Cyberwarfare and Law Enforcement: Top 5 Things to Know

Andy Igonor  
*Franklin University, andy.igonor@franklin.edu*

Jonathan McCombs  
*Franklin University, jonathan.mccombs@franklin.edu*

Taylor Rosecrans  
*Franklin University, taylor.rosecrans@franklin.edu*

Follow this and additional works at: https://fuse.franklin.edu/ss2018

**Recommended Citation**

https://fuse.franklin.edu/ss2018/50

This Book is brought to you for free and open access by FUSE (Franklin University Scholarly Exchange). It has been accepted for inclusion in Scholars Showcase 2018: Innovations in Leadership and Learning by an authorized administrator of FUSE (Franklin University Scholarly Exchange). For more information, please contact karen.caputo@franklin.edu.
Abstract

Cyberwarfare has been dubbed the third world war. If you have been following the news media, then you know it is practically here; nations spying on each other, allegedly meddling in elections or even in their democratic processes. So what is the role of Law Enforcement in this? What should Law Enforcement know, in order to deal with Cyberwarfare?

Cost of Cyberwarfare

1. Cybercrime damage costs to hit $6 trillion annually by 2021
2. Cybersecurity spending to exceed $1 trillion from 2017 to 2021
3. Cybercrime will more than triple the number of unfilled cybersecurity jobs
4. Human attacks surface to reach 4 billion by 2020
5. Global ransomware damage costs are predicted to exceed $5 billion

Top 5 Things to Know

It all comes down to Intelligence

Investigating Cybercrime is a team sport

Collaboration with the private sector is critical including partnering with Universities

Patrol Officers need to know the basics

New Education is critical including community education

Law Enforcement Challenges

- Preventive intelligence to locate sources of potential cyber threats
- Law Enforcement must keep pace with tech-savvy criminals.
- “The GAO cyber-crime report GAO-07-075 identified four major challenges in combating this epidemic:
  - ensuring cyber-crime is reported;
  - ensuring adequate analytical and technical capabilities for law enforcement;
  - working in a borderless environment with laws of multiple jurisdictions; and
  - implementing information security practices and raising awareness”.

To investigate and prosecute cybercrime, law enforcement agencies need skilled investigators, up-to-date computer forensic examiners and prosecutors with cybercrime familiarity

Cybercrime laws in the 21st century

What is Cyberwarfare?

No common definition

On June 12, 2015, the U.S. Department of Defense released the Law of War Manual (LOWM). The LOWM explains that the precise definition of war “often depends on the specific legal context in which it is used.” Nowhere in the Cyber Operations section, or in the entire LOWM, is the term “cyberwar” (or “cyber war” or “cyber warfare”) defined.

References:

- https://www.rand.org/topics/cyber-warfare.html
- https://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf
- http://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf
- https://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf
- https://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf