MOBILIZING INSIGHTS IN DEFENCE AND SECURITY
MINDS
MOBILISATION DES IDÉES NOUVELLES EN MATIÈRE DE DÉFENSE ET DE SÉCURITÉ

Security-Policy NET Nexus of Emerging Technologies

BRIFING NOTE FOR Department of National Defence
Security Issues Regarding Generative Internet

Authors: Saman Asvadi [1] and Mohsen Farhadloo [2]

[1] PhD candidate, John Molson School of Business, Concordia University, Montreal, Canada
[2] Professor, John Molson School of Business, Concordia University, Montreal, Canada.

SUMMARY

- “Generativity” is referred to the characteristic of a technology to promote unwanted changes due to the high number of its users who are not coordinated. [1]
- The more helpful and widely used a technology, the more generative it is. [2]
- The internet is easy to master. Hence a great number of people with malicious reasons can learn how to work with it easily and in a short time. [1]
- The internet is vastly available to most people, increasing the security risks. [3]

CONTEXT

- The grid by which personal computers are connected to the internet has a vast number of uncoordinated users. Hence it is considered generative. Personal computers are designed in a way that almost any code can be run on them; No matter this code is written by the manufacturer, the user, or a third party. When these personal computers are connected to the grid of internet, on which there is only a few controls, any person with malicious intentions can upload codes, and others may run such malware, without even knowing the origin of it or the way it works. [1]
- The internet is highly accessible to people, with low cost. No rule or organization limits the use of internet for anyone. On the other hand, learning how to work with the internet is not hard, and it’s an easy-master skill. As a result, someone with malicious intention can easily have access to the internet, and learn hoe to work with it, to use it to disperse malware and affect any personal computer connected to the network. [1,3]

- People can upload applications on the internet, without needing to worry where and how it may be used; there is no law to hinder application and codes from being uploaded, or to limit the access to such codes. [1]
- The number of internet security attacks, also called incidents is exponentially increasing, according to the CERT coordination Center. The statistics show the need for new legislations to avoid such incidents, and to punish internet criminals.

RECOMMENDATIONS:

- While it is recommended to keep the protocols controlling the internet simple and unsophisticated, the author in [4] believes that, end to end encryption is necessary in the internet network for the sake of safety.
- New laws and protocols should be designed in a way to keep the maximum internet generativity as possible. [1]
- It is important to have legislators with backgrounds in law, technology and economics in the policy making committees to issue proper laws to reduce the rate of security breaches as much as possible. [1]

REFERENCES:

[1] https://dash.harvard.edu/handle/1/9385626

[2] Coquillette, Daniel R. "Iharvard LAW REVIEW I."

[3] https://en.wikipedia.org/wiki/Obfuscation_(software)

[4] Zittrain, Jonathan. "Internet points of control." *The Emergent Global Information Policy Regime*. Palgrave Macmillan, London, 2004. 203-227.