N8 Policing Research Partnership: Innovation Forum on Cybercrime

Market Place Discussions

2. Victims, Harm and Communities

- Communities (common interest groups)
  - Member responsibility
  - Can communities help minimise risk of harm for members
  - What characteristics are there in a 'healthy' community that prevents crime
- Harms
  - Distribution of harms across domains in cybercrime
  - Reducing harms to communities → reduced violence in cryptomarkets
  - People as both victim and perpetrator of cybercrime
  - Measuring harms

Rapporteur Notes (1):

- Crime prevention is needed for cybercrime.
- The definition of community is very important since we engaging with all these people.
- There is a risk of generalisation and categorisation.
- It is important to have in mind that people may not identify themselves in a community that someone may consider them as part of for research purposes. Potential racism issues.
- Children 6-14 are more vulnerable and the risk to become victims of cybercrime is higher.
- Any research project must specify which cybercrimes is dealing with and what communities is taking into account.
- Different projects should emerge for different communities.
- There is the possibility that young people are both victims and perpetrators.
- Replace the focus from identifying a victim and a perpetrator to identify where the act is manifested.
- An educational toolkit should be developed to be used by anyone.
- We may need a motivational factor for private companies to provide more information to some groups.
- How you quantify the success of informing a group of people on a particular issue?
- The concept of privacy for younger people is different. The education on this issue is different in other cultures and countries. Some communities within a nation can understand cybercrime easier. How can we educate the young people? Up to a certain point they are just users but at some point they are just victims and without any applications from them personally this can change overnight.
- There is a gap between understanding how the internet works, when a cybercrime occurs and when the forces are involved.
- Awareness of the fact that you could end up to the criminal justice system from a young age and of the punishments for specific actions
- Awareness of how people will be treated when caught.

- If people are educated and are aware of things can do different choices
- There should be a notion of active citizens that recognise their responsibility to talk about how things should happen.
- A police officer's communication to the community maybe useless because of the fact that he or she is a police officer. However an academic may be more able to communicate with the community and extract ideas and problems.
- We need a definition of what a community is. What are the characteristics of a community? What does it mean to be a member of an online community? What are the responsibilities to minimise the harm of the people that are in that community?
- We need to marry the concept of an online community and a physical area community.
- "Different perceptions of harm" means a different harm. How do you understand and measure this perception?
- What it makes to be a victim of cybercrime?
- Research must be from the victim's point of view.
- What is the difference between traditional harms and cyber ones?
- We need to increase the confidence of victims to communicate the harm.
- For all the cybercrimes we need consistent terminologies.
- People should understand their responsibility as a community member in general. Both as a person in the street and as a user of the internet.
- We should identify the responsibilities of online communities to minimise the potential harm of users.
- We have to take into account that most of cybercrime is not reported. If more crime is reported we will have better regulation of crime.

Rapporteur Notes (2):

This group discussion quickly launched into the issue of 'communities' as a concept, with Simon suggesting that the police must address specific online communities who are most at risk and tailoring specific responses to them. This faced a rebuttal by Alison, who asserted that such a generalisation and categorization went too far and faced the risk of being discriminatory. There was some consensus that the defining of 'community', much like 'cybercrime', was perhaps too difficult a task and that it may be a barrier to research. The communities that are most at risk were thought by the group to be the most tech savvy, i.e. children. This is because they are ignorant of the dangers associated with the tech. It was questioned at this early point which type of cybercrime the research would examine, and which communities and whether that would require multiple projects.

The topic of harm was quickly moved onto, with the group keen to ascertain if it is possible to assess where it is manifest. If it can be viewed where it is manifest, the initiatives that are currently working can be assessed and where initiatives are lacking. Yorkshire police were discussed as bringing out cyber-hazard education, which, if successful, would see an initial spike in cybercrime (due to increased reporting) and then a steep drop. This would amount to a useful case study. A lot of the harm was associated with privacy online and a lack of comprehension as to how the harm can be caused, particularly with using information and images against the original distributor of the image. The group agreed that more should be

done prior to police involvement by parents or teachers, by educating and disciplining for irresponsible use. Early interventions and the way things are 'sold' to internet users is crucial. However, there are particular threats to vulnerable groups from smaller firms who are less concerned with user's safety. Companies can only continue to have an insufficient level of care for their consumers' safety if we let them.

Estonia's methods of teaching children very early were raised (as they were in the earlier session) commenting on the successes of informing parties of the risk early. Other members of the group believed that catchy tunes and games generate good awareness in regards to many issues, and there was a particular need to educate in regards to online stranger danger. However, it was discussed that much of the materials needed to educate children in this way already exist but were not being distributed successfully, leading to a question of how best to go about that. There were talks on whether businesses should be made responsible, but the motivation for companies to do so may be lacking. Reputation and the ability to be publicly shamed are great motivating incentives for companies. The ICO also highlights good practices. Quality marks or seals of approval would be good methods of ensuring compliance with higher corporate responsibility. Fining and punishing companies for non-compliance is of little relevance to consumers, consumers must be appealed to on the basis of ethical compliance of companies as people respond to ethics.

This duty to educate came back in the discussions to community responsibility. The police are responsible for distributing messages and education, but it should incite conversations amongst people, active citizens are responsible for talking to their peers. This is on the basis that communities must build their capacity to self-help. Importantly, the group saw that the police must not be heavy handed in this approach. This made the group consider the importance of communities further, and what the differences are between online communities and offline communities. Discussion moved to whether it was possible to transpose beneficial effects between offline groups and online groups. Particularly useful would be if harm frameworks could be transposed.

The group then altered its trajectory by looking at defining what it means to be a victim of cybercrime in comparison to 'traditional' crime. This incorporated ideas of perception and how to prioritize different types of cybercrime, as this is where a great deal of the fundamental differences occur in the two types of crime. A parallel point to this was the management of expectations of individuals in respect to cybercrime, as a reduction in police forces moves more of the onus onto insurance companies and organisations with a powerful online presence. Police forces need to come to conclusions as to what is acceptable behaviour online and what needs to be cracked down upon, for example, phishing scams are still crimes but do not necessitate investigation in many instances.

Key research ideas then needed to be addressed, and the group found two primary ideas worthy of further study.

1. The Differences in harm to victims of online drug markets in comparison to physical markets.

Which would entail viewpoints and examinations of stakeholders in the issue, such as victims, the PCC and politicians.

2. What are the differences between physical communities and online communities?

Which would involve looking into the responsibilities of communities in comparison to online communities. Whether there is responsibility of these communities to minimize harm to community users. There would be a necessity to relate approximate crimes and a view as to what characteristics a healthy community has. Communities will often have leaders as a factual point, or at least in practicality, and these people should be trained to look after the members of the community. Online norms should be established, and more awareness that training (such as that required for physical groups) would be beneficial.