How do you judge a crook who uses a laptop instead of a gun?

March 20 2014, by Daniel Prince

The 21st Century's most deadly weapon? Credit: Ciccio Pizzettaro, CC BY-NC-SA

Some recent high-profile crimes have started people thinking about how we should handle those who break the law using digital technologies. Criminal sentencing is decided by the type of crime and a range of factors, such as intention, harm and motive. And yet the question remains as to how we deal with criminals and their use of technology.

We've held a series of discussions with solicitors, government representatives and others involved in the collection of cyber-crime data.

The main conclusion was that in the UK we need to do a much better job of gathering the data to help us make informed decisions about the scale of the cyber-crime problem.

Technology evolves incredibly quickly and cyber-criminals are particularly adept at rolling with the changes. You can rely on them to come up with a new way to commit cyber-crime almost as quickly as we can find ways to protect ourselves.

The implication of this is that what is or is not considered to be a cyber-crime is also evolving. This makes it troublesome to answer fundamental questions if you are going to measure criminal acts. And we need to consider what the implications of this evolution are when attempting to arrest, charge, prosecute and sentence those that commit criminal acts that involve sophisticated technology.

Cyber-crime classification is currently divided into two main categories: computer enabled and computer dependent. Some crimes, such as fraud, can be committed with or without the help of technology and can be considered enabled. Whereas others, such as hacking, could not exist with computers and are normally considered dependent.

We're not in a bad place when it comes to computer dependent cyber-crime. We've got new and updated legislation, such as the Computer Misuse Act, to deal with the new crimes that could not have existed before the advent of a new technology, such as writing a virus. So we can be pretty clear on how to deal with a computer dependent criminal act.

We struggle, though, when we come up against old crimes that are covered by existing legislation but have been reinvented for the digital age. Do we need new legislation to deal with financial crime using the latest smartphone? If this is the case, would we be confident that the due process of checks and balances that are needed when we introduce new

legislation could be completed quickly enough to keep up with the rapid evolution of technology?

Impact over technique

Rather than trying to draw up new legislation, perhaps the answer lies in thinking about how criminals use technology to increase the harm they do, just as we already do when we punish acts of violence.

In a fist fight, the impact of physical blows is limited according to the physical strength of the combatants. But if one of them brings a weapon to the fight, their ability to do harm to the other is amplified and is considered an aggravating factor when sentences are handed out.

The use of cyber-attacks to amplify or enhance physical attacks has been a reported military tactic. The Israeli bombing of a suspected Syrian nuclear materials site in 2007 was reported to include a cyber-attack on Syria's radar systems that allowed Israeli jets to fly to their target without being detected. In this case, the digital weapon enhanced the effectiveness of the physical act of combat.

This type of force amplification can be seen in cyber-criminality too. Stock market pump and dump scams are a good example. This is a crime that has been around for years but has become easier and more damaging in the digital age.

As has always been the case in these crimes, dodgy stock brokers spread information to artificially boost the value of dud stock and then encourage unwitting investors to buy them. But while this used to require significant effort on the part of the scammer, who had to make phone calls and press the flesh to fabricate value, it can now be done at the touch of a button. False information can be spread in an instant through emails and online forums, greatly amplifying the scope of the exercise

and the damage that can be done.

Online and in the dock

The idea of using sentencing guidelines to manage computer enabled crime has some interesting implications. It shifts the focus onto the impact a crime has on the victim and the impact of using technology rather than the way that technology works. That means the legal system does not necessarily have to understand the technical details of a technology in order to reach a decision, it just has to look at the effect it has had.

This approach means that our existing legislation and criminal definitions can be left alone. Fraud is still fraud, instead of being "computer fraud", which allows us to avoid having to work out whole new rules for a whole new crime.

There is still much work to be done on deciding how we approach this issue but it's important to start making progress. Cyber-criminals aren't going to wait around for us to make up our minds.

Source: The Conversation