Toward Cognitive Immunization of Potential Criminals against Cyberterrorism

Merrill Warkentin
Department of Management & Information Systems
Mississippi State University
MS STATE, MS 39762 USA
m.warkentin@msstate.edu

Joshua M. Regan
Henry C. Lee College of Criminal Justice
University of New Haven
West Haven, CT 06516 USA
jrega1@unh.newhaven.edu

Amin G. Kosseim
Community Affairs Division
New York City Police Department
New York, NY 10128 USA
agkosseim@gmail.com

***Abstract*—Most research into preventing cyberterrorism, whether by foreign or domestic individuals, has focused on technical measures to detect or prevent the attacks. Such efforts presume that individuals are already radicalized and that events are inevitable. Our investigations look further back; we seek to understand and influence the events which occur long before the cyberterrorism attacks are formulated and perpetrated, when individuals experience psychological processes – both cognitive and affective – that lead them to form the intentions to engage in cyberterrorism. Our focus, inspired by the "Left of Bang" paradigm, looks at three principle root causes – (1) techniques of neutralization, (2) expressive and instrumental crimes, and (3) perceptions of injustice and disgruntlement. We propose further research into these important factors that temporally precede the focal phenomenon.**

Keywords—cyberterrorism, deterrence, criminology, techniques of neutralization, expressive crimes, instrumental crimes, disgruntlement

I. INTRODUCTION

Cyberterrorism as the combination of cyberspace and terrorism is defined as the use of intentional violence against IT systems that support the health of human communities and the information stored in such systems [1]. This type of terrorism is geared toward coercing the targeted people or government to behave in a certain way (influential cyberterrorism) or is designed to inflict damage or revenge (destructive cyberterrorism). Furthermore, it is typically more comprehensive and ruinous than cybercrime in that it harms the health of human communities or threatens such a harm. Reports show that cyberterrorism is currently the fastest growing threat to individuals in the United States has now exceeded illegal drug trafficking [2]. New York Senate digital infrastructure is being attacked on a daily basis (Ibid), indicating that it is crucial to identify and implement protection from these vicious attacks. In this regard, terrorist institutions are actively pursuing the recruitment of young people from Western countries, including and especially those with high-level computer skills. The focus of this research is to understand the factors that make the young generation susceptible and likely to be open to terrorists' recruitments and to identify the ways to neutralize this susceptibility. In other words, investigation of the methods to cognitively immunize young generations from being lured into cyberterrorism activities is central to this work. We draw on Willison & Warkentin [3] concept of "left of bang" in order to understand the mechanisms of countering the emergence of malicious cyberterrorism intentions.

II. ANTECEDENTS OF CRIME & CYBERTERRORISM

Information Security literature has extensively investigated the phenomenon of security violations. Based on the abundance of new and emerging security threats, Willison & Warkentin (2013) called for new perspectives and theoretical lenses that not only include the criminal act and its immediate antecedents of intention to commit the abuses and deterrence crimes, but also the factors that temporally precede these issues. They assert the need to consider the cognition processes of the "potential offenders" and how these are impacted by the organizational and societal contexts prior to deterrence. The interplay between cognitive processes and these contexts can substantially influence the effectiveness of deterrence safeguards.

Drawing on theories in criminology, the Willison and Warkentin [4] paradigm extends the Straub & Welke [5] Security Action Cycle, and proposes three primary recommendations for future research into the fundamental antecedents of deviant cybersecurity behaviors, including insider computer abuse (security policy violation, whether malicious or benign in intent), reckless computer security hygiene behaviors by individuals, and malicious hacking activities including cyberterrorism against organizational targets (companies, governments, etc.) or against society at large. These three research focus areas are (1) the utilization of neutralization (rationalization) techniques, (2) assessment of both expressive and instrumental criminal motivations, and (3) the role of disgruntlement as a result of perceptions of injustice (either organizational or societal). Each of these has been

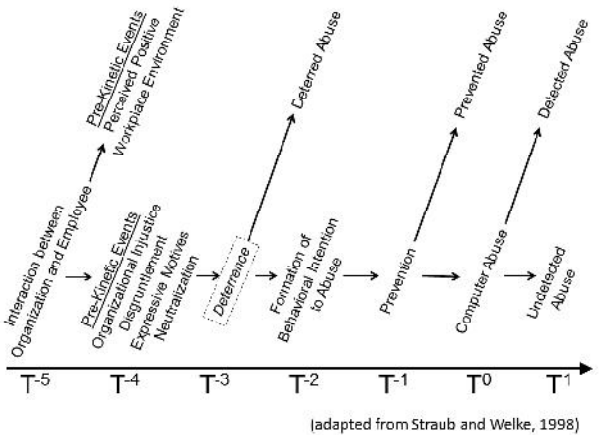

Fig. 1. Events "Left of Bang" (before insider crimes)
(Source: Willison & Warkentin, 2013)

applied to the study of organizational insiders (employees) who commit acts of insider computer abuse; we apply them to gain a more holistic view of cyberterrorism by individuals, whether they have been recruited or were "self-radicalized." This manuscript represents the initial investigation into the phenomenon of cyberterrorism, especially home-grown domestic cyberterrorism, and strategies for intervening "left of bang" to deter and prevent such cyberterrorism acts.

Traditional criminologists infer that deviant behavior can be explained using two facets: human nature, i.e. genetics and brain development [6] and environmental conditions, i.e. residential location and its local supporting institutions [7][8]. We believe that ecological dynamics – including religious and educational influences, peer pressures, insufficient economic opportunities, and institutions – offer greater explanatory power when studying cyberterrorism. Many theories related to crime and deviant behavior rely on rational choice theory, which suggests that individuals are guided by a rational cognitive assessment of the relative risks and rewards for committing an act that is understood to be a crime, policy violation, or behavior that is counter to social norms. The assumption is that we are motivated to avoid negative consequences of our actions, such as punishment from sanctions, unless the potential gains are great enough. Several studies, however, have shown that rationality may not adequately explain real-world decisions. Decision makers have repeatedly been shown to violate the tenets of expected utility in making risk decisions based on framing effects [9][10][11][12]. Tversky and Kahneman [12] show that risk decisions are situational. Further, in the cybersecurity context, individuals are influenced by their social context [13].

III. Techniques of Neutralization

The first research focus recommended by Willison and Warkentin [4] is investigation into the role of the techniques of neutralization. Deviant behavior, including violation of organizational information security policies, is characterized as actions that members of a social group judge to be a violation of their shared rules, values, or accepted conduct. When contemplating such behaviors, most individuals are normally dissuaded by feelings of guilt and shame. However, Sykes and Matza [14] showed how offenders who might otherwise feel guilt and shame are able to neutralize these feelings by justifying or rationalizing their behaviors before committing the deviant act. These "techniques of neutralization" are processes that serve to reduce or eliminate the influence of internal norms and social censure, thereby deflecting the disapproval they would otherwise experience from others in the social environment and protecting the violator from feelings of self-blame, which enables him to engage in the deviant act. Sykes and Matza [14] identified five such techniques, which include denial of responsibility, denial of injury, denial of the victim, condemnation of the condemners, and the appeal to higher loyalties. Later researchers added many more techniques. Siponen and Vance [15] empirically established the role of techniques of neutralization in enabling computer-related violations, and Barlow, et al. [16] empirically showed that the use of such techniques (in the cybersecurity context) can be lessened or eliminated through the effective application of proper training and message framing.

IV. Instrumental and Expressive Crimes

In criminology literature, the difference between instrumental and expressive crime is extensively explicated. Instrumental crimes are conducted in order to gain explicit future goals such as acquiring financial gains. On the other hand, expressive crimes are characterized by unplanned acts of anger and frustration [17]. This distinction usually parallels the differences between premeditated and spontaneous crimes. Accordingly, criminologists consider instrumental acts as qualitatively different from expressive ones. This distinction is also an important one in recognizing the typologies of vehicle theft, vandalism, terrorism, violence in workplace and so forth [18][19]. It is reasonable to argue that the prevalence and nature of instrumental and expressive crime has significant implications for policies. According to deterrence theory, the threat of legal sanctions is the most useful leverage for instrumental crimes by individuals with low commitment to a criminal lifestyle [20][21]. In contrast, expressive crimes are regarded as "undeterrable" actions because the perpetrators do not thoughtfully evaluate options and choices (rational cognitive process), but are influence more by emotional factors. Furthermore, expressive computer crimes are substantially more undeterrable in cases where companies are reluctant to bring in law enforcement agencies.

Though instrumental and expressive crimes can be contrasted in terms of motivation and process, the dominant theory in behavioral cybersecurity area – Deterrence Theory – does not differentiate between these two types. If a crime is expressive, then analyzing a computer abuse through the lens of deterrence theory may not offer adequate insight, and research results may reflect this, leading to a flawed assumption. Therefore, utilizing security countermeasures without recognizing this distinction could result in ineffective IT safeguards.

V. Role of Injustice and Disgruntlement

The final topic into which Willison and Warkentin [4] call for research is the role of disgruntlement. As a "far left" of bang cause of criminal and deviant behaviors, including acts of cyberterrorism, disgruntled individuals – whether they are

employees or citizens – represent a significant cause of concern to those who wish to maintain peace and order. When an individual feels that he or she has been treated unfairly, that person will often attach an emotional response to the perceived source of this unfairness. In the organizational context, the research foundation is the study of "perceived organizational justice" (and injustice), and has been found in numerous studies to cause various negative outcomes, including sabotage against an employer. In the context of society at large, research has indicated that certain individuals, especially within key minority groups such as immigrant communities who may experience reduced economic or educational opportunities, will "blame the system" (and its perceived key representatives, such as law enforcement) and develop a deep-seated sense of disgruntlement. Such individuals often form intentions to lash out against the source of the perceived injustice, whether an employer or society at large. This can be out of retribution or out of a sense of "righting a wrong."

Cyberterrorists may be fully integrated with a group of terrorists (especially when operating in a foreign country) or may be so-called "lone wolf" terrorists (often when they are self-radicalized and living within the target country domestically). In the former case, there may be cultural influences, social pressures, and reinforcing processes that lead to (and "reward") the commission of acts of cyberterrorism. Families, friends, schools, and terrorist organizations may all support and encourage such individual in their home country. However, in the case of a terrorist operating in another country, the inability to undergo the acculturation and assimilation process successfully that would enable them to become fully productive members of their "host" society often leaves them vulnerable and susceptible to the influences of radicalizing forces [22]. Such individuals often fail to enjoy the economic benefits of opportunities in their host countries; they may be unemployed, for example. This can lead to perceptions of injustice and disgruntlement, which has been tied to the formation of intention to retaliate against the unjust system, including acts of cyber-attack [4]. By evaluating this social process, one can see that official efforts to reach disaffected communities, to engage young individuals vulnerable to radicalization, and to build trust between these communities and law enforcement can offer the opportunity to ameliorate and avert the process that can lead to radically-inspired acts of homegrown terrorism, including cyberterrorism [23]. Counter-radicalization efforts should be built upon restoring community trust, building bridges, and developing educational programs aimed at gaining the cooperation of both the immigrant communities and a given population as a whole [24]. Building resilience against violent extremism begins at the local level. Research has established the efficacy of counter-radicalization strategies which are best achieved through the engagement and empowerment of individuals and groups [23].

VI. The Role of Pre-Kinetic Events

Drawing on the military strategy context, Willison & Warkentin [3] introduced the concept of "left of bang" to the security literature. The idea on moving "to the left" is inspired in part by fourth-generation military strategy, which has ascertained the need to consider "left of bang" in order to stop the emergence of malicious intention long before an act of aggression happens. In this regard, security is mainly a thinking game where intellect borne of training and experience should be to be the most prized commodity". The trained individuals can design security systems to minimize risk in the initial stages and thus avoid violations. In military terminology, this is often called pre-kinetic or left-of-bang, meaning that certain actions should be taken long before an incident happens. This could be the most crucial, yet the most underrated dimension of information security management [25] – it is incumbent that we act proactively before kinetic events ensue. Comparably, military strategists advocate winning the hearts and minds of the population, analogous to the way that organizations or governments may try to psychologically affect employees long before any cybercrime occurs. In the context of counter-cyberterrorism, efforts to influence potential terrorists long before they form their dangerous intentions can yield significant payoff in the long run.

VII. Conclusion

The challenges of addressing the increasing threats from cyberterrorism are great. Governments are expending increasing resources to counter such threats, focusing the greatest efforts on technical measures to prevent or detect cyberterrorism events, though the seeds are often sowed far in advance of the perpetration of such acts. We propose greater attention to the processes "left of bang" to understand root causes of the actions of cyberterrorists so that we can establish efficacious methods to break the chain early in the sequence and avert the formation of cyberterrorist intentions.

References

[1] S. Madhava and K. Jaishankar, "Cyber terrorism: Problems, perspectives, and prescription.", 2008. The ACM Digital Library: New York, NY, USA, pp.593-611.

[2] M. Nozzolio, "What can be done to prevent cyber attacks in the future?", New York Senate Report, 2015, Available at:https://www.nysenate.gov/newsroom/press-releases/michael-f-nozzolio/what-can-be-done-prevent-cyber-attacks-future.

[3] R. Willison and M. Warkentin. "The expanded security action cycle: A temporal analysis 'left of bang'. In Proceedings of the The Dewald Roode Workshop on Information Systems Security Research, IFIP WG8, (11), 2010.

[4] R. Willison and M. Warkentin. "Beyond deterrence: An expanded view of employee computer abuse." MIS Quarterly, vol. 37, no. 1, 2013, pp.1-20.

[5] D. W. Straub and R. J. Welke. "Coping with systems risk: Security planning models for management decision making." MIS Quarterly, vol. 22, no. 4, 1998, pp.441-469.

[6] A. Raine, The psychopathology of crime. Cambridge: Academic Press, 1993.

[7] R. K. Merton. "Social structure and anomie." American Sociological Review, vol, 3, no, 5, 1938, pp. 672-682.

[8] C. R. Shaw and McKay, H. Juvenile delinquency in urban areas. Chicago: University Press, 1942 .

[9] T. Gilovich, D. Griffin, and D. Kahneman. Heuristics and biases: The psychology of intuitive judgment. New York: Cambridge University Press, 2002.

[10] R. Hastie and R.M. Dawes. Rational choice in an uncertain world: The psychology of judgment and decision making. Thousands Oaks, CA: Sage, 2010.

[11] D. Kahneman and A. Tversky. "Prospect theory: An analysis of decision under risk." Econometrica: Journal of the Econometric Society, vol. 47, 1979, pp. 263-291.

[12] A. Tversky and D. Kahneman. "The framing of decisions and the psychology of choice." Science, vol. 211, no. 4481, 1981, pp. 453-458.

[13] C. Posey, T. L. Roberts, P. B. Lowry, and R. T. Hightower. "Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders." Information & Management, vol. 51, no. 5, 2014, pp. 551-567.

[14] G. Sykes and D. Matza "Techniques of neutralization: A theory of delinquency." American Sociological Review, vol. 22, pp. 664-670.

[15] M. Siponen and A. Vance. "Neutralization: New insights into the problem of employee information systems security policy violations." MIS Quarterly, vol. 34, 2010, pp. 487-502.

[16] J. B. Barlow, M. Warkentin, D. Ormond, and A. R. Dennis. Don't make excuses! Discouraging neutralization to reduce IT policy violation Computers & Security, vol. 39, part B, November 2013, pp. 145-159.

[17] C. R. Block and A. Christakos, "Intimate partner homocide in Chicago over 29 years," Crime & Delinquency, vol. 41, no. 4, 1995, pp. 496-526.

[18] B. Swanton, Violence and the Public Contact Workers, Canberra: Australian Institute of Criminology, 1989.

[19] M. Whittingham, "Vandalism – The urge to destroy and damage," Canadian Journal of Criminology, vol. 23, no. 1, 1981, pp. 69-73.

[20] R. Parker M. Dwayne Smith "Deterrence, poverty, and type of homicide." The American Journal of Sociology, vol. 85, no. 3, 1979, pp. 614-624

[21] C. Thomas and J. Williams. "Actors, actions and deterrence: A reformulation of Chambliss's typology of deterrence," in Treating the Offender: Problems and Issues, M. Riedel and P. Vales (eds.), New York: Praeger, 1977.

[22] J. Pressman. Power without influence: The Bush Administration's Foreign Policy failure in the Middle East, International Security, vol. 33, pp. 149–179.

[23] A. G. Kosseim, "Counter-radicalization: Best practices in the United States and lessons learned from abroad." Unpublished Master Thesis, Naval Postgraduate School, 2011.

[24] L. Baca, L. The extent of radicalization in the American Muslim community and the community's response. Los Angeles, CA: House Committee on Homeland Security, 2011.

[25] J. Allen, "The Combat Operator," DefenseTech, March 23, 2009. (Available at http://defensetech.org/2009/03/23/guest-blog-the-combat-operator).