The growth of the internet created more in terms of criminal activities

[Student Name]

Introduction

The essay will discuss the internet and its development, which increases the risk of crime. The concepts of cyberterrorism, neoliberalism and globalization continue everywhere. The first part of this essay will explains the security issues people are facing. The internet could be more concerned about the fragile networks and the vital infrastructure where cybercriminals have many criminal opportunities, explained by modern classical methods. The second part of the essay will discuss the concept of risk associated with the internet and how governments are intervening in using the internet. The use of new penology methods is also explained, as these problems hinder the work of government departments and fail to ensure the security of the digital society. **The Internet growth and the Terrorism activities**

In the last 2 decades, there have been tremendous changes in society. This is an introduction to the internet in the late 1900s. The growth of feudalism to capitalism may be one of the many factors that contributed to the development of the internet, as the capitalist system focuses on privatization and profit-making. Therefore, most internet providers are controlled by the private sector, which is showing signs of shifting towards neoliberalism. This is beneficial for these companies, as the internet is used as a new resource and thus increases their income. However, due to the internet growth and globalization in the 1990s, many of the consequences were related to its security and critical infrastructure.

The common debate in these recent years is about the risk associated with security, especially on the internet. The company's cyber security investment in 2007 showed that the electronic systems it owned were not fully protected, and therefore the risk factors were not taken seriously. Companies that participated in cybercrime and security research in 2007 (Brunst, 2008) spent only 5% of their investment in security that means that the data on the internet can be the target of criminal activity. This shows that cybercriminals can easily target them. Therefore, the globalization of the internet creates uncertainty due to "neoliberal individualism" (Aas, 2013).

Cybercrime can be committed in other ways and new traditional types of crime on the internet, such as cyberterrorism, is the main explanation for these new insecurities. If the purpose

of the law is to disrupt the electronic system, that activity is considered cyberterrorism under the Terrorism Act 2000 (Hardy and Williams, 2014). From the last few years, sensitive electronic systems have shown security threats, which mean that the Internet infrastructure may also be at risk" However, when the significant network is at risk, it shows that cyber-attacks can happen anytime, anywhere (Cridland, 2008).

Moreover, in terms of the physical infrastructure and vulnerability of the internet, cyberterrorism data. Research shows us that cyberterrorism is a threat to the internet. Approximately 58% of research participants responded that cyberterrorism posed a major threat, mainly to government and critical infrastructure and computer networks (Macdonald. Et al., 2013). In addition, because multiple cyber-attacks via the internet are relatively easy to capture, it makes terrorism a cheaper option on the land. People don't require a lot of equipment attack and plan as they usually only need a computer or laptop and low bandwidth connection. (Brunst, 2008). While the internet is used for cyber-attacks, it can be carried out anywhere around the globe, making it increasingly difficult for cyber-terrorists to pursue "anonymous and untreated" attacks. (Brunst, 2008).

If we look at weak targets, government control policies, cyber-terrorists, and the internet are the target points; it is related to the theory of normal functioning and criminal activities. The aim is to convey the relationship between crime and personal choice and the ways people and groups choose crime on the internet (Felson & Clarke, 2012). In this case, the target of the attack is an electronic system, criminals such as cyber-terrorists and no conscious Internet guard.

Without a competent guardian, a crime is inevitable, and without protection, we will not know when and where the crime was committed and who committed the crime. This hypothetical criminal approach and the development of the internet have increased electronic systems risks that may face on a daily basis. This can happen when there no or few regulations and enforcement by governments and more private companies have access to the Internet (Innes, 2003), suggesting that the private sector contributes to the increased risk associated with the Internet built environment is at risk of a cyber-terrorist attack, making it a designated target for the criminals (Shahar, 2008).

One of the examples of a terrorist network attack took place in April 2007, when the Estonian authorities were unable to connect to their e-mails due to disruptions or even to use computer systems properly (Traynor, 2007). A large number of pings were sent to the system and

prevented them from responding. This is called a "denial of service" attack. This marked the beginning of three weeks' cyber-attack against the private authorities and government in Estonia. This example proves that the theoretical commentary used in the first paragraph is correct and shows that the globalization of the internet increases the risk of crime because it affects the daily activities of people around the globe, which also include terrorists and criminals (Keen, 2011)

The increased risk has caused many crime-related problems. In the first part, cyberterrorism is a crime and was seen as one of the many challenges that individuals and governments may face. Moreover, because cybercrime, such as cyberterrorism, is very easy to commit, it means that terrorist organizations and cybercriminals have a strong position because they force the government to take action (Knop, 2008). When the government is entrusted with monitoring a specific cyber threat, cyberspace makes it difficult for law enforcement agencies to solve internet problems, as crime is often closely linked to territories and countries (Aas, 2013).

After the 1970s, the government's response to crime changed politically. The change marks the beginning of a new era of sanctions and focuses commonly focus on the risk management, supervision and monitoring that is already carried out on the internet. The Penology approach to digital risk management involves governments and their diversity in large national organizations to work together and share international and national information to identify and respond to attacks. It is possible to launch a cyber-attack anywhere in the world at cheap and fast speed (Knop, 2008), which shows that communicating effectively with various organizations around the globe to administer and disrupt cybercrime. The attacks assist in reducing risk and strengthen government power. The main goal of integrating the Penology approach to the internet is to increase internet surveillance more professionally and manage criminal organizations. The use of this method also points to the increased risk to the internet that led the government to introduce such measures.

In the 21st century, special institutional monitoring is the most likely way to maintain the label of cybercrime on the internet. The associated risk of cyberbullying has led professional intelligence agencies like MI5 and MI6 to conduct surveillance on the internet to protect the targets from cybercrimes. In 2015, Teresa May proposed a new "Investigation Powers Act", proposing new security monitoring measures like the MI5 and MI6 to monitor all websites and personal

communications records for up to 12 months without permission or forensic review (Wintour and MacAskill, 2015).

This new surveillance feature offered by Teresa May shows that due to the nature of the internet, cybercriminals can hide in a digital environment everywhere and hijack critical infrastructure. This is the use of daily tracking in which the government, with the assistance of the police and many agencies, aims to address vulnerable targets on the internet by applying goalsetting, higher-level surveillance methods and by trying to find the perpetrator and the perpetrator before the crime is attacked.

In 2006, the British security services prevented terrorism from "kill the Internet". This is an example of how a specialized agency and a government can successfully work closely together and prevent attacks (Rivington, 2007). The terrorist organization (Al-Qaeda) made tele house Europe the main target for attack, as it is the major network centre in the UK and also contains large servers. Such examples highlight the importance of setting up professional associations like MI5 to protect the UK from attack by infrastructure, as the development of the internet involves great risks.

Perhaps one of the most influential explanations of Internet theory, such as the left-wing realism suggested by Jock Young (1992), is the use of a so-called crime scene model to explain crime and its causes (Young, 2002). This model includes attackers, victims, the public, the police and a number of authorities. The aim of a realistic left-hand perspective is to explain how social interaction in the square affects the outcome of what is happening every day. Regarding the relationship between this model, a realistic approach to policing emphasizes that we need to understand the causes and consequences of crime, manage crime, and improve goals and strengthen police-public cooperation (Newburn, 2012).

The government is using new criminal law methods to reduce Internet risk and have more supervisory powers, and by diversifying criminal justice institutions (at home and abroad) to prevent international cybercrime caused by the globalization of the internet—comments on the law and procedure that should be investigated now. In addition, the United Nations (UN) also recommends that successful domestic and national cooperation can be the next level if they want to reduce the threat of terrorism on the internet. Government departments need to form "a policy and legal framework to promote effective international groups in the investigation and prosecution

of serious organized crime and terrorism (UN, 2012). The main aim set by the United Nations says that governments must act internationally to deal with international terrorist acts on the internet.

Left-wing realism is an effective way to identify the cause of a crime and how to deal with it, as finding the cause can make it easier to find all the means to prevent crime and risks other than the internet. The theory of everyday activities only explains the relationship between rational thinking and convenience and crime and shows that it is not the ideal way to think about how crime is done online because we need to consider how and why it is committed. Assuming how opportunities can lead to cybercrime is not enough; it is the potential problems that create the possibilities that need to be understood that make the subject of left-wing realism the most appropriate theoretical explanation.

Conclusion

As described in the above essay, the key discussions on internet growth and its consequences have encouraged governments to respond by developing more features and providing security services to help identify digital risks. The advancement of the internet has increased criminal activities. This comes from past case studies on terrorist acts, which have shown the government and critical Internet structures many challenges. The globalization and politics of neoliberalism are two of the many causes of cybercrime, providing ample opportunities for cybercrime and global cybercrime to target weak and vulnerable targets. In addition to new penology methods, it should help governments achieve the objectives by reducing the risks posed by the internet.

References

Aas, K. F. (2013) *Globalization and Crime*. London: SAGE.

Brunst, P, W. (2008) ‘Use of the internet by terrorists – A threat analysis -’, in centre of excellence defence against terrorism, Ankara, Turkey. (ed.) *Responses to Cyberterrorism*. Amsterdam: IOS Press, pp. 34-61.

Cridland, C. (2008) 'The history of the internet: The interwoven domain of enabling technologies and interaction', in centre of excellence defence against terrorism, Ankara, Turkey. (ed.*) Responses to Cyberterrorism*. Amsterdam: IOS Press, pp. 1-8.

Felson, M., Clarke, R, V. (2012) 'Opportunity makes the thief: Practical theory for crime prevention, in Newburn, T. (ed.) *Key Readings in Criminology*. Oxfordshire: Routledge, pp. 312318.

Hardy, K. and Williams, G. (2014) ‘What is cyberterrorism? Computer and internet technology in legal definitions of terrorism’ in Chen, T, M., Jarvis, L., and Macdonald, S. (eds.) *Cyberterrorism Understanding, Assessment, and Response*. New York: Springer, pp. 1-25.

Innes, M. (2003) *Understanding Social Control*. London: Open University Press.

Keene, S, D. (2011) 'Terrorism and the internet: a double-edged sword, *Journal of Money Laundering Control*, 14(4), pp. 359-370.

Knop, K, V. (2008) ‘Institutionalization of a web-focused, multinational counter-terrorism campaign – building a collective open-source intelligent system. A discussion paper', in Centre of excellence defence against terrorism, Ankara, Turkey. (ed.) *Responses to Cyberterrorism*. Amsterdam: IOS Press, pp. 8-24.

Macdonald, S., Jarvis, L., Chen, T., Lavis, S. (2013) *Cyberterrorism: a survey of researchers. Cyber project research report (No. 1)*. Swansea University: Available at: www.cyberterrorismproject.org (Accessed: March 2013).

Rivington, J. (2007) *UK foils terrorist plot to kill the internet*. Available at: http://www.techradar.com/news/internet/web/uk-foils-terrorist-plot-to-kill-the-internet-132665

Sen, A. (1984) ‘The transition from feudalism to capitalism’, *Economic and Political Weekly*, 19(30). Pp. 50-66.

Shahar, Y. (2008) ‘The internet as a tool for intelligence and counter-terrorism’ in centre of excellence defence against cyberterrorism, Ankara, Turkey. (ed.) *Responses to Cyberterrorism*. Amsterdam: IOS Press, pp. 104-118.

Traynor, I. (2007) *Russia accused of unleashing cyberwar to disable Estonia*. Available at: http://www.theguardian.com/world/2007/may/17/topstories3.russia

United Nations (2012*) The use of the internet for terrorist purposes*. Available at: http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

Wintour, A, T, P., MakAskill, E. (2015) *Theresa May unveils UK surveillance measures in the wake of Snowden claims*.

Young, J. (2002) 'Ten points of realism', in Jewkes, Y., Wetherby, G. (eds.) *Criminology: A Reader*. London: SAGE, pp. 42-56.

Newburn, T. (ed.) (2012) *Criminology*. 2nd ed. London: Routledge.