MATHEWS Open Access Journals

Mini Review | Mathews Journal of Forensic Research

Converting the Culprits/Reducing International Cyber Security Vulnerability: Garnering Hacker Allegiance Within and Across Borders

Georgie Ann Weatherby*

Department of Sociology & Criminology, Gonzaga University, Spokane, WA 99258-0065 U. S. A.

Corresponding Author: Georgie Ann Weatherby, Department of Sociology & Criminology, Gonzaga University, Spokane, WA 99258-0065 U. S. A, **Email:** weatherb@gonzaga.edu

Received Date: 21 Sep 2018

Accepted Date: 10 Oct 2018

Published Date: 15 Oct 2018

Citation: Weatherby GA. (2018). Converting the Culprits/Reducing International Cyber Security Vulnerability: Garnering Hacker Allegiance Within and Across Borders. M J Foren. 1(1): 006.

ABSTRACT

Cybercrimes are increasingly an international threat. Perpetrators cross borders, whether tangible or invisible, often seamlessly and without regard for security measures. Modern nations and third world countries alike are known targets, and can be held hostage by perceptive technocrats. For instance, the United States has a small number of electric grids which, if paralyzed simultaneously, could entirely block access to power, placing lives in peril (airspace would be compromised, even hospitals with back-up generators would not function at full-strength, food and supplies could not be transported, and communication by all means would be halted). Such destruction would be even easier in island countries and on less developed continents. The question to ponder is this: How do we harness these electronic abilities, turning potential evil into progress for the greater good, to counter cyber-attacks? Answers will be discussed, as ways of pinpointing internal and international weaknesses and turning enemies into advocates for the states in question. Further, in order to combat cyber security threats, how can those with the means to commit these crimes be coaxed to join forces with the governments and corporations in question? How do we identify them, and lure them to our side? Broken Windows Theory will be applied to the opportunity to corrupt cyberspace, and Social Exchange Theory and Rational Choice Theory will be employed to analyze potential reciprocity rewards structures.

CRIMINAL ALLURE

Social Exchange Theory

Adapting Ivan Nye (1978), who laid out a set of theoretical propositions for understanding Social Exchange Theory, individuals choose those alternatives from which they expect the most profit. Hackers target easy, lucrative marks. If a government meets those criteria, it is proclaimed vulnerable, and holes are subsequently explored.

Nye (1978) continues, that cost being equal, criminals choose alternatives from which they anticipate the greatest rewards. Taking a nation-state hostage can be risky, but monumental if the outcome is potentially successful in terms of a pay-off to rescind threats.

Rewards to Nye (1978), being equal, aggressor experts choose alternatives from which they anticipate the fewest costs. Here, a governmental hacking coup that is carefully orchestrated can remain anonymous, and command a high payment rapidly, with limited methods of detection available.

Nye (1978) looks further to immediate outcomes being equal, and choosing those alternatives providing better immediate outcomes. If the nation-state in question offers a direct route in, electronically, the gains are likely to be more substantial (ransom payouts, as an example) than individual targets can yield.

Long-term outcomes being perceived as equal, Nye (1978) contends that one chooses alternatives providing better immediate outcomes. It could be postulated that a sitting government is open to attacks when entry points (such as lapsed

virus protection) become obvious via Internet exploits. The positive outcome to the criminal is one of instantaneous response to seek resolution (pay to resume business as usual or infiltrate viruses initially inflicted by the one now offering costly protection against their own attack). Gratification is quick, with little risk wagered.

Costs and other rewards being equal, individuals choose alternatives that supply or can be expected to supply the most social approval (or those that offer the least social disapproval – Nye, 1978). Among hackers, there is a status conferred in high stakes criminal acts. What could be more of a challenge than taking on a federal government, with the potential to win big, undetected? Vaporizing is easier when only a fleeting electronic presence to begin with.

Costs and rewards being equal, Nye (1978) points out that individuals choose statuses and relationships that provide the most autonomy. What could grant more power and independence than holding an entire country (your own or another) hostage – a faceless criminal versus an entire nation-state's security?

To Nye (1978), other rewards and costs being equal, individuals choose alternatives characterized by the least ambiguity in terms of expected future events and outcomes. With the experimentation of holding various police departments hostage in terms of a total lock on essential computerized data, the aggressor feels confident that the targeted nation will comply with demands, rather than risk the sacrifice of the safety of their citizens. This is perceived as an easy in, easy out approach.

Other costs and rewards being equal, (Nye, 1978), actors choose alternatives that offer the most security for them. As stated previously, the bet is safe that a well-executed plan of attack will be met with timely, lucrative compliance.

Nye (1978) elaborates that other rewards and costs being equal, one chooses to associate with those whose values and opinions generally are in agreement with their own, and reject or avoid those with whom they chronically disagree. Deviants find solace in hanging out with other deviants, according to Differential Association Theory (Sutherland, 1939). They learn from one another, and provide affirmation for wrongful deeds committed, deriving power and confidence from one another by derailing the "establishment."

Other rewards and costs being equal, Nye (1978) elaborates that actors are more likely to form relationships with those equals than with those above and/or below them. (Equality here is viewed as the sum of the abilities, performances, characteristics, and statuses that determine one's desirability in the marketplace.) Actors create alliances with those of comparable status. Allport (1981) adds that one need just to be paired with others perceived as "different" (race, ethnicity, class, gender, talent, etc.) on problem solving tasks to appreciate and develop bonds with those previously determined to share no commonalities or interests. Still, if the status of each is on an equal plane, the perception is maintained that they may smoothly enter relationships/partnerships that will yield positive results for both sides of the equation (brainstorming on major hacking projects, for instance).

Nye (1978) concludes that in industrial societies, other costs and rewards being equal, individuals choose alternatives that promise the greatest financial gains for the least financial expenditures. If a hacker carefully evaluates a country as an easy mark, they can potentially extract large sums of money with little effort and virtually no detectability. The assumption is established that monetary gain is paramount to all else, in terms of both demands and compensation.

Broken Windows Theory

Wilson and Kelling (1982) introduce the idea of Broken Windows Theory. They use neighborhoods as prime examples. They demonstrate how rundown, unattended areas telegraph disorder. The assumption is that these spots are ripe for crime, as the variables of visible disorder and heightened crime are inextricably linked. The presence of foot patrol officers elevate the perception of public order in neighborhoods, and can cancel out threats. Places become safer due to the feeling of security conveyed by this lawful presence.

In 1969, Zimbardo (Wilson & Kelling, 1982) conducted some experiments to test Broken Windows Theory. His first stop was the Bronx, NY, where he left a car with no license plates and the hood up on the street with no one around. He also created the same exact scenario in Palo Alto, CA. Determined to be abandoned, passersby attacked the car in the Bronx within a span of ten minutes. In fact, the first to perpetrate a crime appeared to be an upstanding family – a mother, father, and their young son. They stole the battery and radiator. From there, within a twenty-four hour period, the car had been stripped of everything of value. To add to this, what was left was smashed, ripped, and torn apart. Zimbardo referenced this as "random destruction." Finally, the remains of the car became a playground for children. It should be noted that the majority of adults involved were well dressed, clean-cut Caucasians.

The unattended car in Palo Alto was left alone for over a week. Then Zimbardo himself wielded a sledgehammer to deface it. That set off a chain reaction. Within hours of that destructive

act, the Palo Alto car had been overturned and completely dismantled. The same theme applied. The "vandals" were otherwise upstanding white citizens.

Untended circumstances are an invitation to crime. They reflect the sometimes-unintended consequences that no one cares. Neighborhood homes that are well groomed and well lit do not invite a criminal element. Once even one abandoned house exists there, with weeds and grass growing high, the invitation is clear. Those who care tend to move away, those who do not then fill the void with their presence. Neighborhood vulnerability to criminal invasion is often the result.

Zimbardo's work in 1969 and studies since that time that further validate it can be transferred to computer wizards who seek the thrill of illegality over a 9 to 5 job utilizing their vast skills. They test the systems of Fortune 500 companies, elite universities, big city police departments, powerful financial institutions, and governments as a whole. If they can break encoding without much effort, this is viewed as an "untended" landscape, ripe for illegal intervention. Like credit card thieves, these computer experts begin slowly, to see what they can perpetrate undetected. The "broken windows" here are gauged as system vulnerabilities. Equifax, in the summer of 2017, experienced such a breach. It was widened by the lack of public dissemination of the system compromise, placing in excess of 143 million individuals at risk of identity theft, credit card fraud, and countless other vulnerabilities (New York Times, 2017). Further inquiries into the matter uncovered the fact that unqualified Equifax employees with little to no security training or Internet background were "in charge" of keeping clients safe. These facts are easily detected by criminal experts, offering the "easy in, easy out" approach that was exploited by those who profit from selling information on the "Dark Web."

Every country, large and small, is subject to such intervention on a federal level as well as a local level. If one controls the key electric grids, for example, they are only a few simple steps away from paralyzing a foreign power (or their own nation-state). The stakes run high, detection is low, and the potential payoff is mammoth.

Rational Choice Theory

Cornish & Clarke (1987) shed further light on such threats, from the standpoint of Rational Choice Theory. They argue that we are all reasoning actors who weigh means, ends, costs, and benefits, and then we make what are considered "rational" choices. Crime has purpose. It meets the perpetrator's yearning for money, status, sex, and excitement via decisions and choices and constraints of ability and available data. The individual has self-interested goals. They wish to maximize pleasure as the main motivator. This theory intersects with the previous two laid out here. If one can safely (with minimum risk of detection) move into a rare stratosphere of privileged information which nation-states or even smaller entities would do most anything to protect, then the aggressor wields all the power in the situation. Only their personal conscience/beliefs (see Hirschi's Social Control Theory, 1969) will potentially intervene to keep them tethered to a lawful existence.

Temptation Reversed

What is the proper official response to continuous, looming threats? General Motors (Spokesman-Review, 2018) is hiring hackers to test car bugs that they may be able to neutralize, since they possess extensive knowledge on the criminal side of how to stymie cars. Cybersecurity experts at all levels of companies and nation-states agree that enticing those who pose major threats to lawful business production is merited. The technique developed by GM offers professional computer hackers a bounty or payment of cash incentive for each bug they uncover. This begins to repair the "broken windows" vulnerability syndrome that is plausible in vehicles that are nearly 100% dependent on electronic monitoring these days. The greatest challenge may be locating the best of the best that the hacking world has to offer, however.

This approach has the potential to tip the scales in the opposite direction when employing Social Exchange Theory. When rewards and profits are high, and costs are nonexistent (while working on the side that favors the law), many are coaxed to flip their allegiance away from crime. Long-term outcomes could involve a lucrative career thwarting attacks by other criminals, with little to no extra training required. They come to the job equipped with the knowledge to proceed. Social approval (on the societal level, but also trickling down to personal contacts and family) follows. The benefits are immediate. Autonomy is liberally granted, for one in this type of career works without much supervision necessary. Job security tends to be high, as long as one is productive at uncovering system flaws, and ambiguity is low. They will work with peers in an agreeable environment of equality. Financial gains are immediate, and clear parameters are set. Personal resource expenditures and risk are minimal in this type of controlled environment.

Embracing the tenants of Rational Choice Theory, the hackers reason, weighing means and ends and costs and benefits. If offered a counter to the criminal actor's usual way of illegally proceeding, and that counter is a marked improvement in terms of career potential, salary based on productivity, societal status, and other tangible perks, the temptation is

to move in the lawful direction. The element of excitement sought (such as breaking an elaborate code) is an enticement that appeals to the basic self-interested, pleasure-seeking, goal-maximizing human, which in turn protects society and minimizes further criminal allure.

REFERENCES

1. Allport and Gordon W. 1981. *The Nature of Prejudice.* Reading, MA: Addison-Wesley.
2. Cornish D and R Clarke. (1987). Understanding Crime Displacement: An Application of Rational Choice Theory. *Criminology.* 25(4): 933-947.
3. Hirschi T. (1969). *Causes of Delinquency.* Berkeley: University of California Press. New York Times.
4. Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth and Ron Lieber. (2017). *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.,* page A1, September 7.
5. Nye FI. (1978). Is Choice and Exchange Theory the Key?. *Journal of Marriage and the Family.* 40 (2): 219-232.
6. Spokesman-Review. (2018). *GM Hires Hackers to Test Car Bugs,* News, page 6, August 4.
7. Sutherland and Edwin (1939). *Criminology.* Philadelphia: Lippincott.
8. Wilson JQ and George LK. (1982). Broken Windows Theory. *The Atlantic Online.* March.