Unit 6: Cybercrime and Social Perception

Welcome to Week 6.
This week's learning explores public perceptions and public opinion about internet crime. Being aware of these perceptions is important because in liberal democratic states, public opinion plays an important role in shaping public policy. Therefore, public opinion can play a crucial role in influencing how legislators and policymakers choose to address cyber criminality. Also, shared opinion and perceptions can exercise a decisive influence over people's online behavior. You will also investigate the question of the fiction of cybercrime; 'fiction' is understood here as assumptions and social and legal construction of cybercrime.

On completion of this unit, you will be able to:

- Explore issues concerning social perceptions concerning cybercrime.
- Assess the extent social perceptions have affected the ways the 'crime problem' is dealt with.
- Explore how the costs of cybercrime and its harm have affected the extent of this being dealt with effectively by the Criminal Justice System (CJS).
- Practice research skills.
- Apply critical assessment.

Reflection:

The study investigated how the public thinks digital media affects internet security. Based on the results of this study, the researcher concludes that the growth of digital media has hurt digital security. In the 21st century, when a lot of sensitive information is processed, stored, and retrieved using digital media, it is very important to keep that information safe. Still, some people with questionable minds have come up with creative ways to avoid this kind of security architecture, which would be bad for their wallets and reputations. With its findings, this study has contributed on a conceptual, intellectual, and practical level. In a more real way, the results of the study have given the right people information that could be used as a road map for dealing with cyber security threats. This kind of information could help fight the growing cyber security threat. This study is an academic addition to what we already know about how digital media affects people. The study's results show that Immanuel Kant's assumptions in his theory of perception are true. Taking this experiment's results into account, the researcher suggests the following (Asogwa, 2019):

1. Existing laws about cyber security should be made more effective.
2. When necessary, it's important to make new laws with harsher punishments.
3. The National Orientation Agency and any other government agencies that can help should do more to teach the public how to keep their networks safe from cyber security breaches.
4. The media in Nigeria should come up with and run campaigns to stop people from doing things that hurt cyber security.
5. More research should be done in other places to find more ways to use the results.

Understanding the costs of cyber-Crime

Multiple studies over the last few years have attempted to quantify the costs of cybercrime. The research' past attempts at cost estimation have often used methodologies that conflict with one another. Cost per year, cost per attack, and cost by industry are all quite different measures, yet they are often used together. Results have varied widely even when research have used the same methods. The average yearly cost of cybercrime to the UK public sector in 2012, according to the Ponemon Institute (2015), was assessed at £1.2 million, whereas the Detica (2011) stated that cybercrime cost the UK Government £3 billion. These estimations are comparable since they both use data from the same time frame. Research by Detica and the Cabinet Office, which was extensively referenced, also predicted that cyber-crime would cost the United Kingdom £27 billion. The reliability and accuracy of estimates of this kind were called into doubt in response to this study, which received considerable criticism (see, for example, Anderson et al., 2012 and Home Affairs Select Committee, 2013). In particular, the Home Affairs Select Committee (2013) expressed concern about the lack of current data on the scope and cost of cybercrime. In a broader sense, this concern was shared.

The government acknowledged that "an accurate estimate of the scale and cost of cyber-crime will probably never be established" in the Serious and Organized Crime Strategy (Home Office, 2013a), in response to the various estimates of the costs of cyber-crime that have been presented in the literature. The true scope and financial toll of cybercrime will likely never be known. The government also promised under the same plan to form a new external Working Group to improve the quality of data related to the financial implications of cybercrime. As part of the plan, we made this promise to you. Therefore, this report does not try to arrive at an overall estimate of the cost of cyber-crime; rather, it reports on the efforts made by the Costs of Cyber Crime Working Group, which is operating under the supervision of the Home Office Science Advisory Council (HOSAC), to improve data quality, particularly focusing on the development of a framework to conceptualize how best to estimate costs as part of future research. In other words, the purpose of this research is not to provide a comprehensive cost estimate for cybercrime. Since the research included in this study was conducted between Autumn 2014 and Spring 2016, it does not refer to studies that have been conducted or published on the topic of cybercrime cost estimation since that time. This report covers activities that occurred between Fall 2014 and Spring 2016.

Although it is difficult to assess the expenses involved with cyber-crime, the Working Group noted several important reasons for improving the data quality in this area. Better understanding the scale and costs of cyber-crime is crucial for several reasons, including keeping law enforcement agencies abreast of the issue and allowing for more informed prioritization decisions, and targeting prevention efforts at the businesses and individuals most at risk.

- Costs associated with activities (including preventing or reacting to cyber-crime) must be identified,
- As must the parties most likely to bear those costs.

- Furthermore, knowing who would be most negatively impacted is crucial (for example, which individuals, which business areas).

Improvements in measuring and documenting cybercrime are "essential to understand whether the size of cybercrime is expanding or decreasing and how the nature of the issue is developing over time," according to a previous study paper released by the Home Office (2013c). (Citation required) (p 14). Statistics on cybercrime are also lacking, according to the National Statistician's 2011 Review of Crime Statistics (Government Statistical Service, 2011). As a result, the costs of cyber-crime work program were implemented at the same time as a number of more systemic, continuing modifications were being made to the data that was available on cyber-crime in order to better measurement and recording. These adjustments were made to try to fix the problem of inconsistent data. As a bonus, a report on a field experiment to evaluate new measures intended for inclusion in the Crime Survey for England and Wales was released by the Office for National Statistics (ONS, 2015). (CSEW). Our hope is that this research will help shed light on the scope and magnitude of online fraud and other forms of cybercrime. Without such a thorough understanding of the scope and frequency of cyber-crime violations, it is difficult to offer an accurate evaluation of the entire cost of cyber-crime.

The Working Group thus considered these developments and sought to reduce redundant work. In October 2015, the CSEW expanded to include questions specifically on cybercrime; this information was finally included into the CSEW's general crime count in January 2017. (ONS, 2017). The Office for National Statistics (ONS) thus estimates that 2.0 million cybercrimes were perpetrated in England and Wales for the twelve months ending in September 2016. The Working Group was unable to get the data for the time periods in question, but even without them, our understanding of the scale of these crimes has been greatly enhanced. For similar reasons, the United Kingdom's DCMS revised its Cyber Security Breaches Survey for companies, improving the survey's methodological methodology and, in turn, the precision of its estimations. In May of 2016, the newly compiled survey data was released to the public. Such improvements to the larger data sets already available on cybercrime, when paired with other future discoveries, would undoubtedly help to improve the quality of cost estimates in the future; but they were not accessible for use during the timelines that the Working Group was working with.

The Costs of Cyber Crime Working Group

When it was first formed in October of 2014, the Working Group included members from the Financial Impact of Online Criminality Group for Working Academics as well as government officials from a wide range of ministries with an interest in cybercrime, law enforcement, and other entities responsible for devoting resources to combat cyber-crime. Until its last meeting in March 2016, this Working Group was governed by HOSAC, and a HOSAC member served as its chair.

The Working Group has been tasked with setting an agenda and organizing the necessary effort to enhance data quality and offer more accurate assessments of the social and economic impacts of cyber-crime. More research into, and accurate assessment of, cybercrime's prevalence and/or incidence is necessary for more accurate cost estimations, as are attempts to account for the wider, non-monetary costs and repercussions of cybercrime in addition to the financial losses that cybercrime generates.

The group's mission includes cyber-dependent crimes and cyber-enabled crimes as areas of concentration, according the Serious and Organized Crime Strategy. Individuals were included alongside businesses and non-profits.

During the Working Group's 16-month tenure, numerous studies were conducted, including a literature review on the costs of cyber-crime, the development of a framework for estimating these costs, an evaluation of the frequency and financial impact of website defacement in the UK, the scope and cost of malware infections in the UK, and an estimate of profits and losses to underground markets.

References:

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T. and Savage, S. (2012) Measuring the cost of cybercrime. Available at: http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf.

Asogwa, C. E. (2019). Public Perception of the Influence of Digital Media on Cyber Security in Nigeria. Universal Journal of Electrical and Electronic Engineering, 6(5), 366–372. https://doi.org/10.13189/ujeee.2019.060507

Bossler, A.M., Holt, T.J. and Burruss, G (2016) Examining UK constables’ perceptions of cybercrime. Presentation at the annual meeting of the American Society of Criminology, New Orleans, LA.

British Retail Consortium (2015) BRC Retail Crime Survey 2014. Available at: http://www.soloprotect.com/uk/Data/Lone_Downloads/BRCRetailCrimeSurvey2014.pdf.

Centre for Economics and Business Research (2015) The business and economic consequences of inadequate cybersecurity. Research report prepared for Veracode. Available at: https://info.veracode.com/analyst-report-cebr-business-and-economicconsequences-of-inadequate-cybersecurity.html.

Cifas (2014) Fraudscape: UK fraud trends. Available at: http://www.cifas.org.uk/secure/contentPORT/uploads/documents/External%20-%20Fraudscape%20main%20report%20for%20website.pdf.

City of London Police (2015) The implications of economic cybercrime for policing. Available at: https://www.cityoflondon.gov.uk/business/economic-research-andinformation/research-publications/Documents/Research-2015/Economic-CybercrimeFullReport.pdf.

DCMS (2016) Cyber Security Breaches Survey. Main Report. London: Department for Culture Media and Sport. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cybe r_Security_Breaches_Survey_2016_main_report_FINAL.pdf.

Detica (2011) The cost of cybercrime. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/thecost-of-cyber-crime-full-report.pdf