Detection of Hacking Behaviors and Communication Patterns on Social Media

Olga Babko-Malaya, Rebecca Cathey
BAE Systems
Burlington, MA
{olga.babko-malaya, rebecca.cathey}@baesystems.com

Steve Hinton
StratumPoint, Inc.
Carlsbad, CA
shinton@stratumpoint.com

David Maimon
Department of Criminology and Criminal Justice
University of Maryland
College Park, MD
dmaimon@umd.edu

Taissa Gladkova
Tufts University
Boston, MA
taissa.gladkova@tufts.edu

Abstract [1] **—Hackers make extensive use of online communities, sharing knowledge, tools, as well as performing coordination and recruitment activities. In order to detect such behaviors, this paper proposes a set of indicators which analyze online communication patterns, including technical discussions, expression of positive and negative sentiments and threats, recruitment activities, and user profiling. The indicators are processing streaming social media and search for online behaviors and communication patterns characteristic of hackers with different motivations and skills. Our initial evaluation of indicators using twitter data shows that there is a significant variation in indicator values across different types of hackers. For example, hackers with higher level skills tend to use technical topics in their conversation more often than hackers with lower skills, whereas hackers motivated by profit and ideology tend to express recruitment language more often than attackers motivated by revenge and prestige. These results support our hypothesis that detection of hacking behaviors on social media needs to take into account the differences in intentions, motivations, and skills of different types of hackers.**

Keywords—Hacker Behavior, Hacker Typology

I. Introduction

Hackers, terrorist groups, state actors, and organized crime all demonstrate a sharp increase in the use of social media and similar platforms for surveillance, planning, and coordination of both kinetic and cyber-attack execution. Whereas there have been recent attempts to understand hacker behavior using survey-based methods ([3], [4], [9], [31], [8]), there is a very limited research in developing methods that leverage online social platforms for the purposes of identifying emerging cyber threats ([2], [22], [14]).

Another problem is that most of the current studies lumps all hackers into a single category, not taking into the account the fact that hackers who perform cyber attacks have different intentions, motivations, and skills. Simply comparing hackers to other social media users (cyber researchers, students, and other groups of non-hackers) is problematic due to significant differences in behaviors triggered by alternate motivations ([25], [26]).

This paper presents an approach to development of indicators of actors and groups exhibiting hacking behaviors on social media and provides an initial evaluation of these indicators by using twitter data. To define indicators, we have applied the insights from the DSKRAM model ([15]), a revised version of Parker's SKRAM model ([23]) that is often used by cyber security experts to assess potential threats to organizational information systems. The DSKRAM model extends the five components of SKRAM (Skills, Knowledge, Resources, Access to the target, and Motivation to offend) to include individual attributes and situations and circumstances that are conducive of attacks. Such situations can fuel the attackers motivation to offend and increase the probability that a cyber attack will be launched against the organization.

Driven by this theory, we have developed indicators that measure different components of the DSKRAM model. The indicators are processing streaming social media and search for online behaviors and communication patterns characteristic of attackers with different motivations, knowledge, and skills.

For example, in order to measure skills, we use Technical Communication indicators that analyze technical discussions on social media platforms, identify users and groups who are discussing cyber related topics and ask questions about them, as well as detect experts in relevant technical topics. To analyze motivation, we have developed Sentiment indicators, which analyze negative sentiment towards target organizations, as well as Social Media Communication indicators, which identify potential coordination and recruitment activities and expression of threats. Finally, User Profiling indicators are measuring individual attributes of online users or groups by

[1] Approved for public release; unlimited distribution.

978-1-5386-2715-0/17/$31.00 ©2017 IEEE

analyzing usernames, hashtags, as well as the profiles of users on social media platforms. Whereas a description of a fusion model is outside the scope of this paper, when combined together, the indicators can be used to forecast cyber attacks.

Our initial evaluation of indicators is based on a manually constructed ground truth data set of 100 cyber-attacks. The results show that there is a significant variation in indicator values across different types of hackers. For example, hackers with higher level skills tend to use technical topics in their conversation more often than hackers with lower skills, and generally tend to ask more technical questions about cyber related topics. Another interesting result is that the indicators are not correlated with each other and therefore are expected to make different contributions to a prediction model which combines these indicators to forecast a cyber-attack.

II. Hacker Communication patterns

Current research identifies the existence of hacker communities on social media platforms across various geopolitical regions ([18], [1], [2]) and provides evidence showing that many participants with both sophisticated or little hacking skills are actively utilizing social media resources to gain knowledge, as well as to perform recruitment and coordination activities. In order to detect such behaviors, we are proposing a set of indicators which analyze online communication patterns, including technical discussions, expression of positive and negative sentiments and threats, recruitment activities, and user profiling.

Technical Communication. It is known that hackers are actively communicating in cyberspace and share resources, capabilities, and techniques with other members ([30], [2]). In particular, less skillful hackers often seek help from more experienced individuals, creating a meritocratic hierarchy within hacking culture ([12]). The goal of Technical Communication indicators is to analyze the technical language of participants of cybercrime forums, for example, trying to identify individuals or groups that frequently use attack-specific terminology in their online communication and ask a lot of questions about these terms. Past research also identified some common topics that appear popular in hacker communities. Such topics include information hacking techniques, including discussion of tools, malware, and platforms ([11], [1], [33]), discussion of attack vectors and hacking concepts that demonstrate participant proficiency ([34], [1]), as well as more general topics that include discussion of network technologies, and operating systems ([35]). We have extended this topic list to include Attack Types (Denial of Service, Phishing, Social Engineering, Clickjacking, etc), Attack Stages (e.g. Reconnaissance, Weaponization, Deliver, Exploitation, Installation), Tools, Malware, and Platforms. For each topic, we created a list of terms that is characteristic of this topic. For example, the list of terms for the topic AttackType.Denial of Service includes terms: *DDOS, DOS, Ddosing, Denial of Service, Distributed denial of service, Ping flood, SYN flood, Teardrop attack, etc.*

The indicators are then using the terms from each topic to identify participants and groups who express particular interest in a topic or ask a lot of questions about this topic. Additional indicators detect ‘experts" in Topic, i.e. individuals who frequently talk about attack related events in their online communication and respond to questions about these topics. By analyzing technical terms discussed on social media, these indicators can measure technical background, interests, and experience of potential actors and groups of interest.

Sentiment. Whereas the goal of the Technical Communication indicators is to measure attacker skills, our sentiment-based indicators are aimed to identify ideology, social and religious views, revenge, and other types of motivation. There is a growing evidence that more cyber-attacks are associated with social, political, economic, and cultural conflicts ([19], [6]), which affects online communication of attackers. For example, an analysis of defaced web pages in [30] has shown that hackers who have a certain purpose tend to use more verbal attacks and aggressive expressions on target web pages than other types of hackers. Also, this group of hackers tends to leave bragging remarks in an attempt to be admired within the hacker community.

Our sentiment extractor leverages existing open source sentiment analysis tools ([28]) to detect negative and positive opinions. Applied to cyber security context, sentiment tools have been successfully used to detect threats ([14]), as well as to identify the key players involved in the sale of malware and stolen data ([13]). In our approach, we apply sentiment tools to detect aggressive and negative remarks towards the target organizations, as well as to analyze general trends in negative opinion towards these targets. In addition, we use positive sentiment in combination with technical topics to identify potential "bragging" language, such as messages informing the media about successful attacks and postings containing bragging remarks about attackers skills.

Social Media Communication. In addition to technical discussions and expression of sentiment, hacker communication patterns may include expression of threats, as well as recruitment and coordination activities.To detect threats, we use natural language processing tools to extract predicates that are indicative of threats, identify actors and targets, and take advantage of features that are indicative of threat language, such as the use of first person pronoun for actors, subject-less sentences, and negative sentiment associated with targets. Some examples of the expressions we extract include the following ones:

- *"We are declaring war! Expect us!",*
- *"And Sunday will start the new Revolution of #LulzSec*
- *We will Ddos nsa.gov feel the pain of #TheLulzBoat",*
- *"Charge your lasers and aim them at the Nasdaq and London Stock Exchange").*

Our analysis of the text of messages is also aimed to identify recruitment and coordination activities relevant to preparation for cyber attacks, including logistics/coordination and targeted communities and websites. These indicators include calls to download software, as well as detection of "recruitment" language. To detect communication patterns indicative of recruitment activities, we use a syntactic parser in combination with other features, such as pronouns, universal quantifiers (all, anyone), as well as predicates that express invitations/calls to join or attack. Examples of recruitment language include:

- *"Hackers, ddosers, database dumpers, spammers, all are welcome.*
- *Make sure to send your invites out.",*

- *“For those using android who wish to attack for #Opicarius Phase 4 #OpBlackOct”,*
- *“Invite who you want. Let us share targets, tools and strategies and wipe out the banks”,*
- *“Join the fight against the elites”.*

User Profiling. Given potential users and groups of interest, we further analyze their profiles to detect characteristics that can be indicative of hacking behaviors. For example, it is known that underlying many of the behaviors in hacking community is a strong focus on reputation and trust, as reputation is regarded as extremely valuable and often influences social interactions ([10], [18], [31], [1]). Many hacker forums utilize internal reputation rating systems, allowing participants to rate the trustworthiness and contributions of others ([5], [1]). Other research has considered the effects of tenure, or length of membership within a forum, suggesting that it may help amplify reputation ([36]). It has also been shown that demographic characteristics, in combination with other indicators, may help determine the type of the attacker ([15]). Additional User Profiling indicators include the choice of hashtags and keywords used as part of user or group names (e.g. ‘anon’).

III. Ground Truth Data Set

In order to perform an initial analysis of these hypotheses, we developed a set of Ground Truth (GT) data which included 100 cyber-attacks from November 2015. For each attack, a subject matter expert provided information about the date of the attack, the actor, actor category, target, trigger, country, industry, and motivation. An example of a description of one attack is given below.

TABLE 1. An Example of a Ground Truth Attack Description

Date	2-Nov-2015
Actor	Anonsec
Type	Hacktivist
Target	“Israel Missile Defense Association http://imda.org.il/“
Trigger	Political
Target Country code	IL
Target Industry	Military
Motivation	To show support for Palestine

Our hacker typology builds on Seebruck’s typology ([26]) and integrates past attempts (e.g. [25], [17], [3], [16]) to classify cyber attackers based on two dimensions: motivations and skills.

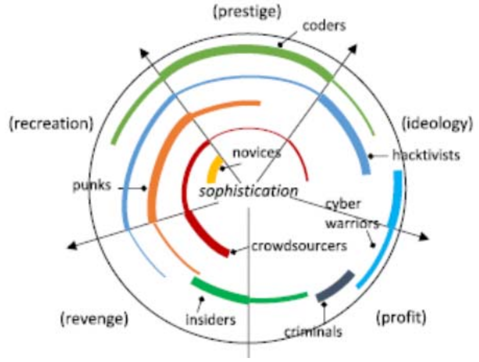

Figure 1. Seebruck’s Hacker Typology

Fig. 1 presents a weighted arc circumplex of hacker types ([26]) which takes into consideration the fact that hackers may have more than just one motivation. For our analysis, we have selected five types of hackers: hobbyist, hacktivist, cyber warrior, criminal, coder, and insider. Hobbyists are a more inclusive category that includes lower skilled hackers such as novices, crowdsources, and punks. While these actors may express the intent/motivation for larger attacks, they typically lack the capability to represent a genuine threat against a majority of targets.

To perform an analysis of indicator values across hacker types, we divided the list of targets into multiple sets, where each set includes the attacks carried out by a specific type of an attacker. For example, to analyze patterns associated with hacktivists, we used a subset of the GT targets that were attacked by hacktivists in November 2015. Our analysis therefore is based on an important assumption: if the ground truth says that a Target was attacked by a hacker of type A, then we assume that the Target was exclusively attacked by hackers of type A.

This assumption is supported by the fact that target selection varies with actor type. For instance, a cyber warrior that represents a terror organization (i.e. Cyber Caliphate) will more likely focus on a target in line with their ideological agenda (i.e. a target with a United States foreign policy-specific focus or line of effort) as evidenced when the Cyber Caliphate conducted a cyber attack against and publicly released “kill lists”, calling on followers to conduct kinetic attacks against physical targets external of cyber space based on their ideology. This is a representation of cyber space intersecting with the non-cyber space and having a physical impact on non-cyber targets. Hacktivists such as Anonymous (which have a broad, disaggregated focus commensurate with their non-hierarchical structure) vary on their target specificity, but typically have a social agenda nexus and could potentially be more easily connected to a social event announcement or development as a trigger event for upcoming action.

To perform experiments, we collected archived twitter data for the same time period (about 12M tweets). We then generated indicators from tweets that include mentions of targets for each attacker type and performed an analysis described below.

IV. Indicator Analysis

A. Technical Communication

The goal of Technical Communication indicators is to analyze technical discussions, looking for individuals or groups that frequently use terminology characteristic of specific topics. Our current analysis explores the following four indicators.

TABLE 2. Technical Communication Indicators

Indicator	Description
talksAbout Topic	Post/User/group/ talks about one of the topics from the Topic list
asksAbout Topic	Post/User/group/ asks questions about one of the topics
Exclusively TalkAbout Topic	User/group is interested in one specific topic. i.e. the user (or a group) mentions this topic in over 20% of their postings
Exclusively AsksAbout Topic	User/group collects information about one specific topic. i.e. the user (or a group) mention this topic in over 20% of their posted questions

Fig. 2 provides a comparison of indicator values for the talksAbout indicator for different topics across different attacker types. The question we are interested in can be defined as follows: out of all tweets that mention attacker specific targets (i.e. targets attacked by hobbyists vs. hacktivists vs. cyber warriors in the November 2015 time frame), how many also talk about technical topics?

The chart reveals that the types of hackers who tend to use technical topics more often include criminals, cyber warriors, and coders. This indicates that hackers with higher skills tend to use technical topics more frequently than hackers with lower skills. It also shows that the topic that is most frequently mentioned in connection with the ground truth targets is Attack Types. On the other hand, in the case of insiders, the most popular topic is different – insiders tend to use terms from Attack Stages more frequently than from the other topics. This indicates that the two topics could be used to distinguish between insiders and other types of hackers.

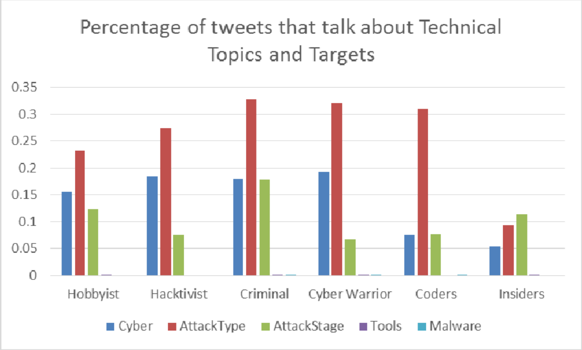

Figure 2. The number of tweets that talk about technical topics in connection with attacker-specific targets divided by the number of tweets that talk about corresponding targets

Looking at the percentage of tweets that ask questions in connection with targets on Fig. 3, we see that less sophisticated hackers (such as insiders and hobbyists) tend to ask less questions, whereas higher skilled attackers (criminals and cyber warriors) ask technical questions more frequently, especially using Attack Types and general Cyber terms.

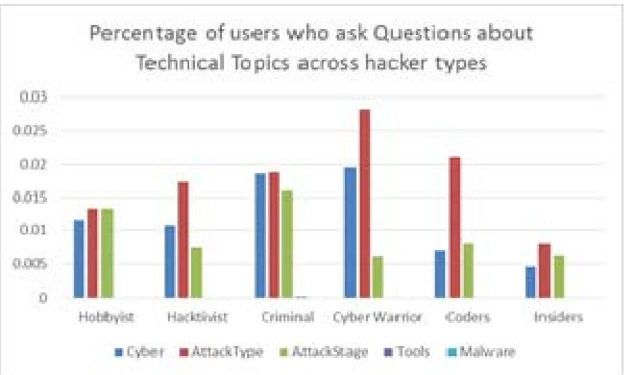

Figure 3. The number of users who ask questions about a technical topic in connection with attacker-specific targets divided by the number of users who mention corresponding targets.

B. *Social Media Communication Indicators*

The goal of the social media indicators is to detect interactions associated with recruitment and coordination activities relevant to preparation for cyber-attacks. It is known that many hackers share links to other communities, underground economies, and deep web hidden services, which can be detected by identifying calls to download software or posts containing links to sites that have malicious software.

TABLE 3. Social Media Communication Indicators

Indicator	Description
callsToDownload	User/Group/post mentions a link to download software
expressesThreats	User/group/post expresses threat language
expressesRecruitment	User/group/post expresses recruitment language

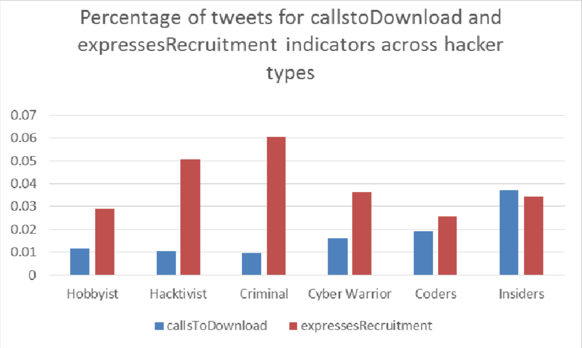

Figure 4. The number of tweets that call to download or express recruitment in connection with attacker-specific targets, divided by the number of tweets that talk about corresponding targets

Fig. 4 presents the percentage of tweets for different hacker types for callsToDownload and expressesRecruitment indicators. It reveals that attackers motivated by profit and ideology (i.e. criminals, hacktivists, and cyber warriors) express recruitment language more often than the other types of hackers. On the other hand, attackers whose goal is revenge and prestige (i.e. insiders and coders) call to download software more often than ideologically motivated hackers.

Fig. 5 presents a similar chart for the indicator which detects threat language. It reveals that the types of hackers who use threat language more often than the other hackers include attackers motivated by ideology (i.e. Hacktivists and Cyber warriors)

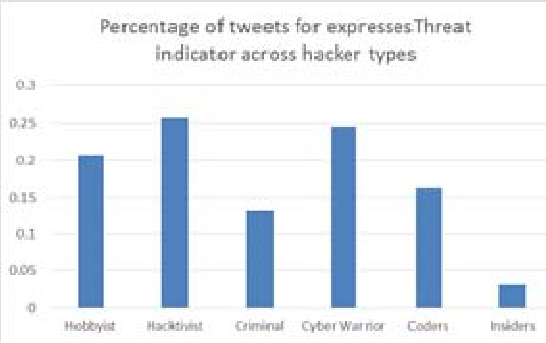

Figure 5. The number of tweets that express threat language in connection with targets divided by the number of tweets that talk about targets

C. User Profiling

The goal of the Profiling sensor is to analyze the profiles of users and groups in order to detect characteristics that can be indicative of hacking behaviors, as described above. Our current analysis is focused on the following two indicators:

TABLE 4. User Profiling Indicators

Indicator	Description
UserHasHackerName	Username includes a string which is typical of hacker names, such as 'anon'
GroupHashackerName	Hashtag includes a string which is typical of hacker groups, such as 'op' or 'anon'.

The results are presented in Fig. 6. Although the percentages are very small, the chart indicates that these two indicators are particularly useful for prediction of attacks planned by hacktivists, i.e. attackers with lower technical skills and motivated by political ideology.

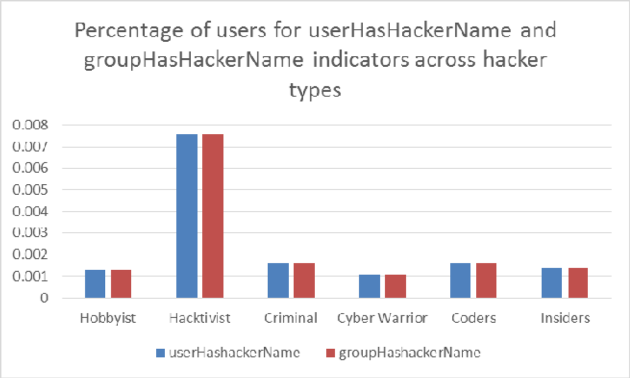

Figure 6. The number of users and groups detected by userHashackerName and groupHasHackerName indicators mentioning attacker-specific targets, divided by the number of tweets mentioning corresponding targets.

D. Sentiment

The Sentiment indicators are aimed to detect messages expressing negative opinion of target organizations. In addition, positive sentiment is used to identify messages containing bragging remarks about successful attacks in an attempt to gain reputation from the community.

TABLE 5. Sentiment Indicators

Indicator	Description
expressesNegativityTo	Post/User/group/ expresses negative sentiment towards the target organization or country
expressesPositivityTo	Post/User/group/ expresses positive sentiment towards a cyber topic or event

The results are shown in Fig. 7. There is a significant difference in the number of negative sentiment associated with targets, relative to positive sentiment. Interestingly, insiders tend to express negativity almost as frequently as the other types of hackers, although as we have seen in Fig. 5, they do not express threat language as often as ideologically motivated hackers, such as hacktivists or cyber warriors.

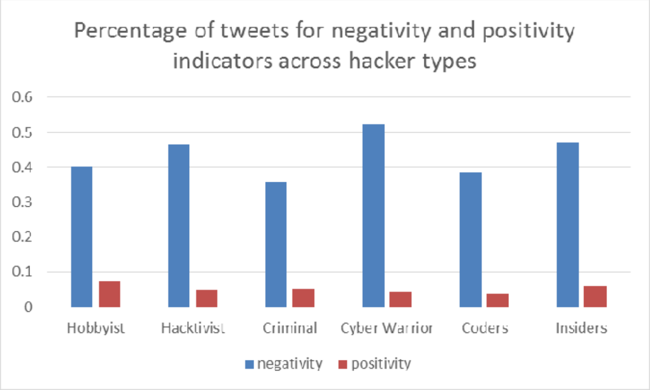

Figure 7. The number of tweets detected by negativity and positivity indicators mentioning attacker-specific targets, divided by the number of tweets mentioning corresponding targets

VI. Conclusion

This paper presented a set of indicators which is aimed to detect hacking behaviors on social media and could be used to predict cyber attacks. These indicators include technical discussions, expression of positive and negative sentiments and threats, recruitment activities, and user profiling. It also described initial results based on a ground truth data set which includes 100 cyber attacks categorized by different types of hackers.

The results show that there is a significant variation in indicator values which are due to differences in alternate motivations, intentions, knowledge, and skills of attackers. Whereas a description of a prediction model which combines these indicators is outside of the scope of this paper, the results described above suggest that such a model needs to take these differences into account. Another interesting result is that the indicators are not correlated with each other and therefore are expected to make different contributions to a model.

The results presented in this paper are limited to evaluation of indicators using one data source - twitter data. We expect that our indicators can be applied to different data sources, including cyber forums. Future work also includes adding indicators with a focus on detection of other components of the DSKRAM model ([15]), such as Access and Resources.

Acknowledgment

This work is supported by the Office of the Director of National Intelligence (ODNI) and the Intelligence Advanced Research Projects Activity (IARPA) via the Air Force Research Laboratory (AFRL) contract number FA8750-16-C-0113. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright annotation thereon. Disclaimer: The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of ODNI, IARPA, AFRL, or the U.S. Government.

REFERENCES

[1] Benjamin, V., & Chen, H. (2012). Securing Cyberspace : Identifying Key Actors in Cybercriminal Communities. Proceedings of the IEEE Joint Intelligence and Security Informatics Conference. 24-29. Washington, D.C. June 11-14.

[2] Benjamin, Victor. "Securing Cyberspace: Analyzing Cybercriminal Communities through Web and Text Mining Perspectives", Ph.D Dissertation, 2016

[3] Chantler, N. "Profile of a computer hacker". Florida: Infowar 1996

[4] Dey D., A. Lahiri, and G. Zhang, "Hacker behavior, network effects, and the security software market," J. Manag. Inf. Syst., vol. 29, no. 2, pp. 77–108, Oct. 2012.

[5] Fallman, H., Wondracek, G., and 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. Bonn, Germany. July 8-9.

[6] Gandhi Robin A , Anup Sharma, William Mahoney, William Sousan, Quiming Zhu, Phillip A. Laplante. "Dimesnions of Cyber-Attacks. Social, Political Economic, and Cultural", In IEEE Technology and Socienty magazine. 2011.

[7] Gawron Jean Mark, Dipak Gupta, Kellen Stephens, Ming-Hsiang Tsou, Brian Spitzberg and Li An "Using Group membership markers for Group Identification", in Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media, 2012; pp. 467-470

[8] Giboney J.S., J.G. Proudfoot, S. Goel, J.S. Valacich "The Security Expertise Assessment Measure (SEAM): Developing a scale for hacker expertise", Computers and Security 60, 2016, pp. 37-51

[9] Giboney JS, Durcikova A, Zmud RW. "What motivates hackers? Insights from the awareness-motivation-capability framework and the general theory of crime". In: Dewald Roode information security research workshop. 2013. p. 1–40.

[10] Gosh S. and E. Turrini (2010) "Cybercrimes: a multidisciplinary analysis," Springer, October 2010.

[11] 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.

[12] Kshetri N., "The Simple Economics of Cybercrime," in IEEE Security & Privacy, vol. 4, no.1, pp. 33-39, January-February 2006.

[13] Li, W., & Chen, H. "Identifying Top Sellers in Underground Economy Using Deep Learning-based Sentiment Analysis". Presented at Intelligence and Security Informatics (ISI), 2014 IEEE International Conference on. 2014.

[14] Macdonald Mitch, Richard Frank, Joseph Mei, and Bryan Monk. "Identifying Digital Threats in a Hacker Web Forum", in 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining

[15] Maimon David, Steve Hinton, Olga Babko-Malaya, Rebecca Cathey "Re-Thinking Online Offenders' SKRAM: Individual Traits and Situational Motivations as Additional Risk Factors for Predicting Cyber Attacks" to appear in Proceedings of the 2017 IEEE Cyber Science and Technology Congress (CyberSciTech), Orlando, FL

[16] McBrayer John. Exploiting the digital frontier: hacker typology and motivation. University of Alabama; 2014. Thesis

[17] Meyers Carol, Powers Sara, Faissol Daniel. "Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches." Technical report LLNL-TR-419041. Lawrence Livermore National Laboratory; 2009

[18] Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). An analysis of underground forums. Proceedings of the ACM SIGCOMM Conference on Internet Measurement Conference. 71-80. Berlin, Germany. November 2-4.

[19] Myers M. and F. Tan, "Beyond models of national culture in information systems research," Advanced Topics in Global Information Management, ch. 1, 2003.

[20] Markoff J., "Internet attacks seen as more potent and complex," 2008, http://www.iht.com/articles/2008/11/10/technology/10attacks.php.

[21] Nov O., M. Naaman, and C. Ye, "Motivational, structural and tenure factors that impact online community photo sharing," in Proceedings of AAAI International Conference on Weblogs and Social Media, May 2009.

[22] Nunes Eric, Ahmad Diab, Andrew Gunn, Ericsson Marin , Vineet Mishra,Vivin Paliath, John Robertson, Jana Shakarian, Amanda Thart, Paulo Shakarian. "Darknet and Deepnet Mining for Proactive Cybesecurity Threat Intelligence", in Proceedings of the IEEE Intelligence and Security Informatics 2016 Tucson, Arizona USA, 2016

[23] Parker, D. B. (1998). Fighting Computer Crime: A New Framework for Protecting Information. New York: John Wiley & Sons

[24] Rasche G., E. Allwein et al. "Modelbased cyber security," in Proc. 14th Ann. IEEE Int. Conf. and Workshops on the Engineering of Computer-Based Systems, 2007, pp. 405–412.

[25] Rogers M. "A two dimensional circumplex approach to the development of a hacker taxonomy. Digital investigation 3(2), 2006, pp. 97-102.

[26] Seebruck, R. "A typology of hackers; Classifying cyber malfeasance using a weighted arc circumplex model". Digital investigation 14, 2015, pp. 36-45.

[27] Slay J., "IS security, trust and culture: a theoretical framework for managing IS security in multicultural settings," J. Campus-Wide Information Systems, 2003, vol. 20, no. 3, pp. 98-104.

[28] Socher Richared, Alex Perelygin, Jean Wu, Jason Chuang, Christopher Manning, Andrew Ng and Christopher Potts 2015 "Recursive Deep Models for Semantic Compositionality Over a Sentiment Treebank", Conference on Empirical Methods in Natural Language Processing (EMNLP 2013)

[29] Woo, H. J. (2003). The hacker mentality: Exploring the relationship between psychological variables and hacking activities. Pd.D. Dissertation, the University of Georgia

[30] Woo, H. J., Kim, Y. R., & Dominick, J. R. (2002). Hackers: Chauvinists or Anarchists-A content Analysis of Defaced Web Pages. presented at Communication and Technology division, International Communication Association, Seoul, Korea, July.

[31] Xu Z, Hu Q, Zhang C. Why computer talents become computer hackers. Commun ACM 2013; 56(4):64.

[32] Xu Radianti, J. (2010). A Study of a Social Behavior inside the Online Black Markets. Proceedings of the International Conference on Emerging Security Information, Systems and Technologies. 88–92. Nice, France. July 24-28. Z, Hu Q, Zhang C. Why computer talents become computer hackers. Commun ACM 2013; 56(4):64.

[33] Yip, M., Shadbolt, N., & Webber, C. (2013). Why Forums ? An Empirical Analysis into the Facilitating Factors of Carding Forums. ACM Web Science. 453-462. Paris, France. May 2-4.

[34] Zhuge, J., Holz, T., Song, C., Guo, J., and Han, X. (2008). "Studying Malicious Websites and the Underground Economy on the Chinese Web". Managing Information Risk and the Economics of Security. 225–244.

[35] Holt, T.J., and Kilger M. (2012) "Know Your Enemy: The Social Dynamics of Hacking". The Honeynet Project, 1-17

[36] Nov O., M. Naaman, and C. Ye, "Motivational, structural and tenure factors that impact online community photo sharing," in Proceedings of AAAI International Conference on Weblogs and Social Media, May 2009.