IS MODELING INFOSEC LIKE MODELING WAR, CRIME, OR TERRORISM?

Norman Pendegraft, College of Business and Economics, University of Idaho, Moscow ID 83844, 208-885-7157, norman@uidaho.edu
Mark Rounds, College of Business and Economics, University of Idaho, Moscow ID 83844, 208-885-4199, mrounds@uidaho.edu

ABSTRACT

A model is offered to categorize computer attacks based on several factors influencing target choice. The factors have direct utility in modeling attacker behavior.

INTRODUCTION

This paper presents a preliminary model to address the question: Is information security (infosec) about war, crime, or terrorism? The question is interesting to those who model information systems under attack because the answer affects how one models attacker behavior. Those involved in criminal activity have different preference functions for targets than do those involved in war planning.

There is significant research about the demographics of the hacker population. They tend to be young males with technical training, but of varying levels of sophistication. They are often socially awkward and resent authority [23]. However, this is not very helpful when trying to model their behavior or determine their future actions. Hence, we did not consider these factors here.

There is an extensive literature that models information system attacker and user behavior. Early efforts to model criminal behavior [2] and terrorist behavior [22] used basic economics and decision theory. Any such model requires that assumptions be made about why attackers behave as they do. There are significant policy implications for such a classification. If they are acts of war, one set of rules applies to the response; if they are criminal acts another set applies. The particular question of interest here is, how should computer attacks be modeled? In particular, how do attackers behave? There are differences in behavior between the categories identified, hence the importance of understanding how real attackers behave. The paper offers a preliminary model to help classify computer attacks.

BACKGROUND

When the authors conducted web search on “is terrorism war or crime?”, there were over seven million hits, and there was clearly no consensus. We note one of them here, merely to demonstrate that there is an ongoing debate [26]. Recent debate about the NSA [19] [28] program illustrates the implications of the debate. If the subjects of the monitoring are combatants then the program is clearly justified. If they are ordinary criminals, then warrants would be required.

Tsakaldis & Vergidis, [27] used the identified offence, the offender, the method of access, the target, the victim, and the harm caused to categorize the various types of attacks. In his testimony to Congress Lewis [10] tried to differentiate between attacks for criminal gain and those that attempt to impact the ability of a government to pursue its ends. These he labeled cyberwar. Nye [11] discussed the similarities and the difference between Cyber and Nuclear Warfare. He asks if we can achieve the equivalent of deterrence in the cyber sphere. Broadhurst, Grabosky, Alazab, Bouhours, & Chon, [4] attempted to categorize cybercrime by looking at the groups behind the incidents and their motives.

The problem of information system security has been widely studied. Some of that work has looked at the human and dynamic aspects of the problem. In [21] it was noted that human behavior is an important factor in computer security. Recently, there has been considerable work using systems dynamics models to study infosec [14] [5].

Rounds, Pendegraft, & Taylor [20] explicitly discussed the ecology of information security including the human element. As part of an effort to use the ecology paradigm to model the interaction between a system, its users, and the attackers who prey upon it, it was recognized that it would be useful to empirically examine attacker and user motivations [13].

MODEL

The model is based partly on work by LaFree & Dugan [9] who offered an analysis of the differences between studying terrorism and crime. They identified a number of characteristics in which they differ as well where they are alike. While we began with LaFree and Dugan's constructs, our reading of the events suggests that other issues may also be useful in distinguishing events. We concluded that there were four issues that affected infosec modeling. For convenience, our constructs are summarized in Table 1.

TABLE 1: CONSTRUCTS

sponsors	are those who finance and plan the acts.
Motive	is viewed as primarily financial or political.
Direct	direct impact on the system (availability or integrity) or take data (privacy)
Target	is the target chosen for its value or for ease of attack

Three of these variables were significant in modeling attacker behavior. Since each can have two values that gives us eight possible cases. There are noted in Table 2 along with examples from recent headlines. In a basic infosec model, there are three types of attack impacts: loss of availability, loss of integrity, and loss of confidentiality [3]. Here, direct attacks here are those that directly affect the availability or integrity of target systems. Indirect attacks are those that steal data that can be used elsewhere, but do not directly affect the target system. Easy targets are those chosen simply because they are easy while value targets are specifically chosen because they have some value to the attacker. Phishing and spear phishing illustrate these two types. Both ideas are useful a priori for modeling target selection and defensive resource allocation. See, for example, for an model that distinguishes between direct and indirect attacks [16].

"Sponsor" and "motive" may be useful for the same purpose, but are more likely to be useful if we extend a model to allow for "offensive" action against attackers [15]. These attributes are likely to be important in selected a method of proceeding. We treated sponsor separately because a sponsor may engage in any of the modes, and it only impacts the government level at which a response in managed. We distinguish three types of sponsors: governments of recognized states, non-state organizations (NSO), and individuals. NSOs may be politically or financially motivated. For example, a state actor must be opposed by the national government, and the nature of the response may differ based on whether the act was politically or financially motivated.

Motive may influence the mode of response. Those who are politically motivated must be, at least partially, opposed via political means while those who are financially motivated may dealt with by law enforcement.

The values noted in the table apply to the specific incident illustrating the general category.

TABLE 2: INCIDENTS

	War	Hacktivism	espionage		piracy	organized crime		crime
	Chechnya	LulzSec	OPM	Piggyback	DDOS	Ransom, DarkWeb	Target	Kingpin cc thefts
	1.	2.	3.	4.	5.	6.	7.	8.
Motive	political	political	political	political	financial	financial	financial	financial
Direct	direct	direct	indirect	indirect	direct	direct	indirect	indirect
Target	value	easy	value	easy	value	easy	value	easy
Actor	state	nso	state	state	nso			individual

1. Chechnya: Russian conducted cyber operations prior to invasion. [18]
2. LulzSec: hacktivist attacks for “fun.” [1]
3. OPM: theft of personnel records of US government employees. [12]
4. Piggyback: Russian espionage. [24])
5. DDOS: a distributed denial of service attack against DYN rendered many web sites inaccessible. [7]
6. Organized Crime

    6.1. Ransom: Unknown attackers shut down several business sites demanding ransom payable in bitcoin. [25]

    6.2. DarkWeb: sale of credit card numbers on the dark web. [17]

7. Target: Credit card numbers were stolen by hacking the point of sale devices in the stores. [6]
8. Kingpin: Stole credit card numbers by intercepting wireless point of sale devices. [17]

DISCUSSION

The utility of these factors in modeling systems under attack is discussed above. Particularly if one is modeling attackers’ choices of targets, then these factor will weigh in the tradeoffs inherent in that choice.

It is clear that no single category like “computer crime” or “compute war” is sufficient to guide researchers and policy makers. Like all models, this one is still imperfect. Not every event fits cleanly into one of our categories. Since we considered only a few events, it is likely that further inconsistences will arise as we delve into it more deeply. There may be disagreement on some of our characterizations, but in general, we think they are reasonable. It is important to recall that we are not trying to definitively categorized these event, but rather to determine a reasonable set of criteria against which to do so. This paper is not intended to be a definitive answer to the title question, but provide a basis for further research. In particular, it is intended to assist in modeling attacker behavior.

Note that violence is also a problem. Generally, infosec events do not involve violence, but as in Chechnya they may support it. Infosec threats to infrastructure [8] may increase the likelihood that cyber-attacks will result in physical damage or casualties. Consequently, infosec violence remains a question for further research.

There continues to be disagreement regarding the meaning of terms like terrorism, crime, piracy etc.. It seems to us that further debate to clarify these terms would be useful. There is also disagreement over the response to terrorism paralleling the evolution of thinking about piracy: should it be a military or civilian response? As the possibility of computer attacks against infrastructure increases, there needs to be a similar debate regarding computer attacks.

Finally, and with no flippancy intended, it is clear to use that the answer to the question posed in the title is “Yes”. This means that those of us attempting to model attacker behavior need to overtly consider the motives underlying the attacks. In particular, target selection is a key issue.

WORKS CITED

[1] Arthur, C. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2013/may/16/lulzsec-hacking-fbi-jail 2013.

[2] Becker, G. Crime and Punishment: An Economic Approach. *Journal of Political Economy, 1968, 78*, 169-217.

[3] Bishop, M. *Computer Security*. Boston: Pearson. 2003.

[4] Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. An Analysis of the Nature of Groups Engaged in Cyber Crime. *International Journal of Cyber Criminology*. 2014.

[5] Dutta, A., & Roy, R. Dynamics of Organizational Information Security. *Systems Dynamics Review, 2009, 24#3*, 349-375.

[6] Edwards, J. *The Incredibly Clever Way Thieves Stole 40 Million Credit Cards from 2,000 Target Stores In a Black Friday Sting*. Retrieved from Business Insider: http://www.businessinsider.com/target-credit-card-hackers-2013-12.

[7] Fitzgerald, D. *Dyn Says Cyberattack Has Ended, Investigation Continues* . Retrieved from Wall Street Journal: https://www.wsj.com/articles/dyn-says-cyberattack-has-ended-investigation-continues-147717877, 2016.

[8] Jian, H., & Bapna, S. The economic impact of cyber terrorism. *J. of Strategic Information Systems*. 2013.

[9] LaFree, G., & Dugan, L. How Does Studying Terrorism Compare to Studying Crime? In M. Deflem, *Terrorism and Counter-Terrorism (Sociology of Crime, Law and Deviance, VOl. 5), 2004,* (pp. 53-74). Emerald Group Publishing Limited.

[10] Lewis, J. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Center for Strategic and International Studies. 2002.

[11] Nye, J. From Bombs to Bytes: Can our nuclear history inform our cyber future? *Bullietin of Atomic Scientists*. 2013.

[12] Paletta, D. *Wall Street Journal*. Retrieved Octorber 2017, from U.S. Intelligence Chief James CLapper Suggests China Behind OPM Breach: https://www.wsj.com/articles/SB10007111583511843695404581069863170899504 , 2015.

[13] Pendegraft, N. User Attitudes Toward Password Security: Survey and Simulation,. *Journal of Information System Security*. 2014.

[14] Pendegraft, N., & Rounds, M. A Simulation Model of IS Security. *International Journal of Information Security and Privacy, 1*. 2007.

[15] Pendegraft, N., & Rounds, M. A Simulation of Various Hacker Populations. *International Conference on Computational Science and Engineering*. 2009.

[16] Pendegraft, N., & Rounds, M. Preliminary Data / Wealth Simulation of an Information System Under Attack. *DSI*. Seattle. 2015.

[17] Poulsen, K. *Kingpin*. New York: Broadway. 2011.

[18] Ring, T. *Russion Information Operations and the Rise of hte Global Internet*. Retrieved October 2017, from https://digital.lib.washington.edu/researchworks/handle/1773/33528. 2015.

[19] Risen, T. *Privacy Watchdog Says NSA Spying Legal, Effective*. Retrieved from U S News: https://www.usnews.com/news/articles/2014/07/02/privacy-watchdog-says-nsa-spying-legal-effective, 2014.

[20] Rounds, M., Pendegraft, N., & Taylor, C. The Ecology of IS Security: A Research Agenda. *Information Resources Management Association International Meeting.* Vancouver, B.C. 2007.

[21] Saltzer, J., & Schrodeder, M. The Proctection of information in computer systems. *Proceedings of the IEEE 63#9*, 1975, 1278-1308.

[22] Sandler, R., & Lapan, H. E. Calculus of Dissent: An Analysis of Terrorists Choice of Target. *Synthese*, *1988*, *76*(2), 245-261.

[23] Schell, B., & Holt, T. A profile of the demographics, psychological predispositions, and social/behavioral patterns of computer hacker insiders and outsiders. In K. Chen, & A. Fadalla (Eds.), *Online Consumer Protection: Theories of Human Relativism.* Retrieved Oct 2017, 2009

[24] Schwirtz, M., & Goldstein, J.. Russian Espionage Piggybacks on a CYbercriminals's Hacking. *New York Times*. Retrieved Oct 9, 2017, from https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html , 2017.

[25] Simmonds, M. How Business Can Navigate the Growing Tide of Ransomware. *Computer Fraud and Security*, 2017, 9-12.

[26] Terwilliger, G. *The War on Terrorism: Law Enforcement or National Security*. Retrieved from The Federalist Society for Law and Public Policy Studies: https://www.fed-soc.org/publications/detail/the-war-on-terrorism-law-enforcement-or-national-security, 2005.

[27] Tsakaldis, & Vergidis. A Systematic Approach Toward Description and Classification of Cybercrime Incidents. IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2017.

[28] Verble, J. The NSA and Edward Snowden: Surveilance in the 21st Century. SIGCAS Comput. 2014, Soc 44#3.