Cybersecurity and law enforcement essay example

Law, Criminal Justice

In the 21st century, there are many technological innovations and invention, but above all the invention of the internet has changed technological world. The internet has brought a lot of good things, but also with it came various negative activities, which include cyber exploration, cyber stalking, as well as pornographic material. As a matter of fact, cyber exploration, pornography, and cyber stalking are a few of the cyber crimes that affect many people adversely. Hence, in order to protect the vulnerable groups on the internet there are various laws that have been put in place to prevent such crimes. Perhaps, law enforces face many difficulties in investigating, detecting, and prosecuting cases of cyber exploration and cyber stalking. Generally, the law enforcing stakeholders are not in a situation to implement and make effective the existing laws.

Globally, there are various laws in areas of cyber exploitations, cyber stalking, and pornography. Various states have enacted laws that will help to curb down cyber crimes, more so there are recent concerns on protecting minors from pornographic materials, cyber stalking and cyber explorations. Cyber stalking is the most dangerous cyber crime because it poses credible threats and harm to victims (Ellison & Akdeniz, 2001). Cyber exploitation is also another form of cyber crimes. The first move taken towards the establishment of laws protecting cyber exploitation and cyber stalking is ensuring that these activities are classified as a crime. In the past, cyber stalking and cyber exploitation was not crimes; hence, no one could be punished for committing the offence. One of the law protecting cyber exploitation is the protect act that was passed in 2003. The intention of this law is to protect children exploitation. Additionally, the law included

provisions to be used in prosecutions of cyber exploitations on computers and internet.

Another law on cyber crime and cyber exploitation is the Anti-social Behavior Act of 2003. In this law, the police and law agents have the mandate to seek ASBO (Anti-social Behavior Order) against those people stalking and exploiting others online. Therefore, breaching of an ASBO leads to a criminal offence, of which one can be imprisoned. In the year 1997, Harassment Act was passed, whereby it was meant to prevent cyber stalking, as well as other forms of cyber unsocial conducts. In addition, the act presents both criminal and civil measures to deal with issues related to cyber stalking (Ellison & Akdeniz, 2001). Perhaps, it creates a summary of an indictable offence and criminal harassment. It was seen as an extension from the Malicious Communication Act of 1988. Moreover, the IAPPA (Interstate Anti-Stalking Punishment & Prevention Act) of 1996 is among the laws protecting people from cyber stalking. In the 2008, the Information Technology (Amendment) Act was enforced to punish cyber stalking, cyber exploitation, pornography, and other types of cyber crimes (Schjolberg, 2010). On pornography, the (CDA) Communication Decency Act was enacted to criminalize the propagation of indent or obscene materials to children through the internet. Nevertheless, the 2004 Information Technology (Security Procedure) Rules help in prescribing various provisions related to secure electronic records and digital signatures. These laws have been enacted to prevent cyber exploitation, cyber stalking as well as pornographic (Siegel, 2010).

In the modern technological world, law-enforcing bodies face a lot of

difficulties in investigating, detecting, and prosecuting cases of cyber exploitation and cyber stalking. One of the reason is that the technology is changing rapidly; hence, those individuals who are perpetrators on cyber exploitation and cyber stalking change their tactics. As a matter of fact, law enforcing bodies and the formati9on of laws is move at a slow pace (Jaishankar, 2011). Additionally, the implementation of laws is done very slowly; in fact, to some extent there are no laws in most countries, which clearly prohibits of cyber stalking and cyber exploitation. Few laws have been formed to counter virtual crimes. Moreover, some laws counter the enforcement of cyber crime laws. For example, the right to enjoy free speech, as well as freedom of expressions protects individuals from being punished for committing cyber stalking and cyber exploitation (Schjolberg, 2010). In other occasions, anti-stalking laws have remained undecided. Scholars assert that the existing laws on cyber exploitation and cyber stalking are too broad and vague. Furthermore, it is difficult to detect cyber stalking and cyber exploitation because the existing laws require real life threat and physical harm in order to justify the damages caused (Siegel, 2010). Detecting and investigating of cyber stalkers and cyber exploiters by law engaging bodies has proved difficult its perpetrators hide their identity as they continue causing damage to their victims. The law enforcing agents had not anticipated the prompt increase of cyber space users; hence, it made it difficult to predict, and investigate online behaviors. Generally, the law enforcing bodies are not in a position to move with the existing trends of cyber stalking and cyber exploitation (Jaishankar, 2011).

Conclusively, the hasty growth of cyberspace has tremendously created new

and complex chances for criminals to perpetrate the crime at a global level. As a matter of fact, cyber exploitation, pornography, as well as cyber stalking are global cyberspace problems; hence, they need global solutions that will involve the public, law enforcing agencies, and all other stakeholders. The law implemented and enforced should be universal, and base on security and peace framework. It is crucial to understand that as technology becomes complex, cyber crimes also increase. Therefore, the law enforcing agents should move fast in implementing and enforcing laws.

References

Ellison, L & Akdeniz, Y. (2001). Cyber Stalking: The Regulation of Harassment on the Internet.

Crime, Criminal Justice and the Internet

Jaishankar, K. (2011). Cyber Criminology: Exploring Internet Crimes and Criminal Behavior.

New York: CRC Press

Schjolberg, S. (2010). International Law as a Framework for Peace and Security in Cyberspace.

Norway.

Siegel, L. (2010). Criminology: The Core. London: Wiley