N8 Policing Research Partnership: Innovation Forum on Cybercrime

Market Place Discussions

5. Investigation, Forensics and Emerging Technologies

The Research Idea	To address the lack of knowledge within the police of cybercrime by (1) making technology that police can use and (2) speeding up processing of information led by police
Stakeholders	Police Academics External agencies
Resources Required	Advisory board Soft engineering academics Police – time = money Project manager Case histories Data access Project funding
Funding Sources	Tbc
Key contacts from Innovation Forum	Cliffe S – Leeds Beckett Emlyn B – Leeds Beckett Tim Ingle – WYP Stu Patterson – WYP Syed Naqvi – Birmingham City University Matthew Millings – Liverpool John Moores
Next Steps/Who will do What and When?	

Notes:

- Improve efficiency of investigation
- Use technology to (a) defend people and (b) increase risk to perpetrator
- Co-create – disclosure?
- Goals behind cyber crime
- Use technology to save officer time

Rapporteur Notes:

What is needed is to improve the efficiency of investigations in terms of productivity. How do we cope with the scale of the increases in data? Moreover, how do we handle the variety of data that needs to be analysed? It was discussed that it's not just textual data but also images, video (multimedia data). In terms of multimedia data it is often metadata, so it is important for us to be able to sort through this data for relevant material. It was also mentioned that we need to make use of technological tools that can reduce the hours spent by investigators trawling through metadata. It was argued that law enforcement shouldn't be expected to be the I.T experts.

It was suggested that cyber crime is a very broad investigation. As in all crime cyber crime can be analysed in terms of means, motive and opportunity. For example, what are the motives behind cyber crime? What are the goals? Do those involved have an ideological

purpose? In other words, the investigation is much broader than the actual offence. Technology is very important in the way we investigate because criminal networks are so large and they transcend traditional geographical boundaries.

Do you look at low-level social media or high level DDos attacks when thinking about tackling cyber crime? Because cyber crime is multi-faceted, there needs to be a flexibility in terms of our approach to tackling the issues presented.

There are different 'layers' to potential projects. For instance, there are the sociological or criminological aspects (e.g. what motivates people to commit cyber crime) and the 'physical' layer such as the devices or technology used. An example challenge for those concentrating on the physical layer is: how do we make searches through metadata more efficient for investigators? Criminologists/ sociologists could help identify and narrow the potential searches.

A few angles for potential projects were raised. 1) Technology that you could use to defend people; 2) Technology to act as a deterrent for committing cyber crime. One of the problems identified with many cyber crimes is that they are incredibly low-risk for highly skilled perpetrators. For example, it is often very hard to source where an attack is coming from.

The point was made that most cyber attacks on financial institutions do not get passed on to the police yet at a national level these same financial institutions are far more likely to communicate to one another about breaches of security.

A counter to the increased deterrence perspective is that by warning potential perpetrators about the risks of getting caught crucial evidence may get destroyed (e.g. giving individuals enough time to delete incriminating information).

It was argued that we could learn from the FBI in terms of preemptive detection of cyber crimes using technology instead of investigating after the crime has been committed.

It was questioned why does it take a year to analyse a hard drive? How can it be made quicker?

Apparently, WYP are currently doing a triage with digital evidence to decide how to solve this problem. The reason for backlogs in processing computers is often the sheer amount of material and devices confiscated (e.g. for homicide cases forces will take all computers/phones/laptops etc. – it takes time to look at them all).

There needs to be a greater automation of digital forensic processes as at the moment it is human intensive. There is also a need to move beyond textual searches and to be able to quickly analyse video clips and other multimedia material. It was suggested that the 'speed to arrest' time is often crucial for the police to fulfill their most important duty of 'protecting life and limb' and mitigating any potential harm.

It was suggested that the use of technology is about using tech to saving time and the human resources (especially time; e.g. looking through hours of CCTV footage). A tension was brought up between the use of technology and traditional ways of investigating. For example, some senior investigators might not trust new technology and rely instead on more human intensive methods (e.g. manually sifting through CCTV footage).

An innovative CCTV system was described. This technology allows an investigator to pinpoint an area (e.g. a doorway to a place of interest) and the technology sifts through and automatically identifies people who move in and out of this area over time. This can significantly reduce the time required for reviewing CCTV footage as the investigator only has to assess footage when someone is actually in the area of interest rather than trawling through the data manually.

However, there was a warning against using technology uncritically. What needs to be considered are issues such as disclosure. Senior investigators may be apprehensive about technology because, for instance, manually viewing CCTV footage may have more weight in court than using technological 'short-cuts'. Need to be mindful of the reasons for current practices. Yes technology could save investigators time but a case could potentially collapse as a result. It was suggested that time and time again, a new invention or gadget is brought in but the police can't actually use it for one reason or another (e.g. legislation, disclosure etc.).

In terms of co-creation projects one person identified that the sheer volume of lower-level cyber enabled crimes needs to be tackled. For example, social media abuse, harassments, threats. It was put forward that a more simplified way of capturing Facebook or other social media posts would be useful to frontline responders. Apparently, the Digital Forensic Unit within West Yorkshire were looking at a simple portal in this fashion.

It was argued that sometimes there is underreporting of cyber crimes and also people are not keen to engage with the police because losing an iPhone is like losing a body part to some people! Thus people often do not want to lose their phones or other digital devices for 6 months+ whilst it is being analysed by the police.

A summary of the previous discussion was suggested: 1) We need to make things that police officers can use (technology), 2) Why is it that things take so long to process and what can we build to help alleviate this?

Project ideas derived from discussions

1) Making technology that police can use (e.g. taking into account issues of disclosure, legislation etc.)
2) Speeding up processing of information – led by police

Potential stakeholders identified: police; academics, external agencies

Resources needed:

- Money
- Software engineers & academics
- Police time
- Project manager
- Case histories
- Data access

Advisory board: Legal, ethics