Time-to-event Modeling for Predicting Hacker IRC Community Participant Trajectory

Victor Benjamin, Hsinchun Chen
Department of Management Information Systems
The University of Arizona
Tucson, AZ 85721, USA
vabenji@email.arizona.edu, hchen@eller.arizona.edu

***Abstract*— As computing and communication technologies become ubiquitous throughout society, researchers and practitioners have become motivated to advance current cybersecurity capabilities. In particular, research on the human element behind cybercrime would offer new knowledge on securing cyberspace against those with malicious intent. Past work documents the existence of many hacker communities with participants sharing various cybercriminal assets and knowledge. However, participants vary in expertise, with some possessing only passing curiosity while others are capable cybercriminals. Here we develop a time-to-event based approach for assessing the relationship between various participation behaviors and participation length among hacker Internet Relay Chat (IRC) community participants. Using both the Kaplan-Meier model and Cox's model, we are able to develop predictions on individuals' participation trajectory based on a series of message content and social network features. Results indicate that participation volume, discussion of pertinent topics, and social interconnectedness are all important at varying levels for identifying participants within hacker communities that have potential to become adept cybercriminals.**

Keywords - Cybersecurity; Hacker community; Hacker IRC; Time-to-event; Survival Analysis

I. INTRODUCTION

Over the past decade a growing amount of critical infrastructures have begun to rely on computer and information technologies in order to meet increasingly complex demands. While use of technology has helped achieve more advanced capabilities within infrastructure, an unfortunate consequence is that many of such systems are facing growing exposure and risk to cyber-attack. To further exacerbate the issue, advancing technologies are enabling hackers to commit cybercrime at a much greater scale now than in the past. The sheer number of emerging security threats necessitates further research and development for mitigating risk and exposure to vulnerabilities. As a result, researchers and practitioners have taken an increased interest in advancing current cybersecurity capabilities.

Traditional research in the security domain has often focused on improving security built directly into computing and networking [1]. Often times this stream of research focuses scrutiny on vulnerabilities at the protocol and system levels, where incremental advancements can be made in order to thwart existing security threats. Conversely, very little work has been done to go beyond technological issues and instead focus investigation on the human element behind cybercrime. For example, much is unknown concerning hacker behaviors, the cybercriminal supply chain, underground hacker communities, etc. Specifically, the development of methods to model cyber adversaries is one of the critical but unfulfilled research need outlined in a 2011 report on cybersecurity by the National Science and Technology Council [2]. More research on "black hat hackers", i.e. cybercriminals, would offer new knowledge on securing cyberspace against those with malicious intent, leading to the development of more effective countermeasures against security threats.

Despite the lack of studies focused on hacker communities, the value of such data has already been demonstrated in real world applications. Recently published news reports detailed how observation of hacker Internet-Relay-Chat (IRC) communities provided actionable intelligence to cybersecurity professionals and government analysts [3]. Observation of hacker IRC data helped uncover cybercriminal operations in motion, allowing for proactive preparation against imminent cyber-attack. In particular, analysts were able to identify botnet operators, track the spread of malicious tools and malware, and identified key community participants that were involved in multiple illicit activities.

However, not all hacker community participants are dangerous cybercriminals; some may participate in hacker communities out of passing interests or curiosity. As researchers and practitioners begin to more closely monitor active hacker communities, it becomes important to possess capabilities for accurately identifying potential cyber adversaries from more benign participants. Thus, we are motivated to develop a method to assess hacker community participants in order to support identification of potential cyber adversaries from more benign hacker community participants. Such capability would be of great value to security researchers and practitioners as it would enable for quick identification of potentially dangerous or risky hacker community participants.

II. LITERATURE REVIEW

To form the basis for this research, literature is reviewed from three relevant areas. First, we review previous hacker community research for better contextual understanding. In particular, studies observing the contents and social interactions within hacker communities will be of use for identifying research gaps. Next, we review literature concerning virtual community participation. This research stream will provide us with direction for operationalizing a research design to study participation behaviors in hacker communities. Lastly, we look to past research in time-to-event modeling as it is useful for developing temporal analyses of data. As its name suggests, time-to-event modeling is useful for understanding how data changes leading up to a particular event; for example, time-to-event modeling can be used to better understand why an individual suddenly stops participating within a virtual community.

A. Hacker Community Research

While cyber security research has had consistent progress in past years, much prior work has focused on technical problems such as improving protocol, network, and system security. While this work is important to preserving the integrity of our computing systems, the contributions of such research are generally limited to more reactive solutions in mitigating security risk and recovering from cyber-attack. It is only within recent years that more attention has begun to be paid towards the human element behind cybercrime, providing researchers with knowledge of hacker operating behaviors, the cybercriminal supply chain, emerging threats, etc. The contributions of this research stream are in improving proactive cybersecurity capabilities through new methodologies for understanding hackers and emerging threats in the wild.

As hacking knowledge is not typically found in formal education, the use of web-based resources to advance skills and knowledge is common. In particular, past studies have identified hackers often congregate within underground online communities to share cybercriminal assets, hacking knowledge, and to find collaborators [4][5]. It is not uncommon for hacker community participants to share hyperlinks to other underground communities or even deep web hidden services, such as Tor network .onion files [6][7]. Thus, it is very feasible for an individual with little to no hacking skills to gain knowledge and capability by simply visiting different hacker communities and consuming their contents. Research identifies the existence of such hacker communities to be common across various geopolitical regions, including the US, China, Russia, the Middle-East, and other regions where information technologies are either ubiquitous or growing rapidly in use [5][6]. Thus, these communities and their participants make interesting candidates for further investigation.

It appears that the majority of hacking communities exist as either web forums or Internet Relay Chat (IRC) channels [4][8]. Methods to identify and collect such communities can be borrowed from previous studies. The major identification techniques used in hacker community research appear to revolve around keyword searches and scrutinizing known communities for hyperlinks and references to other potential hacker communities [9][10]. After community identification, several procedures can be taken to collect data. As forums are based on webpages, traditional web crawling techniques may be taken to collect community contents [11]. Anti-crawling measures are sometimes employed by hacker web forums, which may need to be circumvented through controlling crawling behaviors, using proxy servers, etc. Conversely, IRC channels exist within their own protocol and are not webpage-based communities. Instead of using a web crawler to collect data, automated bots are configured to utilize the IRC protocol and sit within IRC channels to capture data in real-time [9].

The majority of current hacker community work scrutinizes forum data rather than IRC channel data. This may be due to easier accessibility of webpage-based communities when compared to IRC communities. Additionally, forums act as natural archives of data and can be indexed by search engines, while IRC data can only be viewed at real-time, is not commonly archived, and is not indexed by any popular search engines. Forum-based studies often highlight the common sharing of cybercriminal assets among community participants, and point out that such behavior is consistent in hacker communities across various geopolitical regions [4][5]. Reputable hackers also may more closely collaborate or even conduct in black market transactions [6]. Such results indicate that forums act as hubs for hackers to exchange assets and knowledge; continued research in this area will potentially provide greater understanding of hacker behaviors across geopolitical regions, information regarding the cybercriminal supply chain, growing threats, etc. A sample of such contents can be seen in Figure 1, where a channel participants shares a hyperlink to the deep web hidden service "Silk Road" where drugs, stolen financial information, and other illegal goods can be purchased.

Unfortunately, considerably less work has been performed on IRC data, perhaps due to challenges and unfamiliarity with IRC identification and collection. The little work that has been done identifies cybercriminal activity occurring within hacker IRC channels, including asset sharing and black market transactions, similar to observations made in hacker forum research [4][8]. It seems surprising that is a lack of hacker IRC studies, as researchers could capture conversations between participants in real-time, lending to new interesting analyses. Participants would have more frequent, continuous interactions within IRC-based communities, as opposed to the more lengthy response times experienced with web forums. IRC channels also frequently support dozens of users participating simultaneously about the same topics, whereas the number of participants within any forum thread is generally smaller.

Given the results of forum research, it appears pertinent to observe IRC channels for hacker contributions and usage behaviors. Thus, it is worthwhile to explore past research on virtual community participation to understand more about the significance of different participation behaviors.

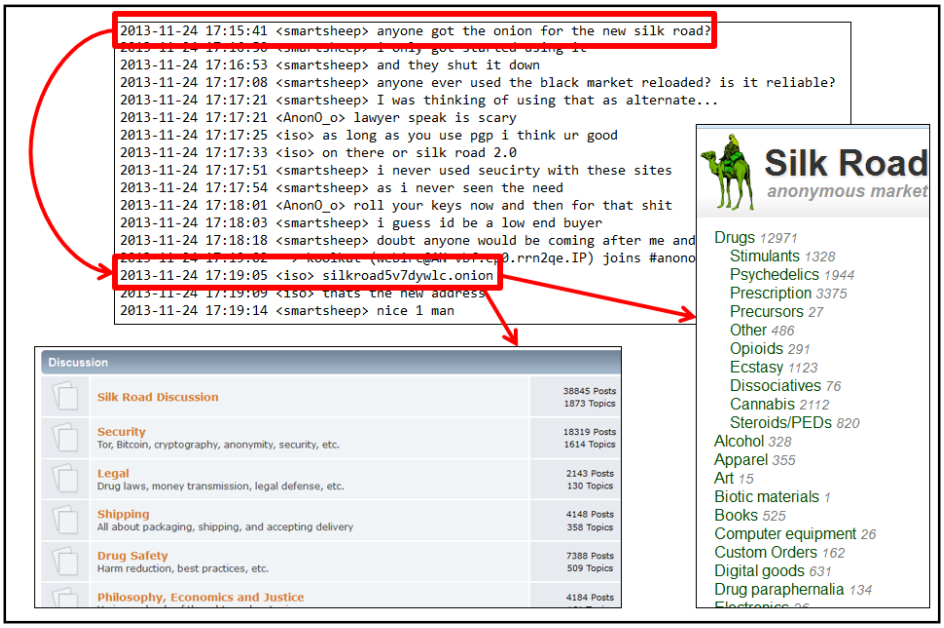

Figure 1 - A user in the IRC channel #anonops on server irc.anonops.org asks if any other participants have the URL to the underground black market Silk Road, which was temporarily taken offline by authorities in October, 2013. Another IRC participants responds with a .onion link which leads to the Silk Road forum and new website. This type of asset sharing is common in hacker communities.

B. Virtual Community Participation

With the advent of web 2.0, researchers became interested in closely examining the behaviors of individuals in virtual settings. In particular, many works have investigated virtual community usage and participation behaviors. This stream of research has grown and yielded many interesting findings relevant to explaining virtual community participation. Such findings can be used to motivate hacker community research design.

Past studies scrutinizing virtual community data do so through both manual and automated methods for analyses. Many researchers make use of traditional methodologies rooted in social and behavioral sciences. First, surveys are frequently used to gather information directly from virtual community participants [12][13][14]. Typically, community participants are sampled at random or through other statistical means depending on context. Surveys are created and sent to selected participants in order to measure various constructs related to virtual community participation. Surveys are especially useful for measuring items not directly observable in data, e.g. computer self-efficacy. Another popular methodology involves field studies or observations of virtual community participants during their normal usage [10][15]. Such analyses produce interesting results because, unlike surveys, there is little to no researcher influence on the subjects of study. However, manual techniques may sometimes be limited in their ability to scale to larger datasets, such as those used in temporal studies or when observing multiple communities simultaneously. Automated analyses are more appropriate in such contexts.

Automated Analyses have been used by researchers to successfully conduct complex statistical analyses of large virtual community datasets. Many text-, content-, and network-based features can be extracted from each participant message to conduct analysis on [16][17]. Such features can be scrutinized through various statistical tests to produce knowledge about topical relevance, user sentiment, etc. [18].Text features can be used in machine learning techniques and methods borrowed from computational linguistics to better understand participant discussions [17].

Other researchers use automated techniques to observe the structure of social networks found within virtual communities. Network "ties" or connections between "nodes" or users are mapped to better understand community structure [19]. Network ties may be built off of direct addressing between users, topical relevance, time between user responses, etc.[19][20]. In the context of IRC, previous researchers have successfully built network ties based direct addressing between users [21]. Researchers commonly utilize such content and network analyses to generate powerful descriptive information and predictions concerning virtual communities and their participants. However, in order to conduct longitudinal studies or temporal analyses that account for the evolution of virtual communities over time, it is necessary to extend such techniques into more advanced statistical analyses. Time-to-event modeling is commonly used for such purposes [19][22].

C. Time-to-event Modeling

Time-to-event modeling, also commonly referred to as "survival analysis", is useful for modeling of data that involves prediction of an event at a given point of time. Specifically, we can use time-to-event modeling to understand why a specific event occurs relative to time and other researcher-defined characteristics. This technique is often used in medical & health domains; for example, can be used to predict when patient hospitalization may occur given age, weight, smoking habits, etc. [23]. In the virtual community context, time-to-event modeling has been used to better understand virtual community participation behaviors, including member retention in online health support groups and tenure of volunteer Wikipedia editors [19][24].

In time-to-event modeling, the dependent variable is time, or specifically, the duration that it takes until an event happens. Other variables include:

- *Event variable* - Whether a specified event occurs to a particular record within the dataset (e.g., a patient experiences hospitalization in a longitudinal study on patient hospitalization rates)
- *Censor variable* – A censor variable is assigned when a particular record within the dataset never experiences the event or otherwise prematurely drops out of the study before the end of data collection (e.g., a patient that experiences no side-effects for the entire duration of a clinical trial for a new pharmaceutical, or one who drops out of the clinical trial before it is over)
- *Hazard rate* – Probability that the event will happen given the amount of time passed where the event has not occurred

Two specific time-to-event modeling techniques stand out as the most commonly utilized models [22][25]. The first of the two models, the Kaplan-Meier model, is used to calculate the "survival function" for a given set of data. The survival function is simply a calculation of the probability that a particular dataset record t will, on average, "survive" S until a specified time variable T. In this case, surviving implies that that a record will not experience the defined event until T.

$$Survival\ Function = S(t) = 1 - F(t)$$

The Kaplan-Meier model is useful for producing descriptive information about how long a specific record within the dataset will exist without experiencing the defined event. The model is a decreasing step-function that maps survival probability against time. However, while the Kaplan-Meier model helps formulate generalized perspective concerning the tested dataset, it fails to describe underlying reasons that explain the survival function's shape.

The second model is Cox's proportional hazards model, which is useful for filling providing explanations as to what features are significantly influencing a given survival model [25]. Cox's model is a natural complement to the Kaplan-Meier model, as it allows for the inclusion of various independent variables that may help explain a given survival function; the Kaplan-Meier model provides a generalized understanding of data, while Cox's model describes which specific features positively and negatively affect survival time. To further elaborate, Kaplan-Meier is useful for exploration of data while Cox's model is useful for deeper understanding. Cox's model can be seen below, where $\lambda(t, X)$ is the hazard at time t, $\lambda_0(t)$ is an arbitrary baseline hazard function, and $\boldsymbol{X}$ is a matrix containing explanatory/independent variables.

$$Cox's\ Model = \lambda(t, X) = \lambda_0(t)exp(\beta X)$$

After formulation, the model is used within a regression framework in order to evaluate the effect of various independent, explanatory variables and hazard [26]. Thus, Cox's model can be utilized in attempt to help explain why virtual community participants are active for different lengths of time, and what factors influence petrifaction length. In the context of our study, the model may be useful for assessing differences in hacker IRC channel participation.

III. Research Gaps and Questions

While there is much work investigating participant behaviors in hacker forums, little attention has been paid towards IRC channels. Although literature documents that hackers actively use IRC channels to support cybercriminal activity, most researchers have conducted analyses on web forum data, perhaps due to familiarity and accessibility of forums over IRC. By further investigating the role of IRC channels, we may develop a deeper understanding of the global hacker community through identifying new hacker social behaviors, tracking the cybercriminal supply chain, developing new methods to model cyber adversaries, etc. Thus, we are motivated to investigate the underlying differences of user participation behaviors within hacker IRC channels, and ask the following questions:

- What factors may positively or negatively impact a hacker's participation level within IRC channels?
- Can we develop a model to accurately predict a hacker's participation behavior within IRC channels?

IV. Research Testbed and Design

Our research design (Figure 2) consists of a series of steps involving automated data processing and analysis. First, we identify and collect hacker IRC channels. Next, we process collected data into a form ready for analysis. We then construct our models and execute experiments. Finally, experiment results are evaluated and conclusions are drawn based on our findings.

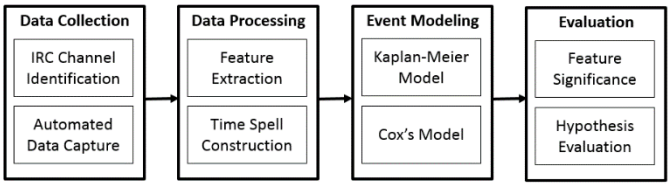

Figure 2 – Research Design

Similar to previous hacker community research, we utilize keyword searches to identify potential hacker IRC channels, e.g. "Carding chat server" and "blackhat irc". After identification, we deployed automated IRC chat logging bots were deployed to identified IRC channels. Multiple bots issued from various hosts to ensure collection and to avoid gaps in data from dropped connections, bans, etc. We also practiced identity obfuscation by routing Internet traffic generated by our collectors through the Tor peer-to-peer anonymization network. We observed captured data and selected our most popular IRC channel for this research; a summary of the data can be viewed in Table I.

TABLE I. RESEARCH TESTBED

Server	Channel	# of Users	# of Messages	Start Date	End Date
irc.anonops.org	#anonops	2,005	125,308	11/20/13	5/11/14

The #anonops community is particularly interesting due to its relevance to the *Anonymous* hacking community. *Anonymous* has been commonly referred to as a collective of hacktivists that regularly disrupt web-enabled resources for a variety of societal or political causes. *Anonymous* makes use of IRC, with the #anonops community being the particular target of a prior government investigation [3].

After IRC chat data is collected, we performed a round of data pre-processing in order to prepare for our analysis. First, we extracted usernames, message dates, and message contents for each record captured by our IRC collector. We limit our analysis to users who have participated in the #anonops channel on at least two different dates in order to restrict skewing data by excluding those who log into the channel only once, potentially out of curiosity or passing interest. This restriction helps us focus the experiment on users who participate over time. To operationalize our time-to-event models, we splice our data into 13 separate time spells based on the172 days (~6 months) of data we captured. This amounts to two-week intervals per time period. Finally, several explanatory features based on prior literature are extracted from IRC chat data. These features can be seen in Table II.

The features in Table II were identified based on our literature. Each feature was a described in previous hacker community research and virtual community research. We compiled term dictionaries based on suggestions in past studies as well as our own manual observation of data. All features were extracted using automated scripts that sifted through our collection.

The last two features we create are our 'event' and 'censor' features necessary for time-to-event modeling. As we are attempting to identify potential hackers from benign participants, it may be useful to consider participation length. Individuals with passing interests may only remain active in the community for a short period of time. Conversely, those with cybercriminal intentions may remain active within underground hacking communities for longer lengths of time. Thus, it is convenient to define our 'event' as dropping out of community participation. In other words, "survival" in our model would describe continued participation within the #anonops community. While it is possible for community participants who are assigned event variables to later start participating again within the #anonops community, this possibility falls outside the scope of the Cox model and it is assumed that community participants do not return [26]. Conversely, failure/mortality would occur when an individual stops participating in the community. To operationalize the event (halting participation), we assume anyone who has not participated in the most recent time spell as no longer active within the #anonops community. Further, for individuals that do participate in the most recent time spell, we assign them the censor variable. Such individuals are assumed to continue participation within the #anonops community as we have no data of these individuals halting participation, and are thus assigned censor variables. This method of assigning censor variables is consistent with previous studies that do not observe an event for a set of records within recorded data [19][22]. This pair of variables allow us to calculate our community's survival curve, as well as to test the explanatory power of each identified feature.

After features are extracted per user, we organize our data into a matrix for use with the Kaplan Meier and Cox's models. We first execute the Kaplan-Meier model to gain generalized perspective of the IRC channel population's survival curve. The Kaplan-Meier model is particularly useful for providing a "big picture" perspective in terms of survival probability, and will help us understand the typical participant's behavior within our selected IRC channel. We then utilize the Cox's proportional hazards model to test the explanatory power of the various extracted content and network features. The Cox model would help us identify behavior differences among participant behaviors that would result in different magnitudes of participation.

TABLE II. EXTRACTED FEATURES

Category	Feature	Description	Source
Content Features	Total Message Volume	Message volume is a commonly used indicator of participation rate, especially in the IRC context.	Motoyama et al, 2011; Benjamn & Chen, 2012
	Total Hacking Terms Used	Demonstrates hacking proficiency, which may indicate increased participation; Examples: Rootkit, XSS, SQL Injection, DDoS, shellcode, PoC	Holt & Lampke, 2010; Benjamn & Chen, 2012
	Total Technical Terms Used	Demonstrates technical proficiency, which may indicate increased participation; Examples: SQL, C++, ASM, .Net, XML	Holt & Lampke, 2010; Benjamn & Chen, 2012

	Total Black Market Terms Used	Demonstrates market activity, perhaps indicating to increased participation for black market purposes Examples: SQL, C++, ASM, .Net, XML	Radianti et al, 2009; Holt & Kilger, 2012
	Hyperlinks Shared	Sharing of cybercriminal or technical resources, knowledge, or other information pertinent to community participants. May indicate to greater investment of time and participation.	Radianti, 2010; Benjamin & Chen, 2012
	Deep Web Hidden Services Shared	Sharing of deep web hidden services, pertinent to community participants. May indicate to greater investment of time and participation.	Martin, 2013
Social Network Features	Total Direct Addresses	Direct addressing is common in IRC channels and is an indicator of network ties. Individuals that commonly direct address others may feel interconnected and participate often.	Garas et al, 2012; Sinha & Rajasingh , 2014
	Total Times Addressed Directly	Similarly, being addressed directly may increase feelings of interconnectedness within a network and lead to increased participation	Garas et al, 2012; Sinha & Rajasingh , 2014
	Total Different Individuals Directly Addressed	We also consider the total number of unique individuals addressed, helping measure the total social interconnectedness of each participant in our channel	Garas et al, 2012; Sinha & Rajasingh , 2014
	Total Times Directly Addressed by Different Individuals	The total number of times directly addressed by different individuals indicates the in-degree of social interconnectedness, which may lead to increased participation	Garas et al, 2012; Sinha & Rajasingh , 2014

V. HYPOTHESES

Based on our extracted features, we posit a set of hypotheses relevant to our analysis. We have extracted a number of content-based features at the participant-level, as such features have been described as possessing explanatory power over hacker behavior in previous works.

H1: Content features will help differentiate between users with passing interest and those that are more vested in the hacker community.

Similarly, network-based features have been successfully used in previous virtual community participation research. Social network features can help reveal interconnectedness and usage behavior of individual participants.

H2: Network features will help differentiate between users with passing interest and those that are more vested in the hacker community.

Finally, we believe that time-to-event modeling can make use of extracted features to provide us with predictive power in assessing participation trajectories of different users in the #anonops community.

H3: The Cox's proportional hazards model will provide us with deeper understanding of how to differentiate between users with passing interest and those that are more vested in the hacker community.

VI. RESULTS AND DISCUSSION

We first apply the Kaplan-Meier model to our data in order to produce a matrix containing information on hazard and survival rates per time period. The information from this matrix can be used to quickly explore and understand the average survival trend within our data. A sample of the outputted information can be viewed in Table III. We plot the outputted data and generate a survival curve useful for generalizing #anonops participant activity, helping us understand the relationship between survival and time spent in the community. The survival curve can be viewed in Figure 3.

TABLE III. KAPLAN-MEIER SURVIVAL TABLE

Time Period	Survival Rate	Std. Err	Lower 95% CI	Upper 95% CI
1	0.535	0.0247	0.489	0.586
2	0.516	0.0249	0.469	0.567
…	…	…	…	…
13	0.279	0.0266	0.232	0.337

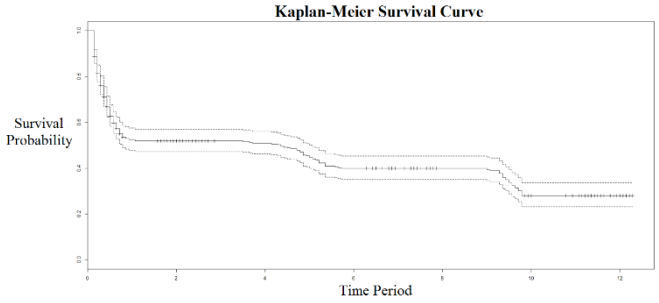

Figure 3– The displayed Kaplan-Meier Survival Curve provides a generalized picture of survival probability over time for the #anonops community.

From the Kaplan-Meier curve, we observe that 50% of our participants continue their participation after time spell 2, while only about 30% continue after time spell 10. One could deduce that the 30% of users that participate for at least 10 weeks are the most engrained within the hacking community, and thus are more likely to become potential cyber adversaries than their peers that participated for much shorter lengths of time. After

exploring our data with Kaplan-Meier model and producing a better understanding of the IRC channel's population curve, we seek to further our understanding of which explanatory variables are significantly impacting survival over time. We make use of the Cox's proportional hazard model to measure the effect of our explanatory variables in a statistically-grounded test. Results can be viewed in Table IV. To interpret a Cox model, we examine coefficients for each feature much like a regression. However, interpretation of Cox's model results is slightly unique; with the Cox's model, the presence of positive variable coefficients indicates that a particular variable contributes towards experiencing the modeled event in a shorter duration of time than normal. Conversely, a negative coefficient indicates a feature would promote a user to participate in the #anonops community for a longer amount of time than normal. The Cox model would help us identify behavior differences among users that would result in different degrees of participation.

TABLE IV. COX'S MODEL RESULTS – FEATURE COEFFICIENTS

Feature	Coef	P-Value
Messages	-0.0596	< 2e-16 ***
HackTerms	0.05653	0.20152
TechTerms	-0.0991	0.00959 **
MarketTerms	-0.4754	0.57127
Hyperlinks	0.0030	0.61536
HiddenServices	-0.5681	0.42637
DirectAddressOut	0.0001	0.88969
DirectAddressIn	0.0005	0.88167
UniqueAddressOut	-0.06369	1.36e-09 ***
UniqueAddressIn	0.0080	0.47754

'***' <0.01 ** <0.05; $R^2 = 0.4193$

Regression coefficients can be converted to "hazard ratios" which provide some information regarding effects of explanatory variables. To do this, one can simply take *e* (approx. 2.718) and raise it to the power of the coefficient. While hazard ratios does not explain the absolute effect of each variable, they are useful for providing understanding of how the variables interact against each other. The conversion between coefficient and hazard ratio results in two outcomes: variables with negative regression coefficients are assigned hazard ratios less than 1.0, while variables with positive coefficients are assigned hazard ratios greater than 1.0. These ratios are often helpful in providing an easier to interpret summary of variable interactions as represented by a Cox's model. We present the hazard ratios for our significant features in Table V.

TABLE V. COX'S MODEL RESULTS – HAZARD RATIOS

Feature	Exp(Coef)	Lower .95	Upper .95
Messages	0.5505	0.5308	0.5835
TechTerms	0.9057	0.8703	0.9462
UniqueAddressOut	0.9383	0.9192	0.9614

The displayed hazard ratios quickly summarize the impact of each feature on survival. Note that each ratio is below 1.0. This is signifying that each feature in Table V may extend a particular user's survival time within the #anonops community.

After observing the results of our model, it appears that there are a few key indicators that can help with predicting participation length of hacker IRC users. First, higher-levels of message contribution is an indicator that a particular IRC user will continue using hacker IRC services for longer than other participants who contribute less frequently, supporting H1. Next, individuals marked by higher levels of active technical discussion are more likely to continue using hacker IRC services for long periods of time. Such individuals may be able to share and exchange knowledge with other community participants, finding value in increased participation length, supporting H1. Further, participants who directly address a number of unique individuals are characterized by longer periods of active participation. It may be that such individuals are increasing their social interconnectedness by taking the time to engage numerous individuals in conversations, and thus increasing their length of stay in the #anonops community, supporting H2. Overall, the Cox's proportional hazards model provides us with deeper insight of the relationship between participation length and participation behaviors, supporting H3.

To our surprise, discussion of hacking and black market activities were not significant influencers of participation time. It may be that more illicit conversations are held through private messages between members, and public chat involves more benign discussion of technology. Analysis of additional IRC channels can assist with investigation of whether such behavior is standard among hacker IRC communities, or unique to the #anonops community. Additional analyses will also help reveal trends of significance among other variables tested in our model. This experiment, and further similar investigations, help contribute to our understanding of hacker community participation behaviors. With additional testing and model validation, cybersecurity researchers and practitioners could use the results of this research to better predict the trajectory of hacker IRC users; that is, to understand why some hacker IRC participants become engrained within their community, while others lose interest more quickly. With this capability, researchers and practitioners could study hacker community participants and predict which participants may become potential cyber adversaries.

VII. CONCLUSION AND CONTRIBUTIONS

In this research, we attempt to explain differences in hacker IRC participation length based on user behaviors. We operationalized this research by extracting hacker IRC channel user participation behaviors, incorporating features in time-to-event models in order to measure explanatory power of features over user participation. Results indicated that participation volume, discussion of pertinent topics, and social interconnectedness were all important features at varying levels.

Future work can expand in multiple directions to extend this research and advance our understanding. More advanced models can be used to more greatly scrutinize the relationship between time and our explanatory variables. For example, the extended Cox's model can provide greater time granularity than the version of the model used in this research. Additional hacker IRC channels, or even forums, can be analyzed to observe participation trends across multiple hacker communities.

Our method provides explanatory power that enables prediction of user trajectory within hacker IRC communities, and can help with prediction of which users will participate on a long-term basis. This research is of great asset to cybersecurity researchers and practitioners seeking to identify key participants of a given hacker community. This work also contributes to greater understanding of contents within hacker IRC communities.

ACKNOWLEDGEMENT

This work was supported by the National Science Foundation under Grant No. SES-1314631 and also under Grant No. DUE-1303362.

REFERENCES

[1] Holt, T. J., & Kilger, M. (2012). Know Your Enemy : The Social Dynamics of Hacking. *The Honeynet Project*, 1–17.

[2] National Science and Technology Council (2011). *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program* (pp. 1–19).

[3] Schone, M., Esposito, R., Cole, M., & Greenwald, G. (2014). *War on Anonymous: British Spies Attacked Hackers.* National Broadcasting Company (NBC). http://www.nbcnews.com/news/investigations/war-anonymous-british-spies-attacked-hackers-snowden-docs-show-n21361

[4] Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). An analysis of underground forums. *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference - IMC '11*, 71.

[5] Benjamin, V., & Chen, H. (2012). Securing Cyberspace : Identifying Key Actors in Hacker Communities. *IEEE Intelligence and Security Informatics*, 24–29.

[6] Holt, T. J., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the Social Networks of Malware Writers and Hackers. *International Journal of Cyber Criminology*, *6*(1), 891–903.

[7] Martin, J. (2013). Lost on the Silk Road: Online drug distribution and the "cryptomarket." *Criminology and Criminal Justice*.

[8] Radianti, J. (2010). A Study of a Social Behavior inside the Online Black Markets. *2010 Fourth International Conference on Emerging Security Information, Systems and Technologies*, 88–92.

[9] Fallmann, H., Wondracek, G., & Platzer, C. (2010). Covertly Probing Underground Economy Marketplaces. *Proceedings of the 7th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)*, 101–110.

[10] Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. *Criminal Justice Studies: A Critical Journal of Crime, Law, and Society*, *23*(1), 33–50.

[11] Benjamin, V. A., & Chen, H. (2013). Machine Learning for Attack Vector Identification in Malicious Source Code. *IEEE Intelligence and Security Informatics*, 21–23.

[12] Abfalter, D., Zaglia, M. E., & Mueller, J. (2012). Sense of virtual community: A follow up on its measurement. *Computers in Human Behavior*, *28*(2), 400–404.

[13] Sun, Y., Fang, Y., & Lim, K. H. (2012). Understanding sustained participation in transactional virtual communities. *Decision Support Systems*, *53*(1), 12–22.

[14] Wang, H., Chung, J. E., Park, N., McLaughlin, M. L., & Fulk, J. (2011). Understanding Online Community Participation: A Technology Acceptance Perspective. *Communication Research*, *39*(6), 781–801.

[15] Onds, I. N. B., Ren, Y., Harper, F. M., Drenner, S., Terveen, L., Kiesler, S. Kraut, R. E. (2012). Building Member Attachment in Online Communities: Applying Theories of Group Identity and Interpersonal Bonds. *MIS Quarterly*, *36*(3), 841–864.

[16] Abbasi, A., & Chen, H. (2008). CyberGate: A Design Framework and System for Text Analysis of Computer-Mediated Communication. *MIS Quarterly*, *32*(4), 811–837.

[17] Liu, X., & Chen, H. (2013). AZDrugMiner : An Information Extraction System for Mining Patient-Reported Adverse Drug Events. In *Smart Health* (pp. 134–150). Springer Berlin Heidelberg.

[18] Garas, A., Garcia, D., Skowron, M., & Schweitzer, F. (2012). Emotional persistence in online chatting communities. *Scientific Reports*, *2*, 1–34.

[19] Zhang, Q., Wang, F.-Y., Zeng, D., & Wang, T. (2012). Understanding crowd-powered search groups: a social network perspective. *PloS One*, *7*(6), e39749.

[20] Garas, A., Garcia, D., Skowron, M., & Schweitzer, F. (2012). Emotional persistence in online chatting communities. *Scientific Reports*, *2*, 1–34.

[21] Sinha, T., & Rajasingh, I. (2014). Investigating substructures in goal oriented online communities: Case study of Ubuntu IRC. *2014 IEEE International Advance Computing Conference (IACC)*, 916–922.

[22] Wang, Y., Kraut, R., & Levine, J. M. (2012). To Stay or Leave? The Relationship of Emotional and Informational Support toCommitment in Online Health Support Groups. *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work*, 833–842.

[23] Lin, Y.-K., Chen, H., Brown, R. A., Li, S.-H., & Yang, H.-J. (2014). Time-to-Event Predictive Modeling for Chronic Conditions using Electronic Health Records. *IEEE Intelligent Systems* (Forthcoming)

[24] Zhang, D., Prior, K., & Levene, M. (2012). How long do Wikipedia editors keep active? *Proceedings of the Eighth Annual International Symposium on Wikis and Open Collaboration - WikiSym '12*, 1.

[25] Bewick, V., Cheek, L., & Ball, J. (2004). Statistics review 12: Survival analysis. *Critical Care (London, England)*, *8*(5), 389–94.

[26] Cox, D. R. (1972). Regression Models and Life-Tables. *Journal of the Royal Statistical Society. Series B*, *34*(2), 187–220.