2017

On the Relevance of Social Media Platforms in Predicting The Volume and Patterns of Web Defacement Attacks

David Maimon

Andrew Fukuda

Steve Hinton

Olga Babko-Malaya

Rebecca Cathey

On the Relevance of Social Media Platforms in Predicting The Volume and Patterns of Web Defacement Attacks

David Maimon, Andrew Fukuda

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

Steve Hinton

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

Olga Babko-Malaya, Rebecca Cathey

BAE Systems
Burlington, MA
{olga.babko-malaya, Rebecca.cathey}@baesystems.com

Abstract[1]— **Social media platforms are commonly employed by law enforcement agencies for collecting Open Source Intelligence (OSNIT) on criminals, and assessing the risk they pose to the environment the live in. However, since no prior research has investigated the relationships between hackers' use of social media platforms and their likelihood to generate cyber-attacks, this practice is less common among Information Technology Teams. Addressing this empirical gap, we draw on the social learning theory and estimate the relationships between hackers' use of Facebook, Twitter, and YouTube and the frequency of web defacement attacks they generate in different times (weekdays vs. weekends) and against different targets (USA vs. non-USA websites). To answer our research questions, we use hackers' reports of web defacement they generated (available on http://www.zone-h.org), and complement with an independent data collection we launched to identify these hackers' use of different social media platforms. Results from a series of Negative Binomial Regression analyses reveal that hackers' use of social media platforms, and specifically Twitter and Facebook, significantly increases the frequency of web defacement attacks they generate. However, while using these social media platforms significantly increases the volume of web defacement attacks these hackers generate during weekdays, it has no association with the volume of web defacement they launch over weekends. Finally, although hackers' use of both Facebook and Twitter accounts increase the frequency of attacks they generate against non-USA websites, the use of Twitter only increases significantly the volume of web defacement attacks against USA websites.**

Keywords— Hackers, Social Learning Theory, Social-Media, Web Defacement

I. INTRODUCTION

The most common approach for cyber security taken by Information Security teams in both the USA and around the globe draws on the application of defensive strategies that are merely responsive and investigatory of cyber related incidents after they occur [1]. Unfortunately, this approach is very costly and ineffective in preventing the occurrence and development of cyber-attacks [2]. Acknowledging this issue, the DoD Science Board [3] has called for moving from the current reactive and ineffective model of cyber security, to a more proactive approach, which involves the collection and production of strategic cyber intelligence, and could potentially lead to termination of cyber-attacks before they actually happen. Accordingly, the collection of cyber intelligence could support identification and understanding of adversarial operational capabilities, partnerships and intensions, as well as support accurate assessment of adversarial plans. This intelligence, in turn, could be used for guiding Information Technology teams' initiatives to manage and counter cyber-attacks against their organizations [4].

Social media platforms could potentially play a key role in serving as a collection source for strategic cyber intelligence [5]. Indeed, prior research has already demonstrated the usefulness of data posted on Twitter, Facebook and YouTube in predicting offline events like election results, stock market trends, infectious disease outbreaks, national revolutions ([6], and even offline crimes [7]. However, to date, no previous study has established an empirical relationship between individuals' use of social media platforms, and their level of involvement in cyber dependent crimes (i.e. all these crimes that emerge as a direct

result of computer technology and the internet and that could not exist without it) [8]. In effort to address this issue, we draw on the social learning theory [9], and generate hypotheses regarding the potential relationship between hackers' use of social media platforms and the volume of web defacement attacks they launch against targets around the world. To test our research hypotheses, we use hackers' self-reports over the website Zone-H [10-11] on web defacement attacks they launched, and append with our own data collection effort that established these hackers' use of social media platforms.

II. THEORETICAL BACKGROUND

Cyber-attacks like malware, phishing, Distributed Denial of Service (DDoS), and system trespassing (i.e. the unauthorized use of a computer system) still pose a major challenge to individuals' and organizations' cyber security in the USA and around the world [12]. Those attacks often target cyber assets like control systems (for example SCADA computers), data acquisition systems, network equipment (for example routers, switches and hubs), and hardware platforms (for example desktops and servers) [13], and may result in physical, financial and reputational consequences to the victims [14]. In effort to address this pressing challenge, large organizations invest substantial funds in building fortress-computing environments that are designed to reduce the probability of a successful cyber-attacks against the organization [15]. However, these efforts tend to be defensive in nature, and apply standard security policies and tools that their effectiveness in preventing cyber-attacks is still unknown. In effort to improve organizations' cyber security posture, several security experts [16-17], as well as the DoD Science Board [3], has urged cyber defenders to adopt a more proactive approach for cyber security, and engage in efforts for collecting tactic cyber intelligence. Collection of information leading to cyber intelligence should support assessment of organizations risks to experience wide range of cyber-attacks, and include intelligence regarding the type of potential attack vectors, tactics, techniques and procedure they may employ, the sort of vulnerabilities and weaknesses they are likely to exploit, as well as a list of potential triggers for the attack [4]. One specific type of attack that could be prevented given the timely and actionable cyber intelligence is web defacement.

A. Website Defacement

Website defacement is the most obvious form of hacking [18]. In this type of cyber-attack an attacker seeks to compromise a server, and then replace the legitimate and authorized content of the website with images and text of his own [19]. As a result, defacing of an organization's website may expose visitors to misleading information, and effect the credibility and reputation of the organization as a whole. The consequences for the organization in this sense, may vary from the loss of trust to losing revenue [20].

Unlike more sophisticated forms of hacking, web defacement attacks do not require attackers to have highly sophisticated technical skills. In fact, numerous tutorials explaining how to infiltrate a server and change the content of a website are available online over social media platforms like Facebook and YouTube [19] and the tools for conducting the attacks are readily available and easy to deploy. Moreover, the underlying goals behind the initiation of web defacement attacks vary considerably from ideological, political and thrill-seeking to peer recognition, challenge and personal accomplishment [18]. Still, only few studies have offered an empirical investigation of the underlying causes of web defacement. Instead, most prior research has analyzed the content of defaced websites in attempt to infer attackers' motivation and goals [18]. One exception to this trend is a recent study by Holt and associates [19]. In that research the scholars attempted to examine predictors for individuals' willingness to engage in web defacement. Analyzing survey data collected from a sample of undergraduate students in the USA and Taiwan, the authors report that nationalist feelings are associated with individual's willingness to deface governmental websites, and that individuals who are willing to perform multiple forms of political protest are likely to engage in web defacements [19]. Although important in revealing some of the correlates of web defacement attack, this study fails to present theoretical rationale for individual willingness to initiate web defacement attacks. Moreover, to gauge subjects' willingness to initiate web defacement attacks, the authors presented their subjects with theoretical scenarios, to which responds had to respond. The current study seeks to advance our understanding of the correlates of website defacement by drawing on the social learning theory [9], and exploring the relevance of social media platforms in shaping the volume, timing and targets of web defacement attacks.

B. Social Learning Theory

The social learning theory [9] has its underpinnings in the psychological literature, and suggests that individuals learn how to become criminals from their social environment. Specifically, this theory proposes that *differential association*, which is defined as the excessive exposure to definitions favorable towards violating the law over definitions that are unfavorable towards the violations of law, is the underlying cause for individuals' adoption of a criminal lifestyle and involvement in deviance and crime [21]. Peer groups, in this sense, play a very important role in exposing the individual to definitions favorable and unfavorable towards the violation of laws. Specifically, the normative orientation of one's peers, the structural characteristics of the peer group, as well as individual position in the group, play important role in determining one's involvement in crime [22]. In addition to excessive exposure to deviant values and norms, the theory also suggests that individuals' learning process involves the acquisition of motivations (i.e. rationalizations for the deviant act) and techniques (i.e. skills and tools), and draws on the balance of anticipated rewards and punishments for engaging in a criminal behavior (i.e. *differential reinforcement*). Finally, Akers [9] proposes that *imitation* plays a detrimental role in the initial learning of a behavior.

All in all, extensive criminological research has found support to Akers' [9] major claims, linking the four theoretical constructs with deviant and criminal behaviors like substance abuse, violent and property crimes [23, 21]. Moreover, past criminological research has already found support for the key theoretical assumption of social learning theory in the context of computer hacking. Specifically, several studies reported that hackers maintain peer relationships with other hackers [24] and that peer associations are important for introducing new hackers to both hacking tools and methods [25]. Still, despite the central role played by online environments in influencing hackers' acquisition of knowledge and deviant peers, the role of social media platforms in supporting computer dependent crimes has received less empirical attention.

C. Social Media and Crime

Social media websites refer to a broad category of websites that support individuals' interpersonal interaction with others while online through a public user created profile [26]. Due to their virtual nature, these websites have changed the traditional composition of friendships networks while allowing them to span over great geographical distances [27]. Moreover, these websites could be established we an important engine of socialization, as behaviors and attitudes that are expressed by their users may be studied and imitated by large audiences. Lefebvre and Bornkessel [28] for example showed that medical information that is shared over social media websites has a direct effect on users' decisions for chronic disease management, medication, and approach to diet and exercise.

Next to serving as an important source for educating users about normative and health related behavior, some criminologist believe that social media platforms could be also employed as a vehicle through which individuals learn how to engage in offline and online crimes [29]. McCuddy and Vogel [30] for example report that social media users' exposure to offending on social media platforms increases users' probability to engage in offending. Moreover, extensive criminological research has revealed the different ways in which urban gangs employ social media websites to facilitate violence and crime. In a recent review of this literature Patton and associates [29] show that gang members use social media platforms like Facebook and Twitter to sell drugs, post videos of violence and threats, display firearms and money, as well as taunt rival gangs' members. Sela-Shayovits [31] also report that gang members with high level of technical knowledge share their knowledge over social media platforms with less technical members of the group in order to facilitate the group's involvement in cybercrime.

Due to the extensive use of social media platforms in facilitating and supporting illegal activities, law enforcement agencies are now employing these websites as a source of intelligence that allows them to obtain information and arrest criminals [32]. To support law enforcement agencies in this task several research teams have developed designated automatic tools that allow surveilling criminals' social media

accounts, collecting relevant data, and analyzing it [33-34]. However, despite the attention in criminals' use of social media websites, relatively little is known with respect to the way hackers employ social media websites as a way to facilitate cyber-attacks.

D. The Current Study

Drawing on both the social learning theory, and past criminological research that demonstrates the importance of social media websites in users' exposure to deviant offline [30] and online behaviors [35, 29], we propose that *hackers' use of social media platforms increases the volume of web defacement attacks they generate*. Specifically, hackers use of social media websites allow them to interact with similar hackers who can expose them to wide range of motivations and that will be conducive toward hacking websites. In addition, similarly to gang members' tendency to advertise their criminal activity over social media platforms [29], hackers may employ social media websites to notify their friends after a successful attack and gain some reputation.

We also believe that *hackers that use social media platforms will be more likely to generate attacks against their targets during work days and not during weekends*. All in all, findings from marketing research indicate that posting over social media websites like Facebook and Twitter during week days reaches more people and is more effective than during the weekend [36-37]. These findings are important in the context of our work because if a hacker faces difficulties during a website defacement attack, he can seek help from their online friends. However, if the online friends are not tuned in then the attacking hacker may not be able to complete the web defacement incident he launched. Moreover, once successfully completing a web defacement incident, a hacker might want to post a note over the social media platforms regarding the attack he completed. However, if the note will be posted during the weekend there is a chance that his friends will not be able to see the actual defaced website since the legitimate owner of the website has enough time to fix the issue.

Finally, given the growing population of social media websites around the globe [38] we believe that *the relationships between hackers' use of social media and the volume of web defacement attacks they generate will be significant both for predicting web defacement attacks against US websites and against websites hosted in other countries around the globe*.

III. DATA AND METHODS

To test our research hypotheses we followed [10] and [11], and employed data hosted by Zone-H (see http://www.zone-h.org/), and that contain hackers' self-reports on their web defacement activities and the URL that correspond to the defacement. Specifically, followed by a successful web defacement attacks, the attacking hacker (may) submit a report of the event to Zone-H server. The Zone-H staff then check if the defacement indeed occurred, and if it did, announce the event over the website. The information that is reported on the

website includes the notifying hackers' names, the defacement date, the domain defaced, the operating system of the defaced server and a mirror of the defaced website. Our research team monitored closely the web defacement reports on the Zone-H website between the months of May and July of 2017, and downloaded those reports to our servers.

Since the information reported on the website included hackers' aliases, we followed Balasuriya and associates [34] efforts to collect open source intelligence on criminals over social media platforms and looked for information about these hackers in key social media platforms- Facebook, Twitter, and YouTube. We then recorded whether we were able to find information about these online offenders on these websites. To ensure causality, once we found evidence for hackers' presence on social media platforms, we searched on the relevant platform for the date in which the hacker established the web presence, and verified that the date in which the account was established preceded in time the month of May 2017. In addition, we looked for evidence for the hackers' own designated websites. We coded all the open source information we collected found, and appended it with the Zone-H data.

Dependent Variable – To investigate our research hypotheses we created the measure *number of web defacement attacks*. Following previous operationalization of measures of cyebr attacks [39], this measure is a simple count of the number of unique web defacement attacks reported by an attacker during the data collection period.

Independent Variables - We used a list of measures designed to indicate hackers' use of social media platforms. First, we composed a dummy variable indicating whether a hacker used any social media platform during the data collection period (1= *used any social media platform*). We also generated a list of dummy variables to indicate which social media platform was used by the attacker, differentiating between *Facebook*, *Twitter, YouTube*, and *own website* (1= yes). Finally, we generated the measure *number of social media platforms* to tap the number of social media websites the hacker was subscribed to. This measure is a simple count measure.

Analytic Strategy - To estimate the relationships between hackers' use of social media platforms and the volume of web defacement attacks they generated, we used a series of negative binomial regression models. Similar to a Poisson regression, a negative binomial regression is designed to handle continuous dependent measures with large positive skews. However, in contrast to the simple Poisson, the negative binomial model corrects issues with over dispersion in cases where the variability around the model's fitted values is larger than what is consistent with a Poisson formulation. Negative binomial models are extensively used by criminologists in studies at both the individual or structural levels of offline [40] or online crimes [39]. Due to the positively skewed distribution of our web defacement count measure, as well as an observed over dispersion when estimating a simple Poisson model, we employed a negative binomial regression in this work.

IV. RESULTS

Before investigating our key research hypotheses, we briefly describe our unique sample charactaristcs. During the 3 months of the data collection period, 352 hackers reported 2824 unique web defacements attacks; 2229 of the attacks occurred during a weekday while the other 595 attacks were launched during the weekend. Moreover, only 201 of the web defacement attacks were launched against USA websites.

In Table 1 we present the means, standard deviations and minimum and maximum values of our key measures. As may be observed in the table, the average number of web defacement incidents reported per hacker was 7.87. Note that the average number of web defacement attacks is significantly higher over week days than over the weekend (6.23 attacks vs 1.67 respectively), and that the average number of web defacement attacks against USA website is relatively small. Exploring how prevalent is social media use among attacking hackers reveals that of the 352 hackers, 187 (53.12%) had some presence on social media websites; 35% of the hackers had a Facebook account, close to 31% of the hackers had a twitter account, 25% of the hackers had a YouTube account, and close to 24% had their own website.

Variable	Mean	Std. Dev	Min-Max
# of Web Defacement (WD) Attacks	7.87	18.06	1-138
# of WD Attacks During Weekday	6.23	14.49	0-134
# of WD Attacks During Weekend	1.67	9.66	0-137
# of WD Attacks on USA Websites	.56	4.93	0-85
# of WD Attacks on Non-USA Website	7.30	18.87	0-138
Use of Any Social Media Platform	.53	.49	0-1
# of Social Media Platforms	1.15	1.26	0-4
Facebook	.36	.48	0-1
Twitter	.31	.46	0-1
YouTube	.25	.43	0-1
Own website	.24	.43	0-1

Table 1. Descriptive Statistics

Turning to our first research hypothesis, we next present finding from a series of Negative Binomial Regression models that estimate the effect of hackers use of social media on the number of web defacement attacks they generated. Results from these analyses are presented in Table 2. In Model 1, we first estimate the effect of hackers' use of any social media website on the frequency of web defacement attacks the generates. Results from this analysis reveal that hackers' use of any social media platform is positively and significantly associated with higher number of web defacement attacks
(b = .87, p<0.01). Calculating the predictive margin from this model suggests that while hackers with no social media accounts produce on average 4.25 web defacement attacks, hackers that employed at least one social media platform generated 10.25 web defacement attacks on average.

Variable	Model 1		Model 2		Model 3	
	Mean (se)	IRR	Mean (se)	IRR	Mean (se)	IRR
Any Social Media Act	.87** (.14)	2.40	-	-	-	-
# Social Media Act	-	-	.25** (.06)	1.28	-	-
Facebook	-	-	-	-	.51** (.17)	1.66
Twitter	-	-	-	-	.38** (.16)	1.46
YouTube	-	-	-	-	-.20 (.17)	.81
Own website	-	-	-	-	.17 (.19)	1.18
Constant	1.44** (.10)		1.67** (.10)		1.65** (.10)	
Pseudo R2 Ln alpha Log likelihood	.02 .45 -1027.2		.01 .50 -1036.4		.01 .48 -1032.4	
**0.01 *p<0.05						

Table 2. Overall Number of Web Defacement Attacks Regressed on Hackers' Social Media Presence

In Model 2 we assess the relationship between the number of social media platform used by a hacker and the volume of web defacement attacks he generated. Results from this analysis suggest that increase in the number of social media platforms that are employed by a hacker increases the number of web defacement attacks he generates (b = .25, p<0.01). Calculating the predictive margin from this model suggests that while hackers with only one social media account produce on average 6.6 web defacement attacks, hackers with four social media accounts generated 14.5 web defacement attacks on average.

In model 3 we estimate the relationships between hackers' use of specific social media platforms and the volume of website defacement attacks they initiated. As may be noticed in the model, using either a Facebook (b=.51 p<.01) or a Twitter (b=.38, p<.01) account significantly increases the number of web defacement attacks that were generated by a hacker. Specifically, while the average number of attacks generated by a hacker with no Facebook or twitter account was 6, the average number of web defacement attacks generated by a hacker with either Facebook or twitter account were 9.9 and 9.4 respectively. In contrast, using the other social media platforms does not seem to be related to the volume of web defacement attacks that were launched by the hackers.

In order to test our second research hypothesis, and investigate whether hackers' use of social media platforms is more likely to generate web defacement attacks during work days than during weekends, we re-estimated our models separately for web defacement attacks that took place during week days, and web defacement attacks that occurred during weekends. Results from these analyses are presented in Table 3, Panels A and B.

Starting with Panel A, one may observe that the patterns reported for the overall sample are consistent for web defacement attacks that were launched during weekdays. Specifically, the relationships between hackers' use of social

Variable	Model 1		Model 2		Model 3	
	Mean (se)	IRR	Mean (se)	IRR	Mean (se)	IRR
Any Social Media Act	.89** (.14)	2.42	-	-	-	-
# Social Media Act	-	-	.28** (.06)	1.31	-	-
Facebook	-	-	-	-	.66** (.17)	1.93
Twitter	-	-	-	-	.30+ (.16)	1.35
YouTube	-	-	-	-	-.07 (.17)	.93
Own website	-	-	-	-	.09 (.19)	1.09
Constant	1.20** (.10)		1.40** (.10)		1.36** (.10)	
Pseudo R2 Ln alpha Log likelihood	.02 .41 -952.8		.01 .45 -961.7		.01 .43 -957.1	

Panel A. Number of Attacks Generated During Weekdays

Variable	Model 1		Model 2		Model 3	
	Mean (se)	IRR	Mean (se)	IRR	Mean (se)	IRR
Any Social Media Act	.88* (.45)	2.41	-	-	-	-
# Social Media Act	-	-	.20 (.16)	1.22	-	-
Facebook	-	-	-	-	-.34 (.67)	.71
Twitter	-	-	-	-	.98 (.64)	2.66
YouTube	-	-	-	-	-.63 (.61)	.53
Own website	-	-	-	-	.52 (.71)	1.67
Constant	-.08 (.33)		.21 (.30)		.19 (.29)	
Pseudo R2 Ln alpha Log likelihood	.01 2.83 -324.4		.00 2.85 -325.5		.01 2.80 -323.4	
**0.01 *p<0.05 +p<0.1						

Panel B. Number of Attacks Generated Over Weekends

Table 3. Overall Number of Web Defacement Attacks generated in Weekday and Weekends Regressed on Hackers' Social Media Presence

media platforms and the number of web defacement attacks they generate is positive and significant. Moreover, the relationship between the number of social media account they use, and using either a Facebook or a Twitter account, significantly increases the number of web defacement attacks that were generated by hackers during the weekday.

However, the findings reported in Panel B of Table 3 reveal a different pattern for web defacement attacks generated during weekends. Specifically, although the effect of using any social media account is still significant in the model, the effect of number of social media platforms used by a hacker is no longer significant. Moreover, none of the unique social media platforms carries significant effect in the model. These findings suggest that hackers' use of social media does not predict the volume of web defacement attacks they generate over weekends.

Finally, to explore our third research hypothesis, and investigate whether the relationships between hackers' use of social media and the volume of web defacement attacks they generate is similar both for predicting web defacement attacks against US websites and against websites hosted in other countries around the globe, we re-estimated our models separately for web defacement attacks that were recorded against USA websites, and web defacement attacks that were recorded against websites hosted in other countries around the globe. Results from these analyses are presented in Table 4, Panels A and B.

Beginning with Panel A, one may observe that the findings observed for the overall sample are consistent for web defacement attacks that were launched against non-USA websites. Specifically, the relationships between hackers' use of any social media platform (b=.86, p<.01) and the number of web defacement attacks they generate is positive and significant. Moreover, using several media platforms (b=.24, p<.01), and using either a Facebook (b=.53, p<.01) or a Twitter (b=.33, p<.05) account significantly increase the number of web defacement attacks against non-USA websites.

Consistent with our research hypothesis, the findings reported in Panel B of Table 4 reveal similar relationships between hackers' use of social media platforms and volume of the web defacement attacks the generate against USA websites. However, in contrast to significant effects of both Facebook and Twitter accounts in the general models, hackers use of Twitter is the only significant predictor of the number of web defacement attacks against USA websites.

V. DISCUSSION

The DoD task force on cyber threat [3] has urged cyber defender to change their cyber security model from reactive to a more proactive approach, which obligates defenders to collect and analyze cyber intelligence. One important source for the collection of relevant information for the creation of cyber intelligence could be found in the various social media platforms, that allow users to engage with other users in interpersonal form [5]. However, to date, no prior research has investigated the relationships between hackers' use of social media platforms and their likelihood to launch cyber-attacks.

In effort to address this empirical void, we collected and analyzed data from ZONE-H and to determine the association between hackers' use of Facebook, Twitter and YouTube and the volume of web defacement attacks they generate. Results from these analyses reveal few important findings.

Variable	Model 1		Model 2		Model 3	
	Mean (se)	IRR	Mean (se)	IRR	Mean (se)	IRR
Any Social Media Act	.86** (.14)	2.37	-	-	-	-
# Social Media Act	-	-	.24** (.06)	1.27	-	-
Facebook	-	-	-	-	.53** (.17)	1.69
Twitter	-	-	-	-	.33* (.17)	1.39
YouTube	-	-	-	-	-.20 (.18)	.81
Own website	-	-	-	-	.16 (.20)	1.17
Constant	1.42** (.11)		1.65** (.10)		1.63** (.10)	
Pseudo R2 Ln alpha Log likelihood	.02 .47 -1015.4		.01 .52 -1024.5		.01 .50 -1020.3	

*0.01 *p<0.05 +p<0.1

Panel A. Overall Number of Attacks Generated Against Non-USA Websites

Variable	Model 1		Model 2		Model 3	
	Mean (se)	IRR	Mean (se)	IRR	Mean (se)	IRR
Any Social Media Act	1.39* (.54)	4.00	-	-	-	-
# Social Media Act	-	-	.44* (.21)	1.55	-	-
Facebook	-	-	-	-	-.41 (.71)	.66
Twitter	-	-	-	-	1.97** (.66)	7.23
YouTube	-	-	-	-	-.11 (.66)	.89
Own website	-	-	-	-	.10 (.79)	1.11
Constant	-2.38* (.27)		-2.11* (.37)		-2.30* (.36)	
Pseudo R2 Ln alpha Log likelihood	.02 2.93 -145.4		.02 2.96 -145.9		.04 2.75 -142.2	

Panel A. Overall Number of Attacks Generated Against USA Websites

Table 4. Overall Number of Web Defacement Attacks Generated in Weekday and Weekends Regressed on Hackers' Social Media Presence

First, we find that hackers' use of social media accounts increase the volume of web defacement attacks they generate. Moreover, our findings suggest that increase in the number of social media accounts that hackers use increases the number of web defacement attacks they generate. However, we also find that among the different social media platforms that are available for hackers to use, Facebook and Twitter are the only two platforms that carry significant effects in the model. In fact, neither the effect of YouTube or having a personal website are significant on the number of web effacement attacks. These findings are consistent with the social learning model [9] and our first research hypothesis. Indeed, it could be that social media websites connect hackers with other hackers who share similar interests, and facilitate direct interaction between them that is conducive toward the acquisition of motivations and skills that support hacking. In addition, it may be that hackers employ social media websites to notify their friends after a successful attack on their illegal activities and gain some reputation among their peers. Future research should investigate the actual content that hackers post on social media websites and explore the potential relationships between this content and the probability of hacker to launch a cyber-attack.

Second, we find that hackers' use of social media platforms increase the volume of web defacement attacks during week days but not during the weekend. These findings are consistent with our second research hypothesis and provide evidence for the importance of supporting audience for completing these types of online crimes. Specifically, these findings may suggest that web defacers who use social media platforms prefer to launch attacks during workdays since if they face difficulties during a an attack, they know they can find their friend online in search for assistance. Moreover, upon successfully completing a web defacement attack, a hacker may get the maximum level of attention for other social media users if posting a note over the social media platforms regarding the attack he completed [36-37].

Finally, we find that *hackers' use of social media platforms is associated with higher volume of web defacement attacks against both US websites as well as websites hosted in other countries around the globe.* Importantly though, while hackers' use of both Facebook and twitter accounts increase the volume of web defacement attacks generated against non-USA websites, hackers' use of twitter account increase the volume of attacks generated against US websites.

These findings are first to reveal empirical relationships between hackers' use of social media platforms and the frequency of website defacement events they launch. Moreover, they facilitate the need to develop new security tools that will collect cyber intelligence from online environments, and support identification of cues for the potential development of situations conducive to cyber-dependent crimes. For example, McCormick and colleagues [41] demonstrated that demographic information could be easily collected from Twitter users' accounts by simply viewing users' profile pictures and webpage page, and assessing users' attributes like gender, age, and race. Similar approach could be taken for collecting data from hackers' Twitter, Facebook and YouTube accounts. Those cues, in turn, could support the generation of predictions regarding potential targets of cyber-attacks, the tools that may be used by attackers, as well as the attackers' motivation.

VI. CONCLUSIONS

Information Security officers should follow law enforcement agencies' efforts to identify and monitor signs of criminal activity over social media platforms, and dedicate resources for collecting relevant strategic cyber intelligence. This practice could increase the effectiveness of cyber security efforts in preventing cyber-attacks from developing and targeting individuals and organizations. Given the significant link we find between hackers' use of social media websites and the volume of web defacement attacks they generate, we believe that these platforms could facilitate an important source of cyber intelligence that may prove useful in preventing the occurrence of different forms of cyber dependent crimes.

REFERENCES

[1] Cole, E. (2011). *Network security bible* (Vol. 768). John Wiley & Sons.

[2] Barnum, S. (2012). Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™). *MITRE Corporation*, *11*, 1-22.

[3] Gosler, J. R., & Von Thaer, L. (2013). Task force report: Resilient military systems and the advanced cyber threat. *Washington, DC: Department of Defense, Defense Science Board*, 41.

[4] Borum, R., Felker, J., Kern, S., Dennesen, K., & Feyes, T. (2015). Strategic cyber intelligence. *Information & Computer Security*, *23*(3), 317-332.

[5] Gritzalis, D., Stavrou, V., Kandias, M., & Stergiopoulos, G. (2014, March). Insider threat: enhancing BPM through social media. In *New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on* (pp. 1-6). IEEE.

[6] Kalampokis, E., Tambouris, E., & Tarabanis, K. (2013). Understanding the predictive power of social media. *Internet Research*, *23*(5), 544-559.

[7] Williams, M. L., Burnap, P., & Sloan, L. (2017). Crime sensing with big data: The affordances and limitations of using open-source communications to estimate crime patterns. *The British Journal of Criminology*, *57*(2), 320-340.

[8] Furnell, S., Emm, D., & Papadaki, M. (2015). The challenge of measuring cyber-dependent crimes. *Computer Fraud & Security*, (10), 5-12.

[9] Akers, R. L. (1985). *Deviant behavior: A social learning approach*. Wadsworth Publishing Company.

[10] Bartoli, A., Davanzo, G., & Medvet, E. (2009). The reaction time to web site defacements. *IEEE Internet Computing*, *13*(4).

[11] Ooi, K. W., Kim, S. H., Wang, Q. H., & Hui, K. L. (2012). Do hackers seek variety? An empirical analysis of website defacements. AIS.

[12] RSA (2016). 2016: Current state of cybercrime. Available at: https://www.rsa.com/content/dam/rsa/PDF/2016/05/2016-current-state-of-cybercrime.pdf

[13] Erbacher, R. F. (2005, October). Extending command and control infrastructures to cyber warfare assets. In *Systems, Man and Cybernetics, 2005 IEEE International Conference on* (Vol. 4, pp. 3331-3337). IEEE.

[14] McQuade, III, S.C. 2006. *Understanding and Managing Cybercrime*, London, England: Pearson.

[15] Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*, *68*, 81-97.

[16] Mattern, T., Felker, J., Borum, R., & Bamford, G. (2014). Operational levels of cyber intelligence. *International Journal of Intelligence and CounterIntelligence*, *27*(4), 702-719.

[17] NIAC 2017.Securing Cyber Assets: Addressing urgent cyber threats to critical infrastructure. Departement of Homeland Security.Avilable at: https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf

[18] Woo, H. J., Kim, Y., & Dominick, J. (2004). Hackers: Militants or merry pranksters? A content analysis of defaced web pages. *Media Psychology*, *6*(1), 63-82.

[19] Holt, T. J., Kilger, M., Chiang, L., & Yang, C. S. (2017). Exploring the correlates of individual willingness to engage in ideologically motivated cyberattacks. *Deviant Behavior*, *38*(3), 356-373.

[20] Kanti, T., Richariya, V., & Richariya, V. (2011). Implementing a Web browser with Web defacement detection techniques. *World of Computer Science and Information Technology Journal (WCSIT)*, *1*(7), 307-310.

[21] Akers, R. L., & Jensen, G. F. (2006). The empirical status of social learning theory of crime and deviance: The past, present, and future. *Taking stock: The status of criminological theory*, *15*, 37-76.

[22] Haynie, D. L. (2001). Delinquent peers revisited: Does network structure matter?. *American journal of sociology*, *106*(4), 1013-1057.

[23] Pratt, T. C., Cullen, F. T., Sellers, C. S., Thomas Winfree Jr, L., Madensen, T. D., Daigle, L. E., ... & Gau, J. M. (2010). The empirical status of social learning theory: A meta-analysis. *Justice Quarterly*, *27*(6), 765-802.

[24] Schell, B. H., & Dodge, J. L. (2002). *The hacking of America: Who's doing it, why, and how*. Greenwood Publishing Group Inc..

[25] Bossler, A. M., & Burruss, G. W. (2011). The general theory of crime and computer hacking: Low self-control hackers. *Corporate hacking and technology-driven crime: Social dynamics and implications*, 38-67.

[26] Boyd, D., & Ellison, N. (2007). Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13, 210–230.

[27] Acar, A. (2008). Antecedents and consequences of online social networking behavior: The case of Facebook.Journal of Website Promotion, 3, 62–83.

[28] Lefebvre, R., & Bornkessel, A. (2013). Digital social networks and health. Circulation, 127, 1829–1836.

[29] Patton, D. U., Hong, J. S., Ranney, M., Patel, S., Kelley, C., Eschmann, R., & Washington, T. (2014). Social media as a vector for youth violence: A review of the literature. *Computers in Human Behavior*, *35*, 548-553.

[30] McCuddy, T., & Vogel, M. (2015). More than just friends: Online social networks and offending. *Criminal Justice Review*, *40*(2), 169-189.

[31] Sela-Shayovitz, R. (2012). Gangs and the web: Gang members' online behavior. *Journal of Contemporary Criminal Justice*, *28*(4), 389-405.

[32] Weir, G. R., Toolan, F., & Smeed, D. (2011). The threats of social networking: Old wine in new bottles?. *Information security technical report*, *16*(2), 38-43.

[33] Wijeratne, S., Doran, D., Sheth, A., & Dustin, J. L. (2015, May). Analyzing the social media footprint of street gangs. In *Intelligence and Security Informatics (ISI), 2015 IEEE International Conference on* (pp. 91-96). IEEE.

[34] Balasuriya, L., Wijeratne, S., Doran, D., & Sheth, A. (2016, August). Finding street gang members on twitter. In *Advances in Social Networks Analysis and Mining (ASONAM), 2016 IEEE/ACM International Conference on* (pp. 685-692). IEEE.

[35] Pyrooz, D. C., Decker, S. H., & Moule Jr, R. K. (2015). Criminal and routine activities in online settings: Gangs, offenders, and the Internet. *Justice Quarterly*, *32*(3), 471-499.

[36] Patel, N. (2015). What are the best times to post on social media. Saatavissa: https://www. quicksprout. com/2015/01/02/what-are-the-best-times-to-post-on-social-media/. Viitattu, 27, 2016.

[37] Trackmaven. (2016). Best times to post on Social Media. Avilable at: https://trackmaven.com/blog/best-times-to-post-social-media/

[38] U.S. Census Bureau. (2013). U.S. and world population clock. Retrieved July 25, 2013, from http://www.census.gov/popclock/

[39] Maimon, D., Kamerdze, A., Cukier, M., & Sobesto, B. (2013). Daily trends and origin of computer-focused crimes against a large university computer network: An application of the routine-activities and lifestyle perspective. *British Journal of Criminology*, *53*(2), 319-343.

[40] Osgood, D. W. (2000). Poisson-based regression analysis of aggregate crime rates. *Journal of quantitative criminology*, *16*(1), 21-43.

[41] McCormick, T. H., Lee, H., Cesare, N., Shojaie, A., & Spiro, E. S. (2017). Using Twitter for demographic and social science research: tools for data collection and processing. *Sociological Methods & Research*, *46*(3), 390-421.