Latest research suggests cybercriminals are not as anonymous as we think

August 7 2017

Understanding a cybercriminal's backstory - where they live, what they do and who they know, is key to cracking cybercrime, new research suggests.

Online crime is of course online, but there is also a surprisingly strong offline and local dimension. Cybercriminals are often seen as faceless, international, computer masterminds, who are almost impossible to identify or understand as a result. But, according to new Oxford University research, contextualising their threat and motivations is key to stopping them. The culprits exist within certain locations, and understanding these locales and the economic situation of those living in them, would help the police to better understand, investigate and counter cybercrime.

In new research published in the journal *Policing*, researchers working on the Human Cybercriminal Project in Oxford's Department of Sociology explored the local and offline dimension of cybercrime. The work suggests hubs of cybercrime are underpinned by frameworks that to a degree, explain how the crime has become so prevalent there. Co-author Dr Jonathan Lusthaus, said: "understanding the human aspects of cybercriminals -where they live, what they do, who they know, how they are organised and operate—is key to addressing the problem in a more complete way".

While cybercrime is a global problem, it is clear that certain regions like Eastern Europe play an outsize role. The study focuses on Romania and

certain towns within it. The paper investigates why Internet fraud is such a problem in the country and finds a number of key factors at play. Understanding a country's infrastructure, economic situation and level of corruption, is vital. Considered together, these factors may help make sense of why cybercrime is so rampant in some societies and not others.

A region's economic situation may be a key indicator of the likelihood of high levels of Internet fraud taking place. With an average monthly salary of €398 per month, Romania is one of Europe's poorest countries. Despite this poverty, the country has a number of successful technology companies and is widely known for its IT expertise. For those not in a position to take advantage of job opportunities in the sector, and outside of the country, a career in cybercrime, known to be financially rewarding, is very tempting.

Additionally, with the legacy of communism and its investment in STEM, the infrastructure exists for fast and successful online operations. Finally, corruption is rife in Romanian society. According to Transparency International's 2016 Corruption Perceptions Index (with 100 indicating a country free of corruption), Romania scores 48 out of a possible 100, and only just above the global average of 43.

The researchers themselves were even the target of a scam. During their fieldwork interviews, a purported and 'unsolicited' fixer offered to introduce them to a network of cybercriminals and high-level enforcement agents, in return for a very significant fee.

However, minor investigations revealed that many of the fixer's connections were in fact fake. Taking this incident into consideration against other evidence gathered, the authors found an openly immoral environment to be fertile ground for those who wish to start a career in internet fraud.

Co-author Professor Federico Varese said: 'Understanding cybercrime isn't just about the victims. You have to look at the supply of the activity. For too long the emphasis has been put on cybercrime as a global activity, but it is a very localised issue. Cybercrime thrives in those places where they can operate with less fear of arrest or punishment.

'The people involved are not necessarily sophisticated or even high tech, criminal masterminds. They are everyday people with a motivation and an opportunity. Almost anyone can do it. If we really focus on where this activity is taking place we should see a reduction in crimes committed.'

During their time in the country, the team visited several Romanian cities and towns for interviews, including Râmnicu Vâlcea which is also known as 'Hackerville' and appears to be the country's most prolific locale for cybercrime. Bucharest comes second on the list. Interviews not only revealed that the criminal activity was widely known about, but that offline activities supported online scams.

The networks of those involved were large, with many people knowing each other personally. Dr Jonathan Lusthaus, said 'one case was spoken about where an entire small community was involved in a particular scam. They said it had spread from neighbour to neighbour 'like a disease.'

Organisers recruit other friends and neighbours to join their scam and perform specific tasks, such as acting as a money mule, or 'arrow', as they are known in Romania. Through this offline dimension, group members are able to meet publically, in social settings and openly discuss operations. In Râmnicu Vâlcea, there were suggestions that cybercrime might intersect with traditional organized crime, with violence used against those who reported on the phenomenon. Local corruption also appeared to help the growth of the phenomenon.

Professor Federico Varese, said: 'On paper Râmnicu Vâlcea should be in the middle of an economic downturn, yet it is rather affluent. Those not involved in cybercrime see their friends in their fancy cars, making money, and facing few consequences, and they want to get involved and the cycle continues'. The paper argues that while the victims can be thousands of miles away and of course should be vigilant, cybercrime needs to be tackled in the places where it originates. The case of Romania suggests that fighting cybercrime at its roots is dependent on good local law enforcement and effective governance - a lesson that could be applied elsewhere. The countries where the victims reside cannot win the fight against cybercrime alone, but need the support of international partners. Varese concluded that, 'As part of the EU we have an opportunity to work with Romania in this area, but that window is rapidly closing'.

More information: Jonathan Lusthaus et al. Offline and Local: The Hidden Face of Cybercrime, *Policing: A Journal of Policy and Practice* (2017). DOI: 10.1093/police/pax042

Provided by University of Oxford