Understanding Cyber Criminals and Measuring Their Future Activity
Developing cybercrime research

Claire Hargreaves and Dr Daniel Prince
Security Lancaster: Security Futures
Executive Summary

The report on the future of understanding cyber criminals and measuring their activity is created to detail the key findings from our workshop which addressed the actions required to tackle the perceived cybercrime wave.

Cybercrime is increasingly seen as a significant criminal activity by governments around the world, whether they are purely digital crimes or traditional crimes which are enhanced through the use of digital technology. Despite the anecdotally growing trend and the significant investment by governments to tackle the issues there are few publically available sources of evidence on cyber criminals. We argue that in order to be effective in tackling cybercrime a strong evidence base is required.

This report draws upon the discussions held in the workshop on defining a cybercrime and understanding the role by which the use of technology enables the criminal. We propose a classification assessment to differentiate between the two fundamental categories of cybercrime: computer enabled and computer dependent crime. We move on to explore the current state of information held, offering a data source taxonomy to facilitate the understanding of these datasets and identify the prominent features to aid data selection. During the workshop it was identified that in order to move forward in our research on cybercrime, an effort to standardise data must come into effect. The theoretical suggestions raised in this area are discussed along with how the information can facilitate research. Furthermore we detail the key points of contact at which valuable data can be collected along with current and advanced mechanisms by which information could be obtained. Following the accumulation of data and its increased quality heightened research can begin. We therefore converse proposed research on both cybercriminals and their victims.

The key findings from the workshop are outlined below.

Understand technologies role in cybercrime

We draw upon the existing literature and the discussion held during the workshop in order to define, for the purpose of this paper, a cybercrime, and to understand the role by which the use of technology enables the criminal and mediates the victim offender interaction.

Defining cybercrime was found to be a difficult task for several reasons, firstly cybercrime encompasses a broad spectrum of offences many of which can be traced back to traditional crimes, the question is then raised as to whether new definitions and laws are needed or whether amendments to existing legislation is all that is required. Cybercrime is a relatively new crime, in which government agencies, law enforcement bodies, businesses and academics have deliberated over in an effort to come to an overarching definition.
Dependent upon the organisation defining the crime some discrepancies exist, however there are two fundamental categories, computer enabled and computer dependent crime. Computer enabled crime is a traditional crime facilitated by technology whilst computer dependent crime is a crime which could not exist without new technology.

With the broad categories of computer enabled and computer dependent crime it is important to develop mechanisms to be able to judge the extent to which either should be selected. The workshop discussed utilising the following concepts:

- **Force Amplification**: A simple analogy here is that of physical harm with or without the use of a weapon. The level of harm that the average person can achieve with a weapon is far greater than that without. Similarly the amount of harm that can be caused with digital technology can be greatly amplified, for example, consider fraud via spam. If a fraudster had to send a letter to each target then the number of targets would be greatly diminished. The use of digital technology and communications enables the criminal to be able to interact with potential victims on a global basis.

- **Entry Barrier**: A significant feature of all technology is that it significantly reduces the entry barrier for people to commit a criminal activity, consider copyright theft. In this instance, the digital replication of any copyright protected information, music, film, literature, is relatively trivial given the currently available technology.

By utilising these two comparative properties crimes involving digital equipment may be compared for equivalency but also classification as computer enabled or computer dependent. This has a potentially significant advantage for the legal system in two respects. Firstly it presents the impact that technology played in the crime via a mechanism that does not rely on technical details that a lay person would find difficult to comprehend. Secondly it facilitates a comparative approach for prosecution and sentencing decisions which are again technology agnostic. This is an important principle that should be considered going forward, *Focus on the impact of the technology not on the technology itself.*

**Standardise data to further our data sources**

Cybercrime data is currently fragmented, this can be put down to a lack of data collection and also reoccurring arguments over the definition of what a cybercrime actually is. However, there are data sources available that can be used to help to understand the domain. The workshop sought to be surgical in its analysis of the available data sources to understand what is available and how this information may start to be combined to develop a complete and realistic understanding of the cybercriminal terrain. What became apparent in the workshop was the need for a step change in research on both cyber criminals and their victims and a more sophisticated understanding of what data is actually required to underpin appropriate analysis.

To facilitate the comprehension of these data sets we propose a classification approach that identifies the salient features of the datasets, aiding researchers to select appropriate
sources for their investigation. The proposed data taxonomy comprises five levels: originator, type, collection methodology, processing methodology and data availability. At the first level, originator, the researcher establishes whether the data is public or private whilst at the second level, type, the quantitative and qualitative levels are assessed. The scope of the target population is evaluated at the third level, collection methodology, and how the information has been developed should be calculated at the process methodology level (fourth level). At the final level, data availability, the level of access to the data should be considered.

Whilst the exploration of current data has its benefits, it is limited. To move forward in this space it was debated that the production and provision of a standardised data frame was needed to develop reliable and valid datasets. Delegates identified several elements mandatory in the construction of standardised cybercrime data: the data must be kept simple, well structured, have high input standards, consistent measurements and definitions, and inclusion of basic variables. Introducing these measures will limit, at the inputting stage, mistakes such as inconsistencies and duplications. What’s more, the datasets will be comparable optimizing sample size. Following the discussion on standardised data delegates debated its operationalization. It became apparent that in order for organisations to provide and maintain information, ownership of such data was key. It was suggested a structured data frame be provided to organisations in conjunction with adequate training.

Although the proposed standardised data will provide stepping stones to fill the knowledge gap, it is not without its limitations. The data will only provide a snap shot of what is occurring in the UK. Furthermore, there will be extreme difficulties in standardising data particularly when the needs of academic, government and private sectors must all be met.

**Utilise mechanisms to capture data**

Utilising both new and old mechanisms of data capture will develop our evidence base. The workshop set out to explore mechanisms that could be utilised to capture data on cybercriminal activity. We propose there are two vehicles of data collection that can be adapted in order to capture appropriate data. The first of these is the key points of contact through the process of criminal investigation, prosecution and sentencing. The second opportunity is periodic or asynchronous crime or impact surveys carried out by governments and businesses. Victims and offenders interact with the investigative and legislative system from the first moment a crime is reported. These interactions provide ideal opportunities to gather information regarding the involvement of technology and therefore are able to classify it as a cybercrime. This approach of, little but often, enables a mass of information to be collated as the criminal justice system process progresses, rather than in an asynchronous survey approach.

Surveys present a platform from which offenders can express their feelings, attitudes, motives and actions without fear of judicial repercussions. This method of data collection
also allows victims the opportunity to talk about crimes committed against them away from the pressures of law enforcement; victims may not feel it appropriate to report to the police or do not wish clients to know they have fallen victim to cybercrime. Furthermore, three advanced collection methods were identified: cyber specials who would be trained in both interview and cyber technology, online forums to gather more personal data and technologists who would have the ability to ascertain how equipment has been used – for better or for worse.

**Broaden analysis on cyber criminals and their victims**

Developing an understanding of who criminals and victims are in terms of their characteristics will help deliver appropriate interventions. Two fundamental areas were identified in the workshop as requiring extensive research: analysis of cyber criminals and investigation of victim profiles. Research on cybercrime data is minimal in comparison to the extensive analysis of traditional crime, the critical reason being the limitations of existing data. Research and its subsequent results are restricted to the quality of its data therefore advancements in cybercrime data must first be made.

Research into why individuals commit crime when others do not, and to ascertain how these individuals are different to law abiding citizens is essential if we are to tackle cyber criminality. Through the use of statistical techniques factors associated to cybercriminals can be identified allowing us to answer such questions as, do cyber criminals have common demographic characteristics? Furthermore, comparing the characteristics of online to offline offenders will help to establish whether these groups of offenders are different. The results of such analysis will assist in shaping policy in terms of detection, intervention and punishment. In addition, the development of criminal career research on cybercrime data will enhance the evidence base used by policy makers and law enforcers.

Establishing whether victims of cybercrime are a specific group of people will help to target preventative methods and resources. Through a victim information database researchers can investigate the characteristics of the victims to develop our understanding of who they are and determine if specific groups of people are more vulnerable to cyber-attacks and if so the reasons why. Following this information the common characteristics of the victims can be identified. For example, it may become apparent that the majority of victims were of the age 25 to 30, if this is the case preventative methods, such as educating them on how to stay safe online, could be targeted to this age group.