Georgia State University

ScholarWorks @ Georgia State University

EBCS Proceedings

Evidence-Based Cybersecurity Research Group

2017

Re-Thinking Online Offenders' SKRAM: Individual Traits and Situational Motivations as Additional Risk Factors for Predicting Cyber Attacks

David Maimon
Georgia State University (at time of archiving)

Steve Hinton
StratumPoint, Inc.

Olga Babko-Malaya
BAE Systems

Rebecca Cathey
BAE Systems

Recommended Citation

Maimon, David, Andrew Fukuda, Steve Hinton, Olga Babko-Malaya, and Rebecca Cathey. 2017. "On the relevance of social media platforms in predicting the volume and patterns of web defacement attacks." Conference Proceeding - 2017 IEEE International Conference on Big Data (Big Data), pp. 4668-4673.

Re-Thinking Online Offenders' SKRAM: Individual Traits and Situational Motivations as Additional Risk Factors for Predicting Cyber Attacks

David Maimon
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]— Cyber security experts in the U.S. and around the globe assess potential threats to their organizations by evaluating potential attackers' skills, knowledge, resources, access to the target organization and motivation to offend (i.e. SKRAM). Unfortunately, this model fails to incorporate insights regarding online offenders' traits and the conditions surrounding the development of online criminal event. Drawing on contemporary criminological models, we present a theoretical rationale for revising the SKRAM model. The revised model suggests that in addition to the classical SKRAM components, both individual attributes and certain offline and online circumstances fuel cyber attackers' motivation to offend, and increase the probability that a cyber-attack will be launched against an organization. Consistent with our proposed model, and its potential in predicting the occurrence of different types of cyber-dependent crimes against organizations, we propose that Information Technology professionals' efforts to facilitate safe computing environments should design new approaches for collecting indicators regarding attackers' potential threat, and predicting the occurrence and timing of cyber-dependent crimes.**

Keywords— Hackers, Cyber-Dependent Crime

I. Introduction

Computers and computer-networks (i.e. an interconnected collection of autonomous computers that allow an easy exchange of information between users) [1] have become an integral part of American industry, business and government. Their efficient operation is increasingly critical to the survival of the USA and its organizations [2]. However, next to supporting legitimate business activities and facilitating opportunities to interact with employees, clients and vendors, the heavy reliance of large organizations on computers and computer networks increases their vulnerability to a wide range of 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) [3,4]. Indeed, numerous reports suggest that large corporations and governmental agencies experience a wide range of computer focused crimes including system-trespassing (or hacking), website defacement, Distributed Denial of Service (DDoS) attacks, and malicious software infections [5-7], with an estimated $400 bilion annual cost to the global economy from these crimes [8].

To deal with these new and increasing threats and facilitate more secure computing environments, CISOs in large organizations and their teams evaluate the threats to their organizations periodically and ensure that their organizations apply up-to-date security solutions that are designed to prevent, detect, and mitigate malicious cyber activities [9]. However, these efforts fall short in predicting the type and timing of an attack against an organization due to the difficulties involved in collecting and analyzing reliable information about hacker groups, their intentions, and tools to develop meaningful indications and warnings of potential attacks. As a result, information technology teams are required to employ scattered security solutions, and only rarely focus attention on concrete and viable threats. This is unfortunate since although online criminals consistently look for opportunities to attack potential targets, attacks against either target of opportunity or targets of choice are launched only under specific set of conditions and circumstnaces. Therefore, we propose that a successful

[1] 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. Approved for public release; unlimited distribution.

organizational cyber security strategy should draw on deep understanding of how conditions conducive to cyber-attacks evolve, as well as awareness to both online and offline circumstances that increase online-offenders' situational motivation to offend. Adopting such an approach for cyber security requires the development and implementation of new tools that allow the collection and analysis of information about online criminals and the concrete emerging threats they pose to an organization in real time. Below, we outline the theoretical rationale that supports the suggested approach.

II. Assessing Attackers' Potential Threat To an Organization

The growing number of victims of cyber dependent crimes in the U.S. and around the world, as well as the wide variation in victims' demographic characteristics (ranging from large organizations to private individuals), encouraged scientific explorations around cyber-criminals and their operations against online targets. Those investigations yielded several hackers typologies that mainly differentiate between hackers' level of malicious intents (for instance white, black and grey hackers [10]), skill levels (i.e. low, mid and high [11, 12]), and motivation to launch a cyber attack (for instance, thrill, monetary gain, revenge, recreation, ideology and exploration) [13]. Consistent with these typologies, Parker [14] developed a model for assessing attackers' (both individuals and groups) potential threat to organizational information systems. Specifically, Parker suggested that when considering the implementation of new cyber-security strategies in an organization, information security professionals should assess five key elements in the potential profile of those who may be interested in launching attacks against the organizations, and address these elements accordingly. The five elements are Skills, Knowledge, Resources, Authority and Motivations (i.e. SKRAM). Skills pertains to potential offenders' aptitude, expertise and competency to launch particular cyber-dependent crimes. Knowledge refers to offenders' familiarity with facts about different attack methods and tools, as well as understanding of information systems that are used by potential targets. Both skills and knowledge could be acquired by online offenders over time through either informal or formal training and collaboration. Resources refers to offenders' access to means like time, money, hardware, software and other types of technologies which enable them to initiate cyber-dependent crimes. Authority pertains to offenders' access to facilities or information systems. And finally, motives refer to the underlying reasons behind online offenders' involvement in online crime. Indeed, online offenders' motives to engage in wide range of cyber-dependent crimes may vary quite a bit, and include a desire to explore computer technology, the thrill of engaging in illegal activities, revenge, ideology, and/or monetary gain. Importantly, Parker [14] suggests that offenders' motives could determine the identity of potential victims, in addition to the methods and tools that will be used by online offenders to launch a cyber-dependent crime event. Reffering to the interaction between these five key elements, Parker proposes that online offender's potential SKRAM can increase over time to become a greater threat to a target. Moreover, the threat potential imposed by multiple online offenders and online crime groups increases substantially through synergistic activities, and in turn, increases the threat potential for the organization.

Parker's model has served as an important guideline to Information Technology officers, security professionals, law enforcement investigators and policy makers who aim to identify the risk of cyber-dependent crimes against organizations and build more effective security policies and defense systems against different type of hackers [15]. However, although useful in identifying potential online risks to organizations, the model carries two main problems. First, it does not take into consideration individual level factors that are known to be antecedents of individual involvement in deviance and crime. Specifically, extensive criminological research suggests that various demographic charactaristics and personality traits are key predictors for influencing individuals' decision to initiate a criminal event [16-17]. Second, this model (like many other recent typologies (for instance [18]) elaborates factors like revenge, monetary gain, obsession and thrill seeking as key motivations for individuals online offend. By doing so, it seems like Parker adopts [19] defenition of individual motivation to launch a cyebr attack as both the reasons for individuals engagement in cyber-dependent crimes as well as the measure of the degree to which the attack will repeat. However, the common premise among modern criminologists suggests that individuals' needs and values cannot explain individuals' involvement in crime since the same needs and values could be obtained through non-criminal behaviors [20]. Accordingly, monetary gain, revenge or thrill seeking are not obtained solely through involvement in crime. In fact, individuals who pursue a normative lifestyle may end up obtaining financial gain, revenge or excitement by simply pursuing legitimate life style (for instance attending school, working for a respectable company or going on an exciting trip). Therefore, these desires and goals cannot explain individuals' involvement in crime, and should not be confused with one's motivation to offend. Instead, extensive criminological literature suggests that individual's motivation to offend comes either from within [21], and/or from the environment [22-23]. We believe that this theoretical elaboration could be of interest to information technology and network security teams in organizations since it factors in valuable information that could predict the occurrence, types and timing of cyber-dependent crimes against organizations.

III. The Motivation to Offend in the Criminological Literature

In general, criminologists who seek to understand the etiology of crime emphasize two approaches that explain individual motivation to offend. The first suggests that the motivation and the drive to offend originate in an individual's psychology and personality traits, while the second approach emphasizes environmental cues as key for the development of the motivation to offend. Criminological explanations that focus on individual attributes and internal processes as key factors that determine an individual's involvement in crime highlight the role of decision-making processes [24], weak self-control [25], and the absence of coping mechanisms that allow individuals to handle with negative emotions in a legitimate way [26]. In contrast, criminological models that perceive the motivation to offend as originated in the environment, emphasize the role of socialization and learning [20, 23], as well as of situations conducive to crime [22] in increasing individual's motivation to initiate a criminal event. We briefly detail the underlying assumptions of these key criminological models, and link them to individual's probability to launch cyber-dependent crimes.

A. *Individual based explanations of crime*

Rational Choice and Deterrence- Rational choice models assume that human beings are rational, self-interested actors who seek to minimize personal cost while maximizing personal gain [24,27]. An important implication of such perspectives in the context of criminal behaviors is that individual behavior can be altered by the threat and imposition of punishment as well as the availability of rewards. While early work on rational choice emphasized the role of sanctions in deterring individuals from engaging in crime [28], contemporary scholars discuss the relationships between various aspects of sanctioning (for instance formal vs informal) and individual deviant outcomes.

Clarke and Cornish's [29] extension of the rational choice theory emphasizes the need to understand criminals' decision-making processes in the contexts of their lifestyles, experiences and situations they encounter. According to these scholars, criminal decision-making takes place within social, physical and situational contexts that shape offenders' perception of the world around them [29]. Thus, individuals' assessment of costs and benefits are subjective and bounded. Accordingly, under certain circumstances, risks that once deterred criminals are no longer effective and deterring, and rewards that were previously ignored become extremely attractive [30]. Applying Clarke and Cornish's rational in the context of cyber-dependent crimes, we argue that when potential rewards for launching a cyber-dependent crime outweigh potential costs, cyber-criminals will be more likely to launch a criminal event [31-33].

Weak Self-Control- Following the classical criminological tradition, Gottfredson and Hirschi [25] perceive criminal behavior as a consequence of the variably restrained human tendency to seek pleasure and avoid pain. In line with this view, these authors suggest that the tendency toward crime and deviance can be explained by an individual's level of self-control. Those lacking self-control are characterized as impulsive, insensitive, physical, risk seeking, short-sighted and nonverbal. In their seminal work, Gottfredson and Hirschi view individuals with low levels of self-control as unable to resist temptations, and as prone to act on criminal opportunities to engage in crime. In line with this theoretical model, we suspect that low self-control individuals are more likely to take advantage of online opportunities to engage in cyber-dependent crimes and launch cyber dependent criminal events then low self-control individuals [36].

Strain, Frustration and Crime- Agnew's General Strain Theory [26] stresses that an individual's experiences of strains such as blocked goals, the removal of valued stimuli, or the imposition of negative stimuli may provoke negative emotions such as anger and frustrations, which in turn, could motivate individuals' use of deviant behavior to deal with the negativity. Agnew assumes that strain is unpleasant and may upset an emotional equilibrium, so a strained individual will try to do something to alleviate the strain or correct the emotional disequilibrium that it creates. Most of the time, and for most people, strain produces conventional cognitive or non-deviant behavioral and emotional coping. However, sometimes, and under some conditions, strain leads to deviant behavior or unconventional, although not necessarily deviant, coping. Agnew details aspects of strain that enhance the likelihood of leading to deviant adaptations. He focuses particularly on cumulatively and the ratio of negative to positive factors, but he also notes the importance of the magnitude, recency, duration and clustering of stress inducing situations. Moreover, strains that are more likely to result in crime are strains that seen as unjust, are seen as high in magnitude, are associated with low social control and create some pressure or incentive to engage in crime (Agnew 2002). Consistent with the General Strain perspective, we propose that negative experiences increase cyber criminals' negative emotions, and in the absence of legitimate coping skills, increase their likelihood to launch cyber-dependent crimes.

B. *Environmental based explanations of crime*

Learning To Be a Criminal- The social learning theory [34] 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 excessive exposure to definitions favorable towards violating the law over definitions that are unfavorable towards the violations of laws, is the underlying cause for individuals' adoption of a criminal lifestyle and involvement in deviance and crime. According to this theory, the learning process involves the learning of motivations (i.e. rationalizations for the act) and techniques (i.e. skills and tools), and draws on the balance of anticipated rewards and punishments for engaging in a criminal behavior. All in all, 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 [35] and that peer associations are important for introducing new hackers to both hacking tools and methods [36].

Situations Conducive to Online Crime- Briar and Piliavin [22] suggested that all people are capable of deviant and exhibit criminal behaviors under the right circumstances. Specifically, according to these theoreticians, situationally induced stimuli of relatively short duration can influence individuals' values and behaviors in such a way that will lead to a decision to engage in illegal behaviors, independent of their personality traits and commitment to conformity. Drawing on Briar and Piliavin's claims, and emphasizing the centrality of offenders' decision-making processes in determining involvement in deviance and crime, Clarke differentiates (1995) between individual decisions to become involved in crime (i.e. criminal involvement) and decisions to become involved in a particular crime (i.e. criminal event). According to Clarke, individuals first decide whether they are willing to become involved in crime. This decision is largely influenced by past learning and experiences (including moral code) and a range of background characteristics (demographic and social)[37]. Once the choice to get involved in crime is made, individuals need to decide to commit particular offenses. This decision is largely determined by the immediate situations individuals encounter. Importantly, Clarke acknowledges the prevalence of situations conducive to crime in the life of most people, and the commission of risky behaviors and illegal acts by both "ordinary citizens" and "hardened offenders." Incorporating this insight with the notion that the decision to initiate a risky behavior is induced by the absence of moral opprobrium attached to criminal opportunities, Clarke contends that offenses like trespassing and theft may be effectively prevented by increasing the pressure to comply with the law. In the absence of such pressure, situations conduce to crime will emerge, and increase the probability of individuals to initiate criminal events. Thus, consistent with the underlying premise of situational explanations of crime we posit that the emergence of situations conducive to online crime increase cyber-criminals' probability to launch a cyber-dependent crime event.

IV. Revised SKRAM (DSK-RAMG) model

Based on the rationale discussed in these criminological models, we propose a revision to Parker's SKRAM [14]. Specifically, although we acknowledge the necessity to consider cybercriminals' *skills, knowledge, resources, authority and motivation* for predicting organizational risks of cyber-dependent crimes, we suggest refining the concept of motivation, and adding two additional predictive elements for assessing organizations' potential risks from cyber-criminals: online offenders' *demographic* and personal attributes and *goals* (i.e. DSK-RAMG). We believe that revision of this model could prove useful in improving Information Technology managers' efforts to assess the risk posed to their organizations by range of cyber criminals.

A. *Attackers' demographic and personality traits.*

Parker's model fails to account for online criminals individuals traits as a potential risk factors to organizations cyber security. However, several psychological and criminological studies identify individual's demographic and personality attributes that are associated with cyber-dependent criminals. For instance, [38] report that hackers tend to be male, obsessive and explorers. [12] profiles hackers as young, intelligent, and loners. Hackers are also reported to come from middle class status, have poor social and communication skills, low self-esteem, and a strong desire to succeed [39]. Bossler and Burruss [36] find that computer hackers are likely to have lower levels of self-control. Finally, Young and associates [40] demonstrate that computer hackers employ rational decision making process before engaging in cybercrime by perceiving high utility value from hacking, little informal sanctions, and a low likelihood of punishment. Moreover, these scholars report that computer hackers tend to exhibit high levels of moral disengagement.

Drawing on these studies, and the criminological school of thought that ties individual's personality traits with the probability to offend, we suspect that knowledge regarding cyber-dependent criminals' demographic and personality traits could be useful in predicting the occurrence, type and timing of cyber-dependent crime against specific organizations. For instance, we suspect that highly impulsive cyber-criminal will be more likely to launch cyber-dependent crimes against organization of interest than cyber criminals who are only slightly impulsive [36]. Moreover, impulsive online criminals are more likely to initiate higher volume and types of cyber-dependent crimes. Similarly, we suspect that online offenders with lower levels of Thoutfully Reflective Decision Making (TRDM) [41] may be more volatile against less sophisticated targets, and less effective in generating well thought and cyber-dependent crimes against large organizations.

B. *Situational motivation to launch a cyber event*

Next to the role of personality, we emphasize the role of situational motivation for increasing online offenders' potential risk to launch cyber-dependent crimes against large organizations. All in all, Cornish and Clarke [42] identify five broad situations conducive to the development of offline criminal events. The first are any circumstances under which offenders need to invest relatively low amount of effort for initiating crime (for instance the absence of locks on doors). The second are situations in which the risk of getting caught and punished are low (for instance the absence of security guards and CCTV cameras in public places). The third type of circumstances are situations in which the potential rewards from the criminal event are relatively high (for instance expensive piece of jewelry). The fourth type of situations conducive to crimes are situations that increase individual emotional arousals (for instance disputes). Finally, the last set of situations conducive to crime are all these situations in which offenders can excuse and justify their involvement in crime (for instance the lack of behavioral rules in a public park).

Translating these situations to the online environment, one can identify a wide range of both offline and online situations that could increase online offenders' situational motivation to launch cyber-dependent crimes. For instance, knowledge regarding computer vulnerabilities reduce online offenders' efforts to break security on a system, and in turn, increase the probability they will try to gain an illegitimate access to organizational computers [43]. The availability of unencrypted data as well we the absence of surveillance on either a computer or computer network, reduce online offenders risk of detection and punishment, and in turn increase their probability to launch cyber dependent crimes [44]. The emergence of online black markets and hackers' forums over the dark net increase online offenders' potential rewards from engaging in online crimes, and in turn, increase the situational motivation to launch cyber-dependent crime events [45]. Political events like wars and military provocations, may increase potential online offenders anger and frustrations, and in turn, increase their situational motivation to launch a cyber-dependent crime against rival political entities (for instance the alleged cyber-attacks initiated by Russia on Estonian organization for several days in response to the relocation of a Soviet-era grave marker (i.e. the Bronze Soldier of Tallinn) in

Tallinn, Estonia [46]). Finally, the absence of clear guidelines with respect to the appropriate ways to use computing environment may increase individual's potential for justifying an online criminal event and result in the development of a cyber-dependent crime.

C. Attackers' Goals.

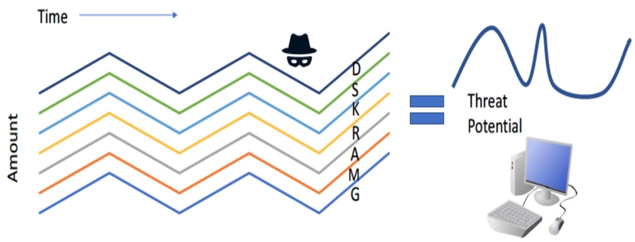
We believe that understanding cyber-criminals' goals in launching cyber-dependent crimes against an organization could improve security officials' assessments of potential cyber-risks to their organizations. Specifically, we suspect that online criminals' goals in launching cyber-dependent events could range from a desire to explore computer technology, the thrill of engaging in illegal activities, willingness to gain prestige among peers, revenge, obsession, ideology, or monetary gain [13]. Moreover, it is possible that cyber-criminals are willing to engage in online criminal behaviors in order to obtain more than just one goal. Importantly, previous works have already identified these goals as important for assessing potential online offender' risks of attacking specific organizations. However, in contrast to past research that listed these goals as motivations, we follow the rationale proposed in the criminological literature, and classify this list of desires as cyber-criminals goals.

V. Concrete Security Implications to Draw from the DSK-RAMG Model

The growing number of online offenders who are willing and capable of launching significant cyber-dependent crimes against organizations, obligates information technology officers to adopt security measures that aim to identify likely threats, harden their organization against likely attack vectors, and replicate the security measures used in a fortress model for protecting a physical space [47-48]. *Fortress computing environments*, which are commonly adopted by major governmental agencies and large financial and industrial organizations, are computing environments within which substantial control is enforced on users' access to the computer network [49]. In line with the value placed in the model-based approach for describing, analyzing and identifying cyber-risk, we posit that similarly to Parker's [14] and Jones's [50] models, our proposed model could be employed for assessing online offenders' potential threat to an organization [15]. However, due to the emphasis placed on situational motivation in the DSK-RAMG model, we propose that this model may be used for predicting the occurrence of cyber-dependent crimes. Specifically, we suggest that *the intersection of attackers' personal traits, skills, knowledge, resources, authority and situational motivation level to offend could be effective in assessing online offenders' threat and predicting the risk that a cyber-dependent crime will develop.*

Indeed, the underlying premise behind Parker's [14] SKRAM model is similar to the aforementioned proposition. However, in contrast to Parker's focus in a unidimensional state in which heightened online offender's SKRAM poses a greater threat to a target, we propose that fluctuations in online offenders' DSK-RAMG components over time, results in variation in targets' vulnerability to a potential cyber attack. Specifically, as indicated in Figure 1, with the exception of two demographic traits which tend to remain constant over time (i.e. gender and race), the magnitude and direction of all the DSK-RAMG model's components could increase at some times, decrease in other times, and yet remain unchanged and stagnate in other occasions. Consider for instance the case of cyber-warrior and their motivation to engage in cyber-attacks during times of political and military tensions vs during time of piece. Indeed, in times of war the situational motivation of cyber warriors to launch cyber-attacks against rival countries' targets will be significantly higher than the situational motivation during peaceful times. Similarly, hacktivists' motivations to launch cyber-attacks will be higher in times in which the group is trying to push a political agenda than during times they are not. Consequently, the potential levels of threat to targets fluctuates over time and can differ across times of day, week and even month.

Figure 1. DSK-RMPG Model For Assessing Adversaries Situational Threat Potential



Since the motivation to launch a cyber-dependent crime is originated in the environment (both offline and online) and could be triggered by unique set of circumstances, we suspect that it is important to identify situations conducive to cyber-dependent crimes, flag their potential influence on different threat agents, and generate predictions regarding the likelihood of these situations to result in specific types of attacks against unique organizations. Moreover, we suspect that the timing in which situations conducive to cyber-dependent crime emerge, may support predictions of the time frame in which cyber-dependent crimes will occur. Thus, we adopt Cohen and Felson's[51] assumption that a successful criminal event requires the convergence in space and time of motivated offender, suitable target and the absence of capable guardian, and suspect that *the timing in which a cyber-dependent crime will be launched against a target organization is a function of the culmination of the various DSK-RAMG model components into a tipping point.*

.

VI. CONDUCIVE ENVIRONMENTS FOR THE COLLECTION OF ATTACKERS' DSK-RAMPG CUES

Reflecting upon potential ways to apply our claims in the context of organizational security practices, one may suggest the potential utility of IDSs and IPSs for predicting cyber-dependent crimes and monitoring their development. However, traditional IDSs and IPSs primarily focus on detection of malicious activity as or after it happens [52-53]. Similarly, one may point out the availability of current approaches for event based predictions, such as the *rule-based* (which are merely expert generate rules [54]), *case-based* (which do not include mechanism for discovering temporal correlations), *Finite State Machine based* (which are rarely available in situations where human actions have significant impact), *Model- based* (which are rarely applicable in cyber domains), and *Probabilistic* (in which exact inference is intractable) approaches [55-57]. Unfortunately, these approaches draw on problematic (and sometime unrealistic) assumptions and methodologies.

Therefore, we suspect that there is a need to develop new security tools that will collect online and offline cues for the potential development of situations conducive to cyber-dependent crimes, and generate predictions regarding the occurrence, timing and later stages of an attacks. Such tools should pick cues for the potential increase in situational motivations to launch cyber-dependent crimes from online environments (for instance hackers' forums and social media sites like Twitter and Facebook which were already proved useful in forecasting flue epidemics [58], and online threats like spam [59]), and use these cues to generate probabilities for the development and progression of cyber-dependent crime events. We believe that the design of these tools should also draw on recent successful attempts to assess social media users' demographic and personality traits using data from the online environment [60,61]. Indeed, McCormick and colleagues [60] have already 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 when colleting data from Facebook's users. Moreover, Sumner and associates [61] showed that Twitter users' profile attributes and use of language could be indicative of personality traits that are associated with the Dark Tried personality (i.e. psychopathy, narcissism and Machiavellianism) and with the Big Five Personality Traits (i.e. extraversion, agreeableness, openness, conscientiousness and neuroticism). Building abilities for data collection and assessment, could improve organizations' security posture and their effectiveness in preventing and mitigating cyber attacks .

VII. CONCLUSIONS

Our proposed model is designed to revise and elaborate the personal and situational circumstances that influence a threat agent's probability to launch a cyber-dependent crime incident against target organizations. In addition to emphasizing threat agents' skills, knowledge, resources, authority, and motivation, our model emphasizes the important contribution of attackers' personal attributes and goals for initiating cyber-dependent crimes. Moreover, acknowledging that the motivation to offend comes both from within and from the environment, we suggest that cyber-dependent crimes are more likely to occur with the culmination of the various DSK-RAMG model components into a tipping point. Drawing on this model, we suspect that efforts should be made to build security tools that allow the predictions of both the target and time of cyber-dependent crimes.

REFERENCES

[1] Tanenbaum, A.S. (2003). *Computer Networks (4th edition)*. NJ: Prentice Hall.

[2] Fritzon, A., Ljungkvist, K., Boin, A., and Rhinard, M. (2007). "Protecting Europe's Critical Infrastructures: Problems and Prospects." *Journal of Contingencies and Crisis Management 15:30-41*.

[3] Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society.* Boston, MA: Addison- Wesley.

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

[5] Rantala, R. R. (2008). Cybercrime against businesses, 2005. *organization*, *15*(14), 9.

[6] 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

[7] Norton. (2016). Norton Cyber Security Insight Report. Available at: https://us.norton.com/norton-cybersecurity-insights-report-global

[8] Mcafee. (2014). Net Losses: Estimating the Global Costs of Cybercrime. Available at https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

[9] Mackey, D. (2003). Web Security for Network and System Administrators. Cengage Learning.

[10] Sabillon, R. ., Cano, J., Cavaller, V., & Serra, J. (2016). Cybercrime and Cybercriminals: A Comprehensive Study. *International Journal of Computer Networks and Communications Security*, *4*(6), 165-176.

[11] Landreth, B. (1985). Out of the Inner Circle: a Hacker's Guide to Computer Security. Microsoft Press.

[12] Chantler, N. (1996). Profile of a computer hacker. *Florida: infowar*.

[13] Seebruck, R. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation*, *14*, 36-45.

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

[15] McQuade, S C. (2006). *Understanding and Managing Cybercrime*. Pearson Education INC

[16] Caspi, A., Moffitt, T. E., Silva, P. A., Stouthamer-Loeber, M. A. G. D. A., Krueger, R. F., & Schmutte, P. S. (1994). Are some people crime-prone? Replications of the personality-crime relationship across countries, genders, races, and methods. *Criminology*, *32*(2), 163-196.

[17] Krueger, R. F., Schmutte, P. S., Caspi, A., Moffitt, T. E., Campbell, K., & Silva, P. A. (1994). Personality traits are linked to crime among men and women: Evidence from a birth cohort. *Journal of abnormal psychology*, *103*(2), 328.

[18] Hald, Sara LN, and Jens M. Pedersen. (2012)."An updated taxonomy for characterizing hackers according to their threat properties." In *Advanced Communication Technology (ICACT), 14th International Conference on*, pp. 81-86. IEEE.

[19] Sykes, J. B. (1981). The Concise Oxford Dictionary, Clarendon Press.

[20] Sutherland, E. H. (1942). Development of the theory. *Edwin Sutherland on analyzing crime*, 30-41.

[21] Nagin, D. S., & Paternoster, R. (1993). Enduring individual differences and rational choice theories of crime. *Law and Society Review*, 467-496.

[22] Briar, S., & Piliavin, I. (1965). Delinquency, situational inducements, and commitment to conformity. *Soc. Probs.*, *13*, 35.

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

[24] Paternoster, R. (1987). The deterrent effect of the perceived certainty and severity of punishment: A review of the evidence and issues. *Justice Quarterly*, *4*(2), 173-217.

[25] Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.

[26] Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology*, *30*(1), 47-88.

[27] Ross, L., & LaFree, G. (1986). Deterrence in criminology and social policy. *Behavioral and social science: Fifty years of discovery*.

[28] Bentham, J. (1970 [1789a]). An Introduction to the Principles of Morals and Legislation, ed. J.H. Burns and H.L.A. Hart. London: Athlone Press

[29] Clarke, R & Cornish, D .(1985). "Modelling offenders' decisions: a framework for research and policy." Pp. 147-85 in M. Tonry and N. Morris (eds.), Crime and Justice: An Annual Review of Research, Volume 6. Chicago: University of Chicago Press.

[30] Copes, H., & Vieraitis, L. M. (2009). Bounded rationality of identity thieves: Using offender based research to inform policy. *Criminology & Public Policy*, *8*(2), 237-262.

[31] Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014). Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology*, *52*(1), 33-59.

[32] Wilson, T., Maimon, D., Sobesto, B., & Cukier, M. (2015). The Effect of a Surveillance Banner in an Attacked Computer System: Additional Evidence for the Relevance of Restrictive Deterrence in Cyberspace. *Journal of Research in Crime and Delinquency*, *52*(6), 829-855.

[33] Testa, A., Maimon, D., Sobesto, B. & Cukier M. (2017). Illegal Roaming and File Manipulation on Target Computers Assessing the Effect of Sanction Threats on System Trespassers' Online Behaviors. Criminology and Public Policy.

[34] Agnew, R. (2002). Experienced, vicarious, and anticipated strain: An exploratory study on physical victimization and delinquency. *Justice Quarterly*, *19*(4), 603-632.

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

[36] 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.

[37] Clarke, R.V. (1995). Situational Crime Prevention. In *Crime and Justice: A Review of Research*, Vol. 19, 91-150

[38] Jordan, T. & Taylor, P. (1998)."A sociology of hackers." *The Sociological Review* 46, no. 4: 757-780.

[39] Wentworth, E. (2002). Theories of Hacker Psychological Motivations and Profiles. available online at www. cs. ucf. edu/ courses/ cgs5132/ spring2002/ presentation/ wentworth. ppt.

[40] Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into the minds of hackers. *Information Systems Management*, *24*(4), 281-287.

[41] Paternoster, R., & Pogarsky, G. (2009). Rational choice, agency and thoughtfully reflective decision making: The short and long-term consequences of making good choices. *Journal of Quantitative Criminology*, *25*(2), 103-127.

[42] Cornish D, & Clarke, RV. (2003). Opportunities, Precipitators and Criminal Decisions: A Reply to Wortley's Critique of Situational Crime Prevention. In: Smith M, Cornish D, editors. Theory for Practice in Situational Crime Prevention, Crime Prevention Studies. Vol. 16. Monsey, NY: Criminal Justice Press, 41-96.

[43] Maimon, D., Wilson, T., Ren, W., & Berenblum, T. (2015). On the relevance of spatial and temporal dimensions in assessing computer susceptibility to system trespassing incidents. *British Journal of Criminology*, azu104.

[44] Willison, R & Siponen, M. (2009) Overcoming the insider: reducing employee crime through Situational Crime Prevention. Communications of the ACM, 52 (9). pp. 133-137.

[45] Hutchings, A., & Holt, T. J. (2014). A crime script analysis of the online stolen data market. *British Journal of Criminology*, azu106.

[46] Kenney, M. (2015). Cyber-terrorism in a post-stuxnet world. *Orbis*, *59*(1), 111-128.

[47] Nosworthy, J. D. (2000). "A Practical Risk Analysis Approach: managing BCM risk."Computers & Security 19 (7): 596-614.

[48] Tregear, J. (2001). "Risk Assessment." Information Security Technical Report 6 (3): 19-27.

[49] Scully, T. (2011). The cyber threat, trophy information and the fortress mentality. *Journal of business continuity & emergency planning*, *5*(3), 195-207.

[50] Jones, A. (2002). Identification of a Method for the Calculation of the Capability of Threat Agents in an Information Environment. School of Computing. Pontypridd, University of Glamorgan: 0-134

[51] Cohen, L.E. and Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review* 44: 588-608.

[52] Scarfone, K.Mell, P. (2007). "Guide to Intrusion Detection and Preventi on Systems (IDPS)". Computer_Security Resource Center (National Insi tute of Standards and Technology) (800–94).

[53] Valeur, F., Vigna, G., Kruegel, C., & Kemmerer, R. A. (2004). Comprehensive approach to intrusion detection alert correlation. *IEEE Transactions on dependable and secure computing*, *1*(3), 146-169.

[54] Müller, A., Göldi, C., Tellenbach, B., Plattner, B., & Lampart, S. (2009). Event correlation engine. Department of Information Technology and Electrical Engineering-Master's Thesis, Eidgenössische Technische Hochschule Zürich.

[55] Valdes, A., & Skinner, K. (2001). Probabilistic alert correlation. In *Recent advances in intrusion detection* (pp. 54-68). Springer Berlin/Heidelberg.

[56] Steinder, M., &.Sethi, A. S. (2004).Probabilistic fault diagnosis in comm unication systems through incremental_hypothesis updating. Computer Networks 45, 4, 537-562.

[57] Steinder, M., &,Sethi, A. S. (2004).A survey of fault localization techniques in computer networks. *Science of Computer Programming* 53, 2, 165-194.

[58] Achrekar, H., Gandhe, A., Lzarus, R., Yu, S.-H., & Liu, B. (2011) Predicting flu trends using twitter data. In *Conferenceon Computer Communications Workshops (INFOCOM WKSHPS),* IEEE, pp. 702–707.

[59] Thomas, K., Li, F., Grier, C., & Paxson, V. (2014). Consequences of connectivity: Characterizing account hijacking on twitter. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 489-500). ACM.

[60] 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.

[61] Sumner, C., Byers, A., Boochever, R., & Park, G. J. (2012, December). Predicting dark triad personality traits from twitter usage and a linguistic analysis of tweets. In *Machine learning and applications (icmla), 2012 11th international conference on* (Vol. 2, pp. 386-393). IEEE.