Journal of Sociology and Ethnology (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/jsoce.2024.060504
ISSN 2616-2318 Vol. 6 Num. 5

Anonymity and Multi-jurisdictionality Hinder Government Control of Cyberspace

Yi Zhou*

Australian National University, Canberra, Australia
**Corresponding author: u7811413@anu.edu.au*

Keywords: Cyberspace; anonymity; multi-jurisdictionality

Abstract: The inherent characteristics of anonymity and multi-jurisdictionality in cyberspace present significant challenges for effective government regulation and control. This essay explores how these characteristics undermine governmental efforts by examining two specific cases: cyberextortion and digital currency. In the case of cyberextortion, multi-jurisdictionality and the lack of inter-jurisdictional cooperation create substantial obstacles to law enforcement, particularly when the subject of a cyberextortion is another government of a country. For digital currencies, as represented by Bitcoin, the decentralized and anonymous nature of transactions poses significant barriers to regulation and taxation. Although governments have employed various prohibitions and regulations to try to control cyberspace, these efforts have often proven ineffective or counterproductive due to the limited reach of single-national jurisdictions and the distinctive nature of the cyberspace. Enhanced international cooperation may offer a potential path for governments seeking to regulate cyberspace, though it is unlikely to fully overcome the challenges presented by anonymity and multi-jurisdictionality.

1. Introduction

In *The Law of the Horse*, Lawrence Lessig refers to a common argument that the anonymity and multi-jurisdictionality of cyberspace make control by government in cyberspace impossible [1]. This essay analyses whether these two features indeed make it impossible for governments to control cyberspace. The essay analyses the impact of anonymity and multi-jurisdictionality on government control of cyberspace by examining two examples in particular, the measures taken by the Australian and other governments in response to the cyberextortion and tax evasion in digital currencies.

2. Example: Cyberextortion

The complexity of cyberextortion issues is manifested in the fact that its criminal activities and perpetrators cover multiple jurisdictions, which makes it difficult for governments to control cyberextortion crimes. Using cyberextortion as an example, this section analyses whether Australian and other countries' governments can control cyberspace by discussing cyberextortion specifically, analyzing the reasons why it is difficult for governments to control cyberextortion, and comparing the efforts and difficulties of governments in Australia and other jurisdictions in controlling

cyberextortion crimes.

2.1 Definition of cyberextortion

The “cyberextortion” discussed in this section contains both “ransomware” and “data theft extortion”. “Ransomware” refers to the use of malicious ransomwares by cyberextortion groups to demand a ransom by locking the system or encrypting the data of the entity being extorted (the victim). The data can only be unlocked or decrypted if the victim pays the ransom [2]. “Data theft extortion” refers to cyberextortion groups that steal a victim's sensitive data and demand a ransom under the threat of disclosing that sensitive data [3]. The discussion in this section does not address other malicious cyber activities.

Cyberextortion has now become one of the serious problems plaguing the Australian government, which is trying to take action to control it. The emergence of Ransomware-as-a-Service can well attest to this [4]. Cybercrime groups develop ransomwares, sell them to other criminals [5], and provide services such as tutorials, negotiation services, and providing URLs for attacks. Criminals buying the ransomwares use them to extort money from companies. This model leverages cyberspace to separate ransomware development from criminal behavior, making it more difficult for governments to control cyberextortion. In a recent paper, the Australian Government described malicious cyber activity as "one of the most significant threats impacting Australians" [6].

2.2 Why governments have trouble controlling cyberextortion?

Because of jurisdictional issues in cyberspace, it is difficult for governments to effectively control cyberextortion. The "jurisdictional issues" here includes two situations. One is the conflict of jurisdiction, where multiple governments have jurisdiction over the same object, and the Australian government's control of cyberextortion or its perpetrators may be impeded by the authorities of other jurisdictions. The other is non-jurisdiction, where the Australian government does not have jurisdiction over some of the objects of cyberextortion, particularly which is dominated by another government.

In the first situation, it is difficult for governments to control cyberextortion through traditional law enforcement methods. On the one hand, in most cases, cyber gangs demand ransom payments usually in the form of cryptocurrencies such as Bitcoin, which have a degree of anonymity and are difficult to trace. On the other hand, these criminal groups usually choose to operate outside of Australian law enforcement [7]. For example, in the Medibank hack case, local authorities refused to cooperate with the Australian Federal Police (AFP) and to a certain extent “stonewalled” the AFP's operations. Indeed, cybercriminal groups have developed a default set of unspoken rules whereby they believe that local authorities will not interfere with their activities as long as their criminal activities are not directed at the country they are based [8]. In such cases, the jurisdiction harbors cyberextortions.

In addition to the conflict of multi-jurisdiction that prevent governments from controlling cybercrime, another reason is that the jurisdiction of one country cannot govern the authorities of another country, as some cybercrimes are committed primarily by the governments of other countries. One of the purposes of states committing cybercrime is that cybercrime can be used as a means of warfare. The ACSC noted that cyberspace “has become a battleground”, and countries continue to “strain the norms and institutions that govern cyberspace as a global common” [9]. For example, after Russian full-scale invasion of Ukraine in 2022, the developers of the ransomware “Conti” publicly declared their full support for Vladimir Putin's government. The organization has since been revealed to be linked to the Russian Federal Security Service. In this case, other governments were unable to take control of “Conti” because their jurisdictions could not govern the government of the Russian

Federation. Therefore, it can be concluded that, in this example, the government lost control of cyberspace.

Another purpose for states committing cybercrime is that some states may use cybercrime as a distraction to achieve specific diplomatic goals. For example, the Five Eyes believes that the cyberattack of "Volt Typhoon" against Guam was supported by the People's Republic of China [10]. The "NotPetya" cyberattack against Ukraine is believed to have been orchestrated by Russia. In addition, the governments of North Korea and Iran are thought to be involved in serious cyberattack campaigns [11]. Traditionally, these attacks could be regulated by the laws of war or diplomacy, but when they occur in cyberspace, it is extremely difficult to assign blame to some countries because of the anonymity of cyberspace. Even if the result of an investigation prove that another government was involved in or even dominated the cyberattack, it is difficult for the victimized country to arrest the criminal group because the victimized country does not have jurisdiction over another state's government if that state is the primary perpetrator or when the primary perpetrator seeks protection from that state. It could equally be concluded that in this example, the government lost control of cyberspace.

2.3 Measures by the Australian government

Although these examples show that government has lost control of cyberspace because of jurisdictional issues, it may be countered that the Australian government is attempting to control cyberextortion by other means. For example, although the Australian government does not have the power to prosecute and arrest other countries' governments because of jurisdictional issues, it can adopt specific measures for victims. This is because the victims of extortion are also the financiers of cyberextortion groups. On the one hand, the Australian government can legislate to improve the protection of victims, and on the other hand, the government can restrict the payment of ransom to criminal groups by ransomed companies, thus indirectly controlling the source of funding of criminal groups.

In terms of improving protection for victims, Australia already has a well-established system in place. The Australian Securities and Investments Commission noted in the RI Advice Group case that companies are expected to "adopt an enhanced cybersecurity position to improve cyber resilience in light of the heightened cyber-threat environment". Failure to ensure that a company has adequate cybersecurity measures in place may constitute a breach of a company director's duty of care and diligence [12]. For example, the Australian government has sought to amend the *Privacy Act 1988* (Cth) to force companies to invest more in cybersecurity by significantly increasing the fines imposed for privacy violations [13]. Specifically, companies will face increased fines if they fail to take reasonable measures to protect personal information, resulting in damage from the misuse, interference, unauthorized access or modification of personal information. The Office of the Australian Information Commissioner has already begun enforcing this element and has launched investigations into Medibank and Latitude.

On the other hand, due to the growing demand for mandatory cybersecurity standards for companies [14], governments may consider restricting or prohibiting ransom payments by ransomed companies. For example, Florida passed legislation prohibiting state agencies from complying with ransom demands. North Carolina explicitly prohibits communication with cyber extortionists and the ransom payments. The New York Senate is considering a bill that would prohibit businesses or healthcare entities from paying cyber ransoms [15]. The benefits of such a ransom ban are clear, as paying ransoms is in fact providing more money to cybercriminal groups, helping them to scale up cybercrime and launch more cyberattacks, and the implementation of ransom bans can indirectly combat cyberextortion by cutting off the revenue streams of cybercriminal groups. Thus, the

counterargument seems to be proven, that is, even if there are jurisdictional issues that prevent a government from controlling cybercrime groups, the government can still achieve control of cyberspace within the limits of its own jurisdiction.

2.4 Do these measures truly represent government control of cyberspace?

These two government's measures mentioned above show that, while governments cannot control cybercrime groups because of jurisdictional issues, they can indirectly combat cyberextortion groups by controlling the victims, which may seem like evidence that governments can control cyberspace. However, while it is true that the Australian government can improve victim protection, there does not seem to be a necessary causal link between improved victim protection and the fact that the government can control cyberspace. Imagine a scenario in which a cybercrime group is unable to successfully attack any company's cyber data because of the government's heightened protection. In this scenario, although the victims disappear, the cyberextortion act is still taking place, and this attempted crime behavior is likewise subject to the control of the Australian legislation. Because of the jurisdictional reasons mentioned earlier, the government remains unable to arrest or prosecute members of cybercrime groups. This means that while the government can take measures to improve the protection of victims, it does not mean that it can control cyberspace.

In contrast, another measure does not seem to have this problem, as it could help governments combat cyberextortion groups. However, while a ransom ban does indirectly combat cyberextortions, the fact that it can prove that governments can control cyberspace is not convincing. Firstly, it would be difficult for the government to require companies refusing to pay ransom. In fact, companies usually tend to pay ransom directly when they suffer from cyberextortion. According to research by McGrathNicol Advisory, four in five ransomware-attacked companies paid the ransom directly [16]. One reason is cost considerations. Cartwright et al wrote a literature on "ransomware pay decision" to predict the behavior of "rational victims" [17]. Their study shows that companies are more likely to pay the ransom directly when they are under extortion because it is less costly to do so than relying on their own power to decrypt data or recover system. In addition, Fanga's research also shows that victims are more inclined to pay ransom considering the financial benefits [18]. Another reason is corporate reputation. If a company is exposed as having cyber data security vulnerabilities, their customers tend not to continue choosing that company. As can be seen from these examples, paying ransom is often a company's first option.

Secondly, back to the anonymity of cyberspace. Companies can pay ransoms through anonymous cryptocurrencies while hiding that they are being cyber-ransomed, and in doing so de facto circumvent the ransom ban. And because of the anonymity of cyberspace, it is difficult for the government to find companies that choose to pay ransoms in violation of the ban. In this example, the ransom ban instead helps the cyberextortion groups. Because it is illegal under the ransom ban for companies to hide the fact that they have been subjected to cyberextortion, the cyberextortion group is likely to threaten to extort the company again by disclosing the fact of the extortion. This would lead to further expansion of cyberattacks by cyberextortion groups.

Thirdly, ransom bans are impossible for some entities. Imagine a scenario where a hospital is subject to cyberattacks and is required to pay ransoms. Under the ransom ban, the hospital is not allowed to do so. If the hospital is unable to restore its systems through its own efforts in a short period of time, the ensuing paralysis of the hospital systems would result in risking the lives or even deaths of many patients, which is clearly unreasonable. Similarly, the ransom ban does not apply to other entities providing essential services, as this could lead to social paralysis.

These examples show that while ransom bans may appear to combat cyberextortion groups and demonstrate government control over cyberspace. However, companies are often reluctant to comply

with ransom bans, and they can leverage the anonymity of cyberspace to pay ransoms without being detected by governments. On the other hand, ransom bans cannot be applied to all entities. As a result, it is likely that ransom bans will not work to combat cyberextortions and may even help them to some extent.

In summary, although governments have taken measures within their jurisdictions to manage cyberextortions, these measures have proved to be ineffective or even difficult to implement. Without international cooperation, it is difficult for a single government to control cyberextortions because of jurisdictional issues and the anonymity of cyberspace. This example may provide some evidence of the inability of governments to control cyberspace.

3. Example: Digital Currency

Digital currency transactions in cyberspace combine both anonymity and multi-jurisdictionality, and it is recognized that through digital currencies it is possible to evade national currency controls and enable tax evasion or money laundering [19], making it difficult for governments to regulate them. Because Bitcoin is the most widely known and used, this section uses Bitcoin as an example to analyze whether governments can control cyberspace by specifically discussing the difficulties of controlling Bitcoin transactions and examining government efforts to control them.

3.1 Introduction of Bitcoin

Bitcoin is a digital cryptocurrency which is unique in its application of peer-to-peer technology [20]. Specifically, Bitcoin's account records are stored and managed by individual users rather than central computers, which provides Bitcoin with anonymity. This feature of Bitcoin is known as decentralization, and while it increases the security and efficiency of global financial transactions, it also raises challenges for regulators, with the most serious regulatory issue being taxation. For example, Marian refers to Bitcoin as a potential “super tax haven”.

3.2 The Dilemma of Taxation and Regulation of Bitcoin

There are two main aspects of the difficulty for tax authorities to regulate Bitcoin due to its anonymity. First, Bitcoin is decentralized, which means that there is no intermediary, like a bank, to monitor and report transactions to tax authorities. In this case, it is easy for individuals to hide their personal transactions and income from tax authorities, leading to tax evasion. And it is technically impossible for tax authorities to regulate every Internet user. As Milton Friedman noted, “cyberspace make it much more difficult for government to collect taxes” [21].

Secondly, although Bitcoin transactions are associated with Bitcoin addresses, users can still transact anonymously because they can create Bitcoin addresses without providing personal information. This makes it difficult for tax authorities to specifically trace the entities associated with the transaction, even if they have information about it. It may be argued against that the blockchain records all transactions even though there is no intermediary to monitor transaction information. This argument is untenable because individuals behind the wallets are often false identities. As a result, it is difficult for tax authorities to control Bitcoin transactions.

On the other hand, it is difficult for tax authorities to control Bitcoin, as Bitcoin is also characterized by a lack of jurisdictional link. While traditional tax systems rely on the existence of entities to define locations of transactions, Bitcoin cannot be used for tax purposes because they lack a clear link to a specific jurisdiction [22]. Specifically, a government's jurisdiction is within its national sovereignty [23]. As a result, government's ability to control taxpayers is diminished once the funds leave its jurisdiction. The Internet, on the other hand, dilutes the concept of national

boundaries [24]. The transnational nature of the Internet, as well as Bitcoin's statelessness and valued intangibles, leads to jurisdictional confusion [25], which will result in certain transactions evading tax jurisdiction altogether. In summary, the anonymity and jurisdictional confusion of Bitcoin makes it almost impossible for tax authorities to control digital currencies.

3.3 Are measures taken by Governments effective?

Even though these examples show that tax authorities have virtually lost control over Bitcoin transactions, it may be counterargued that governments are in fact taking measures to control Bitcoin. One of the extreme approaches is to ban digital currencies, including Bitcoin, altogether. For example, the termination of e-gold Ltd in the US with the prosecution of its instigators [26]. The reason of this potential counterargument may be that while tax authorities cannot control bitcoin transactions, governments can achieve control over cyberspace by banning them.

While governments have power to ban anonymous currencies, it is not convincing that such a measure reflects government control over cyberspace. While governments can easily shut down centralized administrative systems for digital currencies, it is difficult to effectively ban decentralized peer-to-peer networks altogether. For example, when the government shut down Napster, more difficult-to-regulate technologies emerged to replace it [27]. Thus, a total ban on bitcoin could lead to its trading going underground and the development of new technologies that are harder for governments to detect. As a result, rather than ameliorating the tax evasion, this approach may make it more difficult for tax authorities to gain tax revenue from bitcoin transactions, potentially “increasing the cost of enforcement” [28]. Therefore, the government's ban on digital currencies does not demonstrate the government's control over cyberspace.

Another measure governments have taken to control Bitcoin is to legislate a specialized Bitcoin regulator. For example, New York State has legislated specifically for Bitcoin, establishing a complex and stringent regulatory approach [29]. The primary target of this regulator is bitcoin intermediaries. It may be argued that such legislative regulation of Bitcoin intermediaries is effective in countering bitcoin's anonymity and achieving government control over Bitcoin.

However, while regulation of Bitcoin intermediaries can keep Bitcoin transactions under government control, such regulation is not necessarily appropriate for Bitcoin due to its nature. First, there is problems of over-regulation. Many of the strict regulatory requirements for financial transactions are aimed at the activities of large, resource-rich banks or companies, so the regulatory rules tend to be burdensome. The Bitcoin industry, on the other hand, is generally composed of small companies, and burdensome regulatory rules can limit the growth of them [30]. For example, the collapse of Mt. Gox, the largest Bitcoin exchange, was due to its failure to comply with complex regulatory requirements. And if regulatory standards are lowered, under-regulation can also have serious consequences. For example, fraudulent transactions resulting from under-regulation could prevent consumers from accessing Bitcoin market [31].

The counterargument might further note that the above discussion is about regulation of Bitcoin intermediaries, and that regulators are not limited to this, but could also regulate individual Bitcoin users. However, on the one hand, because of the anonymity of Bitcoin, it is impractical to directly regulate Bitcoin users. On the other hand, because of the jurisdictional confusion of digital currencies, Bitcoin users could abandon Bitcoin and switch to digital currencies in other jurisdictions. Overall, without considering multinational tax authority cooperation, it is currently almost impossible for a single government to effectively control Bitcoin transactions due to Bitcoin's anonymity and jurisdictional issues. This example may likewise provide some evidence of the inability of governments to control cyberspace.

4. Analysis

By comparing both examples, the core reason for the government's inability to control cyberextortion is jurisdictional issues, while for Bitcoin transactions is anonymity. It can be concluded that both issues greatly hinder government control over cyberspace. On the other hand, while governments have actively taken measures to attempt to deal with these issues, the result has been that governments have been virtually unable to effectively control cyberextortion and regulate Bitcoin transactions. Therefore, both examples provide evidence of the inability of governments to control cyberspace.

However, all the above discussions are limited to the control of cyberspace by a single government and do not involve international cooperation. In fact, international cooperation can be a good response to the conflict of jurisdictions. In the area of digital currency trading, to deal with tax evasion with offshore accounts through digital currencies, multiple governments are seeking cooperation. For example, through international treaties, transnational tax networks have been established to enhance cooperation in tax collection and information exchange [32]. This approach has been effective in limiting tax evasion by transferring funds out of a jurisdiction through intermediaries. It can therefore be concluded that international cooperation can help governments to effectively control digital currency transactions.

However, contrasting these two examples, while they both involve jurisdictional issues, the example of cyberextortion contains not only conflicts of jurisdictions, but also the non-jurisdiction. In this case, because cyberextortotion can be seen as being dominated by the government of a country, it is clearly unlikely that this government would be willing to engage in international cooperation. Therefore, government of the victimized country of cyberextortion is not able to address the problem through international cooperation. The contrasting results show that although international cooperation can solve part of the problem, it still cannot be assumed that governments can achieve control over cyberspace through international cooperation.

5. Conclusion

Due to the anonymity and multi-jurisdictionality of cyberspace, it is nearly impossible for governments to control cyberextortion and Bitcoin transactions. While governments have taken many measures to try to address them, it is still impossible for a single government to effectively control them, especially in the face of multi-jurisdictionality.

International cooperation can be used to effectively address multi-jurisdictionality in Bitcoin transactions but cannot be applied to the non-jurisdiction situation in cyberextortion. As a result, governments are currently unable to address the impediments that anonymity and multi-jurisdictionality pose to their control of cyberspace.

References

[1] Lawrence Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113(2) Harvard Law Review 501, 505.
[2] Cyber Security Industry Advisory Committee, Locked Out: Tackling Australia's Ransomware Threat (Report, March 2021) 2.
[3] Rachael Falk and Anne-Louise Brown, 'Exfiltrate, Encrypt, Extort: The Global Rise of Ransomware and Australia's Policy Options' (2022) 14(2) Australasian Institute of Policing Journal of Professional Practice and Research 29, 29.
[4] James McIntosh, 'The Case for a Prohibition on the Making of Cyber Ransom Payments' (2024) 40 Company and Securities Law Journal 158, 160.
[5] Allianz Global Corporate and Specialty, Cyber Insights Ransomware Trends: Risks and Resilience (Report, 2021) 4.
[6] Australian Government, Australia's Cyber Security Strategy 2020 (Report, 6 August 2020) 10.
[7] CyberCX, CyberCX Best Practice Guide Ransomware and Cyber Extortion (Report, 2021) 4.
[8] Kristina Keneally and Tim Watts, Beyond the Blame Game: Time for a National Ransomware Strategy (Policy

Statement, 2021) 5.
[9] Australian Cyber Security Centre, July 2021–June 2022 Annual Cyber Threat Report (Report, 2022) 30.
[10] United States National Security Agency, People's Republic of China State-sponsored Cyber Actor Living off the Land to Evade Detection (Joint Cybersecurity Advisory, 24 May 2023) 1.
[11] Dean Armstrong, Thomas Steward and Shyam Thakerar, Cyber Risks and Insurance: The Legal Principles (Bloomsbury Professional, 2021) 165.
[12] Corporations Act 2001 (Cth) s 180–181.
[13] Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Cth).
[14] Australian Government, Strengthening Australia's Cyber Security Regulations and Incentives (Discussion Paper, 13 July 2021) 21.
[15] The New York State Senate Bill S6806A (2021).
[16] McGrathNicol, Ransomware on the Rise (Report, 14 November 2022) 1.
[17] Anna Cartwright et al, 'How Cyber Insurance Influences the Ransomware Payment Decision: Theory and Evidence' (2023) 48 The Geneva Papers on Risk and Insurance – Issues and Practice 300, 303.
[18] Rui Fanga, Maochao Xub and Peng Zhao, 'Determination of Ransomware Payment Based on Bayesian Game Models' (2022) 116 (102685) Computers & Security 1, 12.
[19] Omri Marian, 'Are Cryptocurrencies Super Tax Havens?' (2013) 38 Michigan Law Review First Impressions 112, 113.
[20] Joel Emery and Miranda Stewart, 'The Taxing Challenge of Digital Currency' (2017) 28 Journal of Banking and Finance Law and Practice 236, 238.
[21] Robert Schlimgen, 'Virtual World, Real Taxes' (2010) 11(2) Minnesota Journal of Law, Science & Technology 877, 882.
[22] Senate Economics References Committee, Inquiry into Digital Currency (Report, 2014) 5.
[23] Burgess et al, Cooper, Krever, Vann's Income Taxation (Thomson Reuters, 2012) 309.
[24] Dempsey v Federal Commissioner of Taxation (2014) 98 ATR 698, [115].
[25] Uta Kohl, 'The Horror-Scope for the Taxation Office: The Internet and its Impact on Residence' (1998) 21(2) University of New South Wales Law Journal 436, 438.
[26] United States v e-gold Ltd, 521 F 3d 411 (DDC, 2008).
[27] Uta Kohl and Andrew Charlesworth, Information Technology Law (Routledge, 4th ed, 2012) 77-79.
[28] Danton Bryans and Franne Jelske Anema, 'Bitcoin and Money Laundering: Mining for an Effective Solution' (2014) 89 Indiana Law Journal 441, 472.
[29] Emily M. Little, 'Bitcoin' (2014) 21(5) Investment Lawyer 22, 23.
[30] Terence Wong, 'Bitcoin Deconstructed: Part 2 – Real and Virtual Worlds' (2014) 30(8) Australian Banking and Finance Law Bulletin 122, 126.
[31] Terence Wong, 'Bitcoin Deconstructed: Part 1 – Concepts and Signposts' (2014) 30(6) Australian Banking and Finance Law Bulletin 70, 72.
[32] Miranda Stewart, 'Transnational Tax Information Exchange Networks: Steps Towards a Globalized, Legitimate Tax Administration' (2012) 4(2) Word Tax Journal 152, 153.