International Review of Law, Computers & Technology

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/cirl20

The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted

Paul Arnell & Bukola Faturoti

To cite this article: Paul Arnell & Bukola Faturoti (2023) The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted, International Review of Law, Computers & Technology, 37:1, 29-51, DOI: 10.1080/13600869.2022.2061888

To link to this article: https://doi.org/10.1080/13600869.2022.2061888

INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY
2023, VOL. 37, NO. 1, 29–51
https://doi.org/10.1080/13600869.2022.2061888

Routledge
Taylor & Francis Group

The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted

Paul Arnell [a] and Bukola Faturoti[b]

[a]Law School, Robert Gordon University, Aberdeen, UK; [b]Law School, University of Hertfordshire, Hatfield, UK

ABSTRACT

Cybercrime is a scourge that blights the lives of many around the globe. It has a significant transnational component. Despite established international and national regulation, its growth in scale and breadth persists. One result of which has been increased recourse to transnational and extraterritorial jurisdiction. This is misplaced. There are a number of factors militating against it. The foundations of international law, human rights, the interests of justice, complexity and cost and the underlying purposes of criminalisation conspire to demand a reconsideration of the use of transnational and extraterritorial jurisdiction in the fight against cybercrime. While there are undoubted difficulties attendant to the alternative, enhanced subjective territorial regulation and enforcement, it is undoubtedly the most effective long-term means of fighting cybercrime. The normalisation of transnational and extraterritorial cybercrime jurisdiction should be resisted.

ARTICLE HISTORY
Received 22 October 2021
Accepted 31 March 2022

KEYWORDS
Cybercrime; jurisdiction; territory

Introduction

Cybercrime is a scourge that blights the lives of many around the globe. It has a significant transnational component. Despite decades-old national and international regulation, the phenomenon's scale and breadth continue to grow.[1] The legal response is failing. As Europol has observed; 'The threat landscape has also evolved, attribution is complex in cyber contexts, cybercrime is growing in scope, number of attacks, financial impact and sophistication, jurisdiction is problematic, and the range of offenders and threat actors continue to grow' (Europol 2021).[2] These facts beg a number of questions. What has the response been? Why is it failing? Is there another approach that can be more successful?[3] These questions underlie the present article. Particularly, it is argued that the exercise of transnational and extraterritorial jurisdiction as regular or routine facets of the response to cybercrime is misplaced.[4] Attendant to it are flaws, inefficiencies and, at times, injustice. It detracts from the optimal approach, reliance upon the law and enforcement machinery within the territory where the individual acted in pursuance of her crimes. While not without difficulty and appropriate exception, the exercise of subjective territorial

CONTACT Paul Arnell p.arnell@rgu.ac.uk Law School, Robert Gordon University, Aberdeen, AB10 7QE, UK

jurisdiction is almost certainly the most effective long-term response.[5] If vigorously pursued and collaboratively supported, the purposes of cybercrime criminalisation, including deterrence and punishment, would be better served. Importantly, redress to the application of transnational jurisdiction would become increasingly exceptional. The temptation felt by certain states to rely on extradition or partake in irregular or unlawful rendition would also be lessened. The international and the national rule of law, existentially rooted in territorial sovereign states, would retake centre stage in the fight against transnational cybercrime.[6] This article argues that the normalisation of transnational jurisdiction should be resisted. It does so by demonstrating its deficiencies and weaknesses. It then outlines the steps that should be taken to enhance the effectiveness of subjective territorial jurisdiction.

Why transnational jurisdiction should be resisted

States are primarily territorial. Concomitantly, so is criminal jurisdiction.[7] Cyberspace definitionally transcends borders and provides existential challenges to orthodox notions of territory and jurisdiction.[8] Amongst the reactions by states to the rise of cybercrime has been the extension of their criminal jurisdiction on a transnational basis over alleged cybercriminals situated abroad. This has been done explicitly or implicitly on one or more extraterritorial bases.[9] The United States, for example, in 18 USC § 1030, criminalises fraud and related activity against protected computers. They are defined to include computers used in or affecting foreign commerce or communication, including computers located outside the United States.[10] In the UK, the core statute is the Computer Misuse Act 1990.[11] It relies upon the concept of a significant link to found jurisdiction over the offences listed in Sections 1–3, including unauthorised access to computer material. While the precise definition of the requisite link varies according to offence, Section 5 refers to criteria including the accused's nationality, the presence of affected computers within the UK and a significant risk of damage to human welfare, the environment, economy and national security. Internationally, the leading treaty is the Council of Europe's Convention on Cybercrime 2001 (Budapest Convention 2001).[12] It obliges state parties to adopt measures criminalising a number of acts, including illegal access to a computer system and data interference. Jurisdictionally, article 22 mandates state parties to provide for, *inter alia*, territorial and nationality-based jurisdiction.[13] While relatively conservative jurisdictionally, the Convention does not exclude any criminal jurisdiction provided for within the law of state parties.[14] Notably, it also, in Chapter III, provides for international cooperation, which is vital in the prosecution of cybercrime on territorial and transnational bases, see further below.

The legislative approaches taken to cybercrime by the US and UK largely mirror those taken by states more generally. Simply, their jurisdictional provisions are broad, and explicitly or implicitly apply on intra-territorial, transnational and extraterritorial basis. They do not impose or apply definitive limits upon their jurisdictional ambit, nor focus upon a single facet linking a particular act or accused to them in order to justify taking cognisance of that alleged crime. This is the natural approach to have been by countries, individually and collectively, to the emergence of crimes that transcend borders so readily. Failure to criminalise activity outside a state's borders that has an inimical effect within it was simply not tenable.[15] Legislative enactment was extended for that reason and judicial jurisdiction was exceptionally exercised on that basis.

The reaction to cybercrime by certain states has gone further. The US, in particular, has relatively regularly engaged taken cognisance of cybercrimes commenced outside its borders. On occasion, this has occurred in circumstances where the link between the alleged criminal, her act and the assuming state appeared relatively weak. Admittedly, however, transnational jurisdiction is normally assumed in co-operation with the subjective territorial state. As a result of this practice, transnational jurisdictional claims have become regularised or normalised. At the same time, and more importantly, efforts have been deflected from the only approach that will succeed in the medium and long-term in addressing cybercrime; recourse to subjective territorial jurisdiction. Transnational action, by not tackling cybercrime at its source, provides only a temporary reprieve. At worse, it undermines more fundamental rules and may lead to an exacerbation of the problem. Of course, the ability, and indeed objective desirability, of states to act against cybercrime on a subjective territorial basis varies. The argument is not that subjective territorial jurisdiction is a widely applicable near-term solution. Nor that recourse to transnational jurisdiction should not be exceptionally taken. It is rather that it is time to step back and re-think the way forward in line with the origins and basis of international and national law and to adopt the necessary steps to enhance the prospects of long-term success in the fight against cybercrime.

Ill-accordance with basic tenets of international law

There are a number of reasons why the normalisation of transnational cybercrime jurisdiction should be resisted.[16] Perhaps the most fundamental objection is that it ill-accords with basic tenets of international law. Specifically, the assumption of transnational jurisdiction may conflict with the subjective territorial state's sovereignty.[17] This is almost certainly the case where custody is acquired via unlawful or irregular means.[18] A conflict may also pertain in a more general sense, however. The globe remains comprised of sovereign territorially delimited states and the most widely accepted rules of international law protect that fact. The UN Charter and the Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty continue, of course, to act in that way.[19] An assumption of jurisdiction entailing cognisance being taken of an act committed within a third state arguably impinges upon a state's territorial integrity and undoubtedly interferes with it if unilateral action is taken to give effect to it. Simply, that state's law has primacy in such circumstances.

This is not to suggest that the assumption of transnational jurisdiction is unlawful. Clearly, that is not the case. There are widely recognised and accepted principles of jurisdiction that act to legitimise it.[20] There are, however, areas of contention and uncertainty related to the limits of transnational jurisdiction, including in relation to the effects doctrine as a basis of jurisdiction. This opacity is connected to cybercrime and the objective territorial principle of jurisdiction, under which claims to jurisdiction, where a crime is concluded within the assuming state are substantiated.[21] The point to be emphasised presently, however, is that states and their criminal law remain primarily territorial. There is no realistic alternative. The position accords with one of the most analysed international law precedents, the Lotus Case.[22] Here the Permanent Court of International Justice supported the exceptionality of extraterritorial jurisdiction. The case provides that only in the presence of a justificatory cause is it lawful for a state to extend the reach of its law

extraterritorially. The rarity of objection to the exercise of transnational jurisdiction does not lead to the conclusion that it can, or should be, readily assumed.[23]

Contributing to the argument against transnational jurisdiction based upon the tenets of international law is the absence of rules governing, and particularly delimiting, the permissible ambit of jurisdictional reach. There are, of course a range of treaties stipulating that jurisdiction may be assumed on a number of bases (although, as noted, the Budapest Convention is somewhat limited in that regard). There is not a multilateral convention on criminal jurisdiction *per se* or a settled proper law of the crime doctrine in customary international law.[24] A proper law approach would act to identify the place where jurisdiction should be, or is best, exercised. It would consider a range of factors, including the locus of the accused and her acts, where the effect or result of the act was felt, the scale or degree of harm done, the intention of the accused and her nationality and domicile. In the absence of either conventional or customary delimiting rules, the assumption of transnational cybercrime jurisdiction can go beyond objectively appropriate limits such that the sovereignty and territorial integrity of the state where the individual acted is not accorded due respect. This possibility is particularly pronounced where cybercrime is in play because an act may have a general and random effect in multiple territories and take place in the absence of a specific intent to harm individuals or societies in any one country. These factors, in turn, affect the strength of the link between the accused and transnational state taking cognisance of the act.[25]

Human rights

A cogent argument militating against transnational jurisdiction is that its assumption may engender, or facilitate, a violation of an accused cybercriminal's human rights, a greater risk thereof, or the possibility of an infringement going unremedied. Of course, a contravention of the rights of an accused person can also arise during a subjective territorial prosecution. A violation is unlikely to be litigated in the subjective state subsequent to rendition – with that law governing at the time of the alleged offence. Further, there may well be disparities in the understanding of human rights between the relevant states that prejudice the accused. This has been suggested to be the case as regards UK to US practice, for example, as regard 'special administrative measures', mentioned below. Developed in that context and more generally has been an established body of jurisprudence. This has emerged where human rights grounds have been put forward in opposition to the assumption of transnational jurisdiction.[26] The cases usually arise in extradition hearings or satellite human rights litigation.[27] The gist of such arguments is that rendition will give rise to a violation of the accused's human rights by virtue of her removal from the requested state (a domestic case) or the treatment she will receive in the requesting state (a foreign case).[28] Soering v UK[29] is the seminal case in the area.

Amongst the jurisprudence addressing challenges to transnational jurisdiction cybercrimes cases are notable. This is because they are particularly amenable to giving rise to transnational effects and that they may entail a relatively weak link between the accused, his acts and the state seeking to assume jurisdiction. An early UK case is that of Gary McKinnon.[30] He had been charged in the US with fraud and related activity in connection with computers.[31] He had hacked into various US computer systems while in the UK. A British national suffering from Asperger syndrome, he had never set foot in the US in

pursuance of his alleged crimes. One of the arguments advanced in opposition to his extradition centred upon his right to a fair trial. It was ultimately unsuccessful in the courts.[32] Of some relevance was the fact that the jurisprudential hurdle that must be met to successfully resist extradition on the basis of human rights is particularly high.[33] Notably, in McKinnon's case, at that point, the Home Secretary held a degree of discretion when making the final decision to extradite. It was exercised in McKinnon's favour. The then Home Secretary, Theresa May, barred his extradition on the basis of human rights.[34]

A range of human rights have been forward in opposition to the exercise of transnational jurisdiction.[35] In the Canadian case of United States v Viscomi[36], sections 6(1) and 7 of the Charter of Rights and Freedoms were relied upon where the accused faced internet luring and child exploitation offences in the United States. Section 6(1) guarantees the right to remain in Canada and Section 7 protects one's right to life, liberty and security of the person. Viscomi's arguments were rejected. It had not been established that the possible length of the US sentence was an extreme punishment in violation of Section 7. Section 6(1) was also not violated. The court held the Minister had properly weighed the relevant factors in deciding in favour of extradition as opposed to domestic prosecution. In the Scottish cybercrime case of Craig (James) v Lord Advocate,[37] the right to respect for private and family life was put forward in opposition to the assumption of transnational jurisdiction. Craig had been accused in the US of distorting share prices on the Nasdaq stock exchange through his use of Twitter.[38] His arguments were dismissed. The right to private and family life interestingly illustrates the decision-making process in many such cases. The question for the court is '… whether the interference with private and family life of the person whose extradition was sought was outweighed by the public interest in extradition'.[39] Significantly, courts have come to place considerable weight upon the public interest behind international criminal co-operation in human rights cases opposing transnational jurisdiction.

In the extradition hearing of Julian Assange several human rights were invoked in resistance to the assumption of US jurisdiction.[40] These were the rights to be free from torture and inhuman and degrading treatment and punishment and retrospective criminal law and the rights to a fair trial and the freedom of expression. While Assange successfully resisted extradition, this was on the basis of his mental health, not his human rights.[41] His human rights arguments were rejected, in line with most cases where they are pled in opposition to extradition and transnational jurisdiction. This latter fact is itself noteworthy. As noted, the jurisprudence requires stringent tests be satisfied for human rights arguments to be upheld. The desire by states to act against transnational criminality, in part manifest in extradition agreements, has given rise to a strong presumption in favour of claims to transnational jurisdiction. Indeed, this has gone so far as to affect the once sacrosanct universal nature of the prohibition of torture and inhuman treatment in ECtHR jurisprudence.[42] The law is rightfully criticised on this basis. More generally, it is evident that the assumption of transnational jurisdiction in cybercrime cases gives rise objectively tenable human rights concerns. These include the fairness of an accused's trial and, if convicted, the particularly punitive sentencing policies and harsh prison conditions she may face in certain countries. These concerns would be obviated in many cases if jurisdiction was exercised on a subjective territorial basis. Some of them underlie a distinct but related argument against transnational jurisdiction; that it can conflict with the interests of justice.

The interests of justice

The interest of justice as a basis of opposition to the normalisation of transnational cybercrime jurisdiction differs from human rights in that it entails a holistic consideration of the accused, her crime and its circumstances. Human rights, of course, relate to the plight of the accused alone.[43] A germane development here is the introduction in the UK in 2013 of the forum bar to extradition.[44] It specifically allows a requested person to oppose rendition on the basis of the interests of justice and as such, lends considerable weight to this aspect of the argument against transnational jurisdiction. The forum bar only applies where a substantial measure of the accused's activity was performed within the UK. As such, it is particularly suited to transnational cybercrime. In considering the bar, the judge must consider the place where most of the harm occurred or was intended to occur, the interests of victims, a prosecutor's belief that the UK is not the most appropriate jurisdiction, the availability of evidence, any delay that might arise, the desirability and practicability of all prosecutions taking place in one jurisdiction and the connections between the requested person and the UK.[45] An analysis of all these factors, and no others, guide the judge in deciding what is in the interests of justice.

The forum bar was successfully invoked for the first time in the cybercrime case of Lauri Love. The High Court, on appeal, held that it would not be in the interests of justice to extradite him to the US on various hacking-related charges. The US attempt to assume transnational jurisdiction failed on account of the forum bar.[46] In considering the interests of justice, the High Court notably held that the interests of victims would not be served if he were extradited. This was due to the high risk he would not be able to stand trial for mental health reasons. While admittedly unusual, this case counters the view that the interests of victims are always best served through the exercise of transnational jurisdiction. Of further relevance was the view of the High Court that Love's trial could realistically take place in the UK – a point that lends credence to the exercise of subjective territorial jurisdiction in cybercrime cases.[47]

The interests of justice may be impacted by differences in sentencing policy and prison conditions within a state exercising transnational jurisdiction. In Ahmad v UK[48] these were argued at the ECtHR in opposition to a US attempt to exercise transnational jurisdiction against six suspected terrorists. Cybercrime was relevant on account of two of the accused's charges centring upon a Connecticut computer server that had hosted a jihadi-related website. The applicants claimed, *inter alia*, that mandatory life sentences without the possibility of parole and a prison a regime of 23 h a day in solitary confinement violated their human rights. The ECtHR rejected five of the six applicant's cases.[49] All six were ultimately extradited, tried and jailed in the United States. While the ECtHR did not bar rendition, the case illustrates an acceptance of the considerable gulf in criminal justice practice between states in the exercise of transnational jurisdiction. Rendition in the face of extreme differences in criminal justice policies ill accords with the interests of justice. UK and ECtHR jurisprudence are rightly subject to criticism for too readily acceding to the exercise of transnational jurisdiction in the circumstances such as these.[50] An avenue to reduce such cases is, of course, found in the exercise of subjective territorial jurisdiction.

Complexity and cost

Complexity and cost can provide the basis for distinct arguments against the regularisation of transnational cybercrime jurisdiction. They arise on account of the considerable evidential and procedural challenges affecting its exercise. In most cases, the intricacies and expense are greater than those attendants to subjective territorial cases, not least on account of the necessity of securing the accused.[51] This fact militates against transnational jurisdiction for two reasons. Firstly, it limits its effective use to well-resourced and sophisticated prosecution services. There are relatively few countries that are able to readily meet the need for the required legal and investigative expertise and its associated cost. Indicating the scale of resources is the fact that the 2019 budget of the US Secret Service was approximately 2.1 billion US dollars.[52] While that budget is only partially devoted to transnational investigations, within the Global Investigative Operations Center, the cost is evident. Indeed, the Secret Service is but one of five agencies investigating cybercrime in the US, with the FBI, Homeland Security Investigation, the IRS Criminal Investigation and the US Postal Inspections Service also involved.[53]

The complexity of transnational investigations is clear. In March 2021, for example, a Russian and Macedonian were sentenced in the US state of Nevada for their role in the Infraud Organisation, described as 'a transnational cybercrime enterprise engaged in the mass acquisition and sale of fraud-related goods and services'.[54] They had been extradited from Croatia. Investigating and prosecuting in the US were several agencies. Only the US and a limited number of other states are able to direct such intricate transnational cybercrime prosecutions. Most states cannot. Clearly, this is sub-optimal. The involvement of a wide range of states in prosecuting and punishing cybercriminals – especially on a subjective territorial basis – would democratise the fight against cybercrime, limit unilateralism, rebut several of the arguments iterated above and, critically, enhance the cumulative global effectiveness of the fight against cybercrime. Reflecting the concerns, it has been noted there is an

> … apparent willingness of certain nations, such as the US, to commence criminal proceedings for a wide range of offences to protect narrow commercial, moral or law enforcement interests. These objectives … serve to undermine the very types of transnational justice cooperation envisaged by the Budapest Convention.[55]

The second reason why complexity and cost weigh against the normalisation of transnational cybercrime jurisdiction follows the first. It is that such action deprives subjective territorial states from further developing their expertise and experience in fighting cybercrime. While in the example above, it was undoubtedly expedient for Croatia to accede to the US request and rid itself of two non-national alleged cybercriminals, developing a national capacity is more likely to effectively contribute to the long-term fight against cybercrime within the subjective territorial state and, therefore, generally. The provision of legal and evidential assistance by states affected by cybercrime can be, in essence, applied capacity building. As noted, the overall complexity and cost of subjective territorial prosecutions are generally less than those attendants to transnational action. The diversion of resources from transnational to subjective territorial prosecutions would undoubtedly benefit cybercrime law enforcement capacity in the latter state. This would result in a more efficient and coordinated approach to the global issue of cybercrime.[56]

Underlying purposes of criminalisation

The underlying purposes of criminalisation are overall not best served through the exercise of transnational jurisdiction.[57] While iterations differ, those purposes include deterrence, punishment, retribution and rehabilitation.[58] Transnational cybercrime jurisdiction generally fails to satisfy these purposes as readily or appropriately as subjective territorial jurisdiction. As to deterrence, the likelihood of a particular individual being arrested, extradited and prosecuted through the exercise of transnational jurisdiction is so remote that the deterrence effect of such action is greatly restricted.[59] Transnational enforcement is unlikely in any particular case simply because states simply cannot act in that manner in any way akin to how they can intra-territorially. Detection, investigation and evidence gathering, extradition and prosecution in cases of transnational jurisdiction is simply too geographically distant and slow. As such, it runs counter to two of the three essential elements of deterrence in classic theory; speed, severity and certainty.[60] Only in severity might transnational jurisdiction satisfy the requirements of deterrence. The deterrent effect of cybercrime sanctions is most likely to be maximised where the criminal justice system in which the alleged is present acts diligently and in good faith to detect, investigate and enforce cybercrime proscriptions against those within it committing such acts (regardless of the locus of their intended or actual victims).

The punishment purpose of criminalisation may be better served by either the subjective territorial or transnational jurisdiction dependent upon the particular policies of germane states and whether the purpose is conceived in a general or individualised sense.[61] The policies adopted within the subjective territorial state are, of course, crucial here. Where that state is unable or unwilling to act, the greatest likelihood of punishment, however remote, will be found in third state action. On the other hand, where concerted efforts are made to enforce cybercrime proscriptions where the acts are being carried out then the punishment purpose will most likely be best met in the subjective territorial state. Germane here is the fact that cybercriminals not uncommonly choose a particular situs, a cyber-haven, in order to minimise the possibility of punishment. The Philippines, for example, is one such state.[62] What is clear, though, is that the immediacy of law enforcement significantly heightens the prospect of its success – should that jurisdiction attempt to act against a particular conduct.[63] As to a general or individualised conception of punishment, transnational jurisdiction may be effective in ultimately meting out punishment for a particular malefactor. Particularly notorious cybercriminals, for example, may be sought out and eventually apprehended by a state exercising transnational jurisdiction. The cybercriminal 'Hushpuppi' is one such individual, mentioned below. In a general sense, however, transnational jurisdiction ill-serves the punishment purpose. Only a minute percentage of those involved in cybercrime will be subjected to criminal justice processes in a third state.[64] The imposition of punishment against cybercriminals *per se* within a particular territory is most effectively meted out by the authorities within it.

Retribution as a purpose of the criminalisation of cybercrime stands apart from the other aims because it appears to be most readily met through the exercise of transnational jurisdiction. This is due to it entailing the prosecution of cybercriminals where their acts had an immediate effect upon individual victims or their society or government.[65] Retribution stems from the idea that a '… criminal deserves to be punished

because he has violated a legal system from which everyone benefits' (Young 1983, 317). Similarly, ' … the entire community – save the criminal – is victimized by crime. The criminal's act of usurpation is equally unfair to everyone else' (Bradley 2003-2004, 23). The number of direct victims and the societal costs are, of course, the highest where a cybercrime had its greatest effect. Punishment in that state is most likely to satisfy the retributive purpose of cybercrime criminalisation, with the law applied being that of the victim's community.

Giving effect to the retributive purposes of cybercrime criminalisation is not straight forward. This follows the considerable difficulty of ascertaining and quantifying the locus and relative effects and costs of a particular cybercrime, and doing so both on an individual and generalised basis. The state with the greatest claim to retribution is logically that where the largest number of victims are situated and the greatest societal cost was incurred. While cybercriminals normally target developed nations for reasons of high internet usage and greater personal wealth, adjudging the relative impact upon one or other state is almost impossible.[66] A further consideration is that society and, in some cases, individuals within the subjective territorial state are also victimised by transnational cybercrime. This arises in the sense of the national law being violated, crime being committed within it, proceeds of crime entering the country and money laundering and tax evasion most likely taking place. Individuals are necessarily victimised where cybercrime entails certain forms of internet pornography. Overall, then, while retribution is *prima facie* met more readily through the exercise of transnational jurisdiction, the position is not straightforward.

The rehabilitative purpose of cybercrime criminalisation can be met in either the subjective territorial or transnational state. A particularly relevant consideration here is the considerable disparity in approaches to rehabilitation between countries. While increasingly important within a number of European states its position within many other countries is, at best, secondary.[67] Indeed, amongst all states, the US is notable for the length of certain sentences and the harsh conditions in particular prisons, not its emphasis on reforming the convicted person.[68] Rehabilitation is not apparent within it as a material consideration in sentencing transnational cybercrime cases. Somewhat similarly, a number of Commonwealth states in Africa continue to adhere to pre-independence penal policies centring upon retribution and general deterrence.[69] Clearly, whether a rehabilitative purpose of cybercrime criminalisation exists, and is served or not, turns upon the identity of the state exercising transnational jurisdiction.

Germane to the rehabilitative purpose and the exercise of subjective territorial or transnational jurisdiction is the evidence that prison visitation reduces recidivism.[70] It is likely that the geographic proximity of a convicted cybercriminal to family, friends and community is of considerable benefit to her rehabilitation. This fact militates in favour of subjective territorial jurisdiction or, in the alternative, the transfer of the convicted person subsequent to trial under an international agreement governing that possibility.[71] Overall as to achieve the purposes of cybercrime criminalisation, it appears that the exercise of subjective territorial jurisdiction is generally more effective. Punishment and deterrence particularly are normally better served through it. There is no doubt, however, that the position in any particular case turns upon the criminal justice, prosecutorial and rehabilitative policies followed by the states in question and in certain instances transnational jurisdiction will meet the goals of criminalisation more effectively.

The way forward

Fundamentally affecting the argument that the normalisation of transnational cybercrime jurisdiction should be resisted is the availability of a better alternative that could and should be the usual basis for action. That is subjective territorial jurisdiction. The exercise of effective legislative, executive and judicial jurisdiction by the state where an alleged cybercriminal is physically present is, in the long term, the best and indeed only approach through which it can be adequately countered. This is not to suggest such a tack will be readily realised, or indeed ever fully attainable. Transnational jurisdiction must remain for use in exceptional cases. What must be prioritised, however, is individual and collective state action to enhance the effectiveness and use of subjective territorial jurisdiction. This takes six forms. Required are increased ratification of the Budapest Convention, capacity building, action to counter the unwillingness to prosecute in subjective territorial states, enhancement of the extradite or prosecute provision in the Budapest Convention, an increase in private sector participation in the fight against cybercrime and the development and extension of sanctions against cyber-havens.

Greater ratification of the Budapest Convention

A widely subscribed international agreement providing for subjective territorial jurisdiction and encouraging and facilitating its effective exercise is vital in the fight against cybercrime. Regrettably, attempts to conclude a global agreement on the subject have so far failed.[72] The lack of convergence between countries on the required international and domestic approaches is largely responsible. This, in turn, is affected by the vital importance technological infrastructure plays within states, in particular in terms of national security and privacy. Accordingly, United Nations-based attempts to conclude a cybercrime treaty have to date failed.[73] By default, therefore, the leading agreement is the Budapest Convention. Notably, however, non-Council of Europe members may become party to it.[74] As of March 2022, there are 66 state parties. While some way beyond the 47 Council of Europe members, it is only just over one-third of the UN membership, presently at 193.[75] Clearly, greater membership would be an important step in enhancing the role of the territorial state. As noted above, the jurisdictional terms of the Convention are relatively limited as compared to a number of other criminally related conventions.[76] It terms do not encourage expansive claims to transnational jurisdiction. Greater ratification, therefore, would fully align with an increased focus upon subjective territorial jurisdiction. Indeed, the thrust of the Convention and the machinery created under it seeks to enhance territorial prosecution through capacity building and information and evidence exchange.[77] The challenge for enhancing subjective territoriality as regards the Convention, therefore, is to achieve greater membership. Ultimately what is required is greater political convergence and trust between states on the issue – the same stumbling blocks in the way of a wider international agreement. Heightened and sustained diplomatic efforts encouraging non-state parties to accept the wisdom of co-operation according to the terms of the Budapest Convention must take place.[78]

Prioritise capacity building

Capacity building in the states where individuals are active in cybercrime in the form of directed assistance in resources and expertise is critical in facilitating subjective territorial

states to investigate and prosecute cybercrime cases themselves. Current efforts are lacking, '… focus on capacity building to advance governments' ability to implement such cooperation on cybercrime and enforce norms is not sufficiently prioritized' (Peters and Jordan 2020, 488). This is not to suggest efforts at the capacity building are not being made, however. The Cybercrime Programme Office of the Council of Europe (C-PROC) was created for that purpose and is not restricted in its activities to state parties to the Budapest Convention.[79] More generally, also under the Council of Europe is the Cybercrime Convention Committee (T-CY). It acts in pursuance of the co-operative goals of the Convention under article 46, including the exchange of information and possible supplementation. A notable development here is the approval by the T-CY of the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence in May 2021.[80] The protocol seeks to enhance co-operation generally and as regards the provision of electronic evidence in particular.[81] As drafted, it focuses on mutual legal assistance, co-operation between authorities and service providers, access to information by authorities in third countries and data protection requirements.[82] This is to be welcomed. More generally, however, there is no doubt that the lack of capacity affects the exercise of subjective territorial jurisdiction. Capacity alone, however, is insufficient. It must also be accompanied by the willingness to prosecute on that basis.

Address unwillingness to prosecute

The capacity to adequately investigate and gather evidence[83] is of little import if the prosecution service in the subjective territorial state is not willing to prosecute alleged cybercrime in its midst. An unwillingness can manifest itself both generally and in the context of an extradition request. Generally, states may naturally be disinclined to act against persons where their activities have not caused direct harm within their territory. Relevant here are prosecutorial guidelines and codes. In England and Wales, for example, decisions to prosecute are generally made by the Crown Prosecution Service applying the Full Code Test.[84] The public interest element of which includes consideration of a number of factors, including the seriousness of the offence, the circumstances of, and harm caused to, the victim and the impact upon the community.[85] Where an act within England and Wales affects individuals outside those nations, a CPS decision that it is not in the public interest to prosecute may not be unreasonable. On the other hand, cybercriminals may not be so discerning in targeting their victims. They may be found both inside and out of the subjective territorial state. Further, even where the immediate victims are outside the country, cybercrime will normally engender incidental criminality and may also entail harm in its commission. There is no doubt, however, that efforts must be made to convince states and their prosecution services that acts of cybercrime *per se* demand prosecution regardless of the situs of the direct and immediate victims.

An unwillingness to prosecute transnational cybercrime within subjective territorial states can be particularly evident in the extradition context. Here countries display a reluctance to engage in 'forum shifting'.[86] This refers to the subjective territorial state assuming jurisdiction over acts committed within it in the face of an extradition request. In some circumstances, forum shifting may not be appropriate. This could be where the individual is a national of the requesting state or the impact of the cybercrime was particularly

pronounced within that state. In other cases, however, it can be reasonable and desirable. Strong links between the alleged criminal, her acts and the subjective territorial state militate in favour. The unwillingness to prosecute is not limited to developing states and non-parties to the Budapest Convention, where it may be thought to occur for lack of capacity reasons or the absence of a treaty obligation. Several germane examples are found in UK practice. These include the case of Lauri Love.

In the judgment upholding the forum bar in Love's case the High Court considered a that a UK prosecution would follow its decision.[87] It stated 'The CPS must now bend its endeavours to his prosecution, with the assistance to be expected from the authorities in the United States, recognising the gravity of the allegations in this case, and the harm done to victims'.[88] In the case, there was concurrent UK and US jurisdiction. Both were legally and evidentially able to prosecute. The accused was present in the UK and had considerable connections to it. The CPS was not willing to prosecute. Love remains untried. The UK is not alone in acting in this way. Similar cases are found in states including Canada[89] and Dubai.[90] Countering prosecutorial deferral in favour of forum shifting presents considerable challenges. While agreements and unilateral policy statements on concurrent jurisdiction exist, prosecutorial discretion in most states ultimately limits whether, and if so under what circumstances, decisions to defer to a requesting state, or not to prosecute, can be challenged or conditioned.[91] That noted, what is required first and foremost is political recognition that the exercise of subjective territorial jurisdiction over cybercrime is the most effective course of action in the long term. Appropriate action by states, individually and jointly, can then be considered and agreed.

Enhance the Budapest Convention extradite or prosecute provision

Commonly found in criminally related treaties, the extradite or prosecute principle *inter alia* obliges state parties to either, upon discovering a suspect of a particular crime in its territory, to extradite her or submit her for possible prosecution.[92] The principle can act to enhance subjective territorial jurisdiction on account of requiring the consideration of a prosecution in the absence of an extradition request. This aspect of the obligation is absent from the articles within the Budapest Convention related to the obligation. Article 24(6) *inter alia* provides that if a party refuses to extradite on the basis of the nationality of the requested person or because it considers that it has jurisdiction over the offence it shall submit the case to its authorities for possible prosecution if asked by the requesting state. By way of contrast, article 7 of the Convention on the Prevention and Punishment of Torture 1984 provides that where a person alleged to have committed a relevant offence is found in the territory of a party, it shall, if it does not extradite him, submit the case to the appropriate authorities for the purpose of prosecution. There is no doubt that an amendment to the terms of the Budapest Convention in line with such an obligation would be a useful step in enhancing subjective territorial jurisdiction. Such a move would not affect non-parties, however.

Further develop private sector participation

A key aspect of cybercrime is the network over which it takes place. The extent of private ownership of the infrastructure and software is considerable. The private sector, therefore,

plays a material role in the facilitation of cybercrime. This can affect the ability of subjective territorial states to act against cybercrime. A question arising is whether, and if so how, it can be harnessed to combat it.[93] The answer is, simply, that its integral role, little doubt that its participation is required.[94] The evidence of cybercrime required for detection prosecution is often be held on private servers, be they inside or outside the subjective territorial state. This fact gives rise to considerable and indeed at times, insuperable difficulty for states in acquiring subscriber information and traffic data (metadata), for example. Indeed, that information may be held 'in the cloud', where its location may be difficult to determine at any particular point in time (Maillart 2019, 381). The Budapest Convention goes some way to address these difficulties. Article 18(1)(b) provides that state parties shall adopt measures to ensure that they have the power to order service providers to submit subscriber data relating to such services in its possession or control. Excluded are traffic and content data, however. It is also limited through service providers often being situated outside the territory of the investigating law enforcement agency.

Designed to counter evidential difficulties, it is the Second Additional Protocol to the Budapest Convention. It seeks to enhance the role of the private sector in fighting cybercrime. Its preamble *inter alia* provides ' … evidence … is increasingly stored in electronic form on computer systems in foreign, multiple or unknown jurisdictions [and] convinced that additional measures are needed to lawfully obtain such evidence in order to enable an effective criminal justice response … '.[95] While the Budapest Convention itself, pursuant to article 32(b), stipulates that state parties can access, through a computer system in its territory, computer data located in another Party this does not apply if the metadata are held on the territory of a non-state party or somewhere online in 'the cloud' (Maillart 2019, 383). Further, article 32(b) provides that the consent of the person with the lawful authority to disclose that data is required.[96]

The goal of the Second Additional Protocol is to ' … significantly improve the ability of the Parties to enhance co-operation … between Parties and service providers and other entities and to obtain the disclosure of electronic evidence for the purpose of specific criminal investigations or proceedings'.[97] Articles 6 and 7, for instance, provide for procedures enhancing direct cooperation with service providers and entities in the territory of another party. While very useful, the limitations affecting the Budapest Convention will, at minimum, apply to Second Additional Protocol, particularly its relatively limited membership. Indeed, state parties to the Convention may not agree to it. That noted, the Second Additional Protocol is welcome, evidentially and more generally. As to the latter, it appears to indicate increased convergence in approaches to cybercrime by states. The tripolar order, comprising a state-led arm supported by China, a citizen-first approach advocated by the EU and a private sector view taken by the US, may be evolving into a bipolar approach response, in essence, conflating the traditional positions of the latter two.[98]

Strengthen policies and sanctions against Cybercrime Havens

A final step towards enhancing subjective territorial jurisdiction entails the strengthening of sanctions against states who fail to attempt to counter cybercrime within their territories. This is necessary due to certain states ignoring, or indeed encouraging, cybercrime

originating within their territories directed towards individuals in third states. Russia and China are particular malefactors in this regard.[99] Cybercrime-related sanctions can exert a degree of pressure on such states to act against such activity. They have been applied with increasing frequency in recent years. The US has taken the lead in such action. It has enacted the Countering America's Adversaries Through Sanctions Act.[100] The majority of US sanctions have been aimed at Russia, Iran and North Korea.[101] In April 2021, the Biden Administration imposed further sanctions on Russia, in part for engaging in and facilitating malicious cyber activities.[102] In August 2021, the Sanction and Ransomware Act was introduced into the US Senate. If enacted it would sanction states involved in state-sponsored ransomware attacks.[103]

The US is not alone in employing cyber-sanctions. An EU regime was instituted in 2019. It first took the form of Council Regulation concerning restrictive measures against cyber-attacks threatening the Union or its Member States.[104] Pursuant to these regulations, as renewed, the EU imposed its first-ever sanctions against cyber-attacks in July 2020. Their basis was Council Decision (CFSP) 2020/1127.[105] These included a travel ban and asset freeze for six persons and three entities responsible for cyber-attacks, including 'Wanna-Cry' and 'Operation Cloud Hopper'.[106] Outside the EU, and following Brexit, the UK has made the Cyber (Sanctions)(EU Exit) Regulations 2020.[107] Section 4 provides that their purpose is to further the prevention of relevant cyber activity, including that which 'directly or indirectly causes, or is intended to cause, economic loss to, or prejudice the commercial interests of, those affected by the activity'. As a means to enhance subjective territorial jurisdiction, and lessen the impetus to exercise transnational jurisdiction, the impact of US, EU, UK or indeed other sanctions is clearly moot. It appears clear that they have not, to date, stemmed the flow of cybercrime from individuals based within target states. On the other hand, sanctions clearly have some merit. In addition to limiting the activities of certain individuals and companies, sanctions carry a symbolic value in expressing the formal disapproval of states failing to act against cybercrime within their territories.

Conclusion

Enhanced efforts at preventing and punishing cybercrime are being made by many states, within the Council of Europe and the United Nations. Both subjective territorial and transnational efforts are being made, with seemingly similar import. Action by subjective territorial states, however, is the only effective long-term solution and must be prioritised. The exercise of transnational cybercrime jurisdiction, and in particular its normalisation, is subject to cogent criticism. The basic tenets of international and domestic law, human rights, abuse of process, complexity and cost, the interests of justice and the purposes of criminalisation all militate against its use. It should be employed only rarely. Circumstances arise, and will continue to arise, where it is appropriate to exceptionally exercise jurisdiction on a transnational basis. Ideally, these exceptions would be made in pursuance to an internationally agreed scheme allocating jurisdiction according to a proper law of the crime methodology.[108] That is not likely, at least in short to medium term.[109] In the absence of such an agreement, considerable deference should be shown to the subjective territorial state. States affected by transnational cybercrime should proactively seek to assist that country through the provision of evidence,

intelligence and expertise. Equally, states must act against cybercriminals within their midst, regardless of the locus of the victims of their acts.

Concerted efforts at expanding the membership of the Budapest Convention, capacity building, securing commitment to exercise subjective territorial jurisdiction, harnessing the private sector in an effective and regulated manner and acting against cyber-havens will go some considerable way in creating an approach to address cybercrime in the long-term. Technical, evidential, legal and financial assistance combined with jurisdictional deference is required. Adherence to the rule of law, and human rights is crucial. There is no doubt that cybercrime has posed the most difficult of questions for states and orthodox notions of criminal jurisdiction. The answer is not to forgo territoriality but rather to redouble co-operative efforts in order to maintain its original and existential essence so that the purposes of cybercrime criminalisation can be most effectively met.

Notes

1. 'Cybercrime' here is used to describe the use of digital technologies in the commission or facilitation of crime (Clough 2011, 150). It excludes state-sponsored hacking. As to scale, it has been estimated that cybercrime comprises over 85% of malicious activity on the internet, see Hackmageddon, August 2019, https://www.hackmageddon.com/2021/07/22/q2-2021-cyber-attack-statistics/, Accessed 25 May 2022.
2. In Scotland, recorded cybercrime in 2020–2021 was double the previous year, see https://www.gov.scot/publications/recorded-crime-scotland-2020-2021/, Accessed 25 May 2022.
3. The subject matter of these questions is well-trodden. Amongst the voluminous literature, see UN Office on Drugs and Crime (2013), Peters and Jordan (2020) and Bell (2002). The present piece stands apart by iterating the arguments against transnational and extraterritorial jurisdiction and advocating subjective territoriality.
4. Note it is the normalisation or regularisation of recourse to such jurisdiction that is presently criticised, not their employment per se. Heretofore transnational and extraterritorial jurisdiction will be referred to as transnational jurisdiction.
5. 'Subjective' denoting the place where the alleged offender, the 'subject', carried out her acts.
6. This approach is far from universally accepted. Maillart, for example argues that the adequacy of territoriality's '… subjective facet with regard to the Internet is dubious as it prevents states from effectively investigating and prosecuting cybercrimes' (Maillart 2019, 376). See also Maillart (2021). In line with the present author is Kennedy who writes that '… greater credence should be given to holding transnational trials in the geographic location where the harm emanated' (Kennedy 2020, 3). Also of note is Velasco (2015).
7. In Compania Naviera Vascongada v The Christina, [1938] AC 485 Lord MacMillan stated

   > It is an essential attribute of the sovereignty of this realm, as of all sovereign independent States, that it should possess jurisdiction over all persons and things within its territorial limits and in all causes civil and criminal arising within these limits. (496–497)

   Cases discussed in this article will emanate from the UK unless stated otherwise. As to territoriality in cyberspace Wong states it is '… indisputable that the generally accepted view in public international law is that the primary basis of criminal jurisdiction for any state is territorial' (Wong 2000, 96). In contrast, see Goldsmith (2000).
8. See as regards borders and cybercrime (Zekos 2011). A seminal work is in the area is Johnson and Post (1996).
9. The United Nations Office of Drugs and Crime's Cybercrime Module notes that in addition to territory cybercrime jurisdiction has been founded upon the nationality of the offender, the nationality of the victim and the interests and security of the state, see https://www.unodc.

org/e4j/en/cybercrime/module-7/key-issues/sovereignty-and-jurisdiction.html, Accessed 25 May 2022.

10. In 18 USC § 1030(e)(2)(B). US jurisdictional requirements may be met by 'the inexorable connection between the Internet and interstate commerce' (The Office of Legal Education of United States Attorneys 2015, 113).
11. Further relevant UK legislation includes the Regulation of Investigatory Powers Act 2000 and the Fraud Act 2006. There has been a debate in the UK over the locus of criminal prosecutions for some time. The Baker Review of extradition law specifically examined the question of forum in extradition practice including claims of exorbitant US claims to jurisdiction. See Baker, Perry, and Doobay (2011); and Home Office (2012); House of Lords (2014-2015) and Home Office (2014-2015).
12. Whilst there is no UN-based treaty, an open ended ad hoc intergovernmental committee of experts was convened under GA Res. 74/247 to elaborate an international cybercrime convention in May 2021, see https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home, Accessed 25 May 2022.
13. Reference to, in the parlance of international law, the passive personality, protective and universal bases of jurisdiction is eschewed.
14. As of June 2021 64% of states had substantive criminal law provisions roughly corresponding to the criminal law articles of the Budapest Convention, see Council of Europe Cybercrime Programme Office (2021).
15. There is a long pedigree of states acting in such circumstances. Treason, immigration crimes and currency counterfeiting, for example, have been applied on an extraterritorial basis by many states for a considerable time. As regards the UK, see Arnell (2012).
16. Some of these arguments apply to the exercise of transnational jurisdiction generally. Others, however, apply with particular import to cybercrime.
17. Taken further, transnational jurisdiction has been considered a form of legal imperialism. See Whitman (2009). In a civil law context, see Buxbaum (2016).
18. Whilst indubitable, there is a mixed body of case law on the effect of an unlawful or irregular rendition upon the jurisdiction of the abducting state's courts, including R v Commissioner of Police of the Metropolis ex parte Bennett [1995] QB 313, United States v. Alvarez-Machain, 504 U.S. 655 (1992) and Attorney General of the Government of Israel v Eichmann (1968) 36 Int. L. Rep. 277. In Scotland see Arnell (2004).
19. General Assembly Resolution 2131(XX), 21 December 1965, cited at https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/2131(XX), Accessed 25 May 2022.
20. See generally Arnell (2000a) and Ryngaert (2015).
21. Both the effects doctrine and objective territoriality are, of course, particularly relevant in the cybercrime context. It is not argued presently that the assumption of transnational jurisdiction in most cybercrime cases is unlawful under international law but rather that such action is often at odds with the global system of territorial sovereign states.
22. Case of the SS Lotus, (France v. Turkey), (1927) PCIJ Rep, Series A, No. 10. Sir Robert Jennings wrote of the case

    > … the Lotus judgement, properly understood, is in no ways inconsistent with the scheme set out in the great classical work on the subject, the Harvard Research on Jurisdiction with respect to crime, published in 1935. This assumes that, although the territorial principle is not absolute, *an exercise of extraterritorial jurisdiction requires a justifying principle* … . (Jennings 1967)

23. States are generally unwilling to defend alleged criminals within their midst. Jurisdictional conflict is more evident in the field of competition law, Botteman and Patsa (2012).
24. An argument is tenable that international law has been developing a proper law of the crime doctrine akin to that applicable in contract and delict. See Arnell (2000b).
25. As to the development of phishing schemes see Ghazi-Tehrani and Pontell (2021).
26. Internationally, the UN's Human Rights Committee considered the right to life and freedom from torture in the extradition context in NG v Canada, 7 Jan 1994, CCPR/C/49/D/469/1991,

UN Human Rights Committee (HRC), available at https://www.refworld.org/cases,HRC,4028b5002b.html, Accessed 25 May 2022. Note the facts did not concern cybercrime.

27. Other proceedings may include challenges to jurisdiction following irregular rendition, see Weissbrodt and Bergquist (2006).
28. The terminology comes from Lord Bingham in Regina (Ullah) v Special Adjudicator, [2004] UKHL 26 at para 9.
29. (1989) 11 EHRR 439.
30. Further cybercrime cases include those of Lauri Love and Julian Assange, mentioned below.
31. Under section 1030 of title 18 of the US Code. See Arnell and Reid (2009).
32. R. (on the application of McKinnon) v Secretary of State for Home Affairs [2007] EWHC (Admin) 762 (Admin) in the High Court, and McKinnon v the United States [2008] UKHL 59 in the House of Lords.
33. See Arnell (2013).
34. The specific right was not mentioned, but she referred to his mental health and suicide risk, see https://www.bbc.co.uk/news/uk-19957138, Accessed 25 May 2022.
35. The right to be from torture and inhuman and degrading treatment and punishment is mentioned below.
36. 2019 ONCA 490. The case is discussed by Kennedy supra note 6. In Sriskandarajah v United States 2012 SCC 70 the Supreme Court of Canada dismissed an argument that a United States' extradition request be rejected in a cybercrime case in the face of arguably weak links between the US and the accused. The accused's conduct in Canada entailed the use of email accounts, companies and bank accounts based within the United States.
37. [2020] HCJAC 22. The Supreme Court has allowed an appeal in his case on the basis of the non-extension of the forum bar to Scotland and the effect of that on Craig's article 8 rights, in Craig v US, [2022] UKSC 6. The case has been remitted to the High Court.
38. See https://www.bbc.co.uk/news/uk-scotland-south-scotland-53904358, Accessed 25 May 2022.
39. Celinski v Poland, [2015] EWHC 1274(Admin) at para 6.
40. Assange successfully resisted US extradition attempts at first instance, see US v Assange, 4 January 2021, Westminster Magistrates' Court, https://www.judiciary.uk/wp-content/uploads/2021/01/USA-v-Assange-judgment-040121.pdf, Accessed 25 May 2022. The US successfully appealed, in US v Assange, [2021] EWHC 3313 (Admin). A decision on Assange's application for leave to appeal to the UK Supreme Court is pending.
41. USA v Assange, Assange successfully resisted US extradition attempts at first instance, see US v Assange, 4 January 2021, Westminster Magistrates' Court, https://www.judiciary.uk/wp-content/uploads/2021/01/USA-v-Assange-judgment-040121.pdf, Accessed 25 May 2022. The US successfully appealed, in US v Assange, [2021] EWHC 3313 (Admin). A decision on Assange's application for leave to appeal to the UK Supreme Court is pending, 76–93. The right to be free from retrospective criminal law is unlikely to be tenable in extradition on account of the double criminality principle.
42. See Mavronicola and Messineo (2013).
43. Note that in UK law the approach under article 8 in an extradition decision involves a 'balance-sheet' exercise where a variety of factors akin to those falling under the head interests of justice are considered, see Celinski v Poland, supra note 39.
44. See Arnell and Davies (2020).
45. Found within ss 19B(3) and 83A(3) of the 2003 Act.
46. [2018] EWHC 172 (Admin). His extradition was also barred on under the oppression bar on account of his mental health. See further Arnell (2018) and Arnell (2019).
47. See further below on Love's possible UK prosecution.
48. (2013) 56 EHRR 1, article 3 was invoked. As seen, US prison conditions formed the basis of one of the arguments put forward in the Canadian case of United States v Viscomi, supra note 36. Also related to the interests of justice are possible bias and extreme forms of plea bargaining. These were considered in R (on the application of Bermingham) v Director

of the Serious Fraud Office [2006] EWHC 200 (Admin). Note that this is not a cybercrime case.

49. The sixth was suffering from a severe mental illness such that further US assurances as to his treatment were required.
50. See Mavronicola and Messineo (2013). The disquiet engendered by the *Bermingham* case, supra note 48, was such that it was a factor behind the enactment of the forum bar.
51. Certain evidence in the form of computer hardware and witness accounts will necessarily be within the subjective territorial state. Clearly, however, international cooperation is required to establish the nature of the effects of transnational cybercrime. Countering this point is that the cost of trial and incarceration is met by the transnational jurisdiction where it has been exercised. The cost argument, then, turns on one's perspective.
52. United States Government Accountability Office, US Secret Service – Investigative Operations Confer Benefits, Jan. 2020, at page 1, cited at https://www.gao.gov/assets/710/703990.pdf, Accessed 25 May 2022.
53. United States Government Accountability Office, US Secret Service - Investigative Operations Confer Benefits, Jan. 2020, at page 21, cited at https://www.gao.gov/assets/710/703990.pdf, Accessed 25 May 2022.
54. See https://www.justice.gov/opa/pr/foreign-nationals-sentenced-roles-transnational-cybercrime-enterprise, Accessed 25 May 2022.
55. Kennedy, supra note 6.
56. The preamble to the Budapest Convention *inter alia* provides that the parties are convinced ' … of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation'.
57. There are, of course, long-standing debates on the purposes of criminalisation. Germane works include Beccaria (1963); Oldenquist (1988); Simester and von Hirsch (2011) and Chehtman (2020). Simester and von Hirsch describe criminalisation as a 'complex, public, and coercive act, one that articulates both deterrence and desert *ex ante*' (6).
58. Rehabilitation is a relative newcomer. In Dickson v United Kingdom, (2008) 46 EHRR 41 the Grand Chamber of the ECtHR stated ' … in recent years there has been a trend towards placing more emphasis on rehabilitation … ', at para 28. The protection of the public is a further purpose.
59. Cybercrime deterrence as between states *per se* is discussed in Geers (2010).
60. Bailey and Smith (1973), referring to Bentham and others.
61. Discussing the punishment (and deterrent) purpose is Hornle who notes 'The criminal law is a … "morally-loaded regulatory tool". Modern penal laws convey two messages: don't do this because it is a) wrong, and b) the price you have to pay is too high', in Hornle (2016, 302), referring to Simester and von Hirsch.
62. See Brenner and Schwerha (2007).
63. Capacity building and sanctions for cybercrime havens are discussed below.
64. Providing some insight is the fact that only 53 of a total of 15,939 European Arrest Warrants received by the UK over the financial year 2020–2021 sought persons for offences of cybercrime, including facilitation, malware and network intrusion. The UK sought no one for a cybercrime under an EAW over that period, see https://nationalcrimeagency.gov.uk/what-we-do/how-we-work/providing-specialist-capabilities-for-law-enforcement/fugitives-and-international-crime/european-arrest-warrants, Accessed 25 May 2022. There are, of course, a number of factors behind this statistic.
65. See generally as to retribution Bradley (2003-2004).
66. Arising here is the complexity and cost point. In this light retribution in this light is available only to those individuals and societies whose governments can afford it.
67. See Dickson v UK, supra note 58 and more generally Martufi (2019).
68. These issues arise in challenges to US transnational jurisdiction on the basis of article 3 of the ECHR, protecting persons from torture or inhuman or degrading treatment or punishment. See, for example, Ahmad v UK (2013) 56 EHHR 1.

69. See Coldham (2000). He notes the need for capacity building in Africa as regards transnational crime (238).
70. See Cochran et al. (2020).
71. An example being the Agreement between UK and India on the Transfer of Sentenced Persons 2005, cited at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/273283/6793.pdf, Accessed 25 May 2022.
72. See Walker (2019). As noted, an ad hoc UN committee was created in May 2021 in this vein, supra note 12.
73. See Walker (2019). As noted, an ad hoc UN committee was created in May 2021 in this vein, supra note 12.
74. The Committee of Ministers of the Council of Europe may invite states to accede, and agreement of existing members of the organisation and treaty must agree, see https://rm.coe.int/16808ff396, Accessed 25 May 2022. Increasing membership, therefore, is not a matter of non-parties merely acceding. As of March 2022, 14 states have been invited or signed the Convention.
75. See https://www.un.org/en/about-us/growth-in-un-membership, Accessed 25 May 2022.
76. Article 6(2) of the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation 1988, for example, *inter alia* provides state parties may establish jurisdiction over specified offences where a national is injured or killed in its commission or it is committed in an attempt to compel that state to do or abstain from any act.
77. This is mentioned below, along with the Second Protocol to the Convention.
78. Other regional approaches can also be useful. Within the EU Europol has been particularly engaged in cybercrime cooperation. Outside Europe the Commonwealth of Independent States, the African Union and the League of Arab States have also concluded agreements in the area.
79. See https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-, Accessed 25 May 2022. A list of the six capacity building projects undertaken by the office is found here https://rm.coe.int/cproc-about-eng-v9/16809f3996, Accessed 25 May 2022.
80. It is expected to be opened for signature in May 2022, see https://www.coe.int/en/web/cybercrime/t-cy-drafting-group, Accessed 25 May 2022.
81. The importance of evidence sharing cannot be over-emphasised. Insufficient evidence is one of the greatest challenges facing subjective jurisdiction (Maillart 2019, 379–384).
82. See https://www.coe.int/en/web/conventions/new-treaties, Accessed 25 May 2022.
83. Discussing the investigative difficulties as regards crimes committed via the dark web is Davies (2020).
84. The Full Code Test entails evidential and public interest stages. Simply, a prosecution will only proceed if the evidence is such that it is felt that there is a reasonable prospect of conviction and that there are public interest factors in favour of prosecution outweighing those against, see https://www.cps.gov.uk/publication/code-crown-prosecutors, Accessed 25 May 2022.
85. The Full Code Test entails evidential and public interest stages. Simply, a prosecution will only proceed if the evidence is such that it is felt that there is a reasonable prospect of conviction and that there are public interest factors in favour of prosecution outweighing those against, see https://www.cps.gov.uk/publication/code-crown-prosecutors, Accessed 25 May 2022.
86. See Mann, Warren, and Kennedy (2018), who make the case for forum shifting as an alternative to extradition.
87. Love v US, supra note 46. See Arnell and Davies (2020).
88. Love v US, supra note 46. See Arnell and Davies (2020). at para 126.
89. A notable case where Canada deferred to the US is that of Marco Viscomi, supra note 36.
90. In 2020 the US took custody of the alleged Nigerian cybercriminals, 'mrwoodbery' and 'hushpuppi' in the UAE. Whilst their cases have given rise to accusations of irregular rendition, it appears the authorities acquiesced in US action. See https://www.bbc.co.uk/news/world-africa-53309873, Accessed 25 May 2022. 'Hushpuppi' subsequently pleaded guilty to money laundering in the US, see https://www.justice.gov/usao-cdca/pr/six-indicted-

international-scheme-defraud-qatari-school-founder-and-then-launder-over-1, Accessed 25 May 2022.

91. Unilaterally, there is UK's DPP's Director's Guidance on the handling of cases where the jurisdiction to prosecute is shared with prosecuting authorities overseas 2013 https://www.cps.gov.uk/publication/directors-guidance-handling-cases-where-jurisdiction-prosecute-shared-prosecuting, Accessed 25 May 2022. Bilaterally, there is UK-US Guidance for handling criminal cases with concurrent jurisdiction between the UK and the US 2007, http://www.publications.parliament.uk/pa/ld200607/ldlwa/70125ws1.pdf, Accessed 25 May 2022. Multilaterally there are the Eurojust Guidelines for Deciding 'Which Jurisdiction Should Prosecute? 2003, updated in 2016, https://www.eurojust.europa.eu/sites/default/files/Publications/Reports/2016_Jurisdiction-Guidelines_EN.pdf, Accessed 25 May 2022.
92. See generally, Bassiouni and Wise (1995). There is an academic debate about the extent of the obligation in customary international law, see van Steenberghe (2011).
93. Arguing in favour of an enhanced role is the World Economic Forum (2020). A further germane question is whether the owners of networks and platforms should be criminally or civilly liable themselves, see for example Radbod (2010).
94. There are undoubted privacy and human rights-related concerns, as is recognised in the final two paragraphs of the preamble to the Second Additional Protocol, mentioned presently.
95. Cybercrime Convention Committee (2021).
96. Evidential difficulties have led to unilateral action, viz., the enactment of the US Clarifying Lawful Overseas Use of Data Act (CLOUD Act) in 2018. The EU has been considering an e-Evidence regulation for some time, see https://www.euractiv.com/section/data-protection/news/e-evidence-regulation-controversy-continues-in-trilogue-discussions/, Accessed 25 May 2022, and Maillart (2019, 386) et seq..
97. Cybercrime Convention Committee (2021, 25).
98. As to the tripolar approach, see Walker (2019; 3).
99. See Bartlett and Ophel (2021).
100. Bartlett and Ophel (2021) note that the US introduced its sanctions policy into its cybersecurity strategy in 2012.
101. Bartlett and Ophel (2021) note that the US introduced its sanctions policy into its cybersecurity strategy in 2012.
102. See https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/, Accessed 25 May 2022.
103. See https://thehill.com/policy/cybersecurity/566610-senators-introduce-legislation-to-sanction-nations-involved-in, Accessed 25 May 2022.
104. Council Regulation (EU) 2019/796 of 17 May 2019. The UK had given effect to them through the Cyber-Attacks (Asset-Freezing) Regulations 2019, SI 2019/956.
105. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=EN, Accessed 25 May 2022.
106. See https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/, Accessed 25 May 2022.
107. Cited at https://www.legislation.gov.uk/uksi/2020/597/regulation/4/made, Accessed 25 May 2022.
108. See Arnell (2000b). The UN Office on Drugs and Crime (2013, 196), makes a similar point in the context of minimising jurisdictional conflict, noting '… the avoidance of jurisdictional conflicts must depend upon the maintenance of a sufficiently high threshold for the "genuine link" – together with clear inter-state communication channels for coordination of extraterritorial criminal justice actions'.
109. Earlier attempts have led to a binding treaty, they being the Harvard Draft Convention on Jurisdiction with Respect to Crime (1935) 29 AJIL (Supp) 439 and the Council of Europe's Draft European Convention on Conflicts of Jurisdiction in Criminal Matters in 1965, http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=14457&lang=en, Accessed 25 May 2022.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Paul Arnell http://orcid.org/0000-0001-7874-2272

References

Arnell, P. 2000a. "Criminal Jurisdiction in International Law." *Juridical Review* 3: 179–189.
Arnell, P. 2000b. "The Proper Law of the Crime in International Law Revisited." *Nottingham Law Journal* 9 (1): 39–52.
Arnell, P. 2004. "Male Captus Bene Detentus in Scotland." *Juridical Review* 3: 252–263.
Arnell, P. 2012. *Law Across Borders: The Extraterritorial Application of United Kingdom Law*. London: Routledge.
Arnell, P. 2013. "The European Human Rights Influence upon UK Extradition — Myth Debunked." *European Journal of Crime, Criminal Law and Criminal Justice* 21: 317–337.
Arnell, P. 2018. "The Case of Lauri Love." *Criminal Law and Justice Weekly* 182: 136–137.
Arnell, P. 2019. "Extradition and Mental Health in UK Law." *Criminal Law Forum* 30: 339–372.
Arnell, P., and G. Davies. 2020. "The Forum Bar in UK Extradition Law: An Unnecessary Failure." *The Journal of Criminal Law* 84 (2): 142–162.
Arnell, P., and A. Reid. 2009. "Hackers Beware – the Cautionary Story of Gary McKinnon." *Information and Communications Law* 18: 1–12.
Bailey, W. C., and R. W. Smith. 1973. "Punishment: Its Severity and Certainty." *Journal of Criminal Law and Criminology* 63: 530–539.
Baker, S., D. Perry, and A. Doobay. 2011. "A Review of the United Kingdom's Extradition Arrangements." Accessed 25 May 2022. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/117673/extradition-review.pdf.
Bartlett, J., and M. Ophel. 2021. "Sanctions by the Numbers: Spotlight on Cyber Sanctions." Accessed 25 May 2022. https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber.
Bassiouni, M. C., and E. M. Wise. 1995. *Aut Dedere Aut Judicare: The Duty to Extradite or Prosecute in International Law*. Brill Publishing: Leiden.
Beccaria, C. 1963. *On Crimes and Punishments*. Indianapolis: Bobbs-Merrill.
Bell, R. E. 2002. "The Prosecution of Computer Crime." *Journal of Financial Crime* 9: 308–325.
Botteman, Y., and A. Patsa. 2012. "The Jurisdictional Reach of EU Anti-Cartel Rules: Unmuddling the Limits." *European Competition Journal* 8 (2): 365–382.
Bradley, G. V. 2003-2004. Retribution: The Central Aim of Punishment. *Harvard Journal of Law and Public Policy* 27: 19–31.
Brenner, S. W., and J. J. Schwerha. 2007. "Cybercrime Havens Challenges and Solutions." *Business Law Today* 17: 49–51.
Buxbaum, H. 2016. "Foreign Governments as Plaintiffs in US Courts and the Case Against 'Judicial Imperialism'." *Washington & Lee Law Review* 73: 653–717.
Chehtman, A. 2020. *The Philosophical Foundations of Extraterritorial Punishment*. Oxford: Oxford University Press.
Clough, J. 2011. "Data Theft: Cybercrime and the Increasing Criminalisation of Access to Data." *Criminal Law Forum* 22: 145–170.
Cochran, J. C., J. C. Barnes, D. P. Mears, and W. D. Bale. 2020. "Revisiting the Effect of Visitation on Recidivism." *Justice Quarterly* 37 (2): 304–331.
Coldham, S. 2000. "Criminal Justice Policies in Commonwealth Africa: Trends and Prospects." *Journal of African Law* 44: 218–238.
Council of Europe. 2001. "Council of Europe's Convention on Cybercrime." Accessed 25 May 2022. https://www.coe.int/en/web/conventions/full-list?module = treaty-detail&treatynum = 185.

Council of Europe Cybercrime Programme Office. 2021. "The Global State of Cybercrime Legislation 2013-2021: A Cursory Overview." Accessed 25 May 2022. https://rm.coe.int/3148-1-3-4-cyberleg-global-state-jun2021-v5-public/1680a302be.

Cybercrime Convention Committee (T-CY). 2021. "Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, Draft Protocol Version 3." Accessed 25 May 2022. https://rm.coe.int/0900001680a2aa1c. The Protocol is followed by an Explanatory Report.

Davies, G. 2020. "Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers." *The Journal of Criminal Law* 84 (5): 407–426.

Europol. 2021. "Internet Organised Crime Threat Assessment." Accessed 25 May 2022. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021.

Geers, K. 2010. "The Challenge of Cyber Attack Deterrence." *Computer and Security Law Review* 26: 298–303.

Ghazi-Tehrani, A. K., and H. N. Pontell. 2021. "Phishing Evolves: Analysing the Enduring Cybercrime." *Victims and Offenders* 16 (3): 316–342.

Goldsmith, J. 2000. "Unilateral Regulation of the Internet: A Modest Defence." *European Journal of International Law* 11 (1): 135–148.

Home Office. 2012. "The Government Response to Sir Scott Baker's Review of the United Kingdom's Extradition Arrangements." Accessed 25 May 2022. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228566/8458.pdf.

Home Office. 2014-2015. "The Government Response to the Second Report from the Select Committee on Extradition Law." Accessed 25 May 2022. https://www.gov.uk/government/publications/extradition-uk-law-and-practice-the-governments-response-to-the-second-report-from-the-select-committee-on-extradition-law.

Hornle, T. 2016. "Theories of Criminalization." *Criminal Law and Philosophy* 10: 301–314.

House of Lords. 2014-2015. "Extradition Law: UK Law and Practice." Accessed 25 May 2022. https://publications.parliament.uk/pa/ld201415/ldselect/ldextradition/126/12602.htm.

Jennings, R. Y. 1967. "General Course on Principles of International Law." Accessed 25 May 2022. https://referenceworks.brillonline.com/browse/the-hague-academy-collected-courses.

Johnson, D. R., and D. Post. 1996. "Law and Borders: The Rise of Law in Cyberspace." *Stanford Law Review* 48 (5): 1367–1402.

Kennedy, S. 2020. "The Legal Geographies of Extradition and Sovereign Power. Internet Policy Review." Accessed 25 May 2022. https://policyreview.info/articles/analysis/legal-geographies-extradition-and-sovereign-power.

Maillart, J.-B. 2019. "The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime." *ERA Forum* 19: 375–390.

Maillart, J.-B. 2021. "The Need to Think Beyond Objective Territoriality to Better Protect the Rights of the Suspect of a Cybercrime." In *Rethinking Cybercrime*, edited by T. Owen, and J. Marshall, 105–120. London: Springer.

Mann, M., I. Warren, and S. Kennedy. 2018. "The Legal Geographies of Transnational Cyber-Prosecutions: Extradition, Human Rights and Forum Shifting." *Global Crime* 19 (2): 107–124.

Martufi, A. 2019. "The Paths of Offender Rehabilitation and the European Dimension of Punishment: New Challenges for an Old Ideal?" *Maastricht Journal of European and Comparative Law* 25 (6): 672–688.

Mavronicola, N., and F. Messineo. 2013. "Relatively Absolute? The Undermining of Article 3 In Ahmad v UK." *The Modern Law Review* 76 (3): 589–603.

Office of Legal Education of United States Attorneys. 2015. "Prosecuting Computer Crimes Manual." Accessed 25 May 2022. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf .

Oldenquist, A. 1988. "An Explanation of Retribution." *The Journal of Philosophy* 85 (9): 464–478.

Peters, A., and A. Jordan. 2020. "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime." *National Security Law and Policy* 10: 487–524.

Radbod, S. T. 2010. "Craiglist – A Case for Criminal Liability for Online Service Providers?" *Berkeley Technology Law Journal* 25: 597–615.
Ryngaert, C. 2015. *Jurisdiction in International Law. Second Edition*. Oxford: Oxford University Press.
Simester, A. P., and A. von Hirsch. 2011. *Crimes, Harms and Wrongs – On the Principles of Criminalisation*. Oxford: Hart Publishing.
UN Office on Drugs and Crime. 2013. "Comprehensive Study on Cybercrime." Accessed 25 May 2022. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.
van Steenberghe, R. 2011. "The Obligation to Extradite or Prosecute: Clarifying its Nature." *Journal of International Criminal Justice* 9 (5): 1089–1116.
Velasco, C. 2015. "Cybercrime Jurisdiction: Past, Present and Future." *ERA Forum* 16: 331–347.
Walker, S. 2019. "Cyber-Insecurities: A Guide to the UN Cybercrime Debate." Accessed 25 May 2022. https://globalinitiative.net/wp-content/uploads/2019/03/TGIATOC-Report-Cybercrime-in-the-UN-01Mar1510-Web.pdf.
Weissbrodt, D., and A. Bergquist. 2006. "Extraordinary Rendition: A Human Rights Analysis." *Harvard Human Rights Journal* 19: 123–160.
Whitman, J. Q. 2009. "Western Legal Imperialism: Thinking About the Deep Historical Roots." *Theoretical Inquiries in Law* 10: 305–332.
Wong, C. 2000. "Criminal Jurisdiction Over Internet Crimes." In *Recht und Internet*, edited by G. Hohloch, 93–107. Baden-Baden: Nomos.
World Economic Forum. 2020. "Partnership against Cybercrime." Accessed 25 May 2022. http://www3.weforum.org/docs/WEF_Partnership_against_Cybercrime_report_2020.pdf.
Young, D. B. 1983. "Cesare Beccaria: Utilitarian or Retributivist?." *Journal of Criminal Justice* 11: 317–326.
Zekos, G. I. 2011. "Globalisation and States' Cyber-Territory." *Web Journal of Current Legal Issues* 5. Accessed 25 May 2022. https://warwick.ac.uk/fac/soc/law/elj/jilt/1999_3/zekos/.