CASIS - VANCOUVER - ACERS
SAPERE AUDE

THE DARK AGE OF ONLINE CIVIL SOCIETY (AKA: A WAR OF 1)

Date: January 18, 2020

Disclaimer: This briefing note contains summaries of open sources and does not represent the views of the Canadian Association for Security and Intelligence Studies.

EXECUTIVE SUMMARY

Online civil society is vulnerable to various malicious actors who conduct cyberattacks against individuals, companies, and governments. Victims of these attacks are using strike backs, hack backs, and defensive cyber actions as a means to send a message to the attacker, we are not a victim (Neal, 2019). My research presents one model of "revenge attacks" whereby the individual defends themselves online without the assistance of the government.

POSITION OR PURPOSE STATEMENT

The online civil society is an extension of our real-world civil citizenship and consumerism. However, individuals victimized online are severely restricted in their ability to defend themselves due to legal constraints. This research demonstrates how someone can defend themselves online and thus potentially create an online civil society model. Moreover, without a new deterrence model, the current model of protecting the online civil society is governed by the individual's revenge, retaliation, and retribution—not a civil society informed by law, policy, and procedures.

THE SECURITY PROBLEM

The public safety and national security problem presented is twofold. The first problem is the shifting roles and responsibilities of who should be protecting the citizen and consumer: government, corporation, or a combination of both. This security problem affects all segments of society regardless of socio-economic status. The second problem is the escalation of cyberattacks, the intensification of information warfare targeting civil society, and the broadening range of information technologies (internet of things, smart cities, autonomous vehicles, drones, nanobots) that will result in citizens not being able to make informed decisions.

BACKGROUND AND KEY FACTS

Informed citizens and consumers, the funding of public infrastructure, and access to the essentials of living are directly affected by online cyber-attacks. In 2017, 16 billion USD was the cost for cyber victimization to the individual (Grant, 2017). Corporations spend 76 billion USD on location-based advertising but lost 7 billion USD in revenue (Cook, 2019). For corporations and governments who use Facebook to engage consumers and citizens, 10% of Facebook accounts and between 9-15% of Twitter accounts are fake (Greiner, 2018). The collective impact of these threats and actions is a loss of confidence in an online environment which could arguably lead to lost opportunity to engage the consumer and citizen effectively.

KEY CONSIDERATIONS AND IMPLICATIONS

The consideration is summed up as a question: Who protects me (as a consumer or citizen), and if I do not feel like the government or the company protects me, then what are my options? Answering this question: there are emerging groups and individuals actively posting examples of how to conduct active defence operations online. These operations range from the following:

- Passive activities, such as creating inventories of fake banks (Artists Against 419, 2017);
- Actively engaging the suspects/offenders through passive email chats which prevents them from attacking real victims (Veitch, 2016); and
- More aggressively conducting full cyber-attacks, such as those conducted by Hexxium, against the suspects/offenders' computer network effectively destroying/damaging the hardware and software of the suspect/offender (Hexxium, 2016).

For policy makers responsible at the government level, the implications include the knowledge dissemination of these techniques which will arguably enable or embolden cyber victims to take law into their own hands and the offenders/attackers/suspects who will consequently learn to harden their networks and adapt cyber techniques to better conceal themselves.

For corporations, healthcare facilities, education institutions, and infrastructure entities—such as hydro, telecommunications, transportation, air traffic—connected to the internet, victims seeking online revenge may accidentally harm these critical infrastructures. The harm may result in death, disruption of power supplies, water service, or other essential services.

ALTERNATIVE PERSPECTIVES TO BE CONSIDERED

Two alternative perspectives need to be considered. The first perspective addresses the key issue of complex software and hardware. Conducting root cause analysis of faulty hardware and software could help design and develop robust computing and information systems and technology resilience. The second perspective involves embracing online cyber deterrence at the citizen level in order to build out models of online cyber deterrence which can be used to promote and protect online civil society participants (citizens and consumers).

WHAT IS NOT KNOWN

Research into active cyber deference, online revenge, relation, and retribution is limited. The ability to measure the real and perceived harms of online victimization is not well understood. For example, if someone is victimized online once, what is the frequency or likelihood of being victimized online again? Furthermore, what is not known is the ability to effectively measure the impact of online deterrence.

NEXT STEPS

The next steps consist of several components. Step one: create a baseline dataset of online victimization and then conduct a longitudinal study of victimization experience. Step two: codify cyber response models which are consistent with existing deterrence models. Step three: utilize various social theory models to examine technology adoption and adaption of cyber victims and cyber attackers.

AVAILABLE OPTIONS

Some current options to consider are amendments to the criminal codes, telecommunication legislation and related laws, policies, and procedures. The final option is to enable, through funding and education, cyber deterrence research.

RECOMMENDATION AND JUSTIFICATION

Moving forward, enabling cyber deterrence research would arguably be the best option. It would send a signal to citizens and consumers that the government and corporations are serious about taking an active stance in protecting the emerging civil society. The research would also signal industry and investors that active defence is a viable public, consumer good which needs to be debated and regulated.

References

Aa419. (2017). Fake bank list. Retrieved from https://db.aa419.org/fakebankslist.php?comd=reset

Cook, S. (2019). Indentity theft stats and facts: 2018 - 2019. Comparitech. Retrieved from https://www.comparitech.com/identity-theftprotection/identity-theft-statistics/

Grant, K. (2017). Identity theft, fraud cost consumers more than $16 billion. CNBC. Retrieved from https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-tofraud-and-identity-theft-last-year.html

Greiner, A. (2018). The hidden costs of identity theft. Forbes. Retrieved from https://www.forbes.com/sites/forbesagencycouncil/2018/06/01/thehidden-costs-of-identity-theft/#1ac92749357b

Hexxium. (2016). Revenge against a Microsoft Tech support scammer! Youtube. Retrieved from https://www.youtube.com/watch?v=USu7CDkmBsw

Neal, P. (2019). Protecting the information society: Exploring corporate decision makers' attitudes towards active cyber defence as an online deterrence option. Royal Roads University. Victoria: BC.

Veitch, J. (2016). This is what happens when you reply to spam. Ted Talk published Feb. 1, 2016. Retrieved from https://www.youtube.com/watch?v=_QdPW8JrYzQ

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University

Available from: https://jicw.org/