emails
3	Citadel botnet	Unknown	3+	Unknown	11+ million	1+	1.2 million per week
4	Blackshades botnet	Unknown	Unknown	Unknown	500+ thousands	1+	Unknown
5	Gameover Zeus botnet	15+	Unknown	10+	500+ thousand	1+	678,205+
6	**Summary**	**Value: 15 - 25+**	**Value: 3 – 5+**	**Value: 10 – 15+**	**Value: 500,000 - millions**	**Value: 1+**	**Value: 600,000 - millions**

Table B.5. Value of the four dimensions of the "Sharing arrangements" construct for scenarios on botnet-enabled cyber-attacks

	Scenarios	Club 1 Attacker				Club 2 Defender			
		Rent and/or purchase facility and customised services	**Sell stolen data**	**Grow facility**	**Order from authority**	**Rent and/or purchase facility and customised services**	**Sell stolen data**	**Grow facility**	**Order from authority**
1	US banks	De-centralised web market for product sales/rent	Not applicable (No data was stolen)	Affordable, customised, easy-to-use and multiple variant malware	Anonymous to evade arrest	Contractual agreement for product and or service	Not applicable	Network capacity upgrade	Order to arrest and prosecute culprit
2	Spamhaus	De-centralised web market for product sales/rent	Not applicable (No data was stolen)	Affordable, customised, easy-to-use and multiple variant malware	Anonymous to evade arrest	Contractual agreement for product and or service	Not applicable	Network capacity upgrade	Order to arrest and prosecute culprit
3	MasterCard	De-centralised web market for product sales/rent	Not applicable (No data was stolen)	Affordable, customised, easy-to-use and multiple variant malware	None	Contractual agreement for product and or service	Not applicable	Network capacity upgrade	Order to arrest and prosecute culprit
4	Target	De-centralised web market for product sales/rent	De-centralised web market for cash-out on stolen goods	Affordable, customised, easy-to-use and multiple variant malware	Anonymous to evade arrest	Contractual agreement for product and or service	Not applicable	Network capacity upgrade	Order to arrest and prosecute culprit
5	NY Times	Not applicable	Not applicable (Data stolen was for political reasons)	Customised and multiple variants malware	Anonymous to evade arrest	Contractual agreement for product and or service	Not applicable	Network capacity upgrade	Order to arrest and prosecute culprit

6	**Summary**	**De-centralized web market**	**De-centralized web market**	**Affordable, customised, easy to use and multiple variants malware**	**Anonymous to evade arrest**	**Contractual agreement for product and services sale**	**Not applicable**	**Network capacity upgrade**	**Order to arrest and prosecute culprit**

Table B.6. Value of the four dimensions of the "Sharing arrangements" construct for scenarios on botnet takedowns

		Club 3 Botnet beheader				**Club 4 Botnet operator**			
	Scenarios	**Rent and/or purchase facility and customised services**	**Sell stolen data**	**Grow facility**	**Order from authority**	**Rent and/or purchase facility and customised services**	**Sell stolen data**	**Grow facility**	**Order from authority**
1	Mariposa botnet	Contractual agreement for information sharing and botnet takedown	Not applicable	-Web market for information capturing - R&D	Order to takedown botnet, arrest and prosecute culprit	De-centralised web market for product sales/rent	Underground market for cash out on stolen data	Centralised C&C network topology	Anonymous to evade arrest
2	BredoLab botnet	Contractual agreement for information sharing and botnet takedown	Not applicable	-Web market for information capturing - R&D	Order to takedown botnet, arrest and prosecute culprit	De-centralised web market for product sales/rent	Not applicable	De-centralised C&C network topology	Anonymous to evade arrest
3	Citadel botnet	Contractual agreement for information sharing and botnet takedown	Not applicable	-Web market for information capturing - R&D	Order to takedown botnet, arrest and prosecute culprit	De-centralised web market for product sales/rent	Not applicable	De-centralised C&C network topology	Anonymous to evade arrest
4	Blackshades botnet	Contractual agreement for information sharing and	Not applicable	-Web market for information capturing - R&D	Order to takedown botnet, arrest and	De-centralised web market for	Not applicable	Centralised C&C network topology	Anonymous to evade arrest

		botnet takedown			prosecute culprit	product sales/rent			
5	Gameover Zeus botnet	Contractual agreement for information sharing and botnet takedown	Not applicable	-Web market for information capturing - R&D	Order to takedown botnet, arrest and prosecute culprit	De-centralised web market for product sales/rent	Not applicable	De-centralised C&C network topology	Anonymous to evade arrest
6	**Summary**	**Contractual agreement for information sharing and botnet takedown**	**Not applicable**	**Web market for information capturing and R&D**	**Order to takedown botnet, arrest and prosecute culprit**	**De-centralised web market**	**Not applicable**	**Mixture of centralised and de-centralised C&C network topologies**	**Anonymous to evade arrest**