Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory

Olukayode Adegboyega

> *"I don't want to belong to any club that will accept me as a member."*
>
> Groucho Marx (1890–1977)
> Comedian, actor, and host

A model for executing and resisting botnet-enabled cyber-attacks and botnet takedowns does not exist. The lack of this representation results in ineffective and inefficient organizational decision making and learning, hampers theory development, and obfuscates the discourse about the "best-case" scenarios for the future of the online world. In this article, a club theory model for botnet-enabled cyber-attacks and botnet takedowns is developed. Initiatives to execute and resist botnet-enabled cyber-attacks and botnet takedowns are conceptualized as collective actions carried out by individuals and groups organized into four types of Internet-linked clubs: Attacker, Defender, Botbeheader, and Botmaster. Five scenarios of botnet-enabled cyber-attacks and five scenarios of botnet takedowns are examined to identify the specific dimensions of the three constructs and provide examples of the values in each dimension. The developed theory provides insights into the clubs, thereby paving the way for more effective botnet mitigation strategies. This research will be of particular interest to executives and functional personnel of heterogeneous organizations who are interested in improving the quality of their communications and accelerating decision making when solving botnet-related problems. Researchers applying club theory to examine collective actions of organizations linked by the Internet will also be interested in this research. Although club theory has been applied to solve problems in many fields, this is the first effort to apply it to botnet-related problems.

Introduction

A botnet is a network of infected hosts that carry out commands sent by a botmaster. The impacts of botnet-enabled cyber-attacks on individuals and organizations are diverse and have necessitated a collaborative approach that leverages technical and non-technical systems to mitigate botnet-enabled cyber-attacks. However, such collaborative initiatives carried out to solve botnet-related problems are costly, complex, and time consuming due to poor communication among the executives and personnel in technical, legal, security, and research functions of heterogeneous organizations, including law enforcement agencies. Although many collaborative initiatives have been successful, some have not (Lerner, 2014; Schmidt, 2012).

This article provides a representation for executing and resisting botnet-enabled cyber-attacks and botnet takedowns. The intent is to improve communications, learning, and decision making among the various actors that need to come together to effectively and efficiently address botnet-related problems, accelerate theory development, and clarify the discussion about the "best-case" scenarios for the future of the online world.

In this representation, the initiatives to execute and resist botnet-enabled cyber-attacks and botnet takedowns are conceptualized as collective actions carried out by Internet-linked clubs. Collective action refers to actions undertaken for a collective purpose, such as the advancement of a particular ideology or idea, or the polit-

Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory

Olukayode Adegboyega

ical struggle with another group (Postmes & Brunsting, 2002). Collective action requires a definition of who "we" are and an understanding of what "we" can do (Drury et al., 2014).

Botnet-enabled cyber-attacks executed by groups such as Wonderland, Anonymous, Drink or Die, The Ukranian ZeuS, Dark Market, Operation Olympic Games, Ghost Net, and PLA Unit 61398 provide examples of collective actions of Internet-linked groups. Membership of such groups is comprised of both willing and unwilling members whose devices were compromised without their consent (Grabosky, 2014).

Other examples of collective action include initiatives to takedown botnets. In 2009, organizations including Defence Intelligence, Panda Security, Neustar, Directi, Georgia Tech Information Security Center, and security researchers came together to form the Mariposa Working Group for the purpose of taking down the Mariposa botnet (Sully & Thompson, 2010). In 2013, Symantec and Microsoft collaborated to obtain a court injunction to dismantle the ZeroAccess botnet (Whitehouse, 2014). In 2014, a group of more than 30 organizations comprised of law enforcement agencies, the security industry, academia, researchers, and service providers cooperated to takedown the GameOver Zeus botnet (Whitehouse, 2014). The group identified the criminal elements and technical infrastructure, developed tools, and crafted messages for users. However, little is known about the inner workings of the collective actions of such groups. By inner working, the author means the arrangement employed by the groups to carry out their activities (e.g., to recruit members or to distribute technical and non-technical infrastructures among members).

Club theory has proven useful in examining the inner workings of collective action in private and public settings (Crosson et al., 2004; Medin et al., 2010). Extant literature on the applications of club theory has focused on non-Internet applications. Club theory has been applied to solve problems related to: highway congestion, highway pricing, provisioning, and financing (Bergias & Pines, 1981; Glazer et al., 1997); grid services (Shi et al., 2006); and the simultaneous deepening and enlargement of the European Union (Ahrens et al., 2005; Thiedig & Sylvander 2000).

A few Internet-related problems such as those related to self-organizing peer-to-peer networks have been solved by the club theory (Asvanund et al., 2004). Raymond (2013) suggested that the Internet can be considered as a set of "nested clubs", and Hofmokl (2010) suggested that Internet goods such as broadband Internet access, proprietary software, and closed databases can be categorized as club goods because they are non-rivalrous in consumption and excludable.

Club theory has been applied to solve problems in many different fields. However, to the author's knowledge, this is the first application of club theory to solve botnet-related problems. In this article, information on five botnet-enabled cyber-attacks and five botnet takedowns are used to conceptualize four types of Internet-linked clubs. The article identifies the dimensions of three constructs and their values observed in ten scenarios.

The remainder of this article is structured as follows. First, the four types of Internet-linked clubs and the three constructs of club theory that anchored the research are described. Then, the method used to carry out the research is explained, and the results are presented. The results include the dimensions of the three constructs for examining the clubs that execute and resist botnet-enabled cyber-attacks and botnet takedowns as well as the characterization of each of the four clubs. The last section provides the conclusions.

Types of Internet-linked Clubs

Definitions of a club has 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: i) a group of consumers sharing a common facility (Glazer et al., 1997); ii) a group of persons who share in the consumption of a good which is not purely private, nor wholly divisible among persons (Pauly, 1970); iii) a consumption ownership-membership arrangement justified for its members by the economies of sharing production costs of a desirable good (Buchanan, 1965); and iv) 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 & Sandler, 1996). These definitions indicate that a club is a group that shares a good.

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 ex-

Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory

Olukayode Adegboyega

cludable (Sandler & 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 club good has two major characteristics: i) partially rivalrous and ii) excludability. A good is partially rivalrous in consumption when one person's consumption of a unit of the good detracts, to some extent, from the consumption opportunities of another person (Sandler & Tschirhart, 1980). A key feature of the good shared by a club is that it is possible to prevent individuals who have not paid for the good from having access to it. Examples of club goods include hospitals, health clubs, trauma clinics, libraries, universities, movie theatres, telephone systems, and public transport (Sandler & Tschirhart, 1997).

According to club theory, members of a heterogeneous population partition themselves into a set of clubs that best suits their taste for association (Schelling, 1969) and cost reduction derived from team production (McGuire, 1972). Therefore, the individuals and organizations that execute and resist botnet-enabled cyber-attacks and botnet takedowns can be thought of as partitioning themselves into many Internet-linked clubs, each comprised of a group who derive mutual benefits from sharing a good. By "execute" the author means the imposition of rights that were not intended by owners of computer systems, assets, data, and capabilities. By "resist", the author means the enforcement of rights that were intended by owners of computer systems, assets, data, and capabilities. A company such as Microsoft, a law enforcement agency such as the Federal Bureau of Investigations, or a nation state such as China can be members of various clubs, and these clubs can be of different types.

Table 1 shows that the Internet-linked clubs that execute and resist botnet-enabled cyber-attacks and botnet takedowns can be organized into four types based on the nature of the good that members share. Clubs whose members share a botnet belong to Type 1 (Attacker). Clubs whose members share a socio-technical system belong to Type 2 (Defender). Clubs whose members share a botnet termination method to takedown a botnet belong to Type 3 (Botbeheader). Clubs whose members share a command-and-control server network belong to Type 4 (Botmaster).

Type 1: Attacker

Members of an Attacker club share a botnet to compromise or gain unauthorized access to an institution's systems and technology (Gallagher et al., 2014). As introduced earlier, a botnet is a network of bot-infected hosts that carry out commands sent by a botmaster, typically unbeknownst to the owners of the hosts (Yahyazadeh & Abadi, 2015). Botnets are used to carry out cyber-attacks that can cause devastating effects to individuals, organizations, and nation states.

Botnet-enabled cyber-attacks are considered one of the most prevalent and dangerous threats to connected devices on the Internet today. These attacks leverage several thousands of compromised hosts and use complex network structures which are quite difficult to detect, trace and takedown (APEC, 2008; Czosseck et al., 2011; Lerner, 2014). Such malicious activities include distributed denial-of-service attacks (DDoS); Simple Mail Transfer Protocol (SMTP) mail relays for spam; ad-click fraud; and the theft of application serial numbers, login IDs, and financial information such as credit card numbers and bank accounts (Cremonini & Riccardi, 2009; Khattak et al., 2014; Li et al., 2009).

Type 2: Defender

Members of a Defender club share a socio-technical system to detect or counteract the effects of botnet-en-

Table 1. Types of Internet-linked clubs organized by the good members share

Club Type	Shared Good	Main Activity	Activity
1. Attacker	Botnet	Attack using botnet(s)	Execute
2. Defender	Socio-technical system	Defend system(s)	Resist
3. Botbeheader	Termination method	Attack botnet(s)	Execute
4. Botmaster	Command-and-control server network	Control botnet(s)	Resist

Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory

Olukayode Adegboyega

abled cyber-attacks. They share the interactions between the social and technical factors that create the conditions that drive organizational performance. Members of this club leverage the socio-technical system to detect deviations from normal activities on systems, identify abuse of systems, mitigate known vulnerabilities, and counteract known threats.

The literature on how to defend 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. For example, the North Atlantic Treaty Organization's (NATO) new cyber-defence 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 2000, the defence against cyber-attacks on Estonia was successfully carried out by a working group comprised of the ICT security community, banks, legal authorities, Internet service providers, telcommunication companies, and energy companies (Schmidt, 2012).

Type 3: Botbeheader
Members of a Botbeheader club share a method to terminate a botnet – a particular procedure used to identify and disrupt the botnet's command-and-control infrastructure (Dittrich, 2012; Nadji et al., 2013). Typically, this termination method embodies a legal regime (i.e., a system of principles and rules created by international or domestic law) and is denoted by words such as "behead", "takedown", "takeover", or "eradication" (Dittrich, 2012; Lerner, 2014; Nadji et al., 2013; Sully & Thompson, 2010).

In recent years, governments, not-for-profit organizations, and companies have launched aggressive attacks to disrupt and disable botnets. The techniques used to takedown botnets are as varied as the botnets themselves. Many of the botnet takedown initiatives employ the use of the court system to obtain injunctions to initiate a takedown (Shirazi, 2015).

Type 4: Botmaster
Members of a Botmaster club share one or more command and control servers and a communications network for a particular botnet. These members are called "botmasters".

The botmasters leverage the large network of infected machines, vast underground economy, and forums on the Internet (made possible by the anonymity provided by the Internet) to operate illicit businesses such as false advertising of cheap pharmaceutical drugs, malware distribution, performing a variety of scams, and sending spam emails on behalf of third-party customers (Stone-Gross et al., 2011).

Club Theory Constructs

Club theory 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 club theory 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).

A construct refers to a single theoretical concept that represents one or several dimensions. Club theory builds on three constructs: i) optimal size of products, ii) optimal membership size, and iii) sharing arrangements. Size is a central characteristic of organizations that is typically measured by the number of employees, members, or total revenues. 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. The optimal size of a club is the size at which members derive maximum benefits from the consumption of the shared resource. 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. This means that the provisional decisions of the good are based on the contribution of the club members: members who contribute more enjoy a larger share of the club goods (Buchanan, 1965).

Method

The objective of this article is to develop a model for representing botnet-enabled cyber-attacks and botnet takedowns initiatives in terms of the dimensions of the three constructs used in club theory to explain collective action. The model provides insights into the clubs, thereby paving the way for more effective botnet mitigation strategies. To identify the dimensions that can be used to measure the club theory's three constructs and provide examples of the values for each dimension, an interpretative approach to content analysis was used.

Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory

Olukayode Adegboyega

The author's interpretation of the results was based on the conceptualization of the four types of Internet-linked club and the three constructs of club theory described above.

A sample comprising 10 scenarios, five for botnet-enabled cyber-attacks and five for botnet takedowns, was selected and the author collected information from the Internet for each of the scenarios in the sample. The information about the scenarios was collected from January 1st, 2009 to December 31, 2014 from sources including: reputable news organizations such as *The New York Times,* CNN, BBC; articles, books, and peer-reviewed research papers; security reports published from well-established security companies such as Kaspersky, Symantec, Defence Intelligence, and Hewlett-Packard; well-established magazine outlets such as T*he Times, Forbes,* and *Foreign Policy.*

Three spreadsheets, one for each construct, were prepared. Each spreadsheet captured the potential dimensions and values collected for the 10 scenarios in the sample. Each scenario had two Internet-linked clubs. Five scenarios focused on botnet-enabled cyber-attacks and included information on two rival Internet-linked clubs, the Attacker and Defender. The five other scenarios focused on botnet takedowns and included information on two rival clubs, the Botbeheader and Botmaster.

The interpretative approach of content analysis was used to identify the sets of dimensions for each construct. A final set of dimensions considered to be essential to a unified representation of botnet-enabled cyber-attacks and botnet takedowns was identified by eliminating ambiguities and inconsistencies. For each dimension, values for each scenario were identified. Finally, these values were used to compare the four types of Internet-linked clubs.

Representation for Executing and Resisting Botnet-Enabled Cyber-Attacks

Figure 1 illustrates a unified representation for executing and resisting botnet-enabled cyber-attacks and botnet takedowns. This representation identifies the eight dimensions that can be used to measure the three constructs from club theory for all four Internet-linked club types.

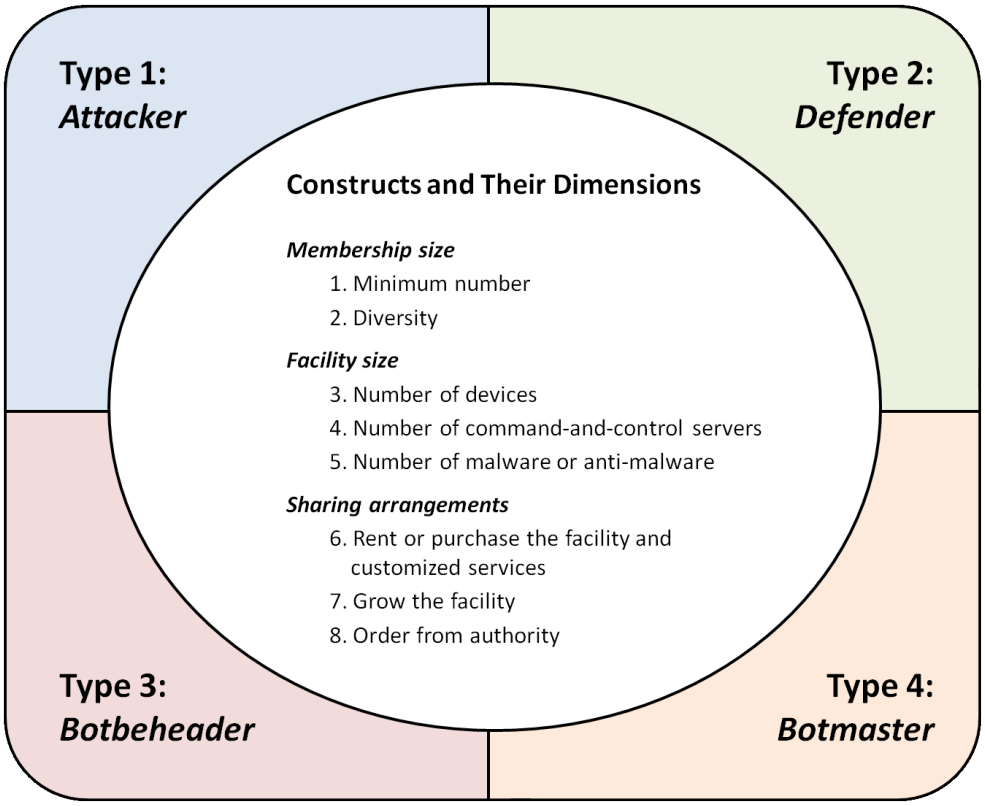

Figure 1. Representation for executing and resisting botnet-enabled cyber-attacks and botnet takedowns

Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory

Olukayode Adegboyega

Membership size construct

The construct "Membership size" has two dimensions: minimum number and diversity. "Minimum number" can be measured as: minimum number of individuals and minimum number of organizations. Minimum number of individuals refers to the fewest possible people responsible for executing or resisting cyber-attacks. Minimum number of organizations refers to the fewest possible organization responsible for executing or resisting cyber-attacks. The principle of minimum number was defined by White (1952) and has been used in forensic anthropology and other disciplines. The dimension "Diversity" is a measure of the uniqueness of the entities responsible for executing or resisting cyber-attacks. There exist at least four diversity types: role diversity (e.g., developer, operator, marketer, and accomplices), organization diversity (e.g., private, academic, and government), sector diversity, and country diversity.

Facility size construct

In club theory, facility size is determined by the provision level of the shared resource, which is negatively related to the congestion that characterizes a sharing group (Sandler & Tshirhart, 1997). The results of this research suggest that the construct "Facility size" has three dimensions: number of compromised or end-user devices, number of command-and-control servers, and number of downloadable instances of malware or anti-malware. The dimension "Number of devices" refers to the number of devices leveraged to execute or resist cyber-attacks with or without their owners' consent. The dimension "Number of command and control servers" 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 compromised computers. The dimension "Number of downloadable instances of malware or anti-malware" refers to the number of software applications and resources used to exploit or defend against vulnerabilities in computer systems.

Sharing arrangements construct

The construct "Sharing arrangements" has three dimensions: arrangements to rent or purchase facility and customized services; arrangements to grow the facility; and arrangements to take order from authority. The dimension "Arrangement to rent or purchase facility and customized services" refers to agreements to derive financial benefits from the use of attack or defence infrastructures. The dimension "Grow the facility" refers to the arrangement to expand infrastructures to execute or resist cyber-attacks. There are at least three means to grow the shared facility: affordable customized products and services, hardware or software capacity upgrade, and network topology that provides control to the owner. The dimensions "Order from authority" refers to the arrangements made with one or more legal authorities to execute or resist botnet-enabled cyber-attacks. Individuals and groups leverage legal frameworks to remain anonymous, takedown botnets, and apprehend and prosecute those who cause botnet-related problems.

Salient Characteristics of Each Club Type

Table 2 provides the results of examining the information collected for the 10 scenarios, five of which focused on botnet-enabled cyber-attacks and five focused on botnet takedowns. For each club type, Table 2 provides the values of the eight dimensions of the three constructs that were extracted from the information collected from the scenarios. For example, for each of the five scenarios in the Type 1 (Attacker) club, the minimum number of individuals who were known to have carried out attacks were 5, 5, 6, 7, and 62. Therefore, the first cell in Table 2 shows the range 5–62. Similarly, the minimum number of organizations collaborating to resist each of these five botnet-enabled cyber-attacks were: 8, 8, 8, 9 and 10. Therefore, the range shown in the second row of Table 2 is 8–10. These results suggest that a Type 2 (Defender) club has at least eight organizations engaged in resisting botnet-enabled cyber-attacks.

The information on the five botnet-enabled cyber-attacks sampled scenarios presented in Table 2 suggests that an Internet-linked Attacker club that fits Club Type 1 (Attacker) is comprised of at least five individuals. Members of this club type assume at least four individual roles to execute cyber-attacks, access millions of compromised devices and downloadable malware programs, use a minimum of one command-and-control server, remain anonymous to evade arrest, use web markets to sell products and services, and grow the facilities members share through access to multiple low-cost customized malware variants.

Also, the five botnet-enabled cyber-attacks scenarios examined suggest that a club that fits Club Type 2 (Defender) club comprises at least eight organizations that act to resist a cyber-attack. These organizations operate in different sectors and countries. These organizations establish contractual agreements for product and service sales, grow their facility using hardware and software upgrades, and actively engage with legal authorities.

Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory

Olukayode Adegboyega

The information on the five botnet takedowns sampled scenarios in Table 2 suggests that a Type 3 (Botbeheader) club has at least three organizations engaged in a botnet takedown. These organizations are diverse in terms of operations, sectors, and countries, and they use tens of compromised devices and at least three command-and-control servers. Members of this club type engage in legal and contractual agreements for information sharing and grow the shared facilities via research and development as well as learning from observing information available in web markets.

The results of the five botnet takedown sampled scenarios shown in Table 2 show that the minimum number of members in a club that fits Type 4 (Botmaster) ranges from one to three. These results suggest that this type of club may exists with only one member. Therefore, not all clubs of this type may embody collective action. Members of a club that fits Club Type 4 (Botmaster) have access to at least 500,000 compromised devices, 600,000 downloadable malware programs, and at least one command-and-control server. These members rely on web markets for products and services sales, grow the shared facility using network topologies designed to make botnet takedown difficult, and remain anonymous to evade arrest.

Conclusions

This research applies club theory to examine the collective actions of individuals and groups organized for the purpose of executing or resisting botnet-enabled cyber-attacks and botnet takedowns. The representation developed takes the club theory perspective that collective action can best be understood using three constructs: club membership size; size of the facility that club members share; and arrangements to operate, purchase/rent and grow the shared facility. The representation identifies four Internet-linked club types (i.e., Attacker, Defender, Bottbeheader, and Botmaster) and the eight dimensions of the three constructs of club theory. The representation offered is expected to enhance knowledge on the inner working of the collective actions responsible for executing and resisting botnet-enabled cyber-attacks and botnet takedowns and thereby improves communications among individuals working to solve botnet related problems in heterogeneous organizations and expedite theory development.

Using club theory enhanced our understanding of the various types of Internet-linked clubs that execute and resist botnet-enabled cyber-attacks and botnet takedowns. At least three issues require further research. First, what are the specific learning-related benefits of sharing a botnet, a socio-technical system, a termination method, or a command-and-control server network? The author was not able to extract learning-related benefits from the information collected for the ten scenarios. Thus, answers to the following research questions should be found: How do clubs of the same type learn from one another? How do clubs of different types learn from one another? The author believes that answer to these questions may provide insight to the understanding of inherent motivation for forming and or joining an Internet-linked type of club.

The second area of research entails the study of congestion problems that prevent members of the clubs from deriving maximum benefits from the shared resources. It is surmised that congestion is different across the four club types. For example, congestion in Type 1 (Attacker) clubs may be related more to monetization of products and services in web markets whereas court orders may be causing congestion in Type 3 (Botbeheader) clubs.

The third area of research can focus on the study of the likely rivalry that exists within and among the four types of Internet-linked clubs to offer useful conclusions that can be used to address botnet-related problems.

About the Author

Olukayode Adegboyega holds an MASc degree in Technology Innovation Management (TIM) from Carleton University in Ottawa, Canada and a Bachelor in Electrical and Electronics Engineering from the Federal University of Technology in Akure, Nigeria. He has worked as an IP Network Service Engineer at LM Ericsson Nigeria Limited and as a Data Communication Network Engineer at Globacom Limited of Nigeria.

Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory

Olukayode Adegboyega

Table 2. Dimensions of three constructs and examples of their values for each club type

		Botnet-Enabled Cyber-Attacks		Botnet Takedowns	
Dimension		**Club Type 1 Attacker**	**Club Type 2 Defender**	**Club Type 3 Botbeheader**	**Club Type 4 Botmaster**
Minimum number	Individuals	5–62			1–3
	Organizations		8–10	3–8	
Diversity	Role	Developer operator, marketer, and accomplices			Operator
	Organization			Private, academic, and government organizations	
	Sector		Multiple sectors	Multiple sectors	
	Country		Multiple countries	Multiple countries	
Number of devices		50–millions	Tens	Tens	500,000–millions
Number of command-and-control servers		1–2		3–5	1
Number of instances of malware or anti-malware		50–millions	Tens	Tens	600,000–millions
Arrangements to rent or purchase facility and customized services		Web market for selling products and services	Contractual and legal agreements for products and services	Contractual and legal agreements for information sharing and botnet takedown	Web market for selling products and services
Arrangements to 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 command-and-control network topologies
Arrangements with legal authorities to execute or resist cyber-attacks		Anonymous to evade arrest	Order to arrest and prosecute culprits	Order to takedown botnet, arrest and prosecute culprits	Anonymous to evade arrest

Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory

Olukayode Adegboyega

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. http://dx.doi.org/10.1080/07036330500367366

APEC. 2008. *Guide on Policy and Technical Approaches against Botnet.* Singapore: Asia-Pacific Economic Cooperation (APEC) Secretariat. http://www.mtc.gob.pe/portal/apectel38/spsg/08_tel38_spsg_012rev1_botnet-guide-version6-4.pdf

Asvanund, A., Krishnan, R., Smith, M. D., & Telang, R. 2004. *Interest-Based Self-Organizing Peer-to-Peer Networks: A Club Economics Approach.* Working Paper: September 2004. Pittsburgh, PA: Carnegie Mellon University. http://dx.doi.org/10.2139/ssrn.585345

Bergias, D., & Pines, D. 1981. Clubs, Local Public Goods and Transportation Models. *Journal of Public Economics,* 15(1): 141–162. http://dx.doi.org/10.1016/0047-2727(81)90030-X

Buchanan, J. M. 1965. An Economic Theory of Clubs. *Economica,* 32(125): 1–14. http://www.jstor.org/stable/2552442

Cheng, J. 2014. Raising the Stakes: NATO Says a Cyber-Attack on One is an Attack on All. *Defense Systems,* September 8, 2014. Accessed June 1, 2015: http://defensesystems.com/Articles/2014/09/08/NATO-cyber-attack-collective-response.aspx

Cremonini, M., & Riccardi, M. 2009. The Dorothy Project: An Open Botnet Analysis Framework for Automatic Tracking and Activity Visualization. *2009 European Conference on Computer Network Defense (EC2ND):* 52–54. http://dx.doi.org/10.1109/EC2ND.2009.15

Crosson, S., Orbell, J., & Arrow, H. 2004. 'Social Poker': A Laboratory Test of Predictions From Club Theory. *Rationality and Society,* 16(2): 225–248. http://dx.doi.org/10.1177/1043463104039878

Czosseck, C., Klein, G., & Leder, F. 2011. On the Arms Race Around Botnets – Setting Up and Taking Down Botnets. *2011 3rd International Conference on Cyber Conflict (ICCC):* 1–14.

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 (LEET 2012):* 6. Berkeley, CA: USENIX Association.

Drury, J., Evripidou, A., & Van Zomeren, M. 2014. The Intersection of Identity and Power in Collective Action. In D. Sindic, M. Barreto, & R. Costa Lopes (Eds.), *Power and Identity:* 94–116. Hove, UK: Psychology Press.

Gallagher, H., McMahon, W., & Morrow, R. 2014. Cyber-Security: Protecting the Resilience of Canada's Financial System. *Bank of Canada: Financial System Review,* December 10, 2014. Accessed June 1, 2015: http://www.bankofcanada.ca/2014/12/fsr-december-2014/

Glazer, A., Niskanem, E., & Scotchmer, S. 1997. On the Uses of Club Theory: Preface to the Club Theory Symposium. *Journal of Public Economics,* 65(1): 3–7. http://dx.doi.org/10.1016/S0047-2727(97)00002-9

Grabosky, P. 2014. *Organized Crime and National Security.* RegNet Working Paper, No. 40, Canberra, Australia: Regulatory Institutions Network. http://dx.doi.org/10.2139/ssrn.2464377

Hofmokl, J. 2010. The Internet Commons: Towards an Eclectic Theoretical Framework. I*nternational 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. http://dx.doi.org/10.1109/SURV.2013.091213.00134

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.

Li, Z., Liao, Q., & Striegel, A. 2009. Botnet Economics: Uncertainty Matters. In E. Johnson (Ed.), *Managing Information Risk and the Economics of Security:* 245–267. New York: Springer. http://dx.doi.org/10.1007/978-0-387-09762-6_12

McGuire, M. 1972. Private Good Clubs and Public Good Clubs: Economic Models of Group Formation. *The Swedish Journal of Economics,* 74(1): 84–99. http://www.jstor.org/stable/3439011

Medin, F., Andres, J., Antonio, G. L., & Jesus, L. R. 2010. International Organizations and the Theory of Clubs. *Revista de Metodos Cuantitativos Para La Economia Y La Empresa,* 9(1): 17–27.

Nadji, Y., Antonakakis, M., Perdisci, R., Dagon, D., & Lee, W. 2013. Beheading Hydras: Performing Effective Botnet Takedowns. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security:* 121–132. New York, NY: Association for Computing Machinery. http://dx.doi.org/10.1145/2508859.2516749

Postmes, T., & Brunsting, S. 2002. Collective Action in the Age of the Internet: Mass Communication and Online Mobilization. *Social Science Computer Review,* 20(3): 290–301. http://dx.doi.org/10.1177/089443930202000306

Raymond, M. 2013. Puncturing the Myth of the Internet as a Commons. *Georgetown Journal International Affairs,* Special issue on International Engagement on Cyber III: State Building on a New Frontier, December 23*, 2013:* 53–64.

Sandler, T., & Tschirhart, J. T. 1980. The Economic Theory of Clubs: An Evaluative Survey. *Journal of Economic Literature,* 18(4):1481–1521. http://www.jstor.org/stable/2724059

Sandler, T., & Tschirhart, J. T. 1997. Club Theory: Thirty Years Later. *Public Choice,* 93(1): 335–355. http://dx.doi.org/10.1023/A:1017952723093

Schelling, T. C. 1969. Models of Segregation. *The American Economic Review,* 59(2): 488–493. http://www.jstor.org/stable/1823701

Schmidt, A. 2012. The Estonian Cyberattacks. In J. Healey (Ed.), *The Fierce Domain – Conflicts in Cyberspace 1986-2012.* Washington, DC: Atlantic Council.

Shi, Y., Lau, F. C. M., Tse, S. S. H., Du, Z., Tang, R., & Li, S. 2006. Club Theory of the Grid. *Concurrency Computation,* 18(1):1759–1773. http://dx.doi.org/10.1002/cpe.1027

Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory

Olukayode Adegboyega

Shirazi, R. 2015. Botnet Takedown Initiatives: A Taxonomy and Performance Model. *Technology Innovation Management Review,* 5(1): 15–20. http://timreview.ca/article/862

Stone-Gross, B., Holz, T., Stringhini, G., & Vigna, G. 2011. The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-scale Spam Campaigns. In *LEET '11 Proceedings of the 4th USENIX Workshop on Large-Scale Exploits and Emergent Threats.*

Sully, M., & Thompson, M. 2010. *The Deconstruction of the Mariposa Botnet.* Ottawa: Defence Intelligence. http://defintel.com/docs/Mariposa_White_Paper.pdf

Thiedig, F., & Sylvander, B. 2000. Welcome to the Club? - An Economical Approach to Geographical Indications in the European Union. *Agrarwirtschaft,* 49(12): 428–437.

White, T. E. 1952. Observations on the Butchering Technique of Some Aboriginal Peoples: I. *American Antiquity,* 337–338.

Whitehouse, S. 2014. Opening Statement. In *Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks.* Washington, DC: U.S. Senate Judiciary Subcommittee on Crime and Terrorism. https://www.hsdl.org/?view&did=756247

Yahyazadeh, M., & Abadi, M. 2015. BotGrab: A Negative Reputation System for Botnet Detection. *Computers & Electrical Engineering,* 41(January): 68–85. http://dx.doi.org/10.1016/j.compeleceng.2014.10.010

Citation: Adegboyega, O. 2015. Representing Botnet-Enabled Cyber-Attacks and Botnet Takedowns Using Club Theory. *Technology Innovation Management Review,* 5(6): 35–44. http://timreview.ca/article/905

Keywords: botnet, botmaster, botnet takedown, cyber-attack, cybersecurity, collective action