Influence, infrastructure, and recentering cybercrime policing: Evaluating emerging approaches to online law enforcement through a market for cybercrime services

Ben Collier[a], Daniel R. Thomas[b], Richard Clayton[c], Alice Hutchings[c], Yi Ting Chua[c]

[a]Science, Technology, and Innovation Studies, University of Edinburgh
[b]Computer and Information Sciences, University of Stathclyde;
[c]Department of Computer Science and Technology, University of Cambridge

The Version of Record of this manuscript has been published and is available in the *Journal of Policing and Society* XX/02/2021
http://www.tandfonline.com/10.1080/10439463.2021.1883608

ABSTRACT

We document and evaluate two emerging policing strategies that are reshaping how centralised law enforcement agencies deal with online cybercrime markets. The first of these strategies we term infrastructural policing, a strategy drawn from law enforcement campaigns to disrupt international drug markets which involves targeting the small number of administrators who maintain the infrastructure supporting cybercrime markets. The second, we term influence policing, a strategy drawn from the UK's approach to counter-radicalisation, which involves the delivery of highly targeted messaging campaigns to potential customers. We illustrate these with a study of the online market for Denial of Service (DoS) attacks, conducting a quantitative longitudinal analysis of five years of time series attack data to establish the effect of these interventions on this illicit market. While arresting and sentencing key players had little lasting effect on DoS attacks (due to the jurisdictional issues which the Internet poses), after infrastructure administrators were targeted with takedowns there was a significant reduction in attacks and a dramatic reshaping of the market structure. Additionally, the use of search engine advertisements targeted at potential customers for these services in the UK was associated with a cessation in growth in attacks in this country. We interviewed law enforcement to explore the rationales behind the interventions, and also interviewed DoS attack providers and observed their online communication channels to explore these intervention effects in depth. From this, we argue that these emerging forms of online policing constitute (apparently successful) attempts by law enforcement to recenter themselves as key actors in online enforcement coalitions. This rests on them enrolling the capacities of the platform intermediaries who provide the very Internet infrastructure which so complicates traditional, jurisdictionally-bound forms of policing.

KEYWORDS

POLICING; CYBERCRIME; INTERVENTIONS; INTERNET; ILLICIT MARKETS; EVALUATION

1. Introduction: influence and infrastructure

This paper explores and evaluates the ways in which policing interventions are evolving in contemporary societies, in particular, how law enforcement is beginning to find effective methods for disrupting online cybercrime markets. Online criminal markets rely on the distributed international communications infrastructure of the Internet, which connects people and services around the world (Williams, 2006). The Internet's connective properties, in particular how it links together people, social spaces, and infrastructure in different nations, is often at odds with the topology of sovereignty and jurisdiction on which policing relies (Castells, 2002; Wall, 2007; Bojarski, 2015). The enmeshing of providers, infrastructures, users, and victims of online illicit services between different international jurisdictions is an important factor in both the character of cybercrime and the apparent

resilience which many online illicit markets exhibit towards traditional forms of police intervention. The weak ties and international dispersion which characterise cybercrime markets and their communities make them particularly resilient to traditional forms of policing, such as arresting and prosecuting key players (Yip, Shadbolt, Tiropanis, & Webber, 2012; Leukfeldt, Kleemans, & Stol, 2017). However, as we describe in this paper, law enforcement agencies have drawn approaches from two other areas of globalised policing, namely organised crime and anti-terror policing, in order to overcome these challenges, with apparent success.

The first of these approaches, which we term *infrastructural policing*, targets the Internet infrastructures on which these international markets rely and the people who maintain them, drawing inspiration from the policing of international organised drug trafficking (Florez & Boyce, 1990; Levi & Maguire, 2004; Ritter & McDonald, 2008). The second, which we term *influence policing*, draws on approaches used in tackling global terrorism and online radicalisation, repurposing (in the interests of crime prevention) the surveillance and advertising infrastructure which Internet companies have created as powerful tools for targeted behavioural change (Smit, Van Noort, & Voorveld, 2014; Qurashi, 2018).

To date, there has been very little research that evaluates the effects of cybercrime interventions (Brewer et al., 2019). We evaluate these strategies and compare them to the more traditional approaches through a mixed-methods case study of interventions in the illegal online market for Denial of Service (DoS) attacks – known as 'booter' services.

We first set out the challenges facing law enforcement interventions in online criminal markets and describe previous research on the market for DoS attacks. In the following sections, we discuss our methodological framework and the fieldwork and analysis we carried out. Next, we analyse each intervention strategy in turn, evaluating its effectiveness by quantitatively analysing DoS attack data. We qualitatively explore potential explanations for these effects through interviews with law enforcement and booter service providers. We find that traditional policing methods, such as arrests and prosecution of individual key players, have little effect on the market for booter services, facing as they do the jurisdictional challenges of a globalised Internet. However, infrastructural policing (wide-scale takedowns of infrastructure) and influence policing (targeted messaging directed at search engine users) constitute attempts by law enforcement to re-establish themselves in the globalised spaces of the Internet, and our analysis suggests that they are effective (though potentially controversial) approaches to disrupting cybercrime markets.

2. Policing the Internet

State law enforcement agencies are only one of a range of different organisations involved in enforcing order in contemporary globalised societies (Shearing & Wood, 2003). Increasingly over the course of the second half of the 20th Century (and the first two decades of the 21st), social issues which affect nation states and their populations have taken on the characteristics of what Beck terms the 'risk society': they have become increasingly globalised, complex, and operate at a distance, affecting societies in extremely negative ways but often indirectly, appearing random and unpredictable (Beck, Lash, & Wynne, 1992). The international, distributed character of these phenomena often makes them hard to tackle for local law enforcement whose powers are drawn within, rather than between, nation states. Equally, a range of other international policing concerns, such as maritime policing, require complex networks of collaboration to manage (Gould, 2020).

Accordingly, the response by contemporary states to these threats has often been to attempt to preserve their sovereign claims over their populations while coupling themselves up to the developing international networks of profit, power, and control. This has emerged

as *securitisation* (Schuilenburg, 2017), through which a range of these previously-contained and now progressively globalised social issues such as street-level crime, fraud, public health issues, or immigration are increasingly conceived through the lens of national security, and the reconfiguration of state-driven, top-down approaches as international *assemblages* of institutions, companies, and actors of different kinds. Both of these involve the decentralisation of coercive power throughout (and between) societies, with traditional state bodies such as the police becoming only a single 'node' among many (Shearing & Wood, 2003; Abrahamsen & Williams, 2010).

Cybercrime is no exception, taking as it does its qualities and contours both from the international infrastructure of the Internet and the general processes of globalisation of which this infrastructure is a part (Castells, 2002). Cybercrime causes a range of problems for traditional state institutions of control, and as a result, in accordance with a more general move towards 'responsibilisation' (Garland, 2012), neoliberal states have generally devolved much of the policing of cybercrime to actors in the private and nonprofit sector. Policing of cybercrime in this neoliberal mode is distributed throughout and between societies (rather than centralised in the state) through international assemblages of private and public bodies and actors which together have responsibility for policing cybercrime and ensuring cybersecurity (Wall, 2007), often theorised as a 'deterritorialisation' of policing and security (Behr, 2008).

Many of these relationships have developed into 'multi-agency' partnerships, in which law enforcement, constructed as generally lacking the capacity to take effective action alone, either form partnerships with private sector organisations, or devolve whole aspects of enforcement to them entirely. Mapping these broad coalitions of partners and stakeholders, theorised elsewhere as 'eCrime controllers' (Williams & Levi, 2015), has revealed extensive networks of data sharing and capacity between diverse actors, including government departments, regulatory bodies, law enforcement, international collaborative organisations, private security, platforms, voluntary groups, and other stakeholders (Williams & Levi, 2015). This can be theorised as a form of nodal governance, with discrete actor groups or clusters forming partnerships around particular issues in a fairly dynamic and 'centreless' way, with sovereign law enforcement only one of the relevant actors (and not necessarily the dominant one) (Nhan & Huey, 2013).

Clear divisions exist between 'high policing' functions and 'low policing' functions within these partnerships (Brodeur, 1983), and this too reveals the gaps within these capacities, particularly in the mid-level, where a crowding of the space around cybercrime issues, competing priorities, and lack of effective co-operative relationships can lead to problems of online crime and security slipping through the cracks, or leave key actors unable to participate (Levi & Williams, 2013). The relative lack of capacity generally attributed to law enforcement mean that platform intermediaries and other infrastructural actors (such as Google or Facebook, or Internet Service Providers) loom large in these partnerships, often taking the lead in taking down illicit infrastructure or through the formation of public/private partnerships (Dupont, 2017).

However, within this picture of decentralised governance, there is increasing appetite within the centralised specialist agencies which dominate global law enforcement issues, such as the the US Federal Bureau of Investigation (FBI) and the UK National Crime Agency (NCA), and, at the international level, Interpol, and Europol, to take a more central role in tackling more organised forms of cybercrime. Thus, this paper focuses on these centralised law enforcement agencies and their efforts.

There has been substantial research into the effects of police action on offline illicit markets and services (Koper & Reuter, 1996; J. Cohen, Gorr, & Singh, 2003; Bouchard, 2007; Mazerolle, Soole, & Rombouts, 2007). However, the ways in which law enforcement interventions affect online communities and online markets are less well understood. Online

markets differ from traditional illicit markets in a variety of ways due to the properties of the technological platforms, infrastructures and social spaces on which they rely, meaning that not only supply chains (as with traditional drug markets) but also customer-facing markets themselves are globally distributed (Holt, 2013; Hutchings & Holt, 2017).

This poses a host of challenges for traditional policing approaches. The effective use of anonymity tools can make it harder to identify participants, and jurisdictional problems are particularly challenging for law enforcement (Wall, 2007), as the international nature of cybercrime means that arrests can involve slow and expensive international operations and actors in these markets can simply host services in countries which are less likely to co-operate with investigations (Hutchings & Holt, 2017). Unlike offline markets, where new entrants need to learn the location of the market from others, online services are widely advertised and easily discoverable with search engines, and can be relatively easily accessed across jurisdictions (Liang & Mackey, 2009). For mass market online crimes like Denial of Service attacks, the volume of attacks and offenders dispersed across many jurisdictions make investigations difficult, particularly as an individual attack may cause only limited harm (Santanna et al., 2016).

3. Framing law enforcement intervention in cybercrime

While existing frameworks for making sense of police action online have merit (see, for example, (Dupont, 2016) and (Hutchings & Holt, 2017)), we propose our own categorisation in order to draw out particular functions which relate to the issues we outline above. Each of these is grouped by the broad function they fulfil in tackling online harm (reactive, incapacitative/deterrent, disruptive, and preventive), and hence the rationale behind their efficacy. None of these are solely police duties, generally involving a coalition of different actors, however we are particularly interested in the law enforcement role.

The first set of functions is *reactive*, involving responding to online harm which is reported or detected directly. Although traditionally the domain of law enforcement, for online harms this is largely the prerogative of platforms and intermediaries through content moderation and responding to abuse reports, with most of this never reaching the police (Dupont, 2017). The police do have some capacity (if people or businesses report cybercrime to them through e.g. Action Fraud) but this tends to focus on large investigations of major breaches, with little to no reactive capacity for small-scale fraud or cybercrime.

The second set of functions involve *incapacitation* and *deterrence* (Dupont, 2016). This is generally in the service of proactive, intelligence-led policing, and is based around arrests of key actors (usually those who have either been active long enough or have reached a particular threshold of severity). This follows much the same pattern as offline deterrence policing: arrest (1) (often high profile) individuals involved with coordinated media reporting, followed by sentencing (2) additionally covered in media. Although this doubtlessly does facilitate some disruption, the networked, international nature of cybercrime markets means that displacement to new providers occurs fairly smoothly. The police are the leading actor in these operations, which generally involve international co-operation between police departments, and bring in ISPs and platforms more for the supportive purposes of intelligence and evidence gathering. Arrest and sentencing can generally be considered to be part of this single broader deterrent approach, but as they are temporally dislocated (with people generally being sentenced months after their arrest), we analyse their effects separately.

The third set of functions is *disruptive*, reflecting a wider shift towards disruption-based policing evident over the last 40 years, and especially since the 9/11 attacks on the USA (J. Cohen et al., 2003; Kubrin, Messner, Deane, McGeever, & Stucky, 2010; J. H. Ratcliffe, 2016).

Much of cybercrime disruption is fully devolved to the private or voluntary sector, including platforms handling abuse reports, the efforts of companies such as Microsoft in taking down botnets, IP blacklist operators, and ISPs scanning their own customers. Law enforcement involvement here is often light-touch, either taking the form of operational intelligence-gathering, or where these entities flag up particular customers to police. However, we in this paper consider law enforcement's own 'takedown' campaigns (3) which involve targeting police powers at the infrastructures which support cybercrime and at the administrative staff who run them.

The fourth and last of these functions is *preventive*, including measures targeted at both victims and potential offenders. Victim-focused approaches tend to be security focused, involving communicating safety messages to potential victims, whether they be individuals or businesses, improving security, and generally engaging in 'target hardening'. The law enforcement role here is largely located in centralised agencies, involving outreach to large private sector businesses, or in feeding into awareness campaigns targeted at the general public.

The offender side of cybercrime prevention has been the subject of significantly less academic scrutiny, though it is an increasingly important aspect of online policing. Traditionally, this has been the domain of the platforms and intermediaries, who use design features of their technologies to disincentivise and detect online harm and cybercrime. However, this is an area in which police are rapidly establishing themselves, with law enforcement engaging in a raft of preventive approaches. The rely on essentially behaviourist methods, drawn from PREVENT or 'influence' approaches established in counter-radicalisation campaigns, including the final intervention which we evaluate in this paper (4) repurposing the online advertisement targeting infrastructure for influence messaging campaigns.

For the purposes of this paper, we compare four main interventions from these (which we focus on in the empirical section of this paper). We contrast traditional deterrent approaches, which rely on sovereign policing within and between states and act through the state criminal justice apparatus, such as (1) the arrest of key actors and (2) the subsequent sentencing of those involved in these markets, with emerging approaches (3) the police-led disruption of key infrastructure and (4) the use of preventive influence messaging campaigns targeted at potential offenders.

This allows us to consider in more depth the rationales behind each of the interventions within these law enforcement functions and how this translates to their actual effects. As we seek to evaluate as well as explain these, we draw out the rationales behind these interventions, use quantitative analysis in order to compare the apparent effectiveness of these different approaches, then qualitatively explore why particular types of intervention appear to be effective and others less so.

4. Denial of service attacks and the rise of the booter service

Online crime has evolved over the last decade into a complex, mature ecosystem of different kinds of crime, skills, roles and communities (Holt & Bossler, 2014). The rise of 'cybercrime-as-a-service' (Manky, 2013) defines the present era of online crime. As cybercrime economies have matured and stabilised, they have also become increasingly specialised, with particular skills or elements of online crime giving rise to their own highly interlinked markets, administered by specialised individuals or groups as services (Anderson et al., 2013; Collier, Clayton, Hutchings, & Thomas, 2020). This 'industrialisation' of cybercrime has increased to a global scale the exploitation of weaknesses in computer infrastructures or human behaviour that were previously the subject of targeted, small-scale attacks (Manky, 2013).

The communities centred around these cybercrime-as-a-service markets have a range of features that distinguish them from offline illicit communities. First, they are internationally distributed, with users, victims, providers, and infrastructure located all over the world (Paquet-Clouston, Décary-Hétu, & Bilodeau, 2018). Second, they are characterised by weak social ties, with large populations of weakly-enrolled members and a small core of more committed key actors (Yip et al., 2012). Although customer communities are dispersed and loosely-enrolled, the role specialisation for providers means that they are often dependent on a fairly small number of people to run key parts of the infrastructure, or particular centralised services, such as payment providers (McCoy, Dharmdasani, Kreibich, Voelker, & Savage, 2012).

We use a case study approach to explore the effectiveness of emerging law enforcement strategies in dealing with online harm and illegal markets. We focus on the market for Denial of Service attacks, which are used for a multitude of purposes, including political protest, revenge, extortion, and the cultivation of notoriety (Hutchings & Clayton, 2016). Although they have long been a feature of the Internet, they achieved substantial global media attention as a result of the Anonymous hacktivist movement, for whom they were a key tool of protest. As part of a 'digital sit-in', thousands of protesters would use their computers to direct traffic to target websites, rendering them unusable (Sauter, 2013; Coleman, 2014). As a range of more technically sophisticated means of generating this traffic at scale without the need for mass participation were developed, successor groups were able to use them to harass targets for their amusement (Coleman, 2014). From this, a growing market for DoS-as-a-service has emerged, where users purchase DoS attacks from providers without needing the technical skill to execute them themselves. These services are almost entirely used for 'booting off' or disrupting opponents from gaming servers, with a small percentage of more serious uses, such as extortion (Brunt, Pandey, & McCoy, 2017). Despite the apparently petty nature of much of the activity associated with these services, they form a particular focus for law enforcement. This is partly due to the collateral damage which these DoS attacks can cause to others (as they are often powerful enough to take out far more than just their target). Additionally, there is a general understanding (discussed in our empirical section below) that this low-level volume crime is for many young people a pathway to further illicit activity.

Booter services execute attacks in a variety of ways (Karami & McCoy, 2013; Hutchings & Clayton, 2016), including botnets of infected devices, the use of 'reflectors' (poorly-configured devices which reflect and amplify signals directed to them), and other mechanisms specific to particular services such as directly sending crafted traffic from an attack server. Booter services provide paid access via a website or downloaded application. They often advertise different packages and membership options, taking payment through digital services such as PayPal or through transfers of cryptocurrency (Hutchings & Clayton, 2016). Their customer facing platforms are used for launching attacks, and also offer customer support (Brunt et al., 2017). As commercial enterprises, booter providers need to advertise, and invest substantial time in, dealing with client interaction. These services are set up in the structure of small businesses, with individuals playing different roles, such as marketing or maintaining the server infrastructure.

5. Methods

In this research we explore and evaluate different intervention strategies directed towards the market for booter services and draw wider conclusions about the changing nature of online policing. We first interviewed law enforcement to explore the rationales behind intervention strategies. We then quantitatively evaluated their effectiveness in disrupting

the market for booter services. Finally, we use qualitative data sources to explore the mechanisms underlying the observed effects.

5.1. *Quantitative methods*

Cybercrime is often hard to measure. However, for this particular market we have worldscale representative data about real levels of crime and victimisation. This presents a unique opportunity to understand how interventions work online. We have made use of a range of quantitative data sources to establish and compare the effects of different kinds of interventions, and how these differ in different countries.

We make use of a dataset, provided by the Cambridge Cybercrime Centre (CCC), which measures DoS attacks from around the world in near real-time. This is collected through the use of honeypots; servers which mimic the vulnerable machines exploited by booter providers to launch attacks (Thomas, Clayton, & Beresford, 2017). Booter providers scan the Internet to develop lists of these machines, and then use the machines to deliver attacks. The CCC measures attacks over time by setting up machines which respond to these scans, but which cannot be used for attacks. When booters attempt to use these machines to launch attacks, data is collected about the duration and type of attack being attempted, and the country of the victim's Internet Protocol (IP) address.

We believe this dataset to be representative of booter activity using these kinds of attacks (see (Collier, Thomas, Clayton, & Hutchings, 2019) for in-depth statistical analysis of this dataset). The time series comprises data collected from July 2014 to the present day, constituting a longitudinal indication of attack numbers, and hence victimisation, for the global booter market. There is substantial day-of-week periodicity in booter attacks, and so we have conducted analysis on weekly totals. We also restrict our analysis to the period June 2016 to January 2019, as there is a clear and stable underlying trend throughout most of this period, and it includes a number of important interventions. While not measuring all attacks, we believe the data provide a good indicator of general levels of DoS victimisation, and represent a very accurate measurement of a particular kind of attack, which is highly representative of the booter market. Additionally, as a large number of booters publish information on their own websites detailing number of attacks carried out per week, we collected and analysed this self-reported data (Figure 2).

The high preponderance of attacks on gaming servers and players means that most attacks will be carried out against targets in the same country as the person launching the attack, as online gamers are generally paired by the matchmaking algorithms used by gaming services into 'game lobbies' with those in the same country as them. This means that although our time series is split by country of victim, this is also a useful proxy for country of attacker.

5.2. *Qualitative methods*

Through this quantitative work, we found a number of interventions associated with a reduction in attacks. To support our argument that these observed effects were real suppressions of the market for booter services, and investigate potential mechanisms for their effects, we engaged in substantial additional qualitative research in the booter community. This involved 'netnographic' observation of public chat channels used by the booter community (Kozinets, 2015). We examined a total of 236 chat channels associated with booter activity on the Telegram and Discord services, including a total of around 1800000 messages provided by the Cambridge Cybercrime Centre, who collected them

using specialist scraping software. We analysed these using text search to reduce the data to a manageable size, and coded a selection of relevant posts using inductive analysis.

We drew upon research by Hutchings and Holt (2018) about interviewing cybercrime offenders to inform our strategies when interviewing nine booter providers. In total, eleven interviews took place, with some participants interviewed more than once, and some interviewed in small groups. Participants were recruited using approaches posted on the websites and chat channels used by booter providers to manage their user communities. We also conducted two rounds of interviews (before and after the takedown intervention in 2018) with agents leading the most recent operations by the FBI and a single interview with an official from the NCA involved in leading the messaging intervention which we evaluate herein. Our interview data were transcribed, coded in NVivo and analysed using an inductive coding approach. This involved building up themes through progressive rounds of exploratory low-level coding, focusing on understanding the effects of different kinds of intervention in the booter market and more generally experiences and perspectives within this community.

6. Ethical considerations

As a mixed-methods project involving multiple kinds of data about communities collected in very different ways, ethical concerns were taken into account throughout the research. Our department's ethics committee reviewed and approved our use of scraped data from public chat channels and our approach to carrying out interviews with law enforcement personnel, booter providers, and booter users.

The qualitative interviews were carried out with the assurance of anonymity for participants and under the principle of informed consent. The negotiation of informed consent with the individuals who made the scraped posts which we present in this paper was not possible in this study. The CCC scraped the chat channels within the terms of service of the two platforms, which included notifying Discord explicitly what they were doing. As argued by Martin and Christin (2016), the substantial benefits of scraping this data in preventing harm, both to victims and to potential offenders who may become involved in criminal activity, outweigh the potential harms of collection. We present these quotes anonymously and have removed any details which might potentially reveal the identity of the author.

As these channels, social media sites and forums are publicly accessible and well known to law enforcement, no additional harm is caused to the users by collecting this data. As we only scrape channels which are publicly available and actively advertised by their owners, channel participants are aware that the messages they send are public domain and are more likely than average users to take precautions not to identify themselves or leak sensitive personal information. Established ethical guidelines for online research into criminal activity advise that informed consent may not be required for research into online communities where the data are publicly available and the research outputs focus on collective rather than individual behaviour (British Society of Criminology, 2015).

7. Traditional policing: arrests and sentencing

There were a large number of interventions in the market for booter services of different kinds over the period of study (see Table 1 and [blinded for review] for a more comprehensive overview of the different interventions in the booter market over this period). We modelled our dataset of attack numbers using negative binomial regression in

order to establish which of these, if any, could be linked to statistically significant effects on the number of observed attacks. Negative binomial regression is a statistical technique for modelling time series count data (Davis & Wu, 2009). These models are capable of incorporating components accounting for trend, seasonal variation, and fixed effects which can be used to model intervention periods in the data. In modelling this, we controlled for seasonality and the upward trend in numbers of DoS attacks and then tested the addition of components corresponding to any periods in the time series where recorded attack numbers dropped below those predicted by the model, in order to establish whether these met the criteria for statistical significance (model outputs can be found in Figure 1 and Table 2, with the country effects modelled in Table 3). This is a well-established method for modelling time-limited interventions in time series data (Noland, Quddus, & Ochieng, 2008; Hilbe, 2011). Each of these significant drops corresponded closely with a particular law enforcement intervention, resulting in a set of five statistically significant interventions in the market for booter services which we compare by their duration and effect size. We now consider each of our main kinds of intervention in turn, beginning with traditional forms of policing.

7.1. *Top-level results – arrests and sentencing*

The use of arrests to disrupt illicit markets is based on a rationale of *deterrence*: that beyond the specific disruption which they cause to these markets, they affect the perceptions of risk and reward which other participants associate with them. In the international context of cybercrime markets, carrying out these arrests is far from straightforward, requiring complex international networks of information sharing and collaboration. Over the period we studied, law enforcement made a number of arrests in a range of different countries and these were, to a greater or lesser extent, reported in the computer press. We were able to identify 45 arrests across five campaigns, spanning four different countries (Table 1). Three of these campaigns (totalling 38 arrests) were associated with no statistically significant change to the number of DoS attacks (see Tables 1, 2, and 3). For the two which were associated with significant reductions in attacks (one of which was very short-lived), important additional factors appear to be at play, which we discuss in Section 7.3.

We additionally consider the effects of widely-reported court cases and sentencing decisions featuring the providers of booter services. We observed five sentencing interventions over the period of study. We consider two of these to be close enough to overlap, and so, of the four discrete sentencing interventions, we see two which are associated with significant drops in attack numbers. We could find no consistent effect of widely reported court cases and sentencing on the market for booter services. We did observe short but significant reductions in booter attacks corresponding with some court cases involving booter providers, however others appear to have had little effect (and this did not correlate with, for example, length of sentence, implying that any suppression is not the result of 'classic' deterrence). There does appear to be a counter-intuitive effect visible in the data, with the Mirai and vDOS sentencing appearing to correspond to reductions in Poland, France, and Russia, rather than the countries in which these cases took place, however we believe these drops to be the result of other factors disrupting the market at this time (such as large providers temporarily shutting down for reasons not related to interventions). Equally, the self-reported attack data do not show drops in attack numbers for one of the sentencing interventions where there is a drop in the CCC honeypot data.

7.2. *Exploring our results – arrests and sentencing*

Our qualitative research offers some potential reasons for why arrests may have failed to cause significant reductions in attack numbers. There is considerable discussion of policing on booter chat channels, and between this and our interviews with providers we have developed what we assess to be a representative picture of perceptions of arrest interventions in the booter community.

The general perception of booter providers was that arrests across jurisdictions were unlikely, so providers in non-US and non-European countries felt relatively safe. Furthermore, users and smaller booter providers felt that they would be so low a priority for law enforcement that they too were effectively safe from arrest. Given the expense and complexity of launching cross-jurisdiction arrests for cybercrime offenses, this low estimation of risk has largely held true for the majority of users and providers, and most manage to avoid law enforcement contact.

> Relax boss the FBI aren't interested in anyone in this server – *Booter user, chat channel, 2018*

> The FBI has no control over France – *Booter user, chat channel, 2018*

> Cops or the FBI don't really care about people who does the ddos of someone else's wifi – *Booter user, chat channel, 2018*

Booter providers also employed a range of justifications for their involvement in providing booter services with the assertion (using legal boilerplate on their websites) that their users ultimately take on the legal and moral responsibilities for their attacks. They tended to believe that as their users were the ones directing attacks, they could mount a defence to any arrest that they were merely a service provider (although this view has no legal merit). This rationalisation has been well-documented in the existing literature on booter services (Hutchings & Clayton, 2016) and is compounded by the international nature of this market.

While we do see an impact from some sentencing interventions, we saw no discussion of sentencing in the chat channels we studied, indicating that current users and providers were likely either unaware of these cases, or did not consider them to be worthy of discussion. This implies that the effects of sentencing interventions may operate on entities outside of current booter users and providers. Our interviews with booter providers supported this finding, with participants arguing that these cases rarely registered with them, and that they tended to assume that those who had been caught had made errors which they themselves would be able to avoid.

While we do not observe booter providers dropping out of the market in tandem with sentencing interventions (and hence see no reduction in supply of booter services), we do observe, in some cases, a reduction in attack numbers which we therefore believe to be associated with a temporary reduction in demand for these services. We argue, therefore, that our results demonstrate no consistent, lasting deterrent effect from sentencing on the market for booter services.

7.3. *Webstresser arrest – a special case*

The vast majority of arrests were associated with no reduction in attacks. There were, however, two arrest interventions which appeared to be associated with significant reductions in attacks. The first of these was in April 2016, when four individuals linked by the Dutch police to a single booter provider (Webstresser) were arrested and the booter service, generally held by the booter community to be the most widely-used at that time, was taken down. This resulted in a brief reduction in attack numbers. The second arrest

intervention which significantly impacted the market was shortly before Christmas 2018, the FBI took over 15 domain names (associated with eight working booters) and arrested three individuals who were associated with two of these services. This corresponded with a far deeper and longer suppression of the DoS market. We cover the FBI actions in the following section on 'infrastructural policing', as our qualitative analysis suggests that the substantially larger effects are due to the wider-scale website takedowns and targeting of server administrators. The Webstresser intervention was primarily arrest-based and focused on a single service, and so we now explore it in more depth.

The effect of the Webstresser arrests are visible in both the honeypot datasets and in the booter providers' self-reported data. The arrest of the providers of the Webstresser booter service in April 2016 corresponded to a large (25%) drop in attacks, however this only lasted for two weeks. The effect of this arrest was largely felt in the US and Europe, with Russia showing no significant decrease in attacks. Interestingly, attack numbers significantly increased (by 144%) in the Netherlands over this period, likely in protest against the Dutch police who carried out the arrest. Turning to the self-reported attack numbers (Figure 2), the market pre-intervention appears to be fairly mature, with a number of medium-sized providers and several smaller ones representing a diverse market. The intervention precedes a significant drop in reported attack numbers, with a number of providers appearing to leave the market, however this lasted only two or three weeks, and the post-recovery market appeared much the same as before, constituting six medium-sized providers of roughly equivalent size, one larger provider and a wealth of smaller ones, as attack traffic displaced to other operators.

Although all of the arrest interventions implied the takedown of the individual booter service associated with the arrested individuals (as a side-effect), for Webstresser there were other factors which may have contributed to the short, but significant, drop in overall attack numbers. The scale of Webstresser's market dominance may account for the short-lived drop in attack numbers. When it was seized, its users lost their accounts and any remaining funds they had with the service, necessitating a large proportion of the market having to find other services and establish their trustworthiness. Additionally, it appears to have played an important supporting role in the infrastructure of the broader booter market, with a large number of smaller providers relying on it for their own attack power (which they purchased and then resold at a mark-up). Taken together, this means that the removal of the Webstresser service constituted a much wider disruption of the booter market (albeit for a short period) than would be expected for arrests of other booter services at the time. Even despite this, the effects on the booter market of the arrests appear to have lasted only a fortnight, and were limited in geographical scope.

We find, therefore, that although arrests of the providers of individual services can have a significant effect on attack numbers, these are time-limited and generally restricted to jurisdictions with extradition relationships with the arresting parties rather than globally. The desired 'deterrent' effect of these approaches is not observed, as the international nature of this market and the jurisdictional issues this poses for the police means that users can displace to new providers from around the world (using Google search and Youtube to find them) with the same ease as accessing those hosted in their own country, and mitigates the perceptions of risk by booter users and providers. Thus, arrests of individual booter providers appear to be an ineffective approach to intervening in the market for booter services, causing minimal short-term disruption.

8. Infrastructural policing

In this section, we consider the use of interventions targeted at infrastructure, including police takedowns and domain seizures. Takedowns of key infrastructure and services are intended to proactively disrupt illicit markets, and represent a form of 'policy transfer' from strategies used by the FBI in dealing with historic forms of organised crime. The FBI's foundational duties (and those of similar agencies) in tackling serious organised crime have for many years involved not only tackling leadership figures with arrests (generally as fraught with jurisdictional complications as they are in cybercrime, and facing similar issues of new individuals quickly moving into the gap left by those arrested), but in disrupting the essential infrastructures of supportive illicit services on which these criminal organisations rely for transporting goods, accounting, and laundering money (Nicaso & Lamothe, 1995; Paoli, 2007). This proactive, disruptive work is core both to FBI practice and to the careers of individual agents, and has developed into a crucial component of their approach to tackling cybercrime:

> In the standard field office role, it is important to recognise that most of us as investigative agents deal largely with a lot of complaints coming in from people who have been victimised who want to bring this to the attention of law enforcement. That's where you cut your teeth as an agent – working reactively, on cases which are brought to you. As you become more experienced, you can take more proactive measures – notice trends and try to get ahead of them, seize opportunities where they present themselves. *FBI agent, paraphrased*

Booters in particular are a priority for the FBI's anti-cybercrime efforts, firstly, because of the collateral damage which they can cause:

> This is a huge threat that is not being addressed. Many of these services have a surprisingly high attack bandwidth – which can lead to attacks that could potentially overwhelm entire ISP centres... you can cause an outage over a potentially massive area. *FBI agent, paraphrased*

They also see this as a pathway to more serious forms of online crime:

> Having watched this evolve over the past 6 years, I have had an increasing awareness that something needed to be done... It is a serious on-ramp to other criminal activity. These people are... learning the ins-and-outs of how to maintain a criminal scheme online... they are learning a lot of the skills necessary to branch out into other fields of criminal activity... I'm very concerned about this as an investigator that this is something that folks who are young and curious online are very likely to encounter, and they'll get involved in the types of activities we don't want them to get involved with. *FBI agent, paraphrased*

Our research suggests that these infrastructural interventions are particularly effective at disrupting the market for booter services. Although it might be assumed that the rationale behind these interventions is based on the direct disruptive effect they are likely to have on the technical infrastructure on which these markets rely, in fact, our interviews with law enforcement and with booter providers suggest a rather different picture. The rationale behind these takedowns was not only to disrupt the infrastructure itself, which is fairly easily re-established by providers. Instead, these interventions are targeted at the people who maintain these infrastructures: the server managers.

> At the heart of this intervention is trying to eliminate the narrative whereby some of these sites are purporting that they are offering a 'legitimate' or 'legal' service – it's not. It's a false narrative that they are knowingly spreading... So, we're trying now to force them to take notice. We're going to take control of as many of these domains as we can. We're simultaneously going to put out an announcement about the charges which we will be bringing against the admins. We're going to make it clear, as much as we can, that this is activity that is not going to be

> ignored in the US, or in the world at large... We're putting most of the pressure against the operators, rather than the users. – *FBI agent, paraphrased*

Thus, in addition to the direct disruption, there is a clear *behavioural* component to the intervention, at least as befits the law enforcement rationale. By targeting these infrastructural workers who run the payment systems, manage servers, and administer botnets, the law enforcement personnel we interviewed aimed to undermine their sense of impunity (gained either through shifting blame to the users of their service, or from the jurisdictional issues with prosecution described above).

8.1. *Top-level results – infrastructural policing*

Over the period of study, we observed two major infrastructural interventions: the removal of the booter section on the popular Hackforums cybercrime forum and the combined arrests and seizures of websites by the FBI in 2018. In 2016, the administrator of Hackforums (a popular underground cybercrime forum) announced that they would be removing the euphemistically-named "Server Stress Testing" section of the website, which allowed booter services to advertise their products and was at the time the most popular section. Although it was not announced, this was due to an intervention by US law enforcement, who had contacted the administrator to warn him of legal consequences should this area of the site remain active. At the time, Hackforums was considered an important infrastructure on which the booter market relied, giving them a centralised site in which to access and advertise to a large potential customer base. Having successfully targeted the administrators of this infrastructure, law enforcement effectively took down several 'shop fronts', necessitating displacement to a range of other platforms with smaller, less centralised communities and increasing the work required to advertise a booter service.

The removal of the booter section on Hackforums appears to have been a turning point for the booter service market. From our data, that this intervention was linked to a drop in DoS attack numbers of around 28%, with reductions of 45% in DoS attacks targeting the UK, 38% targeting the US, and 16% targeting Russia. There have also been longer-term effects, as the booter community no longer has a single large communal site (subsequent attempts to create these have been unsuccessful). It is now instead characterised by a highly-dispersed set of small communities, focused on individual booters and hosted on small Discord and Telegram chat channels.

> The reason they're on Discord is an adaptation, because we were able to push them away from HackForums – it used to be the place where booters congregated, it was really active for DoS services in the community. HackForums had a very active marketplace, and booters used to be one of the main services on it, the most profitable thing. We were able to put pressure on, and get it shut down – other forums took some of the traffic, but generally it's moved to Discord, because they lost the other platforms, and a lot of them are on there anyway. – *FBI agent, paraphrased*

The second takedown intervention, the action by the FBI at Christmas 2018, was the largest intervention to date against booter services. The seizure of fifteen domain names, corresponding to eight active services, combined with the arrest of three server managers had a far longer-lasting effect than the single takedown and arrest of Webstresser (despite the fewer number of individuals arrested), suppressing attack numbers by 39% (taking into account previous trend and seasonality) for around two months. This was similarly focused on Europe (41% reduction in UK attacks) and the US (49% reduction in attacks), with no significant effect seen in Russia. After the FBI intervention, the upward trend in attacks appears to have halted for a substantial period.

8.2. *Exploring our results – infrastructural policing*

There are around fifty active booters at any given time, with only the top ten carrying out any significant numbers of attacks, and the rest rarely staying in the market for long. From our qualitative research, we believe that only the larger booters actually run any of their own infrastructure for long, with most smaller booters making abortive attempts to supply their own attack power before reverting to reselling the attack capacity of the larger booter providers. Given the tedious and risk-heavy nature of this server management work, as described in Collier et al. (2020), many smaller and medium-size providers simply purchase access to an API (an automated interface for accessing a booter's attack power) from the larger ones. Taking out one of the major booters can therefore disrupt a range of smaller ones as well, and if a server manager leaves, the skill pool is so low (due to the dispersed nature of the booter community and the low levels of cultural capital which attends this administrative work) that the knock-on effects can be extremely disruptive. This means that the booter market is highly dependent on a relatively small number of server managers.

> There's a lot of reselling. 70% of my power comes from other sites, mostly for security reasons. If I get messed with by law enforcement I just say that I'm a customer of another service and send the police on to them. – *Booter provider interview*

> [takedowns] can effect [sic] providers. If we went down, man literally everything would be fucked. Couldn't count on both my hands and my toes how many others use our API
> – *Booter provider interview*

Centralisation (or 'concentration') of this infrastructural work is a common feature of mass-market cybercrime-as-a-service ecosystems (Clayton, Moore, & Christin, 2015), and in the case of the booter market, these server managers are a particularly effective target for interventions. After the FBI takedowns, we observed from the chat channels that a number of server managers quit the booter market entirely as a result of these seizures. One of our interview participants was an ex-server manager who had quit the market as a direct response to the FBI takedowns, who claimed that they took this as an indication that the risk involved was no longer worth the tedious nature of the work. The exit of these server managers had considerable knock-on effects for their own booter services and those who resold their attack capacity, who lost the ability to provide attacks for their paying users, and hence were accused of scamming their customers or simply shut down.

> It's not a scam it's just gone to shit. It used to be a good booter then the old server manager went, [it] seemed to crumble and just can't recover. Now for the new people this booter is scam. – *Booter provider (chat channel)*

The FBI takedowns caused substantial damage to the booting ecosystem, and also dramatically reshaped the structure of the market (see Figure 2). We estimate that pre-intervention the booter market consisted of 15 booters of any size, with only a handful of large booters and large numbers of much smaller ones. When the intervention occurred, there was an immediate drop in reported attacks, with the taken-down booters and several others leaving the market. The market then appeared to centralise even further, displacing wholesale to a single booter (one of the only larger providers who were untouched by the FBI seizures), with attack growth suppressed for around two and a half months. Following this intervention, the market is at the time of writing dominated by a single booter which accounts for more than 60% of self-reported attack traffic. Given the prevalence of reselling activity, it is likely that a large amount of the attack capacity in the market is now reliant on infrastructure managed and provided by a small number of server managers, leaving the market very vulnerable to intervention. Although a number of smaller providers began to

spring up around two months after the intervention (at the same time as a medium-sized one returned), their attack numbers appear static, and the only growth appears to be from the large booter, which now overwhelmingly dominates the market. At the present moment, this booter remains active as it is hosted outside the US, and has yet to become an immediate priority target for the agency (suggesting that these interventions are still dependent on institutional resources and the amassing and spending of institutional capital).

Both the infrastructural interventions had significant effects on the number of DoS attacks we observed for a prolonged period, and also changed the structure of the booter ecosystem, with the first dispersing the community and the second centralising the market and the provision of the infrastructure on which these attacks rely. Our analysis suggests that that targeting the infrastructure on which these markets depend and the people who maintain it, which we describe as 'infrastructural policing', is particularly effective in disrupting these mass-scale cybercrime-as-a-service markets.

9. Influence policing

The final kind of intervention we evaluate involves targeted messaging campaigns, which make use of the surveillance advertising infrastructures created by companies such as Google and Facebook, as tools for preventative law enforcement interventions. These infrastructures track users around the Internet using cookies and other data-driven approaches, building intensely personal behavioural profiles which are then used to target adverts.

The use of targeted online advertising by law enforcement in 'influence' operations are part of a broader strategy, originally developed under the PREVENT duty in the UK for counter-terrorism and counter-radicalisation, which is based around a behaviourist approach to identifying and diverting 'at-risk' people from pathways which might potentially lead to serious offending. The National Crime Agency has adapted this controversial PREVENT approach to cybercrime through CYBER-PREVENT (more recently "Cyber Choices"), targeting adolescents and young adults whom they deem at risk for becoming involved in online offending with online messaging and diversionary programmes. These include 'knock and talk' interventions where NCA officers visit the homes of adolescents who have exhibited risky online behaviours such as engaging on hacker forums or purchasing illicit services, and more in-depth workshop-based interventions with mentors from the NCA and private security companies (NCA, 2020). From "Cyber Choices", we document and evaluate what we believe to be the first prominent use of targeted digital advertising by police as a cybercrime intervention strategy, which we term *influence policing* – a form of messaging which goes beyond traditional police informational campaigns and adopts techniques more associated with high policing, espionage, and statecraft.

We focused on a particular messaging campaign targeted at booter users in their early stages of involvement which was limited to the UK. This intervention involved targeted Google search engine advertisements featuring prominent NCA branding, which were delivered solely to UK users aged 16 to 24 who were searching for terms related to booter services between December 2017 and June 2018. The adverts were designed with the help of psychologists, focusing on the illegality of booter services, and linked to 'advertorial' blogs on major gaming websites.

> It's quite novel that, with this crime type, that you can be there at the first point that criminal intent is shown. So you've got a youngster who's going, right, someone's been talking about booting, or, someone's been chatting about booting someone off. How do I do it? So he's first formulating the intent to actually go and do it: "I'll find out about it!". Police is nowhere in his

> mind, legality. So, and as soon as he types it into Google, it comes up on the top of the page: "NCA. Booting is illegal". You know, if we could do the same with burglars, they're going out on their first job, [with a message on the front door], or in his thought process. Police is not in their mind, in fact, they've probably done a risk assessment and thought, well, they're not there. But you know, if you could have a police car going past, or something... So, it's unique in the fact that that first step, or that first bit of intent that you can put that up there on the top of the page. Not necessarily click on it, but it's there, so we're showing a presence. We are undermining one of the things that the research into criminal pathways identified. "Police aren't interested", well, yeah, we are, because we're up here. – *NCA officer*

These kinds of messaging are likely to most strongly affect new users of booter services. The rationale behind these messaging campaigns was diversionary, targeting younger potential users, and the use of Google Adverts' sophisticated targeting capabilities allowed law enforcement to engage these at a crucial point in the sequence of events which leads to users having their first interaction with the booter community:

9.1. *Top-level results – influence policing*

The existing upward trend (a positive gradient of 2.9 between July 2016 and November 2017) in UK attacks (Figure 3) appears to entirely flatten (to a positive gradient of 0.1) throughout the course of this campaign, while the trend in worldwide attacks (the trend in US attacks is displayed in Figure 3 as a proxy for this) continues to rise. This appears, therefore, to be a highly successful intervention. We argue that this levelling-out, rather than reduction, in attack numbers is because those who already use booter services are unlikely to see these advertisements, however those attempting to enter the market are likely to search Google (which dominates the search engine market) for booter services and hence be targeted.

9.2. *Exploring our results – influence policing*

We argue that rather than emerging from a simple 'deterrent' effect, our fieldwork suggests that this messaging is most likely effective due to the dispersed, international nature of the booter user community, and the weak enrolment and loose social ties of the (generally very young) users which characterise it. Booting is widely derided even by those within the booter community, and has generally failed to develop a coherent or stable cultural world of its own. The booter community, especially since its exile from Hackforums and dispersion across a range of very small communities, has extremely low cultural capital: possibly to a greater extent than any of the main varieties of cybercriminal activity which we can identify. This is partly due to the low levels of skill required to use or run a booter in comparison to more technically challenging forms of cybercrime. Booters are largely set up using pre-made scripts and website sources found online, and users require no technical skill whatsoever. Booter providers and users are often referred to as 'skids' (or 'script kiddies') in the hacker community: low-skilled individuals who simply use other people's methods without any technical ability or creativity of their own. Even on booter chat channels, individuals are often mocked for using booters, and channel participants often state that they do not use booters
themselves.

I'm at a point were booting is gay asf [as fuck] lol – *Booter user (chat channel)* Yeah tbh

booting is getting boring – *Booter user (chat channel)*

People love spamming attacks because they think booting is cool and they think they are scary haxors [hackers] – *Booter user (chat channel)*

Booting is dead. Has been for a while. Yes a lot of people still do it but not like it used to be. I have a spot on [booter service] web based but I don't use it. – *Booter user (chat channel)*

Denial of service is for kids – *Booter user (chat channel)*

Our evidence from chat channels and interviews suggests that most booter users are young and only involved for a short time. In accordance with the low levels of social capital which we observe in the community, our interviews with booter providers suggest that there appears to be a very high turnover of users, and the market appears largely to rely on large numbers of short-term users who only purchase a small number of attacks before stopping, rather than a small number of users who invest a relatively large amount of money in these services. Thus, targeting these weak ties and the weak techniques of neutralisation which allow these younger users to believe that booting is legal, harmless, and risk-free appears to have a significant and lasting effect on entry to the user community.

The effectiveness of messaging interventions is also backed up by our qualitative interviews, which included an ex-provider who had quit as a result of a targeted message sent by email from US law enforcement as part of a campaign several years earlier.

I would think [messaging campaigns] would work a lot better [than arrests], because when I got messaged [by US law enforcement], like, you always have a, for example, if you've heard of Edward Snowden, you know that you're being watched, regardless, and everyone has that in the back of their mind. But I think if you let people know that you're actively being watched, via a message or, someone knows what you're looking at, it scares you. Especially when it's a younger kid... I think a lot of people would take it as a, sort of a second chance. – *Ex-booter provider*

Drawing from the language used by our law enforcement interviewees, we term this 'influence policing'. We believe that this appears to be effective partly because of the qualitative difference between these targeted adverts and traditional police messaging campaigns. Google has built an incredibly powerful tool for targeting specific populations and delivering targeted messages to attempt to change their behaviour. This form of messaging targets the most susceptible individuals at the very beginning of their potential involvement in illegal online activities. Additionally, this is by far the cheapest form of intervention we studied, costing only a few thousand pounds to achieve a significant reduction in attack numbers for six months.

10. Discussion and conclusions

We argue that the particular structural and cultural features of mass-market cybercrime are responsible for the resilience of the booter market to traditional policing interventions and its susceptibility to emerging forms of policing. The topologies and design of different kinds of Internet infrastructure – and how these interact with culture and practices – concentrate and disperse specific human and technical elements of cybercrime communities, breaching boundaries of international jurisdiction in ways which render traditional policing approaches ineffective, but also giving rise to novel opportunities for disruption.

A potential explanation for the limited effects which we do observe for some sentencing interventions is that they are accompanied by a great deal of media coverage, which invariably mentions that DoS is illegal. This may be the important effect for arrests as well; a time-limited effect on potential new users of these services, who will be searching for booter providers on Google's search engine and may well come across these news stories. Overall, however, the international nature of this Internet-facilitated market means that sentencing and arrest interventions are complicated by jurisdictional issues and displacement.

This international displacement (and the lack of a central community site for booters) also means that the booter community is highly dispersed, characterised by loose ties, low levels of involvement, and weak systems of cultural capital. The market is chiefly supported by large numbers of these low-involvement users who are only weakly enrolled, and who invest small amounts of money before discontinuing. This makes this community susceptible to disruption by influence policing, which also avoids the solidaristic effect and some of the unintended harms which arrests and crackdowns have been shown to generate (Ladegaard, 2019). These are best conceived as *behavioural* interventions, rather than the commonly-heralded situational interventions associated with Situational Crime Prevention and Routine Activities Theory (L. E. Cohen & Felson, 1979; Yar, 2005), which operate on the ecology of criminal opportunity. They exist within a broader network of governmental practice that draws from 'nudge' approaches and the wider practices of counter-terrorism employed by the NCA.

Conversely, although the infrastructure on which this market relies is internationally dispersed, the community of people who administer this is highly centralised, with the majority of the attack capacity supported by a small number of larger providers and their server managers. The tedious nature of the infrastructural work involved and the low levels of cultural capital associated with it mean that these providers are relatively easily dissuaded by infrastructural policing involving wide-ranging takedowns, which makes their work even more laborious and risky (especially when backed up with the threat of widespread arrests) (Collier et al., 2020). The centralisation of the supportive infrastructural work of these markets and the prevalence of reselling means that these interventions therefore have very disruptive effects on the market as a whole.

As law enforcement attempt to establish effective means of intervening in cybercrime markets, so too are the rationales behind online police action changing. Rationales based in exemplary deterrence fail for these cybercrime markets, as they are reliant on fear of a sovereign police force with a capacity to act which is frustrated by the complex jurisdictional environments which these markets straddle (Wall, 2007). The concentrations and dispersions of people which emerge from Internet infrastructure are of particular importance for these emerging methods of policing. The two emerging approaches highlighted in this article show up the micro-contours within the nominally dispersed structures of these crimes. While cybercrime may be a global and dispersed phenomenon at the macro-scale, it has a complex human and technical sub-geography which provides distinct opportunities and challenges for police action. As law enforcement develops approaches to online intervention, they are increasingly reclaiming 'ownership' of cybercrime problems – disrupting and repurposing Internet infrastructure and taking more active roles in partnership with the private sector actors who maintain these infrastructures – bringing themselves to more central positions in these nodal relationships.

This has important implications for how we frame cybercrime policing – rather than arguments about lacking capacity (which are fairly well-supported for arrests and sentencing), we see an increasing desire to own these crime problems. Although sovereign policing is clearly complicated by the Internet, there are some successes with more proactive measures where law enforcement take the lead. These are reliant on their ability to enrol

or subvert the same international infrastructures of the Internet which frustrate more traditional forms of policing. This does not break law enforcement out of their 'nodal' partnerships with the private sector, rather it reorients their centre of gravity, suggesting further roles for the infrastructure providers to directly serve policing needs. The increasing pressure on these intermediaries (and on law enforcement) to tackle online harm augurs a reconfiguration of these 'nodal' relationships into more hierarchical structures, with law enforcement developing more regularised capacities for interception, disruption, and influence using the technical capabilities of these intermediaries (whose appetite for taking this work on themselves has generally been low).

While this clearly merits further theoretical exploration than is possible in a largely empirical article, it particularly notable that the FBI's disruptive strategy for cybercrime interventions draws inspiration from the organised crime policing which has been a focus throughout its long history as a law enforcement institution (Florez & Boyce, 1990; Levi & Maguire, 2004; Ritter & McDonald, 2008), while the NCA's CYBERPREVENT approach (as a much younger institution) is drawn from the preventive anti-terror policing approaches which attained prominence in the UK in the years of its infancy (Smit et al., 2014; Qurashi, 2018). The repurposing of strategies from other globalised areas of policing for cybercrime interventions is a further step in the movement of the traditional role of police as a reactive force towards an intelligence-led, proactive model with a responsibility to actively disrupt crime (J. Ratcliffe & Makkai, 2004; Henry & Smith, 2017). As this form of disruptive policing is moving online, it is taking on distinct forms in reaction to the particular features of the digital environment and online communities involved in illegal activity, but is also shaped by the histories and contexts of the institutions tasked to carry it out. It is additionally worth noting that underneath an apparently disruptive rationale, both infrastructural and influence policing have strong *behavioural* components at their heart.

Despite the apparent effectiveness of the emerging strategies we evaluate, the same questions of democratic policing pertain: about how resources are targeted, which communities are policed and how, and who is responsible when things go wrong (Henry & Smith, 2017). There is a worrying aspect to this repositioning of the police role, which appears to be drawn nearly entirely within the 'high policing' scope, outwith the potentially more democratised (or at least democratisable) and accountable structures, functions, and practices of more mundane or community-oriented arenas of policing. For influence policing in particular, a degree of caution is advised, as the potential harms are largely unknown. It remains for future work to explore what procedural justice and accountability might look like for these emerging kinds of online policing, and to map these developments and their histories in more depth.

References

Abrahamsen, R., & Williams, M. C. (2010). *Security beyond the state: Private security in international politics*. Cambridge: Cambridge University Press.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... Savage, S. (2013). Measuring the cost of cybercrime. In *The Economics of Information Security and Privacy* (pp. 265–300). Berlin: Springer.

Beck, U., Lash, S., & Wynne, B. (1992). *Risk society: Towards a new modernity* (Vol. 17). London and New York: Sage.

Behr, H. (2008). Deterritorialisation and the transformation of statehood: The paradox of globalisation. *Geopolitics*, *13*(2), 359–382.

Bojarski, K. (2015). Dealer, hacker, lawyer, spy: Modern techniques and legal boundaries of counter-cybercrime operations. *The European Review of Organised Crime*, *2*(2), 25–50.

Bouchard, M. (2007). On the resilience of illegal drug markets. *Global Crime*, *8*(4), 325–344.

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). *Cybercrime prevention: Theory and applications*. Cham: Palgrave Macmillan.

British Society of Criminology. (2015). *Statement of ethics.* Retrieved from http:// www.britsoccrim.org/ethics/

Brodeur, J.-P. (1983). High policing and low policing: remarks about the policing of political activities. *Social problems*, *30*(5), 507–520.

Brunt, R., Pandey, P., & McCoy, D. (2017). Booted: An analysis of a payment intervention on a DDoS-for-hire service. In *Workshop on the Economics of Information Security* (pp. 06–26).

Castells, M. (2002). *The internet galaxy: Reflections on the internet, business, and society*. New York: Oxford University Press.

Clayton, R., Moore, T., & Christin, N. (2015). Concentrating correctly on cybercrime concentration. In *Workshop on the Economics of Information Security.*

Cohen, J., Gorr, W., & Singh, P. (2003). Estimating intervention effects in varying risk settings: Do police raids reduce illegal drug dealing at nuisance bars? *Criminology*, *41*(2), 257–292.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 588–608.

Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. London and New York: Verso books.

Collier, B., Clayton, R., Hutchings, A., & Thomas, D. (2020). Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies. In *Proceedings of the Workshop on the Economics of Information Security.*

Collier, B., Thomas, D. R., Clayton, R., & Hutchings, A. (2019). Booting the booters: evaluating the effects of police interventions in the market for denial-of-service attacks. In *Proceedings of the internet measurement conference* (pp. 50–64).

Davis, R. A., & Wu, R. (2009). A negative binomial model for time series of counts. *Biometrika*, *96*(3), 735–749.

Dupont, B. (2016). The polycentric governance of cybercrime: The fragmented networks of international cooperation. *Cultures & Conflicts*, *102*(2), 95–120.

Dupont, B. (2017). Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law and Social Change*, *67*(1), 97–116.

Florez, C. P., & Boyce, B. (1990). Laundering drug money. *FBI Law Enforcement Bulletin*, *59*(4), 22–26.

Garland, D. (2012). *The culture of control: Crime and social order in contemporary society*. Chicago: University of Chicago Press.

Gould, A. (2020). Sovereign control and ocean governance in the regulation of maritime private policing. *Policing and Society*, 1–17. Retrieved from https://doi.org/10.1080/10439463.2020.1732975

Henry, A., & Smith, D. J. (2017). *Transformations of policing*. Oxon: Routledge.

Hilbe, J. M. (2011). *Negative binomial regression*. Cambridge: Cambridge University Press.

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review*, *31*(2), 165–177.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20–40.

Hutchings, A., & Clayton, R. (2016). Exploring the provision of online booter services. *Deviant Behavior*, *37*(10), 1163–1178.

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: disruption and intervention approaches. *Global Crime*, *18*(1), 11–30.

Hutchings, A., & Holt, T. J. (2018). Interviewing cybercrime offenders. *Journal of Qualitative Criminal Justice & Criminology*, *7*(1), 75–94.

Karami, M., & McCoy, D. (2013). Understanding the emerging threat of ddos-asa-service. In *6th {USENIX} Workshop on Large-Scale Exploits and Emergent Threats ({LEET} 13).*

Koper, C. S., & Reuter, P. (1996). Suppressing illegal gun markets: Lessons from drug enforcement. *Law and Contemporary Problems*, *59*(1), 119–146.

Kozinets, R. V. (2015). *Netnography*. London: Sage Publications.

Kubrin, C. E., Messner, S. F., Deane, G., McGeever, K., & Stucky, T. D. (2010). Proactive policing and robbery rates across us cities. *Criminology*, *48*(1), 57–97.

Ladegaard, I. (2019). "I pray that we will find a way to carry on this dream": How a law enforcement crackdown united an online community. *Critical Sociology*, *45*(4-5), 631–646.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *The British Journal of Criminology*, *57*(3), 704–722.

Levi, M., & Maguire, M. (2004). Reducing and preventing organised crime: An evidencebased critique. *Crime, Law and Social Change*, *41*(5), 397–469.

Levi, M., & Williams, M. L. (2013). Multi-agency partnerships in cybercrime reduction. *Information Management & Computer Security*.

Liang, B. A., & Mackey, T. (2009). Searching for safety: addressing search engine, website, and provider accountability for illicit online drug sales. *American Journal of Law & Medicine*, *35*(1), 125–184.

Manky, D. (2013). Cybercrime as a service: a very modern business. *Computer Fraud & Security*, *2013*(6), 9–13.

Martin, J., & Christin, N. (2016). Ethics in cryptomarket research. *International Journal of Drug Policy*, *35*, 84–91.

Mazerolle, L., Soole, D., & Rombouts, S. (2007). Drug law enforcement: A review of the evaluation literature. *Police Quarterly*, *10*(2), 115–153.

McCoy, D., Dharmdasani, H., Kreibich, C., Voelker, G. M., & Savage, S. (2012). Priceless: The role of payments in abuse-advertised goods. In *Proceedings of the 2012 ACM conference on Computer and Communications Security* (pp. 845–856).

NCA. (2020). *Cyber choices: Helping you choose the right and legal path.* Retrieved from https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/ cyber-crime/cyberchoices (Accessed: 2020-05-07)

Nhan, J., & Huey, L. (2013). Policing through nodes, clusters and bandwidth. In *Technocrime* (pp. 89–110). Willan.

Nicaso, A., & Lamothe, L. (1995). *Global mafia: The new world order of organized crime*. Macmillan Canada Toronto.

Noland, R. B., Quddus, M. A., & Ochieng, W. Y. (2008). The effect of the London congestion charge on road casualties: an intervention analysis. *Transportation*, *35*(1), 73–91.

Paoli, L. (2007). Mafia and organised crime in italy: The unacknowledged successes of law enforcement. *West European Politics*, *30*(4), 854–880.

Paquet-Clouston, M., Décary-Hétu, D., & Bilodeau, O. (2018). Cybercrime is whose responsibility? A case study of an online behaviour system in crime. *Global Crime*, *19*(1), 1–21.

Qurashi, F. (2018). The Prevent strategy and the UK 'war on terror': embedding infrastructures of surveillance in Muslim communities. *Palgrave Communications*, *4*(1), 1–13.

Ratcliffe, J., & Makkai, T. (2004). *Diffusion of benefits: Evaluating a policing operation*. Canberra: Australian Institute of Criminology.

Ratcliffe, J. H. (2016). *Intelligence-led policing*. Routledge.

Ritter, A., & McDonald, D. (2008). Illicit drug policy: Scoping the interventions and taxonomies. *Drugs: Education, Prevention and Policy*, *15*(1), 15–35.

Santanna, J. J., Schmidt, R. d. O., Tuncer, D., De Vries, J., Granville, L. Z., & Pras, A. (2016). Booter blacklist: Unveiling ddos-for-hire websites. In *2016 12th International Conference on Network and Service Management (CNSM)* (pp. 144–152).

Sauter, M. (2013). "LOIC Will Tear Us Apart" The impact of tool design and media portrayals in the success of activist DDoS attacks. *American Behavioral Scientist*, *57*(7), 983–1007.

Schuilenburg, M. (2017). *The securitization of society: crime, risk, and social order* (Vol. 12). New York: NYU Press.

Shearing, C., & Wood, J. (2003). Nodal governance, democracy, and the new 'denizens'. *Journal of Law and Society*, *30*(3), 400–419.

Smit, E. G., Van Noort, G., & Voorveld, H. A. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in europe. *Computers in Human Behavior*, *32*, 15–22.

Thomas, D. R., Clayton, R., & Beresford, A. R. (2017). 1000 days of UDP amplification DDoS attacks. In *2017 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 79–84).

Wall, D. S. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research*, *8*(2), 183–205.

Williams, M. (2006). *Virtually criminal: Crime, deviance and regulation online*. Oxon: Routledge.

Williams, M., & Levi, M. (2015). Perceptions of the ecrime controllers: Modelling the influence of cooperation and data source factors. *Security Journal*, *28*(3), 252–271.

Yar, M. (2005). The novelty of 'cybercrime' an assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407–427.

Yip, M., Shadbolt, N., Tiropanis, T., & Webber, C. (2012). The digital underground economy: A social network approach to understanding cybercrime. In *Digital Futures 2012: The Third Annual Digital Economy All Hands Conference.*

Table 1. List of interventions

Operation start	Intervention	Type	Statistically significant impact in our model
2016-09-08	vDOS arrests	Arrests (of 2 people)	No
2016-10-06	Lizardstresser arrests	Arrests (of 2 people)	No
2016-10-28	Hackforums SST shutdown	Takedown	Yes
2016-12-05	Operation Tarpit	Arrests (of 34 people)	No
2016-12-01	Destressbooter sentencing	Sentencing	No
2017-04-25	Titaniumstresser sentencing	Sentencing	No
2017-12-15	NCA messaging campaign	Messaging	Yes (in the UK)
2017-12-19	VDOS sentencing	Sentencing	Yes
2018-03-27	Lizardstresser sentencing	Sentencing	No
2018-04-24	Webstresser arrest	Takedown and arrests (of 4 people)	Yes
2018-09-18	Mirai sentencing	Sentencing	Yes
2018-10-26	Mirai sentencing 2	Sentencing	Yes(overlapping with above)
2018-12-19	FBI mass takedowns	Multiple takedowns and arrests (of 3 people)	Yes

Table 2. Negative binomial regression model showing model composition, including key interventions, seasonal components, first order trend, and constant with significance and effect size. Asterisks indicate if inclusion of an intervention made a significant (*) or strongly significant (**) contribution to the model. The seasonal variables model the month-by-month seasonality of the data. We also included a separate component for Easter as school holidays are linked to rises in attacks and the date of Easter is not fixed.

						95% CI	
	Date	Coef.	Std.error	*z*	*P* > |*z*|	Lower	Upper
Xmas2018	2018-12-19	−0.393	0.039	−10.05	0.000**	−0.469	−0.316
Webstresser	2018-04-24	−0.238	0.0574	−4.15	0.000**	−0.351	−0.126
Mirai sentencing and arrests	2018-10-26	−0.516	0.049	−10.46	0.000**	−0.613	−0.420
HackForums SST forum closed	2016-10-28	−0.360	0.039	−9.16	0.000**	−0.437	−0.283
vDOS sentencing	2017-12-19	−0.275	0.057	−4.83	0.000**	−0.387	−0.164
Easter		−0.016	0.094	−0.17	0.864	−0.200	0.168
seasonal_2		0.076	0.066	1.15	0.25	−0.053	0.205
seasonal_3		−0.051	0.060	−0.86	0.390	−0.168	0.066
seasonal_4		−0.025	0.057	−0.44	0.660	−0.137	0.087
seasonal_5		−0.098	0.062	−1.59	0.110	−0.220	0.023
seasonal_6		−0.134	0.069	−1.95	0.050*	−0.269	0.001
seasonal_7		−0.125	0.054	−2.32	0.020*	−0.230	−0.019
seasonal_8		−0.078	0.060	−1.3	0.190	−0.196	0.040
seasonal_9		0.069	0.058	1.19	0.240	−0.045	0.184
seasonal_10		−0.086	0.048	−1.77	0.080	−0.181	0.009
seasonal_11		−0.111	0.051	−2.16	0.030*	−0.211	−0.010
seasonal_12		0.091	0.047	1.93	0.050	−0.001	0.182
time		0.010	0.000	27.04	0.000**	0.009	0.011
_cons		10.289	0.060	170.88	0.000**	10.171	10.407

Table 3. Estimated effect sizes of statistically significant (at the global scale) interventions by country (UK, US, Russia, France, Germany, Poland, and the Netherlands), showing the effects of each intervention component in separate negative binomial models of attack numbers over time in each country. Asterisks indicate inclusion of intervention in the model made a significant (*, <0.05) or strongly significant (**, <0.001) contribution to the model. Countries were chosen by prominence in number of attacks, or factors which made them of interest (such as NL retaliation for Webstresser takedown)

Intervention		UK	US	RU	FR	DE	PL	NL	Overall
Xmas2018 Intervention 2018-12-19	Mean	-27%	-49%	-33%	-1%	-28%	-23%	-16%	-32%
	L95/U95	-43/-28%	-55/-42%	-43/-22%	-13/11%	-36/-20%	-37/-5%	-27/-3%	-37/-27%
	Duration	9 weeks	9 weeks	9 weeks	N/A	8 weeks	3 weeks	8 weeks	10 weeks
	Signif.	0.000**	0.000**	0.000**	0.828	0.000**	0.014*	0.018*	0.000**
Mirai sentencing and other actions 2018-10-26	Mean	-27%	-31%	-5%	-9%	-32%	-47%	-19%	-40%
	L95/U95	-42/-9%	-41-20%	-16/7%	-31/21%	-40/-23%	-56/-36%	-35/0%	-46/-34%
	Duration	2 weeks	7 weeks	2 weeks	N/A	6 weeks	2 weeks	6 weeks	8 weeks
	Signif.	0.006**	0.000**	0.41	0.533	0.000**	0.000**	0.053	0.000**
Webstresser takedown 2018-04-24	Mean	-10%	-24%	-16%	-22%	-29%	-29%	146%	-21%
	L95/U95	-21%/3%	-40/-4%	-33/6%	-35/-7%	-36/-22%	-42/-14%	94/211%	-30/-12%
	Duration	N/A	4 weeks	2 weeks	4 weeks	9 weeks	6 weeks	4 weeks	3 weeks
	Signif.	0.120	0.022*	0.14	0.006*	0.000**	0.001**	0.000**	0.000**
vDOS sentencing 2017-12-19	Mean	-20%	-4%	-37%	-30%	-4%	16%	-24%	-24%
	L95/U95	-33/-5%	-18/12%	-47/-24%	-37/-23%	-17/10%	-17/62%	-33/-13%	-32/-25%
	Duration	3 weeks	3 weeks	2 weeks	2 weeks	N/A	N/A	3 weeks	3 weeks
	Signif.	0.011*	0.563	0.000**	0.000**	0.532	0.373	0.000*	0.000**
HackForums 2016-10-28	Mean	-48%	-30%	-13%	-52%	-32%	2%	-35%	-30%
	L95/U95	-53/-42%	-37/-21%	-23/-3%	-59/-43%	-41/-23%	-19/28%	-42/-27%	-33/-25%
	Duration	15 weeks	7 weeks	14 weeks	15 weeks	7 weeks	N/A	15 weeks	13 weeks
	Signif.	0.000**	0.000**	0.02*	0.000**	0.000*	0.86	0.000*	0.000**

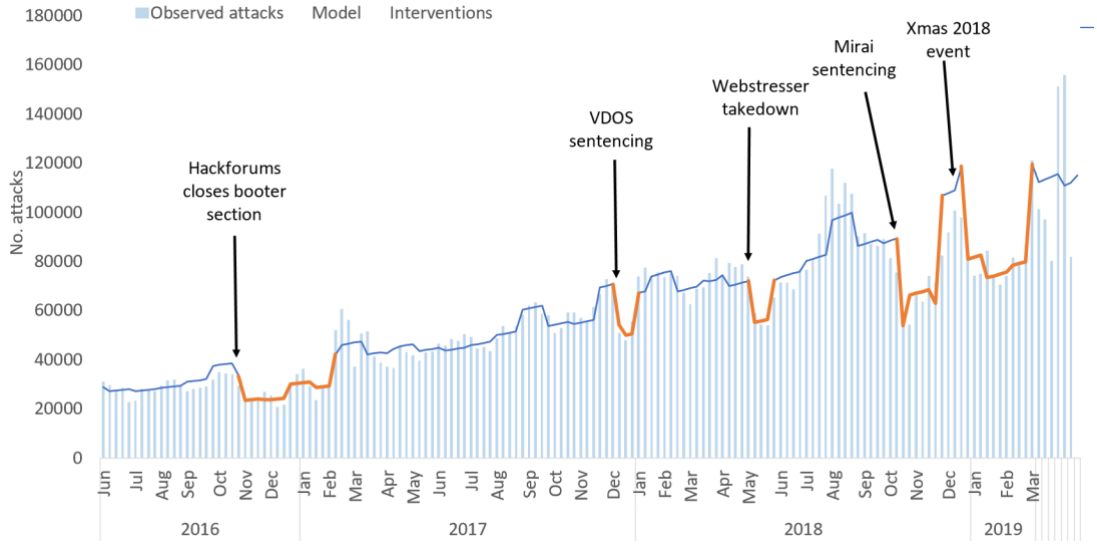

Figure 1. Total attack numbers over time (light blue bars) with negative binomial model (dark blue line) overlaid. Labels indicate the statistically significant interventions (modelled over periods shown by the dark orange line).

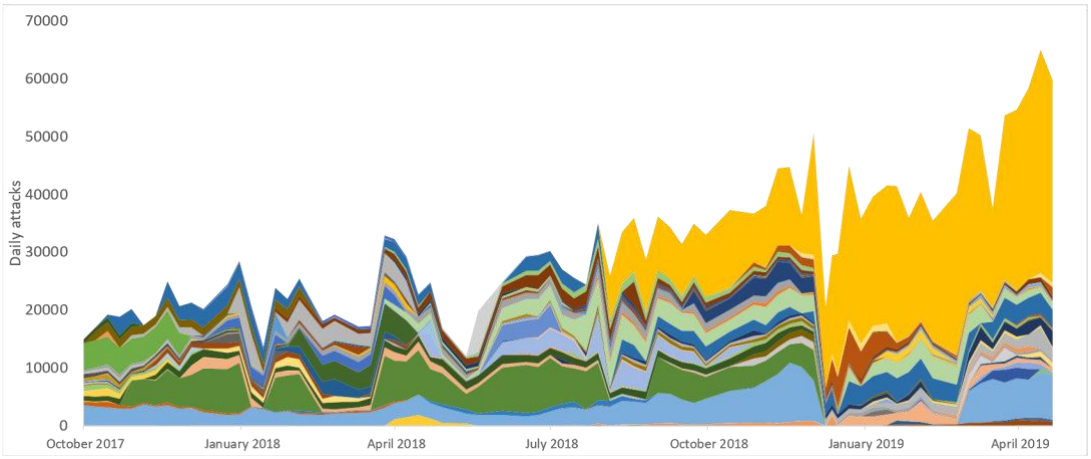

Figure 2. Stacked area graph showing total number of DoS attacks per week over time as self-reported by booter provider websites. Each stacked area series refers to the attacks reported by an individual booter service – as can be seen, the market structure changes in December 2018, where most of the attacks displace to a single service (shown in yellow).

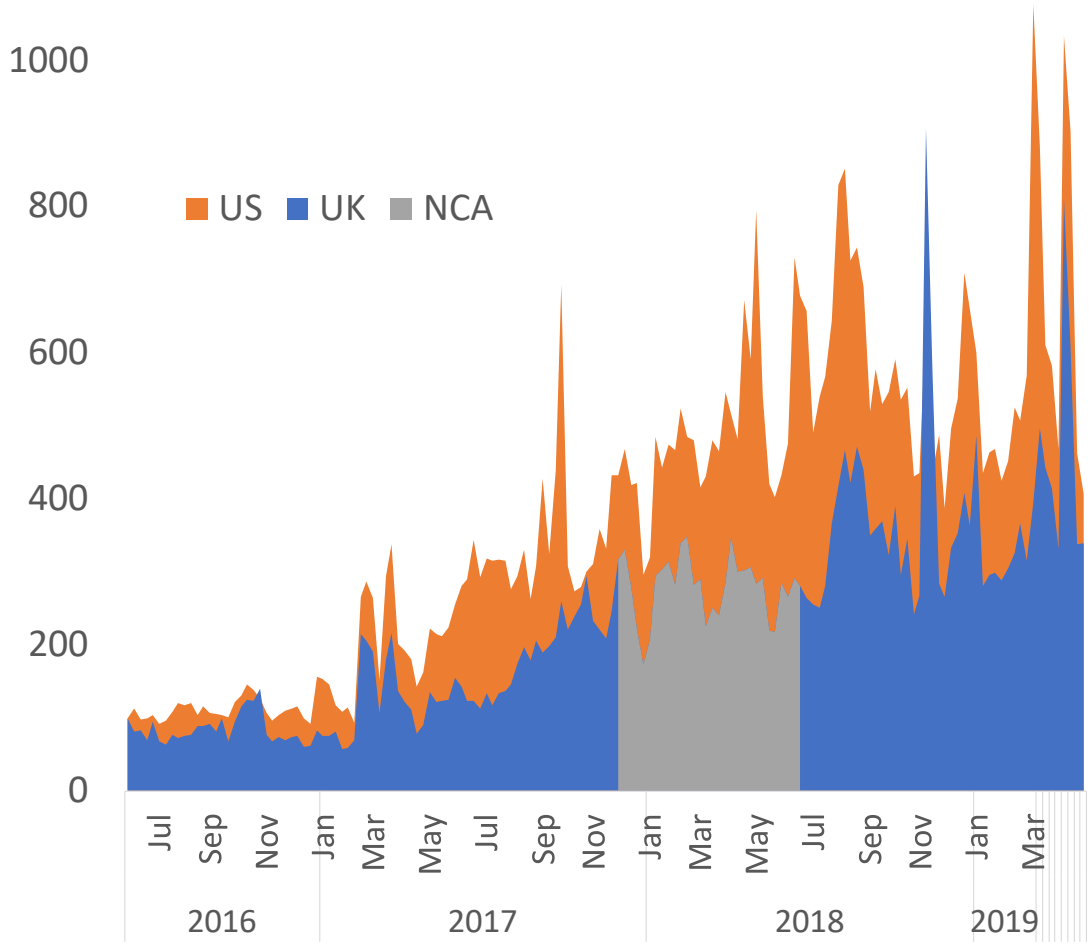

Figure 3. US and UK attack counts comparison. Non-stacked graph with totals scaled so both start at 100 in June 2016, with 200 representing a doubling. The NCA advertising intervention period which affects the UK data is highlighted in grey.