Modelling the Cybercrime Cascade Effect in Data Crime

Maria Grazia Porcedda,
School of Law, Trinity College Dublin,
(maria-grazia.porcedda@tcd.ie),
0000-0002-9271-3512

David S. Wall,
Centre for Criminal Justice Studies, University of Leeds,
(d.s.wall@leeds.ac.uk)
0000-0002-6003-1592.

2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) | 978-1-6654-1012-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/EuroSPW54576.2021.00025

Abstract[1]

This article contributes to the growing debate about the increasing importance of 'data' in modern cybercrime offending. In so doing, it illustrates the linkages between cyber-dependent and cyber-enabled crime bringing into focus the inability of current cybercrime legal categories to reflect such linkages which ultimately reflects how practitioners interpret them. Drawing upon data from court cases the article models the cybercrime cascade effect that results from data crimes. We argue that cybercrime is not a single action, but a process of interconnected social and technical actions in which data from 'upstream' cyber-dependent data crimes cascades 'downstream' to enable additional cyber-enabled crimes, such as scams, frauds and deceptions. By modelling the various tipping points at which stolen data cascades downstream we increase knowledge about the cybercrime ecosystem to highlight points at which interventions can be more effectively targeted. The 'cascade effect' is modelled by using mixed methods from law and criminology which include the "intermediate-N" configurational comparative method. By refining the tipping points of the cascade into decision trees, additional hypotheses, and the identification of the means to test them can be formulated. The article suggests that tipping points occur at each stage of the cascade model, however, the cascade into more crime is not found to be an automatic outcome as more social factors may be involved. Moreover, there exist layers of victimisation, which highlights the need to further research ways to incentivize early-offender interventions. Finally, the article illustrates the complexities of online offending, which include the presence of diverse, distributed and even disorganized actors within organised groups which do not easily fit into the traditional organized crime narrative.

Keywords— data crime, cybercrime, big data, cloud computing, crime decision trees, crime scripts, victimisation, criminal justice

I. INTRODUCTION: DATA CRIME AND THE EVER-CHANGING CYBERCRIME THREAT LANDSCAPE

'Data' creation and processing has become a massive industry in and of itself, creating economic opportunity that attracts cybercriminals as well as legitimate businesses. The increased monetary and strategic value of data has caused it to become an integral part of the cybercrime threat landscape. Arising from increased network connectivity and data processing driven by cloud computing technologies, data is not only generated by modern applications to enable them and the wheels of commerce to turn, but it has also become a valuable commodity which can be sold or traded and an industry has developed around it [1, 2]. Data, particularly of a personal nature, are therefore a popular target for offenders who deliberately 'steal' [2] and trade the data via deep web marketplaces for profit [3-5]. The data are, we argue [4], then used for committing further cybercrime (e.g. phishing, spamming, scamming, doxing)[6, 7] or for use in developing the cybercrime ecosystem, for example, targeted spamming in cybercrime-as-a-service [8-12].

Not surprisingly, data 'theft' (exfiltration) is now central to most modern cybercrimes, either directly as the focus of crime, or indirectly as a facilitator. Not only has there been an overall increase in data breaches [13, 14], but data-related attacks have become more diverse, for example, major ransomware attacks now routinely involve data exfiltration prior to encryption [15]. Furthermore, hacking is now the main cause of data loss [16]. This change reflects the increased appetite for accessing data for financial or intelligence gains [17]. Europol found in their successive IOCTA reports that Member States increasingly reported incidents relating to illegal acquisition of data [9, 18-20]. They also confirm that the illegal acquisition of data via data breaches not only disrupts businesses and organisations, but also facilitates further criminal activity [9, 18, 19].

We have previously argued [4, 21] that 'big' (or volume) data crimes [22] are 'upstream' crimes which can be subsequently used to hold for ransom [23], trade or sell on to other offenders for further criminal purposes. These (upstream) cyber-dependent cybercrimes, solely dependent upon internet technologies, subsequently 'cascade' crime downstream to enable cyber-enabled offences such as fraud, that use the advantages of the network, and even cyber-assisted cybercrimes which are simply facilitated by digital technology [24]. The cascade concept used here was developed independently, but can be connected to the work of scientists such as Pescaroli and Alexander [25] who sought to explain the cause-and-effect relationships that precipitate a chain-sequences of interconnected failures which are a feature of most catastrophic events - the toppling dominoes [25]. Once the cascade begins, it is hard to stop, in the world of data, once the genie is out of the bottle it is hard to put it back in.

The cybercrime cascade effect explains the role played by breached data in the changing nature of cybercrime. This cascade is quite hard to track and counter in practice, but we identify various tipping points where information and data cascade downwards to facilitate further crime. By catching offender actions at such tipping points, such as at the point at which data is sold on or dumped, then the subsequent downstream 'frenzy' of different types of cybercrimes could be prevented or at least mitigated.

[1] This paper was submitted for review on 7 May 2021

[2] 'Stealing' and 'theft' are used figuratively here. Digitised data does not have exclusive property features and thus they cannot be stolen to permanently deprive the owner of their use. N.B. this broader debate is beyond the scope of this article.

DOI 10.1109/EuroSPW54576.2021.00025

Contributing to a broader research project on the effect of cloud computing and large volumes of stolen data on cybercrime[3], this article complements our earlier work [4] to advance and add to the growing body of literature stressing the importance of 'data' in modern cyber offending [21]. The role of 'data' in modern cyber offending features in several multi-disciplinary debates upon which the cascade model draws. Here we contribute to three[4].

Firstly, investigations into criteria that can help dissect and conceptualise various cybercrime processes. In addition to the kill chain model, which we discuss in [4], relevant works include the cybercrime execution stack [26] and dependencies introduced by underground commoditization [27]. Hunton's cybercrime execution stack highlights the pivotal role of data in the cybercrime chain; here we show how offenders can engage in multiple choices that can break or enhance the cybercrime chain engendered by the cascade effect. Thomas et al.'s 'dependencies' [27] stress the faint links of operators of data markets; here we stress how such links are not a given and conceptualise tipping points that may nip the cascade in the bud. It is in this vein that the cascade model could add to crime scripts [8] analysis and preventative interventions.

Secondly, the cascade draws on and contributes to the human factor agenda [28, 29]. These include work on cybercrime harms [30], division of labour [31-33], as well as conceptualizations of specific forms of cybercrime [34, 35], which would assist in enhancing cybercrime prevention. Others have also usefully topologized different levels of offending [36-38] as well as the differential victim impacts upon individual and businesses [39], which includes combinations of online and offline offending [40]. Although not addressing these processes individually, we seek to join them together to model the overall 'cascade effect' and explore the role played by data crimes as upstream cybercrimes in their own right and also as a gateway to other forms of downstream cybercrimes. By means of anticipation, we defer to further work within the human factor literature to explain phenomena that are not adequately captured by the cascade effect.

Thirdly, and relatedly, we seek to add to substantive criminal law debates as to the adequacy of existing cybercrime categories, their interpretation, and the success of strategies of deterrence, as put into sharp focus by The Criminal Law Reform Now Network [41]. This article contributes to challenges to existing legal substantive offences by illustrating the linkages between cyber-dependent and cyber-enabled crime and bringing into focus the inability of current cybercrime legal categories to reflect such linkages, which ultimately reflects upon how practitioners interpret them. The consequences of the mismatch between the legal categories and the reality of the cascade effect upon sentencing and deterrence are beyond the scope of this paper.[5]

We refine our earlier findings by analysing a further 32 case studies to clarify the stages of the cascade effect and its likely 'tipping points' upon which law enforcement action could be focused, as well as drawing more insight into the process. Part II discusses the research design of this study. Part III sums up the cascade effect. Part IV uses the case studies to model the cybercrime cascade effect, discuss findings and illustrate their limitations. Part V focusses on the cascade effect's applications for shaping and applying investigative resources, before concluding.

II. RESEARCH DESIGN

In the first cascade paper, our primary analysis was a deductive, in-depth study of the TalkTalk data breach, drawing upon open-source information [4]. This breach is now fully researchable because the legal processes relating to the case have now completed and are matters of public record. The case enabled us to understand the processes of victimisation, the response of the criminal justice system and it also offered insights into possible incident prevention. Importantly, it also helped us to elaborate our early cascade hypotheses [21] to help identify deductively the tipping points that we frame as 'ideal types'. Here we augment the analysis with "intermediate-N" cases inspired by the configurational comparative method [43]. More specifically, we aim to develop the cybercrime cascade effect further to explain the role played by data in the changing nature of cybercrime.

By drawing upon case studies and mixed methods of analysis from law and criminology, we seek to create generalizable models of the processes involved in cybercrime to assist the criminal justice response [44]. Our choice of case studies was dictated by the need to access narratives of cybercrime-related offences and the responses by the criminal justice system. Because of a lack of data on cybercrimes and the difficulty in accessing official data, we relied on a variety of sources. The case studies were selected from two open access databases that aggregate cybercrime-related cases. The first was Hutchings' Cambridge Computer Crime Database [45], which contains news reports of arrests, indictments, convictions and sentencing of individuals mostly for computer misuse offences. The second was Turner's detailed database of individuals prosecuted under the Computer Misuse Act 1990 [46]. Further observations were drawn from a range of secondary data gathered through open source research (primarily news reports of the cases), plus primary data in the guise of court transcripts (sentencing remarks) obtained on application from English Courts.

Using a grounded theory approach [47], our data was collated from two open source databases [45, 46]. This resulted in more than 550 entries clustered into a group of 247 cybercrime incidents. We performed purposive sampling [44] on them by selecting only cybercrime cases that were resolved (170 entries). We then selected cases for which we had confidence that there was a cloud related aspect (for example, evidence of the use of cloud computing[6], or cloud computing applications such as Software as a Service (SaaS))[7]. Next, we explored cybercrime cases that primarily involved data crime, at both upstream (data crime) and downstream (after being sold on) levels.[8] The three attributes allowed to narrow the

[3] This work is part of the EPSRC CRITiCal Project (EP/M020576/1) funded by the CONTRAILS programme. See funding acknowledgments at rear of article.

[4] The cascade model intersects and contributes to multi-disciplinary literatures on data breaches, though the subject is not addressed as prominently as in [4] and [21].

[5] They are analysed in details in [42] under review.

[6] E.g. there was reference to logs or content of conference calls, emails or social networks communications.

[7] E.g. the use of named VOIP services, named webmail services, named social networks, stressors for-rent etc.

[8] This was assessed through the analysis of news reports of court cases; this was typically but not only identified based on the presence of 'data' (big or small), both at upstream and downstream level, that is cyber-dependent and cyber-enabled/assisted crime respectively.

search down to 34 'cybercrimes incidents' concerning 101 individuals, which were further sampled on the basis of the fourth attribute: availability of sentencing remarks. As the 34th case was not transcribed, we were left with 33 cases [42], listed in tables I and II in section IV.

As explained earlier, the cases discussed here are a mix of upstream and downstream cybercrimes that displayed prima facie cascade features. We carried out an inductive examination of the 33 cases based on a combination of news reports of court cases [9] and, where available, sentencing remarks, and collated them into a dataset (Annex I). Using Qualitative Comparative Analysis (QCA) [10] [43] we qualitatively investigated "intermediate-N" with three objectives in mind. The first was to ascertain the presence of the cascade effect we earlier conceptualized in our TalkTalk case study. The goal was to reach a crisp set, whereby the value can be either Y=cascade or N=no cascade. However, since the absence of complete information means that the value cannot always be univocally found, we used nuanced, fuzzy-like[11] values instead (see section IV and Annex I). The second objective was to pinpoint cascade patterns across the cases and interpret such patterns where possible, particularly as court records can reveal various explanations of the defendants' actions. Cascade patterns are illustrated by describing whether, for each step of the cascade ladder, the tipping point is reached, using again a fuzzy-inspired set (see section IV and Annex 1). The third objective of the analysis was to model the cascade effect by refining its steps into decision trees which help draw out and explain the different offender actions and identify layers of victimisation. The analysis and decision trees are discussed in section IV, but firstly we summarise the cybercrime cascade effect as conceptualized in [4].

III. THE CYBERCRIME CASCADE EFFECT: FINDINGS FROM THE TALKTALK CASE STUDY

In our 2019 [4] case study we demonstrated how completely unrelated individuals who had no desire or intention to collude can collaborate through hacker and other forums to inspire, and even mentor, each other to perpetrate a range of harmful cybercrimes. This type of collaboration allows two or more offenders to scale up the volume and range of cybercrimes to increase the impact of victimisation. The cascade model describes the social enablers that create multiple, overlapping offending chains and comprises of six fundamental stages, which are summarized below.

Stage 1 is where a vulnerability is either identified, learned, or created. The identification of a vulnerability becomes a data point in and of itself – knowledge of a vulnerability has a saleable value [49]. Either the actor does not disclose the vulnerability (in which case nothing happens) or they use it themselves, sell it or inform others. In the latter three instances the first tipping point is achieved thereby precipitating Stage 2, which is about deciding how to run an exploit to take advantage of the vulnerability. If the offenders take criminal advantage of the vulnerability by various technological means that may involve brute force or by illegally obtained access credentials (credential stuffing), they reach stage 3 where the offender acts on the outcomes of the exploit and decides how to dispose of the data. Having exfiltrated the data and made it unavailable to the legitimate users, offenders may either use it themselves to name and shame (dox) victims into paying a ransom [23], or they may make it public (dump) to make a political point. As an alternative, they may also sell the data, especially if it is of commercial value to others, which takes them to Stage 4, where offenders trade the data obtained from the exploit for financial or other gain. Offenders can either use the data themselves, or trade or sell it on a dark web market [8, 50].

Stage 5 is where the initial data is refined and improved, in quality, quantity or both, to use for further offending. Bought or traded data may be developed to increase its value and potency by aggregating or refining it, thus creating new insights which add value to it [51]. At Stage 5 the data may be reduced in number but becomes more powerful and its value increases. This stage also introduces new types of criminal actors into the field, especially those motivated by economic or political gain. Attackers could either use this information themselves to name and shame victims as in stage 3 (but as different actors and possibly for different reasons) or put the data up for sale in a refined state, thereby creating another tipping point and feeding the cybercrime cycle. In this cycle, several different criminal actors can work on the same data sets and develop it independently for different criminal outcomes.

Finally, stage 6 is where scammers, completely unrelated to the initial data crime (or the original hackers or data sellers) exploit the media frenzy and public confusion caused by the initial data crime, especially following a widely publicized data breach. This tipping point is reached when offenders actively build upon media driven public concerns to try to socially engineer victims. Sometimes referred to as pretexting [52], offenders deceive their victims into giving personal information or money. An example of this was found in the TalkTalk case study when offenders posing as cybersecurity experts working for TalkTalk contacted the public blindly offering to remedy the consequences of the breach, but really seeking to defraud victims.

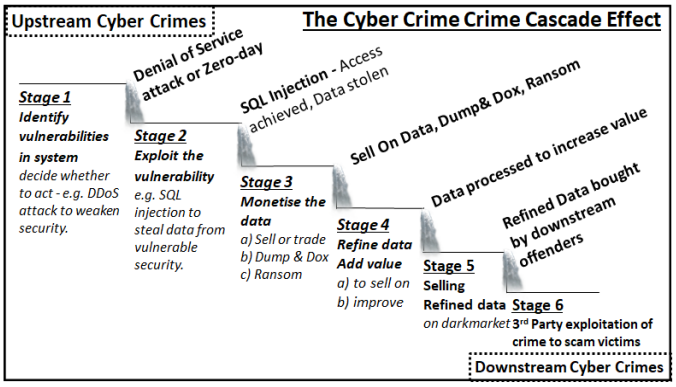
Figure 1 illustrates the relationship between the six stages and tipping points outlined above. Stages 1-3 of the cascade are upstream cyber-dependent crimes. Steps 4-6 are, by comparison, downstream cyber-enabled or cyber-assisted crimes. It is important to reflect here that we have presented them in a cascade form for explanatory purposes. As stated earlier, they are ideal types that explain variations in practice at different points in the flow of crime downstream and as such, they may not be exactly reproduced. In practice, different stages can each become a particular end-game, an independent kill-chain [17] or execution stack [26], or they can occur in different orders, or in parallel. It may even be the case that a stage may be skipped.

[9] As newspaper records are a matter of public record, this research and the cascade findings can be replicated. Note that the articles may no longer be available on the web, as discussed at [48].

[10] The method is inspired by QCA because, for this paper, we did not rely on QCA software. QCA is a method that allows to investigate "intermediate-N" (between 5 and 50) qualitative cases in a way that pinpoints cross-case patterns, typical of quantitative approaches, and allows for theory-testing.

[11] We were inspired by a fuzzy set logic, whereby cascade could be defined within the interval of values [0, 1] and expressed it as strings for clarity of exposure.

Fig. 1. The cybercrime cascade effect



Each of the six tipping points involves different forms of interaction between offenders, such as chat forums, underground data markets, cybercrime-as-a-service, the actions of a monetiser and their networks of money-mules to turn cryptocurrency into fiat money and then launder it, which underlines stages 1-6. These 'pinch points' are locations where law enforcement, crime prevention and regulatory resources can be directed to make for more effective action.

The hallmark of the cascade effect is that a 'cybercrime frenzy', for want of a better description, arises as the data drives one type of cybercrime, then another. This sudden increase in bulk-victimisations can overwhelm law enforcement who then find it hard to know which victims to prioritize and respond to quickly - let alone plan for in the future. Our argument is that it would be more effective for the law enforcement (and cybersecurity) lens to focus upon the tipping points of the cascade. This would enable them to quickly respond to the various stages of cybercrime and, importantly, the different groups of offenders who commit upstream and downstream crimes against different victim groups.

IV. MODELLING THE CASCADE EFFECT: USING INTERMEDIATE-N CASE STUDIES TO REFINE THE FINDINGS

In this section we draw upon newspaper court reports and court records (sentencing remarks) to analyse the 33 cases together, that is the TalkTalk case (#33) [12] (Appendix 1) plus the other 32 cases to: (i) ascertain the presence of cascade effect, (ii) pinpoint cascade patterns across the cases and, where possible, interpret such patterns and (iii) modelling the cascade effect by refining its steps into decision trees which help draw out and explain the different offender actions and identify layers of victimisation (section B).

We address variations in practice by representing them through a dataset inspired by QCA [43] (See Annex I). Tables I and II present the outcomes for the case studies, divided in two groups, depending on whether sentencing remarks could be accessed or not (discussed at [42, 48]. The first column lists the case number (TT, which is case #33, stands for TalkTalk), which will be used throughout the article and the second lists the case name, when available. The third column lists the presence of a cascade (N, N*, ? , Y*, Y). A star symbol (*) means that additional information is needed to confirm the finding. This is particularly the case when either common wisdom or additional information, such as pre-sentencing reports, might lead to question the finding. Therefore, N* is a weak no, whereas Y* is a weak yes. A question mark symbol (?) indicates that the data does not allow to make a firm decision about the case. The outcome (cascade) is, therefore, indeterminate.

TABLE I. CASES FOR WHICH SENTENCING REMARKS COULD NOT BE ACCESSED

Case No	Case Name (or identifier)	Cascade
2	Pair at Harrow Crown Court	N
3	R v Jay Moore	Y
5	R v Vovks, R v Zolotenkovs	Y*
7	R v Hameed (Fizzy)	N
8	R v unnamed, Darlington Borough Council	?
9	R v Buchanan,	Y
12	R v Anderson,	?
14	R v Sergejev,	Y*
20	R v Agrigoraie, R v Savoae	N*
21	R v Kareem, Alonge, Fafore	N*
22	R v Babatunde	N*
23	R v Etu	N
25	R v McLouglin	N*
26	R v Woo	?
27	R v Rigo	Y*
28	R v Yücel	Y
29	R v Cyganok, Zavrevski, Krummins	N*

a. Y= cascade; Y*= likely cascade; ?=indeterminate; N*=unlikely cascade; N=no cascade.

TABLE II. CASES FOR WHICH SENTENCING REMARKS COULD NOT BE ACCESSED

Case No	Case Name (or identifier)	Cascade
1	R v Cassandra Mennim, R v Edward Pearson	Y
4	R v Jennifer Hallam, R v Sean Benson	Y
6	R v Ayotunde Akinwolemiwa	N
6A	R v Joseph Onoriode Ogbogbor	N
10	R v Nazariy Markuta	Y
11	R v Matthew Beddoes, Jasdeep Randhawa and Jandeep Sangha	N*
13	R v Junaid Hussain	Y
15	R v James Jeffery	N*
16	R v Jake Davis, R v Mustafa Al-Bassam, R v Ryan Ackroyd, R v Ryan Cleary	Y

[12] The last individual convicted in relation to the TalkTalk breach was only sentenced after the publication of our TalkTalk case study. This is also the last sentencing remark we were able to collect.

Case No	Case Name (or identifier)	Cascade
17	R v Lewys Martin (appeal)	Y*
18	*R v Gediminas Simkus, R v Volodymyr Kurach*	N*
19	R v Tomasz Skowron,	N*
19A	R v Piotr Ptach	N*
24	R v Rilwan Adesgun Oshodi and Anor, Annette Jabeth and Abdul Hamid, R v Shaharyar Butt, R v Chika Okala, R v Sharna Eve,	Y
30	R v Karina Kostromina, R v Valerij Milka, R Iryna Prakochyk	N*
31	R v Grant West	Y
32	R v Shaun Turner, R. Mcdonagh; D. Drage; Z.	Y
TT	R v Conor Allsopp (appeal)	Y
TT	R v Daniel Kelley	Y

b. Y= cascade; Y*= likely cascade; ?=indeterminate; N*=unlikely cascade; N=no cascade.

The names and parties of the court cases are a matter of public record and are used to identify cases and enable the scholarly community to replicate the research and verify the findings.[13] In the following we discuss the outcome of the analysis (section A), identify new findings and refine the cascade effect with decision trees (section B), and discuss some limitations (section C).

A. Explaining the outcome: analysis of the dataset

Cascade occurs whenever at least one tipping point is reached; in some cases multiple tipping points are reached (in TT, all tipping points were reached). We assume the presence of cascade both when data from a tipping point is used by people other than the offender and when the offenders create tipping points themselves. In the former, defendants exploit a vulnerability after purchasing data or tools to exploit vulnerabilities, as we discuss below. The full dataset is available in Anne I, and summarized in Table III. The table shows aggregate data from the cases. Since some cases reach multiple tipping points, while other cases reach, the total number of tipping points reached does not have a bearing on the total number of cases with cascade. Furthermore, the numbers are not an indication of the volume of breached data: data exfiltrated differ in size and content, for example, one case may contain hundreds of millions of personal data.

In keeping with the, often patchy, nature of cybercrime data, there are some cases where the outcome is obscured by the absence of relevant information, as in case 27. Here the defendant allegedly created a manual for SpyEye, but news reports do not clarify the circumstances surrounding its release. As stated earlier, for a few cases an outcome or assumption could change as further information is obtained. An example is case 5, whereby, according to news reports, the login credentials used in the exploit were "harvested through data breaches from other sites" [54], but it is unclear whether the defendants performed the data breaches themselves or acquired dumped data. We address the issue in section C.

TABLE III. CASCADE DATA SET - SUMMARY

33 Cases	Yes	No	Uncertain	
Stage 1	32	1	0	UPSTREAM
Tipping Pt	6	22	5	
Stage 2	31	0	2	
Tipping Pt	4	21	8	
Stage 3	29	2	2	
Tipping Pt	6	25	2	
Stage 4	8	21	4	DOWNSTREAM
Tipping Pt	7	22	4	
Stage 5	27	4	2	
Tipping Pt	3	24	6	
Stage 6	5	27	1	
Tipping Pt	4	28	1	
Tertiary Crimes	10	20	3	
CA	16	14	3	

c. N.B. starred yes's and no's concatenated. Also please note that this table is a summarised version of a larger table that was too large to show here. Tertiary crimes stands for monetisers.

There are also other cases where a tipping point is formally reached but the outcome (cascade) is not observed; this is marked with a n*. In case 5, the proceeds of the exploit were used to purchase tickets for musical events and then resell them; in case 11, the proceeds of the exploit were put up on sale and traded, but the exploit concerned carbon credits, which could not lead to further exploits. Similarly, in case 29 the proceeds of crime went into purchasing luxury goods for resale. In such cases, upstream crimes lead to traditional crimes, thereby breaking the data crime chain.

Previously, we found that cybercrime-related threats, risks and harms are a function of the vulnerability of technology, the availability of valuable data, and the information contained in the data [4]. The tipping point of stages 3-5 is therefore likely to depend upon the type of information contained in the data on the case study. In other words, if the data are of value, but the information cannot be put back into data crime, then this is unlikely to generate a cascade of the type we analyse here (among others, cases 6, 7, 18 and 19). Conversely, if the data are of value and the information can be used (processed) to create further data crime, this is likely to lead to a cascade (see, among others, cases 3, 9, 10, 13, 16 and 31). This is expressed as the vicious cycle of monetisation connecting stage 2 and 3, which we elaborate upon in the next section. But, however, while this seems necessary, it is insufficient to generate the outcome.

As stated above, offenders may decide, for example, not to feed the proceeds of crime back into data crime, especially if the operations of individuals or a group stay confined within the group. In such situations cascade is less likely to happen. Most cases without a cascade outcome seemingly display some wider organized crime-group features. Half the cases with no cascade (7 out of 14) feature the presence of money

[13] By means of disclaimer, all cases discussed here were reported by recognized media outlets. The only restrictions we are aware of concern case 7 and were reported as being lifted [53]. We therefore assume the information is not subject to reporting restriction orders and consequently that no material appearing in this paper is in contempt of court. We kindly ask any reader who knows otherwise to contact us (the authors) promptly. The names of parties to the proceedings are personal data and a matter of public record. As far as we are aware, only the keywords for this article will be indexed; therefore a search conducted on a search engine of the names of the parties to the proceedings mentioned in these pages should not produce a link to this article. Case law on the right to be forgotten, as laid down in the General Data Protection Regulation and the UK Data Protection Act 2018, has yet to clarify the remit of the right to delinking of personal data contained in scholarly publications.

mules, which may therefore be an indicator of the presence of an organized criminal group (3, 5, 6, 7, 11, 18 and 29). In detail, of the 14 cases with N outcomes, there are 5 cases without mules, 7 with mules and 2 for which a definite finding cannot be made. Of the 16 cases with Y outcome, there are 11 without mules, 3 with mules and 2 with indeterminate mules. None of the 3 cases with a question mark outcome shows the presence of money mules. In other words, there are 10 cases with mules, of which 7 with N outcome and 3 with Y outcome. Of the 16 cases without mules, 5 have N outcome and 11 with Y outcome. Of the 7 cases in which it was unclear whether there were mules, 2 feature Y outcome, 2 N outcome and 3 indeterminate outcome. The question remains as to whether these are traditional sustained organized criminal groups or a new ephemeral form of online crime groupings. While indications available for these case studies are of the latter option, it is for further research that frames the findings within the broader human factor agenda [19, 27, 33], as well as work on money laundering [55], to corroborate this finding. Regardless of structure, they rely on the existence of cascade at an earlier point, and these are the cases marked as N*.

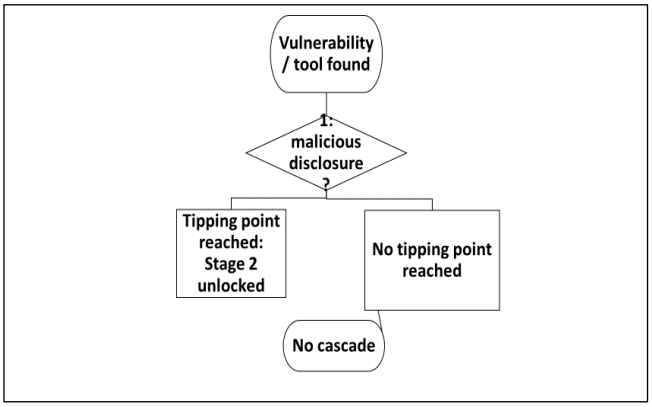
In sum, the cascade is useful to explain cases where the data is fed back into offending. The reason why offenders stop monetizing data and break the cybercrime chain needs to be thoroughly investigated. Our preliminary observations point to the importance of motivation for the offender, but the data we collected do not enable us to make firm conclusions about motivation; the full suite of court data may be needed to this effect. Anyway, we acknowledge that this calls for a new model altogether, which is for future work fitting within the broader 'human factor' agenda [28] to develop.

B. *Refining the cascade model (2): decision trees, the monetisation cycle and layers of victimisation*

Below, we briefly discuss some of the cases to highlight additional elements of the cascade, namely the monetisation cycle, monetisers, layers of victimisation and define (offending) decision trees. A full diagram assembling all decision trees is contained in Annex 3.

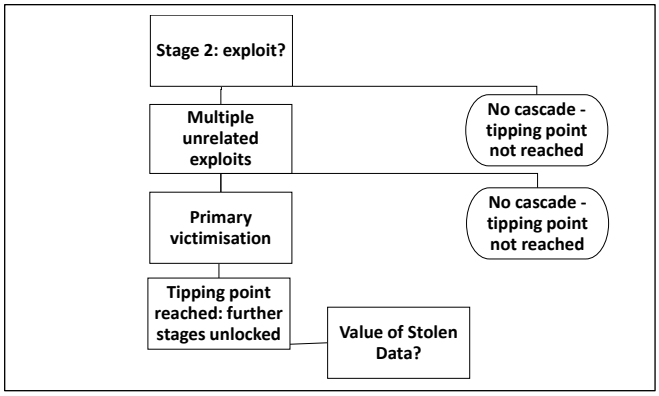
Stage 1 Identifying the vulnerability - The first step of the cascade model covers the dissemination of a vulnerability. However, this may be too restrictive an approach that risks excluding relevant real-life situations for cascade. This is the case of Pearson [56](case 1), who was sentenced in 2012 under the Fraud Act for hoarding eight million personal data filling in 67.500 double-sided A4 [57]. Court records show that Pearson used the banking Trojan SpyEye to capture personal information (usernames and passwords) and that he "made or adapted a Python script to automate multiple logons into PayPal accounts, to confirm the usernames and passwords and the available funds in the accounts", for which he pleaded guilty under Section 7 of the Fraud Act [56]. Those same records seem to show that Pearson shared his script for free with other computer programmers, without "knowing whether those computer programmers might use this information in fraud", which Recorder A Mulligan found "troubling" [56]. By analogy, this stage includes not only dissemination of knowledge of a vulnerability, but also creation and dissemination of tools to exploit vulnerabilities. This leads to the decision tree illustrated in Figure 2.

Fig. 2. Stage one of the cascade effect



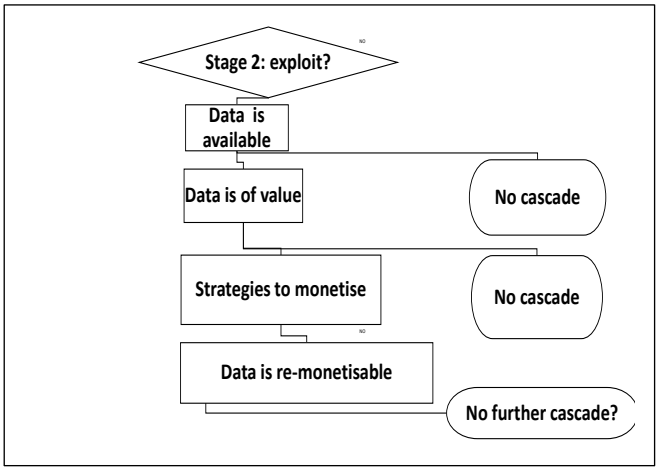
Stage 2 Deciding whether to exploit the vulnerability - As discussed earlier, multiple offenders exploiting the vulnerability is a tipping point triggering the cascade and subsequent crime frenzy. Figure 3 illustrates the decision tree. As currently formulated, this tipping point is always tied to stage 1 (either as a cause or a consequence) and therefore its heuristic value might not be as strong for the criminal justice system. However, this tipping point may be of great relevance to the primary victim: if the vulnerability can be fixed and this is done quickly enough, then logically the tipping point is not reached. This is a point of strong overlap between the cascade and the kill chain model [17] and intersects broader debates on responsible vulnerability disclosure [58].

Fig. 3. Stage two of the cascade effect



The monetisation cycle - If individuals decide to exploit the vulnerability, they have the chance to weigh up the potential value of such a vulnerability and decide accordingly how to exploit it. If, for example, it yields valuable data/ information, offenders may monetise the data by sale or in some cases using it to levy a ransom. In so doing, they also unlock stages 3, 4 and 5 of the cascade. So, the heuristic value of stage 2 may be more relevant in understanding how the offenders will use the vulnerability.

Fig. 4. The monetisation cycle

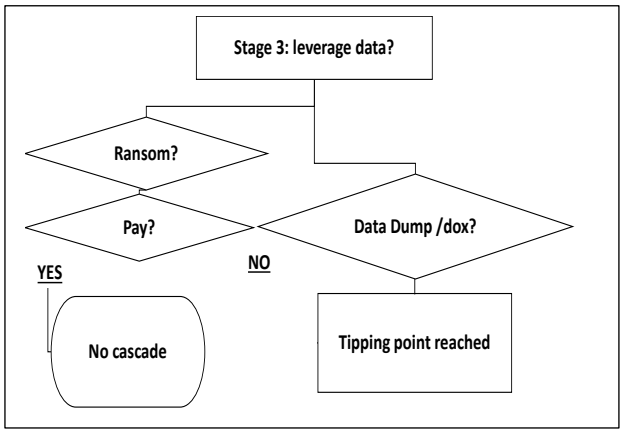


The monetisation cycle depends both upon the availability of valuable information and the decision of the offenders to make it available through a variety of channels. Based on the available information about the cases, the decision of how to monetise the data seems to be tied to the motivation of the offender. If further data (e.g. in the guise of pre-sentencing reports) confirmed this observation, it might represent a useful point of intervention. As stated earlier, futher research is needed to ascertain the precise role of monetisers and their mules.

Stage 3 Acting on the decision on how to exploit the vulnerability - The tipping point in stage 3 is dumping and/or doxing, possibly preceded by demanding a ransom. In some cases, attackers may demand a 'political' ransom, as in the campaigns led by the collective Anonymous, failing which the hacker threatened to publish the exfiltrated data. Irrespective of the request for ransom, the offender(s) may dox for political, moral, reputational or recreational purposes, or a mix of these. In passing sentence against the four members of the hacker group LulzSec (case 16), Judge Taylor said "the name LulzSec encapsulates your desires to cause embarrassment and disruption, while keeping your own identities hidden. You each played your role … using your technical abilities to cause catastrophic losses for amusement" [59, 60]. LulzSec dumped data "including staff usernames and passwords from News International" causing substantial losses even if their "motivation was not financial" [59, 60].

Another case is that of Junaid Hussain, the now-defunct leader of the hacker group TeaMp0isoN. He breached the Gmail account of Ms Kay, the former personal assistant of Prime Minister Tony Blair and subsequently doxed 150 contacts, including email addresses and private phone numbers of Mr Blair, his wife and sister-in-law, as well as contacts in the House of Lords and Parliament [61, 62]. Junaid (case 13) was handed a six-month custodial sentence for an act motivated by "a bit of fun and humour" [63]. However, Hussain told "the probation officer that somebody suggested that Tony Blair's PA should be a target" [63]. The nature of that 'someone' remains unknown, but as a result this case seems to have both recreational and political motives. This is exemplified in the decision tree in Figure 4. Stage 3 features secondary victimization, whereby the victims include not only the breached party (e.g. an organizational database), but also the individuals within that database to whom the data relates (the data subjects).

Fig. 5. Stage three of the cascade effect



Stage 4 Selling or trading data illegally obtained using the vulnerability - Instead of dumping the data, offenders may want to trade it, notably for financial reasons. This typically happens on hacker fora, such as that operated by Markuta [64, 65](case 10). Markuta's forum hosted the dump of 500 million customer email addresses and passwords from Yahoo! Voices [65] obtained by the D33Ds Company hacking group, of which he was reportedly a member [64].

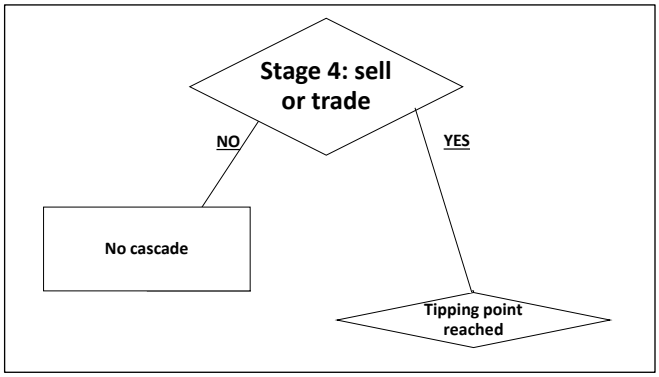
Offenders (typically fraudsters) purchase the data to defraud or otherwise victimise, especially financial data which allows frauds such as carding (trafficking fraud devices), card-not-present and account takeover to take place. Benson and Hallam, for instance, purchased stolen data from Russian operators which would have enabled them to take over at least 2000 bank accounts [66, 67] (case 4). By means of example, Oshodi and Jabeth were able to defraud a British lady of her life savings after purchasing her banking data from a phisher [68, 69] (case 24).

Offenders may also want to resell the data, so long as there is someone willing to buy it. Babatunde orchestrated a phishing campaign whose proceeds were sold on data markets [70](case 21). In the absence of court records[14] it is not possible to know where the phishing material came from, and therefore it cannot be excluded that it resulted from a data breach.

As in stage 3, selling or trading the data involves secondary victimisation, that is individuals can be victimised because of the initial exploit, because their information is leaked. This cycle keeps creating a cascade effect, whereby a single cyber offence spurs several offending opportunities. This provides an area of overlap between stage 4 and 5 which is a potential weakness of the model.

[14] As discussed at [42]and[48].

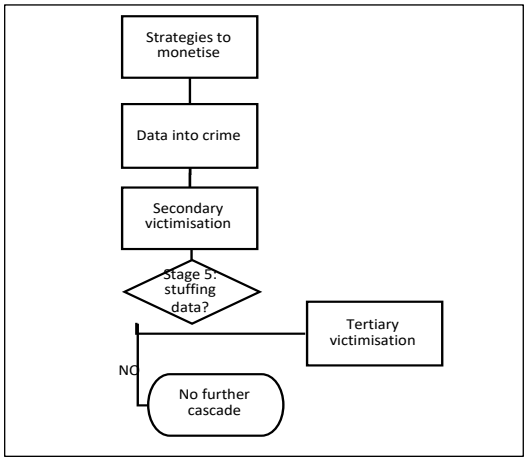
Fig. 6. Stage four of the cascade effect



Stage 5 Increasing the quality of the data pool for further exploitation - This stage is about increasing the quality of the data and putting it into more crime. Sometimes the offender may not be motivated by their financial acumen. For instance, the information in Pearson's possession could have 'earned' him almost a million pound, whereas he exploited a small fraction to pay for hotel breaks with his girlfriend. Recorder Mulligan poignantly said "I accept you did not think through the consequences. This is an unusual case, it seems to me, because your involvement in this, in some ways stupendous criminality with the extent of the information that you had available to you, does, it seems to me, appear to be less about your own personal financial gain and more about the intellectual challenge, because otherwise it just does not add up really" [56] (case 1). Other times such behavior is motivated by financial acumen. Benson and Hallam made above a million pounds off at least 700 victims and laundered the proceeds through a fake company [66, 67] (case 4).

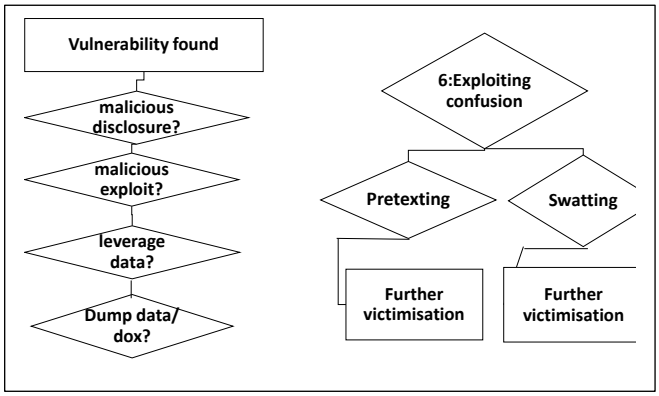
The tipping point of stage 5 is adding credential stuffing to the data and this is observed across the cases. An example of a professional stuffer is 'Courvoisier', possibly also in relation to the TalkTalk breach as he appeared to promise more information than was revealed to have been breached by news reports and the Information Commissioner's Office [71]. The sentencing remarks mention some of the companies targeted by West, such as Sainsbury's, Argos, Ladbrokes, Uber and Asda, and focus on the example of JustEat [72] (case 31). Judge Gledhill explained how West breached into the Just Eat servers and obtained details of more than 160,000 customers. In collaboration with individuals met on the dark web, West sent phishing emails to customers asking them to complete a survey against the promise of a small reward worth £10. To deliver the reward, the survey asked for those individuals' bank accounts, which many provided, and which West collated and sold on the dark Web using the Courvioisier profile. The information was priced in bitcoins according to the amount of data available in the bank account of potential victims. In order to maximize victimisation, not only of JustEat customers but of all customers, West used malware Sentry MBA [72] to attack login frames. Security expert Temple explained that "while Sentry MBA is being traded on hacker forums, the real value is in combo and config lists, which contain user credentials for websites" [73]. Another apprehended stuffer was 'tetereff', a.k.a. Andrei Sergejev, who, based on news reports, seemed to trade stuffed stolen financial data online [74] (case 14). Moreover, stage 5 could lead to tertiary victimisation, due to the identification of a new pool of potential victims via credential stuffing.

Fig. 7. Stage five of the cascade effect



Stage 6 Tertiary exploitation of a publicised incident - Besides pretexting, discussed in section III, dissemination of news about successful data crimes may also lead to 'swatting', whereby offenders send emergency services to unwitting individuals whose contact information is doxed via data crime. This is what happened after the breach and dox of 3,000 Mumsnet accounts by hacker collective DadSec, which was made possible by a script created by David Buchanan, who was subsequently sentenced [75, 76](case 9).

Fig. 8. Stage six of the cascade effect



Beyond stage 6. Monetisers, the criminal group and tertiary crimes - A further 'crime stream' underlying stages 3-6 are the monetisers who help to facilitate downstream crimes (and possibly some upstream). They launder money, extract or broker cryptocurrency from crimes. Depending upon the scale of the crime, they may either turn Bitcoin and other cryptocurrencies from ransomware into fiat money, or employ money mules to extract money in cash from live accounts via ATMs, or else transfer money in short-term legitimate accounts that they 'loan' or set up specifically for the purpose. For instance, Hameed relied on a network of monetisers to launder the proceeds of his exploit. The offender, known as Fizzy, created the vulnerability himself, though it is not clear how he obtained the thousands of numbers he used to call RBS customers and trick them into disclosing their banking details (case 7).

We argue that the presence of monetisers might be an indicator of the presence of organized criminal groups, but this is a circumstantial observation which further research needs to establish. In our dataset, the absence of cascade seems to be associated with offenders that keep their exploits within a particular offender group. One such case is that of a trio (case 23) that was in possession of 70 million customer email addresses and information of 30,000 bank customers. The offenders created the vulnerabilities to be exploited themselves, in this case by disseminating more than 2,600 phishing pages mimicking banking websites and waiting for phishing-enabled social engineering to play its part.

Two observations are that the absence of cascade seems to be associated with the use of social engineering and/or organised crime-like features (cases 19 and 19A), even though, as mentioned earlier, offenders acting like tight crime groups may actually base their activity on existing cascade. Based on the above analysis, the cascade model can be refined as illustrated in table IV.

TABLE IV. CASCADE EFFECT, REMODELLED

Stage	Cascade	Tipping point
1	Learning about a vulnerability/ creation thereof	Disseminating the knowledge
	Software on sale to exploit vulnerability	
2	Exploiting the vulnerability	Exploiting the vulnerability by multiple individuals
	Software bought to exploit vulnerability	
3	Valuable info obtained (dump)	Doxing or ransom + dox
4	Putting up data for sale	Information sold
5	Retaining information for (future) use	Data stuffing for resale
6	Attack is publicized	Pretexting or hoaxing
7	Monetisers	Use of money mules

C. Limitations of the Study

The study has limitations, some of which are inherent in the subject matter: two of our sampling criteria – cloud and data – are fuzzy and their contours cannot always be traced with precision. In the cases analysed, the cloud, for example, could be both the target of an attack as well as its enabler. The sample of cases used here is also not representative, because there is no defined population as there are no official statistics on data crime [41]. Because of the 'patchy' statistics, the data set could also be analysed by using 5-variable fuzzy set analysis [43], where y=1, n=0, n*=0,33, y*=0,67 and ?=0,5, which could yield different interpretations to those we offered here (see Annex 2).

The model proved weak regarding stage 2, or with its ability to explain cases based on social engineering or organized crime-like features. In such cases data and the cloud are still present, but we do not observe cascade and crime frenzy. The use of case studies is for theory-building rather than for theory-testing, therefore more analysis is needed in future to validate/test the cascade effect as a model (and account for any biases), as this is an endeavor that requires a more robust and more broadly interdisciplinary effort.

Insofar as the news reports of court cases are available, the study can be fully replicated following the steps illustrated earlier. However, media reports are neither permanent nor easily available, and court transcripts can only be *accessed in situ* or obtained through lengthy and cumbersome transcript application procedures. These issues cut across the literature on court data [77] and media law, and have such vast implications that a separate discussion is necessary [42, 48].

Finally, the cascade is only useful to explain cases where the data is fed back into offending. The reason why offenders stop monetizing data and break the cybercrime chain needs to be thoroughly investigated. Our preliminary observations point to the importance of motivation for the offender further; however, we acknowledge that this calls for a new model altogether, which is for future work fitting within the broader 'human factor' agenda [28] to explain.

V. CONCLUSION AND THE WAY FORWARD

In this article, we have sought to explain the relational, rather than the technical side of how a cloud-based, data-rich technological environment is fueling data crime with multiple levels and outcomes of victimisation. While we complement existing narratives, such as 'kill chain' [17] and the MITRE ATT@ck framework [78], which emphasize technical solutions, or the cybercrime execution stack [26], we refine our original ideas using an intermediate-N, qualitative comparative analysis-inspired study to (i) ascertain the presence of cascade effect described in our 2019 article across the 33 cases [4], (ii) pinpoint cascade patterns across the cases and, where possible, interpret such patterns and (iii) model the cascade effect by refining its steps into decision trees which help draw out and explain the different offender actions and identify layers of victimization. These tipping points illustrate how upstream data-based cyber-dependent cybercrime can result in further cyber-enabled and cyber-assisted cybercrimes, thereby making contributions relevant to the study of cybercrime processes, preventative strategies, the conceptualization of offences and their interpretation in legal proceedings.

Current cybercrime legal categories appear unable to reflect such linkages, which, ultimately reflects upon how practitioners interpret them, as discussed in a separate contribution [42]. It is, however, for others to examine the links and contribute to existing criminological [79] and legal debate, also in light of calls for reforming the Computer Misuse Act 1990 [41].

Our analysis of offending patterns suggests that tipping points can occur at each stage of the cascade model, but in different ways and with very different implications. For instance, a cascade can happen not only when a vulnerability is disclosed, but also when tools to exploit this vulnerability (including cybercrime as a service) are utilized. The tipping point may also depend upon whether the information found is of value and fed back into the data crime cycle, which, in turn, we believe is linked to the particular motivation (e.g. economic, revenge, political) of offenders. Such interrelations, our data suggests, may not only define the different actor groups, but also shape the links between primary, secondary, and even tertiary victimisation, monetisation and the demographics of offending.

Our analysis of the data set finds that the involvement of monetisers may indicate the presence of an organized crime group on top of the other organized parts of the emerging cybercrime ecosystem – now a regular part of the offenders' ability to scale up levels of crime in order to make it pay [86]. Such finding reinforces the complexities of online offending identified within the broader literature, especially with the co-presence of diverse, distributed and even disorganized actors [80, 81] existing sometimes alongside organised groups which fit more into traditional organized crime narratives [82]. On the one hand, data-brokers who buy and sell data, darkmarketeers who provide the darkmarket facilities to sell the data, crimeware as a service operators (inc. Ransomware) who hire out software to facilitate data crimes, bullet proof hosters who host clandestine websites, crime IT skills brokers who write code all contribute to a cybercrime ecosystem which not only uses stolen data but also facilitates data crime [21, 83]. On the other hand, although the assumption that idealistic hackers choose to become career hackers when they realise that they can make a living from cybercrime seems to be logical and common sense, our study has found that the progression may be more nuanced, as demonstrated by R v Pearson (case 1). This suggests that criminal justice strategies of intervention designed for the "burly street criminal" such as prison [24] might be counter-productive or even have disastrous consequences, as evidenced by R v Hussain (case 13), whose encounter with the criminal justice system seems to have catalysed his decision to join ISIS.

Finally, the observed layered victimisation highlights the need to do further research into ways to incentivize early intervention to stop the cascade effect. An example is the data breach suffered by UK supermarket chain Morrisons who acted promptly on the doxing of payroll data of 99,998 employees by Skelton, their senior IT internal auditor. The data included names, addresses, gender, date of birth, phone numbers, national insurance numbers, bank sort codes, bank account numbers and salary. Skelton doxed the data on "a file sharing website" [84](§9) and CDs which he sent to local newspapers in the hope that they would also publish the data. Instead, the newspapers immediately alerted Morrisons which took "steps to ensure that the website had been taken down" [84](§11-12) to prevent outsiders accessing employees' bank accounts or stealing their identities [84](§11). The Morrisons case [85] is arguably best practice and is perhaps the antithesis of our original case study [66]. Testing the cascade effect against best practice not only helps to refine the model further, but also demonstrates its usefulness as a risk management strategy, which brings us to our last point.

Thus far we have used the cascade effect as a descriptive tool, however, by isolating and identifying the main tipping points and key offender groups we hope that the cascade model will help law enforcement to focus their resources upon key areas. One is to assist in the analysis of the overall seriousness of the offence. By identifying layers of victimization, and contextualising the motivation behind the offender's decision to reach one or more tipping points, courts could more easily identify aggravating or mitigating circumstances and choose appropriate sentences, as discussed in a separate contribution [42]. Also, by contextualizing the offender's decision to reach a particular tipping point, or conversely not to reach it, as in R v Buchanan (case 9), could be a useful indicator of the potential impact of displacement programmes which intervenes to catch potential cybercriminals very early on and divert them along more useful career tracks and away from prison.

A. FUNDING

This research is based upon work funded by the CRITiCal ('Combatting cRiminals In The Cloud' - EPSRC EP/M020576/1) and the EMPHASIS projects ('EconoMical, PsycHologicAl & Societal Impact of RanSomware' - EPSRC, EP/P011772/1).

B. ACKNOWLEDGMENTS

We thank our CRITiCaL project partners at Newcastle and Durham Universities and the various judicial agencies which have helped us in conducting this research. We also thank colleagues from the Centre for Criminal Justice Studies at Leeds, particularly Dr Adam Hardy [now at Leeds Beckett University], Dr Jose Pina-Sánchez and Dr David Churchill. We would also like to express our gratitude to the participants at the SLSA 2019 and BILETA 2019 conferences, whose comments have greatly helped in shaping this work. Needless to say, the views expressed in this article are our own views and not those of partners, funding agency or other participants in the project.

As part of the open-review model followed on WACCO this year, all the reviews for this paper are publicly available at https://github.com/wacco-workshop/WACCO.

REFERENCES

[1] Press Association, "Hacker jailed for selling Asda and Uber customers' data on dark web," in *The Guardian*, ed, 2018.

[2] S. Zuboff, "Surveillance Capitalism and the Challenge of Collective Action," *New Labor Forum,* vol. 28, pp. 10-29, 2019.

[3] E. D. P. B. (EDPB), "Guidelines 1/21 on Examples regarding Data Breaches, V1.0," 14 January 2021 2021.

[4] M. G. Porcedda and D. Wall, "The chain and cascade effects in cybercrime: lessons from the TalkTalk case study," in *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Stockholm, 2019.

[5] A. Hutchings, "Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission," *Crime Law Soc Change,* vol. 1, pp. 1-20, 2014.

[6] M. Levi, A. Doig, D. Wall, and M. L. Williams, "Cyberfraud and the implications for effective risk-based responses: themes from UK research," *Crime, Law and Social Change,* vol. 67, pp. 77-96, 2017.

[7] M. Levi, "Assessing the trends, scale and nature of economic cybercrimes: overview and Issues," *Crime, Law and Social Change,* vol. 67, pp. 3-20, 2017.

[8] A. Hutchings and T. J. Holt, "A Crime Script Analysis of the Online Stolen Data Market,"

British Journal of Criminology, vol. 55, pp. 596-614, 2015.
[9] Europol, "Internet Organised Crime Threat Assessment (IOCTA) 2018," ed, 2018.
[10] C. Bradley and G. Stringhini, "A Qualitative Evaluation of Two Different Law Enforcement Approaches on Dark Net Markets," in *Proceedings of WACCO 2019: 1st Workshop on Attackers and Cyber-Crime Operations, IEEE Euro S&P 2019*, Stockholm, Sweden, 2019.
[11] J. Saunders, "Tackling Cybercrime – the UK response," *Journal of Cyber Policy,* vol. 2, pp. 4-15, 2017.
[12] R. Wainwright and F. Cilluffo, "Responding to cybercrime at a scale: operation Avalanche – a case study," Europol2017.
[13] L. Whitney, "2020 sees huge increase in records exposed in data breaches," in *TechRepublic*, ed, 2021.
[14] Symantec, "Internet Threat Security Report 2019," Symantec2019.
[15] C. Cimpanu, "Here's a list of all the ransomware gangs who will steal and leak your data if you don't pay," in *ZDNet*, ed, 2020.
[16] IDTC, "2019 End-of-Year Data Breach Report, Identity Theft Resource Center," 2020.
[17] E. Hutchins, M. Cloppert, and R. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," Lockheed Martin2011.
[18] Europol, "Internet Organised Crime Threat Assessment (IOCTA) 2019," 2019.
[19] Europol, "Internet Organised Crime Threat Assessment (IOCTA) 2020," ed, 2020.
[20] Ponemon, "Cost of a Data Breach Report 2020," CAPITA2020.
[21] M. G. Porcedda and D. S. Wall, "Data crime, data science and the law," in *Research Handbook on Data Science & Law*, V. Mak, E. Tjon Tijn Tai, and A. Berlee, Eds., ed London: Edward Elgar, 2018.
[22] D. S. Wall, "How Big Data Feeds Big Crime," *Current History: A journal of contemporary world affairs,* vol. January, pp. 29-34, 2018.
[23] M. Krebs, "TalkTalk Hackers Demanded £80K in Bitcoin," in ***Krebs on Security***, ed, 2015.
[24] D. S. Wall, "Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing," in *The Oxford Handbook of the Law and Regulation of Technology*, R. Brownsword, E. Scotford, and K. Yeung, Eds., ed: Oxford Univeristy Press, 2017.
[25] G. Pescaroli and D. Alexander, "A definition of cascading disasters and cascading effects: Going beyond the "toppling dominos" metaphor'," *Global Forum Davos,* vol. 3, pp. 58-67, 2015.
[26] P. Hunton, "Data attack of the cybercriminal: Investigating the digital currency of cybercrime," *Computer Law & Security Review,* vol. 28, pp. 201-207, 2012.
[27] K. Thomas, D. Yuxing Huang, D. Wang, E. Bursztein, C. Grier, T. J. Holt, C. Kruegel, D. McCoy, S. Savage, and G. Vigna, "Framing Dependencies Introduced by Underground Commoditization," presented at the Workshop on the Economics of Information Security, 2015.
[28] R. Leukfeldt, Ed., *Research Agenda. The Human Factor in Cybercrime and Cybersecurity*. The Netherlands: Eleven International Publishing, 2017, p.^pp. Pages.
[29] M. Weulen Kranenbarg and E. R. Leukfeldt, Eds., *Cybercrime in context: the human factor in victimization, offending, and policing*. Springer, 2021, p.^pp. Pages.
[30] I. Agrafiotis, M. Bada, P. Cornish, S. Creese, M. Goldsmith, E. Ignatuschtschenko, T. Roberts, and D. M. Upton, "Cyber Harm: Concepts, Taxonomy and Measurement," Oxford2016.
[31] Holt Thomas J., D. Strumsky, O. Smirnova, and M. K. M. (2012), "Examining the Social Networks of Malware Writers and Hackers," *International Journal of Cyber Criminology,* vol. 6, 2012.
[32] Proofpoint. (2014). *Analysis of a cybercrime infrastructure*. Available: https://cdn2.vox-cdn.com/uploads/chorus_asset/file/2340876/proofpoint-analysis-cybercrime-infrastructure-20141007.0.pdf
[33] R. Leukfeldt and J. Jansen, "Cyber Criminal Networks and Money Mules: an analysis of low-tech and high-tech fraud attacks in the Netherlands," *International Journal of Cyber Criminology,* vol. 9, pp. 173-184, 2015.
[34] C. Kopp, R. Layton, J. Sillitoe, and I. Gondal, "The role of love stories in romance scams: a qualitative analysis of fraudulent profiles," *International Journal of Cyber Criminology,* vol. 9, pp. 205-217, 2015.
[35] R. Broadhurst, P. Grabosky, M. Alazab, and S. Chon, "'Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime'," *International Journal of Cyber Criminology,* vol. 8, pp. 1-20.
[36] E. R. Leukfeldt, E. R. Kleemans, and W. Stol, "Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis," *Crime, Law and Social Change,* vol. 67, pp. 39–53, 2017.
[37] E. R. Leukfeldt, E. R. Kleemans, and W. Stol, "A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists," *Crime, Law and Social Change,* vol. 67, pp. 21-37, 2017.
[38] J. Lusthaus, *Industry of Anonymity. Inside the Business of Cybercrime*: Harvard University Press, 2018.
[39] L. Paoli, J. Visschers, and C. Vestraete, "The impact of cybercrime on businesses: a novel conceptual framework and its application to Belgium," *Crime, Law and Social Change,* vol. 70, pp. 397–420, 2018.
[40] J. Lusthaus and F. Varese, "Offline and Local: The Hidden Face of Cybercrime," *Policing: A Journal of Policy and Practice,* vol. 15, pp. 4-14, 2021.

[41] S. McKay (Editor), A. Guinchard, P. Sommer, L. Harris, S. D. Walker, A. Woolfson, A. Nair, D. Campbell, D. Wall, R. Clayton, I. Walden, M. Turner, I. Henderson, A. Evans, K.-L. Payne, K. Maras, O. Sallavaci, A. Charlesworth, N. Searle, R. Bratu, N. Colvin, W. Grossman, C. Marsden, R. Kaye, S. Demetriou, O. Shaanika, H. Crombag, R. Gimson, K. Sommer, K. Petreczky, P. Horsfall, and J. Underwood, "Reforming the Computer Misuse Act 1990," The Criminal Law Reform Now Network2020.

[42] M. G. Porcedda, "Sentencing data-driven cybercrime. How UK courts tackle data crime with cascading effects," under review.

[43] B. Rihoux and R. C, *Configurational Comparative Methods. Qualitative Comparative Analysis (QCA) and Related Techniques*: Sage, 2009.

[44] T. Newburn, *Criminology (third edition)*: Routledge, 2017.

[45] A. Hutchings, "Cambridge Computer Crime Database," ed, 2020.

[46] M. Turner, "Computer Misuse Act 1990 cases, Computer Evidence," ed, 2020.

[47] J. Corbin and A. Strauss, "Grounded theory Research: Procedures, Canons, and Evaluative Criteria," *Qualitative Sociology,* vol. 13, 1990.

[48] M. G. Porcedda, "The Strange Case of Researching Cybercrime with Sentencing Remarks," presented at the 2nd Methods and Data in Sentencing Research: Quantitative and Qualitative Approaches Conference, Sheffield, 2019.

[49] S. Gatlan. (2020). *$100 million in bounties paid via HackerOne to ethical hackers*. Available: https://www.bleepingcomputer.com/news/security/100-million-in-bounties-paid-via-hackerone-to-ethical-hackers/

[50] C. Cunningham, "Norwich teen who hacked TalkTalk on trial for stealing people's personal data and selling it to criminals," in *Eastern Daily Press,*, ed, 2019.

[51] G. Corfield, "US govt accuses four Chinese army soldiers of hacking Equifax and siphoning 145m Americans' personal info," in *The Register*, ed, 2020.

[52] R. Anderson, *Security Engineering. A Guide to Building Dependable Distributed Systems (3rd edition)*. Indianapolis: Wiley, 2020.

[53] J. Grierson, "Ringleader of gang responsible for £113m fraud jailed for 11 years," in *The Guardian*, ed, 2016.

[54] Pcpro.co.uk. (2013). *Stubhub fraud: how hackers stole 1M using tickets*. Available: http://www.pcpro.co.uk/news/389965/stubhub-fraud-how-hackers-stole-1m-using-tickets

[55] M. Levi and R. Reuter, "Money Laundering," *Crime and Justice,* vol. 34, pp. 289-375, 2006.

[56] "R v Cassandra Mennim, R v Edward Pearson," in *A Mulligan* vol. Unreported, ed: Southwark Crown Court, 2012.

[57] The York Press, "York Computer Hacker, Edward Pearson, jailed for identity fraud," ed: The York Press, 2012.

[58] M. Schaake, L. Pupillo, A. Ferreira, and G. Varisco, "Software Vulnerability Disclosure in EuropeTechnology, Policies and Legal Challenges. Report of a CEPS Task Force," ed. Brussels: Centre for European Policy Studies (CEPS), 2018.

[59] C. Arthur, "LulzSec hackers jailed for string of sophisticated cyber-attacks," in *The Guardian*, ed, 2013.

[60] "R v Jake Davis, R v Mustafa Al-Bassam, R v Ryan Ackroyd, R v Ryan Cleary, R v James Jeffery," in *Judge Taylor* vol. Unreported, ed: Southwark Crown Court, 2013.

[61] The Telegraph, "'Team Poison' hacker who posted Tony Blair's details is jailed," in *The Telegraph*, ed, 2012.

[62] L. Murphy, " The Curious Case of the Jihadist Who Started Out as a Hacktivist," in *Vanity Fair*, ed, 2015.

[63] "R v Junaid Hussain," ed: Southwark Crown Court, 2012.

[64] A. Martin, "London-based Yahoo! hacker gets 11 years for SQLi mischief," in *The Register*, ed, 2016.

[65] "R v Nazariy Markuta," vol. Unreported, ed: Southwark Crown Court, 2016.

[66] M. Robinson, "Couple made £1.3million stealing bank details from 700 victims then splashed the cash on a lavish wedding and honeymoon to Hawaii," in *Daily Mail*, ed, 2015.

[67] "R v Jennifer Hallam, R v Sean Benson," vol. Unreported, ed: Southwark Crown Court, 2015.

[68] A. Bond, "Gang of 'phising' [sic] fraudsters who stole woman's £1m life savings blew it on cheeseburgers, champagne and gold," in *Mail Online*, ed, 2013.

[69] "R v Rilwan Adesgun Oshodi, Annette Jabeth, Abdul Hamid, Shaharyar Butt, Chika Okala and Sharna Eve " vol. Unreported, ed: Southwark Crown Court, 2013.

[70] Spamfighter. (2013). *UK-based Internet Crook gets Jail for Over 5 Years*. Available: http://www.spamfighter.com/News-18624-UK-based-Internet-Crook-gets-Jail-for-Over-5-Years.htm

[71] Information Commissoner's Office (ICO), "Monetary Penalty Notice against TalkTalk Telecom Group PLC, 30 September 2016," 2016.

[72] "R v Grant West," in *Judge Gledhill*, ed: Southwark Crown Court, 2018.

[73] D. Raywood, "Sentry MBA Tool Used in Attacks on Login Forms," in *Info Security*, ed, 2017.

[74] Nguyen, "London-based cyber criminal jailed over financial data fraud," in *ComputerWorld UK*, ed, 2014.

[75] G. Cluley. (2016). *Teenager charged over Mumsnet hack and DDoS attack*. Available: https://www.welivesecurity.com/2016/05/23/teenager-charged-mumsnet-hack-ddos-attackraham

[76] Farnham Herald, "Mumsnet hacker spared jail," in *Fernahm Herald*, ed, 2016.

[77] M. Dhami and I. Belton, "Using Court Records for Sentencing Research: Pitfalls and Possibilities," in

Exploring Sentencing Practice in England and Wales, J. V. Roberts, Ed., ed: Palgrave Macmillan, 2014.
[78] Mitre Corporation, "MITRE Att&ck Cloud Matrix," ed, 2019.
[79] R. Chiesa, S. Ducci, and S. Ciappi, "HPP- The Hacker Profiling Project: A General Overview," presented at the Hack.lu 2006 conference, 19- 21 October, Luxembourg, 2006.
[80] A. Lavorgna and A. Sergi, "'Serious', Therefore Organised? A Critique of the Emerging "Cyber-Organised Crime" Rhetoric in the United Kingdom," *International Journal of Cyber Criminology,* vol. 10, pp. 1-23, 2016.
[81] D. S. Wall, "Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime," *The European Review of Organised Crime,* vol. 2, pp. 71-90, 2015.
[82] R. Leukfeldt, A. Lavorgna, and E. R. Kleemans, "Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime," *European Journal on Criminal Policy and Research,* vol. 23, pp. 287-300, 2017.
[83] M. G. Porcedda, "Brexit, cybercrime and cyber security. From en masse opt-out to creative opt-in in the AFSJ and beyond?," in *Brexit and Internal Security. Political and Legal Concerns in the Context of the Future UK-EU Relationship*, H. Carrapico, A. Niehuss, and C. Berthelemy, Eds., ed: Palgrave Macmillan, 2019.
[84] "WM Morrisons Supermarket LPC v Various Claimants," vol. EWCA Civ 2339, ed, 2018.
[85] "WM Morrisons Supermarket LPC v Various Claimants," vol. UKSC 12, ed: Supreme Court of the United Kingdom, 2020.
[86] D. S. Wall, "The Transnational Cybercrime Extortion Landscape and The Pandemic: Ransomware and changes in offender tactics, attack scalability and the organisation of offending", *European Law Enforcement Research Bulletin* (2021).

ANNEXES

I. ANNEX 1: CRISP SET AND SAMPLE QUALITATIVE ANALYSES

TABLE 1. CRISP SET OF CASE STUDIES 1-17

	C#	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
upstream	s1	y	y	y	y	y	y	n	y	y	y	y	y	y	y	y	y	y*
	tp	y*	n	n	n	n	n	n	?	y*	n	n	?	n	n	?	?	?
	s2	y	y	y	y	y	y	y	?	y	y	y	y	y	y	y	y	y
	tp	y*	n	?	n	n	n	n	?	y	?	n	?	n	n	?	?	?
	s3	y	n	y	y	y	y	y	?	y	y	y	y	y	y	y	y	y
	tp	n	n	n	n	y*	n	n	n	n	y	n	n	y	?	n*	y	y*
downstream	s4	?	n	y	y	n	n	n	n	n	n	y	n	n	y	n	n	y
	tp	?	N	y	y	n	n	n	N	N	N	n*	n	n	y	n	n	y
	s5	y	y	y	y	y	y	y	n	y	y	n	y	n*	y	n	?	y
	tp	?	n	?*	n	n*	n	n	n	n	n	n	?	n*	y*	n	n	n
	s6	n	n	n	n	n	n	n	n	y	n	n	n	y*	n	y	y	n
	tp	n	n	n	n	n	n	y	n	y	n	n	n	y*	n	n	n	n
	7	n	n	y	n	y	y	y	n	n	n	y	n	n	n	n	n	n
	O	Y	N	Y	Y	Y*	N	N	?	Y	Y	N*	?	Y	Y*	N*	Y	Y

a. C#= case number; s=stage; tp=tipping point; O=outcome. Y= stage/tp reached;Y*= stage/tp likely reached cascade; ?=indeterminate e; N*= stage/tp unlikely reached; N= stage/tp not reached.

TABLE 2. CRISP SET OF CASE STUDIES 18-33

	C#	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	T
upstream	s1	y	y	y	y	y	y	y	y	y	y*	y	Y	y	y	y	y
	tp	n	n*	n	n*	n*	n	n	n*	n	y*	y	n*	n*	n*	y	y
	s2	y	y	y	y	y	y	y	y	y	?	y	y	y	y	y	y
	tp	n	n	n	n*	n	n	n	n*	n	?	n*	n	n	n	y	y
	s3	y	y	y	y	y	y	y	y	y	?	y	y	y	y	y	y
	tp	n	n	n*	n	n	n	n	n	n	?	n	n	n	n	n	y
	s4	n*	n	n	n	n	n	y	n	?	?	n	n	n	y	?	y
downstream	tp	n*	n	n*	n	n	n	y	n	?	?	n	n	n	y	?	y
	s5	y	y	y	y	y	y	y	y	y	?	y	y	y	y	y	y
	tp	n	n	n	n	n	n	n	n	?	?	n	n	n	y	?	y
	s6	n	n	n	n	n	n	n	n	n	?	n	n	n	n	n	y
	tp	n	n	n	n	n	n	n	n	n	?	N	n	n	n	n	y
	7	y	y	n	?	?	n	n	n	n	?	n	y	y	y	n	n
	O	N*	N*	N*	N*	N*	N	Y	N*	?	Y*	Y	N*	N*	Y	Y	Y

b. C#= case number; s=stage; tp=tipping point; O=outcome. Y= stage/tp reached;Y*= stage/tp likely reached cascade; ?=indeterminate e; N*= stage/tp unlikely reached; N= stage/tp not reached.

A. *Analysis of case 1 (outcome Y)*

s1	tp	s2	tp	s3	tp	s4	tp	s5	tp	s6	tp	7
y	y*	y	y*	y	n	?	?	y	?	n	n	n

1. Offender knew of vulnerabilities and created a tool to exploit it, which he talked about/shared on fora; (tp reached)†
2. Offender exploited the vulnerability and other people did too (tp reached)††
3. Offender breached the information but did not dox it
4. It is likely those aware of the vulnerability exploited for sale †††
5. It is likely those aware of the vulnerability kept the data and used it further
6. No other stages known

†: 1y* vulnerability publicised; ††2*=tool created; †††4?: reports mention other people selling credentials

B. *Analysis of case 2 (outcome N)*

s1	tp	s2	tp	s3	tp	s4	tp	s5	tp	s6	tp	7
y	n	y	n	n	n	n	n	y	n	n	n	n

1. They created (learnt) of a vulnerability but did not disseminate knowledge outside group
2. they exploited the vulnerability – others did not
3. no
4. no
5. They retained data to commit crime but seemingly did not use the data/unknown

C. *Analysis of case 5 (outcome Y*)*

s1	tp	s2	tp	s3	tp	s4	tp	s5	tp	s6	tp	7
y	n	y	n	y	y*	n	n	y	n*	n	n	y

1. Vulnerability found but not shared
2. The vulnerability was exploited; it is impossible to say whether it was exploited by multiple individuals at once
3. Data of value was found and seemingly dumped - Note ambiguity in text “login credentials harvested through data breaches from other sites” (y*)
4. No sale of data occur
5. Data was put into crime; the proceeds of crime were used to generate more money (selling tickets), but this does not generate further cascade (n*)†
6. No pretexting
7. Mules involved

†: s2= the offenders exploited vulnerabilities;

D. *Analysis of case 8 (outcome ?= indeterminate)*

s1	tp	s2	tp	s3	tp	s4	tp	s5	tp	s6	tp	>6
y	?	?	?	?	n	n	n	n	n	n	n	n

1. The vulnerability was discovered as part of a loose hacking group, possibly exploited
2. The vulnerability was possibly exploited by multiple people
3. It is not known whether valuable information was found
4. No other information is found about the case

E. *Analysis of case 11 (outcome N*)*

s1	tp	s2	tp	s3	tp	s4	tp	s5	tp	s6	tp	7
y	n	y	n	y	n	y	n*	n	n	n	n	y

1. A program to exploit a vulnerability was created, but not disseminated
2. The vulnerability was exploited
3. The exploit lead to valuable information
4. Valuable information was sold, but it could not convert into multiple exploits (n*)
5. The data was not kept
6. News of the exploit did not spread
7. There were mules

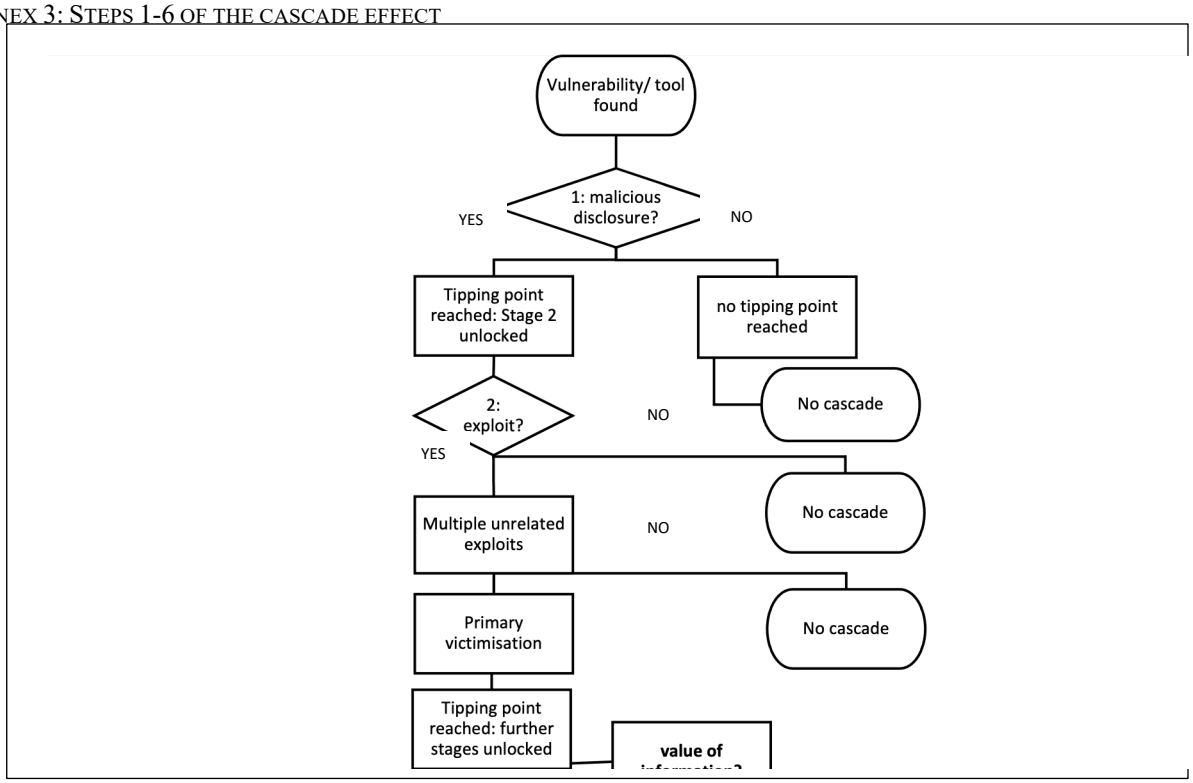
II. ANNEX 2: FUZZY SET OF CASE STUDIES

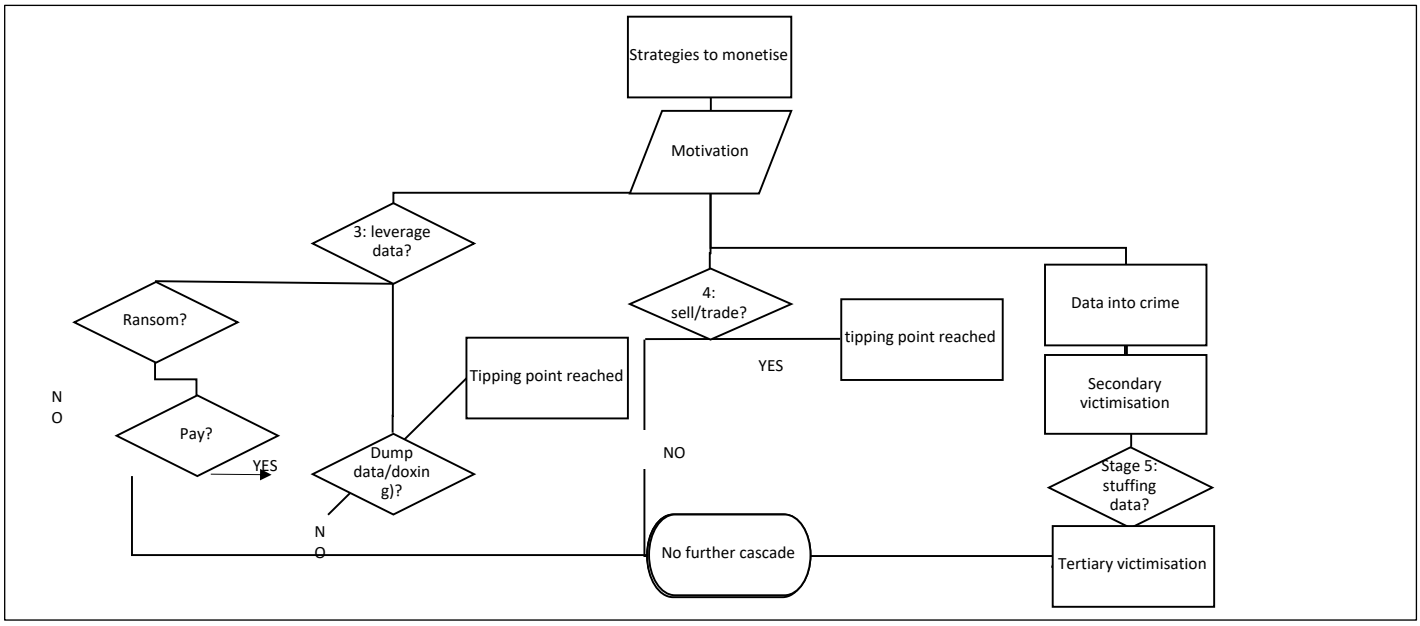
TABLE 3. FUZZY SET OF CASE STUDIES

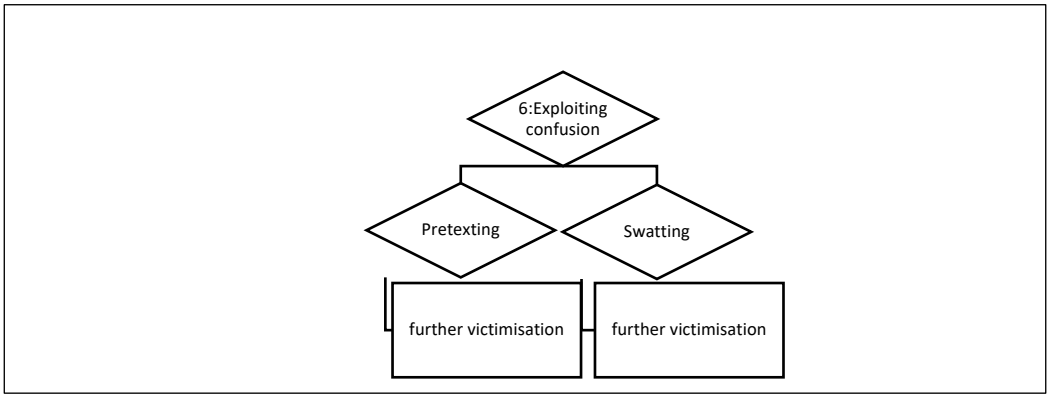
C#	Upstream (stages 1-3)						Downstream (stages 1-7)						
	s1	***tp***	***s2***	***tp***	***s3***	***tp***	***s4***	***tp***	***s5***	***tp***	***s6***	***7***	***O***
1	1	0,67	1	0,67	1	0	0,5	0,5	1	0,5	0	0	1
2	1	0	1	0	0	0	0	0	1	0	0	0	0,33
3	1	0	1	0,5	1	0	1	1	1	?*	0	1	1
4	1	0	1	0	1	0	1	1	1	0	0	0	1
5	1	0	1	0	1	0,67	0	0	1	0,33	0	1	0,67
6	1	0	1	0	1	0	0	0	1	0	0	1	0
7	0	0	1	0	1	0	0	0	1	0	0	1	0
8	1	0,5	0,5	0,5	0,5	0	0	0	0	0	0	0	0,5
9	1	0,33	1	1	1	0	0	0	1	0	1	0	1
10	1	0	1	0,5	1	1	0	0	1	0	0	0	1
11	1	0	1	0	1	0	1	0,33	0	0	0	1	0,33
12	1	0,5	1	0,5	1	0	0	0	1	0,5	0	0	0,5
13	1	0	1	0	1	1	0	0	0,33	0,67	0,67	0	1
14	1	0	1	0	1	0,5	1	1	1	0,67	0	0	0,67
15	1	0,5	1	0,5	1	0,67	0	0	0	0	1	0	0,33
16	1	0,5	1	0,5	1	1	0	0	0,5	0	1	0	1
17	0,67	0,5	1	0,5	1	0,67	1	1	1	0	0	0	1
18	1	0	1	0	1	0	0,33	0,33	1	0	0	1	0,33
19	1	0,67	1	0	1	0	0	0	1	0	0	1	0,33
20	1	0	1	0	1	0,33	0	0,33	1	0	0	0	0,33
21	1	0,67	1	0,33	1	0	0	0	1	0	0	0,5	0,33
22	1	0,67	1	0	1	0	0	0	1	0	0	0,5	0,33
23	1	0	1	0	1	0	0	0	1	0	0	0	0
24	1	0	1	0	1	0	1	1	1	0	0	0	0
25	1	0,67	1	0,33	1	0	0	0,5	1	0	0	0	0,33
26	1	0	1	0	1	0	0,5	0,5	1	0,5	0	0	0,5
27	0,67	0,67	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,67
28	1	1	1	0,33	1	0	0	0	1	0	0	0	1
29	1	0,33	1	0	1	0	0	0	1	0	0	1	0,33
30	1	0,33	1	0	1	0	0	0	1	0	0	1	0,33
31	1	0,33	1	0	1	0	1	y	1	1	0	1	1
32	1	1	1	1	1	0	0,5	0,5	1	0,5	0	0	1
TT	1	1	1	1	1	1	1	1	1	1	1	1	1

[a] C#= case number; s=stage; tp=tipping point; O=outcome. 1= stage/tp reached; 0,67= stage/tp likely reached cascade; 0,5=indeterminate e; 0,33= stage/tp unlikely reached; 0= stage/tp not reached.

VI. Annex 3: Steps 1-6 of the cascade effect







VII. ANNEX 4. CASCADE, VALUE OF INFORMATION & VICTIMIZATION