Policing Cybercrime in the EU: Shall I Stay Or Shall I Go?

David S. Wall, Cybercrime Research Unit, Centre for Criminal Justice Studies, School of Law, University of Leeds

As the Bremain and Brexit campaigners slug it out on the political stage, the terms 'immigration', 'sovereignty', 'economy' and 'security' are bandied about like pawns in a political game of chess. Fired straight from the heart rather than the head, one side will shoot a Brexit or Bremain salvo then the other side will just pooh-pooh it. But these issues, especially when they relate to the economy and security - which for me are most relevant to the referendum debate - are in fact not just a matter of life and death. Paraphrasing the late Bill Shankly OBE, I would say that they are much more important than that! The outcome of this referendum will have a long term impact upon the financial and political security of the UK. In terms of cybercrime, I will argue that the arguments stack up in favour of Bremain: let me explain further.

My own area of criminology is the interdisciplinary (cyber) space that encompasses social science, computer science, the practitioner and the policy maker. Just as I categorise cybercrimes in terms of their transformation by digital and networked technologies; in other words, take them away and what do you have left! Then I am also starting to view the EU in similar terms, take away the EU and what anti-cybercrime capability do you have left. But firstly, what are cybercrimes and why are they any different to more long established crimes; and why are they relevant to the Bremain-Brexit debate?

Why is cybercrime different to offline crime?

Networked technologies have transformed criminal behaviour in three important ways and they possess very different logics of organisation and regulation/ policing to those found in offline crime. Firstly, network technologies not only *globalise* the communication of information, ideas and desires, but they also impact locally by causing a *glocalising* effect, which is the global impact upon the local. For example, a scam committed from one country upon victims in another will create a need to expand policing there in order to deal with it. Secondly, network technologies create the potential for *asymmetric relationships* where one person can victimise many at the same time. Thirdly, network technologies and associated social network media are creating *new forms of networked social relationships* that act as the source of new criminal opportunities and crimes such as stalking, bullying, fraud, sexting and sex-extortion etc. The upshot is that crime can now be global, informational, and distributed, but also simultaneously synoptic and panoptic. In short, cybercrimes can be committed at a distance, much more quickly and in much greater volume. Jurisdictional boundaries no longer contain crimes in the way they once did. This globalised 'cyber-lift' marks out cybercrimes as very different from offline crime.

New forms of criminal opportunity are being created that are *changing the way that crime is taking place*. Criminal labour, which I view crime to be, is rapidly becoming deskilled and simultaneously re-skilled by technology. Furthermore, as indicated earlier, the entry level skills of cybercriminals have fallen as the technologies have become automated to the point that malware can now operate by itself, see, for example, the discussions relating to Fake Anti-Virus/ Ransomware, and Stuxnet. Crime services can be rented or bought off the shelf as 'crimeware-as-a-service'. The visible technology surrounding cybercrime has effectively 'disappeared' for most types of offender in that its operation is intuitive and the programming skills that were once essential are no longer necessary. Another significant development has been the drop in the cost of technologies which has dramatically reduced the start-up costs of crime.

Put in more simple terms, networked technologies create an environment in which there is no need for criminals to commit a large local crime at great personal risk to themselves anymore, because one person can now commit many small crimes with lesser risk to themselves across a global span. The modern bank robber can, for example, contemplate committing 50m X £1 thefts themselves from the comfort and safety of their own home at a distance, rather than commit a single local £50m robbery with its complex collection of criminal skill sets and high risk. The impact of these transformations upon crime is that the average person can, theoretically, now commit many crimes simultaneously in ways not previously imagined and previously beyond their financial and organisational means, and on a global scale. If not a bank robbery, then they can commit a major hack, DDOS attack, hate speech campaign, or fraud; see for example, the case of Lomas who scammed 10,000 victims out of £21m (see Wall, 2015). The fact that one person, or a few, can now control whole criminal processes has profound implications for our understanding of the organisation of cybercrime. In a rather cynical way, the internet has effectively democratised crimes such as fraud that were once seen as the crimes of the powerful and the privileged.

Of course, the term Cybercrime has its cultural origins in 1980s cyberpunk literature, and so, is very broad and imprecise. It also is used to encompass a range of criminal activities that impact upon individuals, businesses and national states in very different ways. First, they need to be differentiated by the degree to which they are mediated by technology. At one end of this spectrum are *cyber-assisted* crimes that use the internet in their organisation, but which would still take place if the internet was removed, e.g. drug deals. At the other end are Cyber-dependent crimes that are the spawn of the internet, and if the internet is taken away, then they simply disappear. Of course this cannot be done and this 'transformation test' is simply a mnemonic that helps establish a principle. Between the cyber-assisted and cyber-dependent crimes are a range of hybrid cyber-enabled crimes that include most types of frauds. They are existing crimes in law, but are given a global reach by the internet. Take away the internet, and these crimes still happen, but at a much more localised level. They lose the global, informational and distributed lift that is characteristic of 'cyber'.

Second, is the need to differentiate cybercrimes by their *Modus Operandi.* <u>Crimes against the machine</u> (hacking, DDOS attacks etc.) are different from <u>crimes that use the machine</u>

(frauds etc.) and crimes that are in the machine (extreme pornography, hate speech, and social networking originated offences). See further Wall (2015) for references of sources of these categories. Yet, the distinction between them is rarely considered, even though each has different implications for understanding the levels of victimisation experienced, the offenders and the way that they organise cybercrimes and then in allocating an appropriate response. Some have local impact others EU-wide and globally.

What the different types of cybercrime have in common, and why their qualities are significant for the EU Brexit/Bremain debate is that they come at you - the public, business and UK nation state - from all different directions and locations. They respect neither borders nor sovereignty, and as long as everyone close by is on the same side to counter them, there is literally safety in numbers. Cybercrime therefore needs to be approached in a collaborative way in order to capture intelligence of the many €1 thefts, mentioned earlier, and join it together to identify the offender and develop a body of conclusive evidence related to their wrongdoing.

Cybercrime and Brexit

If the UK came out of the EU we would retain the arrangements under the Council of Europe Cybercrime Convention (ETS 185), because the UK has signed up to it and will remain a member of the Council of Europe even if we exit the EU. We would also still have NATO and the Tallinn Manual on Cybercrime (ed. Schmidtt, 2013) to guide on dealing with serious cyberthreats to the nation, including cyberwarfare. We would still have the 'special relationships' with the US and Australia. We would still have participation in Interpol. We would still have our UK cybercrime and cybersecurity capability. But these capabilities, the convention arrangements and the 'special relationships' would be considerably weakened by Brexit.

Although the UK is often presented, and indeed has presented itself, as an awkward partner in the EU, the UK has nevertheless been an active member state in EU internal security and in areas such as policing and counter-terrorism measures, it has driven many of the developments. Not only will we lose the headway that has been made in terms of the joint capacity building on policing cybercrimes and the intelligence sharing that is taking place but the UK is a leader in defining security norms in the area of cybercrime and cybersecurity. The benefit of this lead to both the EU and the UK would be lost. Even if some arrangements remained, the data sharing procedures that are central to many current security practices would also need to be renegotiated, which could interfere with the effectiveness of processes. Furthermore, after a Brexit, and without the cooperation and participation of EU member states, some UK ideas about policing practice, specifically the disruptive policing practices often used to great effect by the National Crime Agency could, for example, potentially clash with the policing practices of EU states if they take a different direction. The UK will simply become a big fish in a small pond.

To illustrate this point further, the UK would cease to be part of the EU institutions to which they currently make significant agenda setting contributions to in the field of cybercrime. The intricate layering of agencies, processes and procedures, and the sharing of policy

and practice in intelligence, investigation, training would cease to be as effective as at present. More specifically, participation would likely cease in ENISA, the European Union Network and Information Security Agency, which is the centre of expertise for cyber security in Europe, not just cybercrime. The UK would also have a different relationship to EUROPOL, which coordinates EU wide organised crime intelligence and operations, which also includes EC3, the Europol CyberCrime Centre. The UK would cease its input into the EU Policy Cycle [2013-2017] on SOCTA (Serious Organised Crime Threat Assessment), which helps shape policy. A further loss would be of membership of EUROJUST, the agency which brokers judicial cooperation across EU member state borders with regard to the coordination of serious and organised crime that threaten its citizens, including economic crime and cybercrime. The UK's impact on European policing would be further diminished by loss of expert input into CEPOL the European policing training agency which teaches senior and specialist police officers about latest developments in cybercrime, policy and practice. Plus, there are the many other social, governmental and business oriented information-sharing groups and networks, each in different stages of development. Associated with these cybercrime policing initiatives is the European Arrest Warrant (2002/584/JHA) which enables member states to extradite suspects and criminals across borders and Brexit would also interfere with the operation of the EU Proceeds of Crime directive (2014/40/EU).

Many of the above developments are still in development and are still maturing, having taken many years of negotiation and contributions to get to this stage. They are neither perfectly formed nor free from criticism, but they still are a considerable step forward from the position a decade or two ago. Moreover, they need to continually evolve further because of the evolution of cybercrime (described earlier). New iterations will keep coming, stimulated in the near future by Cloud technology and the Internet of Things, however, it is important to remember that the technology which creates new criminal opportunities, also provides ways of mitigating it. The codes can be turned back on the offender so that we can look down the telescope the other way and identify them. In many ways it is just a matter of having the correct resources to chase the breadcrumbs, but as indicated earlier, the scale of resources required (finance, personnel, technical skill sets) plus the distributed nature of the crimes rather dictates a joint effort is needed.

EU research developments on cybercrime

Accompanying these institutional arrangements are the many EU funded (Horizon2020, previously FP7 and FP6) research projects that have been commissioned on cybercrime, cybersecurity, information security also some related aspects of organised crime. These projects bring many UK academics and stakeholder partners together with colleagues from other EU member states to work on collective research in relation to understanding the implications of cybercrime and how it relates to each other's criminal and civil processes. Without them, transnational cybercrime knowledge sharing and co-production would more or less come to a halt.

Minimising the overall threat from cybercrime

The main reasons, then, for maintaining an EU-wide cybercrime capability and remaining in the union, is to minimise the overall threat to its citizens from cybercrime. Although the problem is global, the immediate threat to the UK is currently from outside the EU. Criminals and criminal groups are preying on EU citizens, businesses and countries and the current coordinated effort is countering many of these incursions. Take them away, as a Brexit would, then there also arises a further potential threat from within EU countries. No matter how flawed they are, current EU-wide arrangements help to ensure that EU member states not only do something about protecting fellow member states and other nations from their own cybercriminals, but also politically and procedurally prevent them from sanctioning those criminals to, in effect, attack other EU nation's infrastructures.

Personally, I find the EU bureaucracy overwhelming at times, if not pedantic to the point that it is sometimes farcical. But I do find that, on balance, the strengths of EU procedures largely outweigh their weaknesses, many of which are, after all, balances and checks on abuse of process. I also don't think that we should get too misty eyed about the referendum, but the way I see it is that a Brexit, especially within the short 2-year time frame, would undo many good works that have been done and are still being done. Brexit leaves the UK more vulnerable to cybercrime attacks against its individual citizens, its business and financial sectors and its national infrastructure. Whilst this may be classed by some as scaremongering, what is crystal clear is that we will lose many useful security and policing co-operations along with the intelligence sharing that takes place; connections that have taken many years to develop and need to be maintained for future security. Shall I stay or shall I go: I think I want to stay. For now at least!

Note 1. My acknowledgement to *The Clash* for the paraphrased title.

Note 2. Many thanks to Lena (Helena Farrand Carrapico) and colleagues at the "Better Safe than Sorry? Possible Consequences of Brexit for the UK's Internal Security", Aston University, 10th June 2016 for helping develop some of the ideas and points raised in an earlier draft.

Wall, D.S. (2015) 'Dis-organized Crime: Towards a distributed model of the organization of Cybercrime', *The European Review of Organised Crime* 2(2): 71-90. ISSN: 2312-1653. http://sgocnet.org/site/wp-content/uploads/2014/07/04_Wall_pp71-901.pdf