Cybercrime and Law Enforcement Training

Jean-Loup Richet

Abstract:

In this article, we discuss law enforcement initiative to respond to cybercrime and its undermining issues (fear, dependencies, culture). This paper highlights the need for a set of globally ratified cybercrime regulations through which the retribution of cybercriminals can be more heavily enforced.

Keywords:

Cybercrime, transnational, collaboration, prevention, law enforcement, education, user awareness, regulations

***

Recently a new bill was announced by Representative Katherine Clark in order to train more federal enforcement in dealing with cybercrime. This Cybercrime Enforcement Training Assistance Act would provide 20 million dollars for law enforcement to get a grip on an area of crime which is evolving faster than anyone can keep up with it. As David Wall (2007) wrote, before we have completely understood a certain criminal technique involving the internet, the information we have already seems to be outdated. How then can we truly train a group of people to deal with this type of crime whose nature is ever-changing?

Fear for Technology

Although the type of crime is continuously changing, there is nothing new to the idea that technology is something harmful and to be feared: a certain fear of technology has always been part of our lives. It is this fear that is at least partly responsible for the decision of a company like AT&T to not invest in the cell phone market in the early 1980s. "*Using mathematical forecasts, the consultants anticipated cell phones being a niche market and not one AT&T should waste its time with*," wrote Ryan Stelzer, co-founder of Strategy of Mind.

But what is this fear based on? Technology is to be understood as a mechanism of understanding the world around us; its need to impose order belongs specifically to this epoch that we live in (Edwards, 2006, pp. 61-62). Technology is that mechanism which frames our reactions and our lives. Interestingly enough, our fear of the internet and new technologies to take over our lives is already part of this technological outlook on life itself. Technology is no longer limited to a specific gadget, it is a total mechanism within life takes place.

Increasing dependency

But as technology takes an ever increasing role in our lives, the way to control and limit its negative uses is underdeveloped. A group of researcher at Team Cymru (2006) already showed how "*insufficient training, limited resources (personnel, equipment, budget), barriers to cooperation, outdated or non-existent legal remedies, a paucity of cross-border cooperation, high-latency cross-border cooperation processes, and individual organizations' cultural paradigms create a fertile ground for success in cybercrime*." And this seems to not even consider our increasing dependency, the global aspects involved and the sheer amount of money and people that are affected by technology nowadays.

But should we reread science fiction novels like 'Neuromancer' by William Gibson (1984), so as to get an understanding of the direction we are heading when we let cybercriminals become the powerful leading sources of information and money? Or are powerful AI's going to take over, limiting our options for us?

Limiting freedom

Perhaps thinking in these terms that science fiction writers started to introduce us with in the 60s and 70s does not bring us any closer to finding a way to handle the ever-increasing and changing cybercrime. Yet it does put a sore finger on what is stopping us from solving it. When in 2001 a convention on cybercrime was signed by the European States, and the United States, Japan, Canada and South-Africa, people started to question whether the US should actually ratify such an agreement. Fighting crime is one thing, but the more important question in these debates seems to be to as to how individual's rights are protected.

That this is difficult question in a country where it is in many places deemed legal and even necessary for individuals to arm themselves in public places. Limiting the individual, and thus the hacker, is an infringement of one's own personal rights to enter a door that one is allowed to enter. The recent debate as to whether large companies such as Apple and Google should open up their encryption to law enforcement so that criminals can be traced, tracked, spied upon, seems to take on the same form. Protecting the individual freedom is more important than protecting the individual. Or are we only dealing with this fear for technology taking over our lives, and limiting our lives, instead of really talking about the issues at hand?

The need for law to enforce

In order to deal with the vast area of cybercrime, from the manner in which big data is used by corporations to the network of money mules and individual hackers, we don't just need to train law enforcement. We need to give them the laws they need in order to stop crime from taking place. The basis would require the harmonization of international law (Calderoni, 2010) which is more than national laws able to meets the global and changing demands that cybercrime requires. And it is questionable whether the convention on cybercrime from 2001 goes far enough to deal with this (Gercke, 2006). Because the growing dependency, together with the human fear of change, makes technology to be much more than simply a

possible criminal means when it comes in the hands of the wrong people. Our technological lives are no longer distinguishable from the technology itself, the Internet of Things is not something out there, it is already in the personal, private space of individuals. And when we want to make sure this technology does not limit our personal freedoms, we need to let international law limit our freedoms – unless we want to live the future science fiction has shown us.

References:

Calderoni, F. (2010). The European legal framework on cybercrime: striving for an effective implementation. In: *Crime, Law and Social Change*, Vol 54, Issue 5, pp 339-357.

Edwards, J.C. (2006) Concepts of Technology and Their Role in Moral Reflection. In: *Surgically Shaping Children, Technology, Ethics, and the Pursuit of Normalcy*. Parens, E. (eds.) John Hopkins University Press, Baltimore.

Gercke, M. (2006). The slow wake of a global approach against cybercrime: The potential of the Council of Europe Convention on Cybercrime as international model law. *Computer Law Review International*, Vol 5, pp. 140-145.

Gibson, W. (1984). *Neuromancer*. Penguin New York.

Team Cymru (2006). Cybercrime: An Epidemic. *ACM Queue Magazine*, Volume 4 Issue 9, November 2006.

Wall, D. S. (2007). *Cybercrime, The Transformation of Crime in the Information Age*. Polity Press, Cambridge.