Legal Response to Technology: Using DDoS as a Case Study

Introduction

Technology is undoubtedly introducing new crimes and Hong Kong is no exception to this phenomenon. Thus, Hong Kong's legal system must respond to technology-driven crimes. Certainly, the Legislative Council may enact laws to address or even preempt them. However, it cannot solely bear the burden — the legal system is composed of other institutions; enacting laws is time-consuming, yet neither offenders or technology developers would wait for the new law to take effect. Hence, courts are compelled to "fill in the gap".

Against this context, this article examines a line of Hong Kong cases relating to a distributed denial-of-service attack ("**DDoS attack**") to discern how the legal system responds to technological advancements. Fortunately or unfortunately, there are only three related cases, reflecting either low levels of DDoS attack or the inability of the legal system to punish these wrongdoers.

What is DDoS

Recently, the Court of Final Appeal ("**CFA**") observed that:

> "*The capacity of the server to deal with requests at any given time (its 'bandwidth') is finite. The method of a DDoS attack is for a number of co-ordinated computers to send a very large number of requests at more or less the same time to exhaust the server's bandwidth, thereby denying access to persons wishing to transact their ordinary business through the website and possibly causing the overloaded system to crash*"[1]

In other words, a DDoS attack involves a network of computers trying to bombard a server. Although exhausting a server's bandwidth is just one type of DDoS attack, the underlying objective of all DDoS attacks is similar — to deny innocent users from accessing a particular website. For the purposes of this article, this would be a sufficient understanding as none of the cases turn to the question of categorisation of DDoS attack.

Case Laws

In *HKSAR v Chu Ting-Ting* (unrep., HCMA 33/2016, Wong J), the Court of First Instance ("**CFI**") held that a DDoS attack constitutes as causing criminal damage under ss 59(1A) & 60 of the Crimes Ordinance (Cap. 200) ("**CO**"), but acquitted the appellant on the ground that "the connection between this computer and the attacks on the police website was not safely established"[2].

In *HKSAR v Tse Man Lai* [2013] 6 HKC 534, the Court of Appeal ("**CA**") refused to grant leave to appeal to the applicant who launched a DDoS attack, contravening CO s 161(1)(c). Construing s 161 purposively, Lunn JA opined that it "catch[es] a person who obtains access to a computer with a view to a dishonest gain, even in circumstances where the earlier access by the person to the computer had been entirely innocent"[3] insofar as the *actus reus* and *mens reus* collide. Thus, it was immaterial that

1 *Chu Tsun Wai v HKSAR* [2019] 1 HKC 589 (CFA) *per* Lord Hoffmann NPJ at §5

2 §64

3 §27

the applicant accessed his own computer, which was continuously switched on, rather than a third-party computer for innocent and criminal purposes.

In *Chu Tsun Wai v HKSAR* [2019] 1 HKC 589, the CFA dismissed the appeal, holding the appellant to be liable pursuant to CO ss 59(1A)(a) & 60 for launching an unsuccessful DDoS attack. Lord Hoffmann NPJ construed the phrase "to function other than as [the computer] has been established to function by or on behalf of its owner" in s 59(1A)(a) liberally, opining that "the statute is concerned with what the owner has set it up to do"[4] and not with the way in which a computer works. Hence, a DDoS attack is a misuse of the server as the owner of the server did not intend it to handle DDoS attacks, rejecting the appellant's technical argument that the server in handling the malicious requests was precisely performing the function it was supposed to do.

Discussion

All cases above involve the CO, manifesting the importance of legislation in dealing with computer crimes. Although the Legislative Council ought not to be solely responsible for crime control, it is apparent that legislation is indispensable for empowering the courts to handle computer crimes.

That being so, courts play a pivotal role in the absence of rapid legislative intervention. Section 59(1A) that extends the concept of criminal damage to cover the misuse of computer and section 161 that deals with access to computers with criminal or dishonest intent were added in 1993. Yet, the three cases above were decided from 2013–2019, at least 20 years after the enactment. This may indicate that the legislation has withstood the passage of time. However, such a proposition disregards the court's reasoning in each case. In particular, the courts' purposive interpretation of the CO is important in achieving a just result.

Chu Tsun Wai v HKSAR is an instructive example. Again, the appellant launched a DDoS attack against a bank's website albeit unsuccessfully. Intuitively, justice demands the appellant to be punished – he intended and acted upon his intention to disturb the operation of the bank's server which would in turn affect innocent bank users. Yet, this case went all the way to the CFA for determination. This is probably because of the tension between producing a just result and being technologically correct as eluded above. The appellant's technical argument if accepted would indeed have far-reaching implications. Considering the rise of automation and artificial intelligence, taking the appellant's proposition to its logical extreme would effectively protect all users of technology as machines/computers are increasingly able to execute operations on its own. To avoid such an anomaly in the law, the CFA resorted to its familiar tool of purposive interpretation, finding that the CO calls for an examination of the owner's intention of using the piece of technology. In so doing, the court circumvents the impact of technology by redirecting the scrutiny to the user's intention, an exercise that is familiar to the courts.

This is also apparent in *HKSAR v Tse Man Lai*. Justice once again demands the applicant to be punished for he had used his computer to launch a DDoS attack for dishonest gain, causing the website to be down for 24 hours. The difficulty the court had to deal with becomes apparent having considered the context. When s 161 was introduced in 1993, computers were not omnipresent. Hence, precedents

4 §13

on s 161 all dealt with situations involving the alleged unauthorisedly accessing a computer owned by wealthy organisations on one occasion. However, as technology improved and society progressed, it became common for a computer to be bought, left continuously on, used on different occasions, but only one of which was responsible for a DDoS attack. Faced with this new context, the CA had to use its tool of purposive interpretation to expand the reach of the CO as seen above.

In contrast with the two appellate decisions, *HKSAR v Chu Ting-Ting* being a first instance judgment provides guidance as to technology's impact when resolving issues of facts. Wong J thus observed that "the finder of fact must focus on the right issue"[5] when establishing recklessness because of the "myriad of ways of misusing a computer"[6]. Technology also puts a heavier burden on the prosecution. Although the appellant here admitted having experience of hacking and using the computer which launched 7,000 attacks on a website within a particular time frame, she was acquitted because the prosecution did not explain how the fact that she used that computer to access the website under attack 3 times within that time frame means the appellant *caused* the attack, especially when she accessed the website again after that time frame. However, a DDoS attack is a powerful tool for wrongdoers precisely because of the difficulty in distinguishing whether a particular request comes from an ordinary user or if it comes from the attacker. Since the principle of presumption of innocence underpins Hong Kong's criminal justice system, the burden of proof is unlikely to be relaxed. Therefore, the prosecution is likely to shoulder the burden of technology, whereas the defendant benefits from it.

Conclusion

In summary, a review of cases involving DDoS attack suggests that the legal system may address technological-crimes by having the legislature to enact laws, whilst addressing rapid technological changes by having courts construing and applying these laws to do justice. Hence, there is a symbiotic relationship between the judiciary and the legislature — the latter provides the former with the necessary toolkit; the former relieving the pressure on the latter to constantly enact new laws. That being so, it is plain that the legislature ought to be progressive and proactive for there is only so much that courts can do. For courts to delivery justice, there must be suitable laws and coherent evidence, both of which are anchored principles that would not bulge due to technological advancements; other actors must adapt.

5 §87

6 §86