THE UNIVERSITY of EDINBURGH

Edinburgh Research Explorer

Not just BANAL

How branding shapes cybercrime ecosystems

Citation for published version:
Collier, B & Clayton, R 2025 'Not just BANAL: How branding shapes cybercrime ecosystems'.

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Other version

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 17. Nov. 2026

Not just BANAL: How branding shapes cybercrime ecosystems

Ben Collier

University of Edinburgh

Richard Clayton

University of Cambridge

Abstract

We consider the trend of (self-)consciously branding bugs and vulnerabilities in what we deem to be a BANAL (Bug with A Name and A Logo) manner. However, there is a great deal more naming and branding going on in cybercrime and cybersecurity than this. We show how the use of names by criminologists, cybersecurity companies and the academics who study cybercrime fundamentally shapes the way in which both attackers and defenders understand cybercrime ecosystems. We argue that there are four main functions of naming present: names as deviant labelling, names as a way of structuring practices and scripts, names as branding or marketing, and names as a tool of information brokerage. We further contend that the cultural functions of labelling and marketing are overwhelming the practical functions of co-ordinating practices and assessing the criminal innovation ecosystem; names are exploding cybercrime rather than integrating it. By applying frameworks from criminology and evolutionary economics, we explore the complex dynamics of naming and branding in cybercrime and suggest interventions.

1 Introduction

Even if you are not a cybersecurity expert you have probably heard of the 'Anonymous' threat actor group and perhaps of 'Fancy Bear', 'Salt Typhoon' or 'APT43'. You may remember the 'Wannacry' malware outbreak or, if your memory goes back to the millennium, the email worm dubbed 'ILoveYou'. You may recall the scramble to fix the 'Heartbleed' vulnerability in 2014 or 'Dirty Cow' in 2016. If you follow academic work on systemic vulnerabilities you will have come across 'RowHammer' and 'Spectre'. In all of these examples a brand has been deliberately invented and the brand-name has become widely used as an appropriate descriptor for the underlying concept. Logos and attendant websites – such as those for Heartbleed[1], Meltdown, and Spectre [2] – are also occasionally deployed to assist these efforts.

However, using these names can easily mislead. As we were finishing this paper a well-known UK High Street retailer experienced a significant ransomware attack causing empty shelves in the stores, suspension of online sales and a projected impact of tens or hundreds of millions of pounds in lost profit. This was of course widely reported in the media; coverage in the Daily Mail being typical [30]:

> An alleged cyber attack which has crippled Marks and Spencer has been linked to notorious teenage hacking gang, Scattered Spider. [...] Now experts assisting M&S have claimed the cartel of cyber criminals – thought to be made up of British and American youths – could be behind the online security breach. [...] Investigators believe the attackers on this occasion

[1] https://heartbleed.com

[2] https://meltdownattack.com

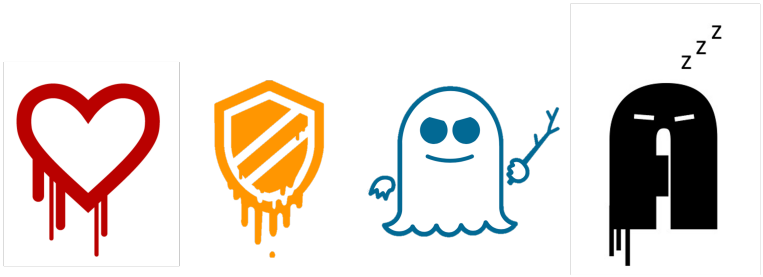

Figure 1: Logos for Heartbleed, Meltdown, Spectre, and our own BANAL bug

> used a hacking tool from a group known as DragonForce, which bills itself as a 'ransomware cartel', to carry out the breach.

Dragonforce is an affiliate scheme set up by a hacktivist group thought to originate in Malaysia which provides ransomware tools on a white-label basis to criminals who can compromise a system [98]. The "cartel" moniker comes from their original announcement of their service. Scattered Spider is the name given by the cybersecurity company CrowdStrike to an "adversary" [88] that emerged out of a broad group of cybercriminals dubbed "The Com" [115]. This suggests, as the Daily Mail says, that this is a specific group, with a specific membership and aims, which is conducting a series of operations. The reality though, as one expert told us, is that this is really just a generic term for "kids in bedrooms".

In this paper we discuss various ways in which branding occurs in cybersecurity settings. As will be apparent from our paper title (BANAL is the acronym we have invented for a "Bug with A Name and A Logo") we are somewhat sceptical as to the motives underlying the creation of many brands – we think it is often more about self-promotion than assisting the wider community. Panic about BANAL vulnerabilities can in many cases direct the attention of companies, CEOs, and defenders to deploy their resources away from the low-hanging fruit that makes most of the difference in securing complex systems. Nevertheless, these brands do play a role in fixing bugs, and in countering groups of threat actors.

We then go on beyond the banal, to consider how names (and branding) are being used in criminology to develop categorisations of deviant behaviour, and to drive the understanding of cybercrime ecosystems, by both attackers and defenders grouping activity and giving it a name. We further suggest that these names create inefficiencies for defenders and that they need to refocus more closely on their task rather than the name of the issue they are tackling.

More widely, we develop a strand of theory that has emerged over the past decade within the broad body of work that applies economic approaches and theories to the study of cybercrime. This takes inspiration from approaches within *evolutionary economics* [73] which act in opposition to models based on the rational individual actor engaging in a series of individual, bounded cost-benefit decisions. In evolutionary ecosystems, actors are able to plan, to strategise, to make sense of the behaviour of others, and to actively create and disseminate their own information. They take positions, identify and fill niches, specialise, take on and perform roles, and try to make sense of the wider landscape in which they act – a landscape which evolves over time. Within this ecosystem, the names, measurements, categories, and models that actors come up with to do this information work and make sense of the market exert powerful shaping forces on the economic behaviour of actors in these ecosystems (they are *performative* in the same sense as the infamous Black-Scholes-Merton equations were for fund managers[69]). Developing this further, we argue that the cybersecurity ecosystem is sorely missing key functions and infrastructure for co-ordinating and producing this information; the local incentives of specific actors to strategically deploy names and brands are taking their place, creating perverse outcomes.

2 Branding in cybersecurity

We start by considering five different examples of the overt use of branding in cybersecurity: bugs and design flaws, threat actor groups, malware, systemic vulnerabilities and law enforcement activity.

2.1 BANAL vulnerabilities

We start by considering BANAL examples: Bugs with A Name And Logo.

In February 2012 RFC6250 [103] documented a way to prevent secure connections from being closed as inactive by sending heartbeat packets back and forth on a regular basis. This new mechanism was soon incorporated within the popular OpenSSL package. Unfortunately, the code contained a bug (a flaw in the code)... you could set a length value that exceeded the size of your packet contents and get the other end of a link to send you back swathes of kernel memory that might contain passwords or cryptographic keying material which could be leveraged to permit unauthorised access.

A Google engineer found the bug and a fix was created on March 21st 2014. It was then independently discovered by Codenomicon, a Finnish company, on April 3rd. The issue was made public on April 7th with the release of patched versions of OpenSSL and a security advisory which credited the Google engineer [50]. Shortly after this was published Codenomicon tweeted that they had also identified the bug and linked to a `heartbleed.com` website they had created with information about the bug. The website named the bug as Heartbleed and featured a striking logo designed by a professional graphic designer. The brand name stuck, albeit it is doubtful that many today remember the Codenomicon name or that of Neel Mehta, the Google engineer.

In 2016 Phil Oester, a Linux security engineer, identified a long-standing privilege escalation bug – a race condition in the way the Linux kernel memory subsystem handled the copy-on-write (COW). This allowed writes to what should have been read-only memory. Oester was investigating a compromised machine – that is the flaw was already being exploited by bad actors. The bug was addressed by an October 2016 patch, but this patch had a flaw, and the issue was not fully fixed until November 2017.

The branding of this bug as "Dirty Cow" seems to have been a little problematic because the website (`dirtycow.ninja`) says "It would have been fantastic to eschew this ridiculousness, because we all make fun of branded vulnerabilities too, but this was not the right time to make that stand. So we created a website, an online shop, a twitter account, and used a logo that a professional designer created." [3]

2.2 Threat Actor Groups

A number of cybersecurity companies track threat actor groups – linking activity by methodology, tool usage or sometimes their public announcements. The companies differ in their use of nomenclature: for example, Mandiant label groups as APT<n>, starting with APT1 (a unit of the Chinese Army) in 2013 [70].[4] The use of APT ("Advanced Persistent Threat") as a wider category of threat actor is itself an exercise in branding and shaping the ecosystem.[5] Several others stick to numeric systems, but Trend Micro uses names that indicate motivation – names with Earth are espionage groups, Water financially motivated, Fire seek to disrupt and destroy and Wind names apply to hactivist groups. As a matter of policy Trend Micro avoids naming that identifies the country of (alleged) origin, but CrowdStrike and

[3]The first sentence was borrowed straight from the website for the BANAL bug "ImageTragick" (`https://imagetragick.com`) which described an ImageMagick bug in May 2016.

[4]Mandiant has now reached APT49 in their naming system.

[5]The UK's National Cybersecurity Centre (NCSC) and others argue that "APT" name serves to overstate the threat, sophistication, and persistence of many of these groups, or at least, of the complexity of the approaches that they use in practice [80].

Palo Alto Networks have no such qualms – CrowdStrike being particularly stereotypical in their choices: Bear–Russia, Panda–China, Buffalo–Vietnam, Tiger–India and so on.[6]

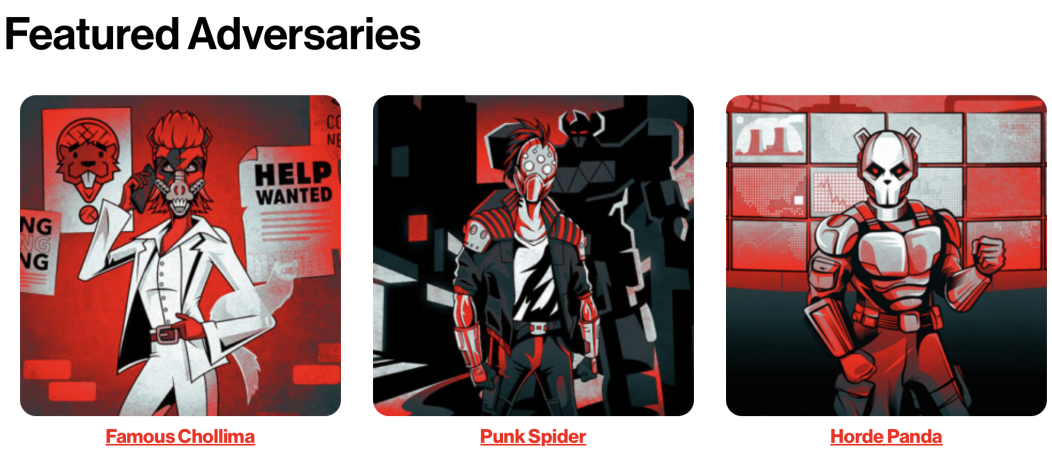

Figure 2: An example of some of CrowdStrike's "Featured Adversaries" and their branding personas.

Figure 3: Palo Alto's logo for the Ursa series, including sub-logos for e.g. the 'Pensive Ursa' Russian threat actor, also known as Turla, Uroburos, Snake, BELUGASTURGEON, Boulder Bear, G0010, Group 88, IRON HUNTER, Iron Pioneer, Krypton, Minime, Popeye, Turla Team, Venomous Bear, Waterbug, White Atlas, WhiteBear, and Witchcoven.

All of this means that a particular threat actor group may be known by many different names – APT43, which Mandiant link to North Korea [91], is also known as Thallium, Kimsuky, Velvet Chollima, Black Banshee and STOLEN PENCIL [92].

Starting in 2019, the Thai CERT has been publishing a list of known threat actor groups, collating information from a range of different sources. They originally produced PDFs, but changed to providing the information on a dynamically generated website. As of the end of 2024 they list 495 groups (at an average of 3.1 names per group) [40].

2.3 Branding malware

Malware has been branded pretty much since it first appeared, spreading over floppy disk 'sneaker-nets'. Examples include Brain (1986 [109]) and Stoned (1988 [42]). At this stage the naming came from the

[6] As can be seen in Figure 2 CrowdStrike go beyond naming to create a full branding universe for their adversary groups – e.g. https://www.crowdstrike.com/en-us/blog/who-is-fancy-bear/

malware itself – Brain wrote `@BRAIN` into the disk volume label and Stoned caused an infected machine to display "`Your computer is now stoned`".

Thereafter naming malware that had any significant impact became *de rigeur* – and when a particular strain was identified by two anti-virus vendors in parallel there were inevitably two (or more names) in circulation. Thus, for example, the first malware to infect an Apple Macintosh computer is variously known as "Oompa-Loompa", "OSX/Oomp-A" or "Leap.A".

There is a standard, dating from 1991, for naming malware. It has been enhanced over the years and currently requires names to be of the form: `Type:Platform/Family.Variant!Suffixes` (so a particular sample might be `Email-Worm:Win32/Bagle.aav!dll`) which does help identify what type of malware is being discussed and what platform it targets, but the Family, Variant and Suffix parts are still just brandnames and there is not necessarily any agreement as to what these may be.

Malware names are sometimes bestowed by the authors of the malicious code. So Mirai was named by the group who wrote this IoT worm [3]. Sometimes, however, these names are eschewed so the malware that its authors seem to have wanted to be called GayFgt is more commonly referred to as BashLite (or sometimes Gafgyt, Lizkebab, PinkSlip, Qbot, Torlus or LizardStresser) [17].

2.4 Systemic vulnerabilities

In January 2018 two related attacks on flaws in CPU architecture were announced, dubbed Spectre and Meltdown. Spectre was a timing attack that used a CPU's speculative execution pipeline to deduce the content of memory in other processes [63]. Meltdown exploits a race condition between memory access and privilege checking and also allows memory contents to be deduced even though reading is forbidden [67]. Along with the academic papers an explanatory website (`meltdownattack.com`) was launched – featuring two striking logos for the two attacks.

It has long been the case that academics give cute titles to their papers (and the authors of this paper are no exception). Promoting academic careers by having websites to explain the import of papers to a wider audience are also nothing new. However, adding logos, in the manner we have been describing in other cybersecurity areas, was new.

Other academics joined in the fun – the original Rowhammer issue (repeatedly reading DRAM memory so that it is not correctly refreshed) did not have a logo or website when it was announced in 2014 [61]. But in 2019 'RAMBleed' (which used RowHammer to read memory bits without permission) was given a website (`rambleed.com`) and a logo [64].

2.5 Naming Law Enforcement operations

The military have been using codenames for their offensives for a very long time. A handful of examples from World War I (both from the Entente and Central powers) can be found in the history books, but it became standard procedure in World War II, and names such as Overlord, Market Garden and Mincemeat have become part of our culture. In the UK the names seem to have been chosen by the commanders, but shortly after they joined the war the USA generated a list of names and assigned them randomly [52].

Although the point of codenames is generally to hide the nature and targets of the plans being made (hence the value of random assignment), the military also understand the value of branding – for example, they publicised from the very start the naming of "Desert Shield" for the 1991 military build-up in the Middle East and "Desert Storm" for the actual liberation of Kuwait. Operation "Just Cause" (the 1989 US invasion of Panama) was renamed from its original randomly-generated moniker, both to buttress the perceived legitimacy of the invasion, but also reportedly after General James Lindsay requested it changed, having asked Lt General Thomas Kelley whether "you want your grandchildren to say you were in Operation Blue Spoon?" [105].

Figure 4: Europol's logo for Operation PowerOFF

Law enforcement also name investigations for reasons of clarity and to keep the actual targets on a need-to-know basis. In UK the names now come from a random set of words in a book to avoid clashes and to avoid the name giving anything away [5]. It seems that over the decades all the simple names have been taken so recent anti-DDoS activity is called "Operation Brombenzyl".[7] However, the multi-year Europol-led initiative to tackle DDoS more generally has been branded "Operation PowerOFF" (see Figure 4) entirely for PR reasons. And PR is important here: the latest version of the 'splash page' placed on seized websites features (alongside the operation's own custom-made logo) a carousel of logos for 22 law enforcement organisations around the world to indicate that citizens of many countries might be at risk of arrest.

2.6 Justifications for branding

Some claim that branding makes it easier to have high-level discussions about topics without getting into the detail and, as we have just discussed, law enforcement and the military may be especially sensitive about the detail. There are many examples of ease of discussion in other fields: the elements Rutherfordium and Seaborgium are easier to distinguish than Unnilquadium and Unnilhexium[76, 85, 87], [8] and for astronomers, Barnard's Star is more useful a designation in public discussions than GJ699.

Talking about Heartbleed was easier than discussing CVE-2014-0160 (its official designation) but it is unlikely that this mattered much in practice. Sysadmins knew they had to fix the problem, it did not require executives to become aware of the name and logo. In some cases, it may be possible for security teams to use media coverage of vulnerabilties of groups to positive effect (getting the C-suite's attention or making the case for resources) however negative effects arguably predominate.

Similar claims are made about the ease of discussing threat actor groups by giving them a brand – but the 'plain white packaging' of Mandiant's APT 1 to 47 designations suggests that it might be more about simplifying filing systems rather than avoiding confusion during water-cooler conversations.

In practice, we believe that the main (and only important) reason for branding vulnerabilities, threat actor groups, and malware is marketing – mainly by defenders promoting their prowess at identifying a new threat, but sometimes by the threat actors who wish to promote their own abilities. This branding also plays an important part in establishing the careers of both attackers and defenders – with the inventors of Mirai generally known as the "Mirai kids" in the press and promotion and retention prospects for cybersecurity professionals at large corporate firms often hinging on a successful talk at BlackHat – where a cute name, a professional logo and an enticing abstract will be needed to get them onto the agenda. This has been much commented upon by cybersecurity practitioners, for example by Stamos [108].

[7] 4-Bromobenzyl bromide, or α,4-Dibromotoluene, or $BrC_6H_4CH_2Br$.

[8] These odd IUPAC names, in fact, were a short-term solution for competing claims by Soviet and US scientists over who discovered some of the so-called 'heavy' elements, and who would hence win naming rights, thus securing valuable scientific prestige, and hence a Cold War marketing victory.

3 Names as deviant labels in cybercrime subcultures

We will now move away from our 'branding' examples to consider more general and more theoretical issues of the use of names within cybercrime and cybersecurity ecosystems. We start by considering the role that names play in criminology, moving on to the importance of names in discussions of groups and subcultures. We then return to cybercrime issues to explore the naming of people, the naming of groups and indeed of the crimes themselves. Finally, for this section we come back to a more in-depth consideration of the use of names by cybersecurity companies.

3.1 Naming in criminology

In criminology, naming – of new forms of crime, criminalised groups of people or subcultures, and new social problems – is an important part of criminalisation, generally understood through theories of labelling and the subcultural and association theories of offending which developed from labelling theory [43].

Initially, any given subculture or criminalised practice is generally inchoate – it emerges out of a mix of different values and cultural currents; people and ideas; different practices and approaches to some communal goal; or reactions to changing social context [53, 77, 104]. Over time, this coheres around a core set of practices, material tools and infrastructure, and a coherent self-identity and set of norms for the group. Names play an important role in this stabilisation – the label allows people to be categorised as 'insiders' and 'outsiders' [6], allows particular scripts and practices to be solidified as the 'proper' ways to engage in the criminalised activity, and permits the internal policing of norms and value systems [104].

This stability is also produced through action from outsiders – with the chosen name allowing wider society to develop a series of opinions and views on the group as a whole, and often signifying this difference. As young people progress through their lives, they negotiate their way between a range of different possible identities and actively attempt to embody or reject them – exclusion from one shapes inclusion to others [72]. This becomes something of a feedback loop – people engaging in behaviours labelled deviant (such as smoking marijuana) [6] become labelled themselves (and stigmatised) by others as possessing a particular identity and so are more likely thus to identify with it [32]. Over time the group seeks to distinguish itself from the rest of society as a result of this stigma, and its members increasingly identify with one another and the shared norms and practices of the group, rather than wider society.

There is a substantial debate within the criminological literature on gangs; namely, what exactly defines a 'gang', including whether a gang has to have a name or one or more other identifying 'brand' features (graffiti, slogans, colours, clothing, etc.) to be called a 'gang' [62, 41]. Notably, Downes argued that despite longstanding concerns about American gangs coming 'over here', British delinquent subcultures were defined more by style than by crime [37].

3.2 Naming of groups and subcultures

The contents of the names which become identity labels – hoodie, chav, stoner, mod, rocker, hacker – are an important part of this order of cultural signals. Sometimes these names or labels are self-selected by groups and subcultures themselves, reflecting their own identity and values. In other cases, names are selected by influential members of society which seek to make the group or its associated practices a 'social issue' worthy of criminalisation. Often called moral entrepreneurs in mid-century criminology, these influential members of the media, political classes, or pressure groups play an important role in mobilising moral panics around the issue to drive legal regulation or enforcement [18].

The cultural content of names signals the values of the group, the value implicit in the activity itself, and hence the kind of person who can take part in it. As, in the mouths of others these names shape the processes of exclusion and stigmatisation, so too do they shape the experiences of those who join, and hence the self-image and values of the group identity [71]. This is important not only in how societies organise a response to criminalised activities, but also in who is able to see themselves within these subcultures and the kinds of things they do. An example of this currently brought to national attention by debates around drug legalisation in the US is the term 'marijuana' – a term initially popularised by

those seeking to prohibit and criminalise cannabis. Choosing a Latin American term was, some accounts argue [11], a deliberate decision by moral entrepreneurs to associate the drug with Mexican immigration and racialised prejudice (though see others for the dissenting case [75]).

3.3 Cybercrime: the naming of groups, activities and people

In the cybercrime context, the name Anonymous was chosen to signify the group's eschewal of formal leadership structures or the cultivation of personal reputation (derided as 'namef*gging') [19]; the practice of 'eWhoring' deliberately evokes both misogynistic rhetoric as well as entrepreneurial values [59]; and even the (now superseded) traditional Black Hat and White Hat designation of different kinds of hacker deliberately called back to Hollywood Westerns, with the frontier, lawless nature of the Wild West mirroring that of the early Internet (and by extension to imply the impropriety of an organised centralised state role in providing security [120]). These names send important signals – to potential new recruits, to the rest of society, and to people involved in the crime themselves – about who is 'in' and 'out' of the community; the values underpinning what they do; and the kinds of practice and people who 'count'. The associated branding of these groups has also proved influential – the Anonymous pseudo-logo (see Figure 5) and Guy Fawkes mask have become major world cultural artefacts and essentially a visual shorthand for hackers.

Figure 5: The semi-official 'logo' of Anonymous

The names associated with particular individuals – often called 'handles' were historically an important part of the hacker subculture. They not only provided anonymity, but also served to perform the 'science fiction' and cool-factor aspects of the hacker subculture aesthetic. Early studies of cybercrime gave significant prominence to the individual names or handles associated with particular hackers (such as Gigabite, SOLO, MafiaBoy, St Jude, or Susy Thunder to name only a few). These handles were crucial repositories for personal reputation, either initially as a skilled hacker, or subsequently as a trustworthy seller of tools [68].

However, contemporary cybercrime is far more a phenomenon of industrialised as-a-service business-style offerings than individual skilled hackers or tool-sellers [22], and as a result we have observed a move away from the prominence of individual handles. Now, the name of the group or service, or the associated product, appears to be more important. In the as-a-service ecosystem individual handles are more a hazard than a benefit. The individual handles of the Mirai Kids or Fancy Bear are of diminishing interest; what is important is the brand that Mirai develops as a technical product or that `boredstresser.xyz` develops as a criminal service. In fact, the names of individuals play far more of a role for system administrators on popular cybercrime discussion forums and for the local celebrities of the cybersecurity defender community:

whether desisted hackers such as Condor (Kevin Mitnick) and MalwareTech (Marcus Hutchins), or security researchers and communicators like Lucky Green, Violet Blue, The Dark Tangent, or the Grugq.

3.4 Naming by cybersecurity companies

The signalling involved in the naming of groups by cybersecurity companies is also relevant, as it shapes the wider responses of defenders – and as a form of marketing affects the economic ecosystem of defence. The choice to use emotive or threatening language signals the size, sophistication, unpredictability, and risk of the threat; hence, it shapes the perceptions of potential customers that high-tech, high-security systems are needed for defence. The choice to use nationalistic language signals the relationship of cybersecurity companies as close partners of (generally) Western state security agencies, and their privileged position as players in arenas of global power and conflict [8, 78]. And the choice to brand differently – such as the APT series – signals seriousness, objectivity, and professionalism but also communicates that these threats are indeed Advanced and Persistent (and – as the number goes up – increasingly numerous).

Regulators, auditors, and standards all play a role in shaping the naming dynamics of the cybersecurity ecosystem as well. For example, ISO27001 provides an auditable international standard for the information security management systems which co-ordinate individual security controls within a wider secure system, particularly focusing on identifying, assessing, and mitigating specific risks and threats. This and other standards (such as the UK's Cyber Essentials) require entities to source an anti-malware solution, and thus competitive dynamics have emerged in the provider space for these. However sensible the requirement, it means that in the absence of wider consensus on naming, companies are directly incentivised to inflate the number of classes and varieties of actor they cover, and to compete on a range of branding activities in order to get the attention of CISOs. Hence the generation and classification of information about threats becomes an area of competitive distinction between providers rather than an attempt to accurately describe the ecosystem.

The result – which can be seen below – is often described by Ian Levy of the NCSC and others as 'Threat Actor Top Trumps' [9]- a dynamic familar to earlier eras of the cybersecurity ecosystem. Previously, anti-virus companies would compete via the scores their products achieved on the AVTest suite evaluation – often extolling the virtues of minor, meaningless variations in percentage scores between different products. The shift from marketing around malware to a focus on adversaries moved the arena of competition to one far more amenable to florid and compelling branding.

Hence, in an ecosystem with little central co-ordination of threat information, where a metric emerges (be it the number of named adversaries generated or a score on a test), incentives emerge to game it. The names of cybercrime groups call attention to a real set of risks, but aim to shape the response – in this case, to frame cybersecurity as a product that can only be produced by high-tech specialist companies rather than a field in which basic but difficult actions (such as those in Cyber Essentials) by companies can clear up much of the 'low-hanging fruit'.

3.5 Shared incentives to misrepresent through naming

From our previous examples, we can trivially observe many examples of naming – both by cybercrime and cybersecurity actors – performing the work of labelling deviance. These names shape how both defenders and attackers conceptualise the 'problem' of cybercrime, in general and specific terms. They very clearly play into a wider moral panic around cybercrime. Of course, cybercrime gives rise to serious harms and the moral panic we see occurring does not alter that. Rather, it means that concerted efforts by both attackers and defenders are being made – deploying naming as a key resource – to establish a moral, cultural and ideological terrain around cybercrime.

[9] Quite literally in the case of BAE Systems, who have produced a deck of Threat Actor cards as a marketing device for young graduate recruitment.

This serves to stabilise and establish the culture of cybercrime groups; in selling the threat to defenders it makes them seem cooler, edgier, more skilled, more dangerous, and more attractive to many potential recruits. Concretely – the self-image, culture, and stickiness of subcultural cybercrime communities (as opposed to serious organised crime or military outfits) is shaped as much by action from law enforcement and defenders as from the groups themselves. Hutchings critiques this process as contributing to the 'amplification of online deviancy' [56]. Equally, we argue that, as these processes establish and reinforce the deviant labelling of cybercrime subcultures, they simultaneously reinforce the culture of self-identified hackers working in security research and defence. This is a complex and changing identity – see Goerzen and Coleman [46] for a longer discussion – but as defence has become increasingly a matter of fairly routine checklist and compliance work for many, its attempts to play up a link to the deviant and exciting subcultures of hacking and its shared history does important work. It grants a countercultural air to what is now overwhelmingly (outside some remaining corners, especially in hacktivism) a corporate, pro-establishment, pro-big business endeavour, amplifies the sense of personal skill on the defence side as much as for the criminalised hackers, and plays an important role in smoothing transitions out of the hacker underground into legitimate penetration testing careers. Thus, participation in this ecosystem of naming and signalling is itself an important – and not always positive – intervention.

4 Names as scripting structures for cybercrime practices

As well as the symbolic or cultural dimension we outline above, names play a practical and material role in crime as well; beyond names for groups and individuals, names of criminalised practices and technologies also shape cybercrime ecosystems. The subcultural literature we discuss above influenced a range of subsequent scholarship, but for cybercrime research it has been particularly influential in shaping theories of Deviant Association and the development and circulation of crime 'scripts' [58]. In contrast to Routine Activities Theory criminological scholarship (studying the patterns of victimisation and criminal opportunity which typify cybercrime [65]), these focus on the development, learning, and evolution of practices within criminal communities.

4.1 Crime scripts

In these criminological accounts cybercrime is framed through the lens of Differential Association [114] – pathways into and out of cybercrime communities and subcultures are mediated by processes of learning and step-by-step induction into a community [35, 57]. In addition to learning core values, internalising a self-identity as a member, and building social links and status with others, this involves learning the technologies and practices associated with the deviant subculture. For the purposes of criminological analysis, these are often understood as scripts – knowledge structures that organise deviant activities (such as particular forms of crime) into a series of steps, each of which bundles up aspects of practice, required material technologies, opportunities, and affordances [29]. In cybercrime communities, these scripts are often formalised and traded as 'how-to' manuals, innovated on, developed, and extended – sometimes in response to law enforcement intervening in one part of the script [55, 118]. Where new vulnerabilities or capabilities emerge in the wider ecosystem, they can be incorporated into these scripts as well – and individuals in practice often improvise or alter scripts in the act of crime commission [57].

Names play an important role in organising and stabilising crime scripts – they give coherence to the practices, allowing them to be taught, communicated, or discussed. The assignment of a name and its acceptance by the community signals that a crime script – which began as a series of innovations and experimentations – has matured and become viable. The assignment of names to these scripts allows differentiation between similar types of crime. Once the innovation itself has formalised, the name allows others to develop it in a systematic way; experimenting with new business models, improved technology, or a social engineering technique that happens to work particularly well. A particular crime type might begin as a subset of another crime and then establish itself – such as eWhoring beginning as a subset of romance scams, and then establishing itself to the extent that it becomes its own category or section on

cybercrime forums [59]. Or a new script entirely might emerge around an external innovation – such as a new class of vulnerability or a newly launched social media platform.

4.2 Crime types

Extending beyond individual scripts – such as the use of a particular configuration of social and technical vulnerabilities to deploy a RAT program to compromise someone's computer – we see multiple scripts bundled into an overall 'crime type' that binds them together. In fact, what is often at issue at this wider scale is a combination of multiple components and scripts that interact and influence one another; a core technology or set of technologies, a characteristic social organisation (such as a large forum community or an archipelago of small Telegram and Discord channels), a set of practices arranged into a repeatable crime script, and a business model, which come together to form a stable criminal phenomenon with internal variations. These higher-level categories for crimes similarly establish their own names, which can then become repositories for a range of linked crime scripts. A subheading on a forum gives structure to these practices, enables people to find them, establishing a community-within-a-community around them [89]. This categorisation function of names serves to differentiate an ecosystem – instead of a general miasma of different forms and variations of low-level scam scripts, the community becomes a series of niches that people can develop, move between, and master. More generally, names as categories serve to structure the field of knowledge and expertise which participants in cybercrime, from neophytes to established players, need to master.

4.3 Evolution of cybercrime

These wider names also develop as the culture and organisation of the crime type changes. An example here is the changing branding of Denial of Service attacks. Initially linked to a set of tools circulating in the underground, these found a wider user base with the early forays of the Anonymous movement. The tools (such as the Low Orbit Ion Cannon), scripts, and branding changed to reflect a 'hacktivist' association [101, 102]. These attack tools then found a new market in gaming – with a lower-skilled user base leading to the success of a more industrialised 'as-a-service' model, and the practice was renamed 'booting' to reflect the gaming context [100]. At this point, the crime type took on a very different set of communities and customers; the people developing the technology prioritised different innovations and developments (as users targeting videogame servers want different things from those targeting major companies and websites, the user base's own links to developers meant more e.g. use of Minecraft servers themselves as attack infrastructure) [23]. The focus here became on maximum usability of the interface due to the younger user community. There is clearly a reciprocal and potentially self-reinforcing relationship between the branding associated with a crime form, the people who do it, and the ways that the technologies develop.

4.4 Cybercrime legislation

These names for categories of crime are of wider importance when a legal response materialises. The emergence of an apparently novel form of crime, and subsequent action by moral entrepreneurs to establish it as a social issue worth responding to, often results in new legislation or government policy 'naming' and defining the crime. In some cases, the crime is already covered by previous, more generally defined, legislation, but the new legislation serves as a wider social signal that authorities are taking it seriously or permits the extension of new powers [97] (for example, 'upskirting' being more generally covered under harassment [7, 45, 116]). In other cases, where law has been required to define a crime around the definition of a core technology, the new law (and name) attempts to match pace with criminal innovation. For example, in the UK, there was a period in which successive novel legislation on drug use attempted to criminalise particular chemical compounds on the basis of their structure [84]. This directly produced criminal innovation – with trivial changes to chemical formulae leading to the development of a range of Novel Psychoactive Substances. Subsequent UK legislation aimed to put this to bed by crudely criminalising all substances which produced psychoactive phenomena, other than specific exceptions such as alcohol and coffee [99].

In fact, we have not had the same problem with computer crime, despite the pace of criminal innovation. The UK's original Computer Misuse Act 1990 expediently does not define what a 'computer' is. This has been criticised down the years – but in fact it means that the law is brilliantly flexible, extensible to include mobile phones, servers, terminals, or cars [86]. One can commit a CMA offence by compromising any of these devices [112]. The CMA was further criticised as it was rarely used for prosecutions. This is because in practice, computer crime is prosecuted as fraud, which was defined in the Fraud Act 2006 which swept up much existing case law and definitions of fraud and simplified this into three broad categories of fraud. This is very broad and flexible, so, unlike with Novel Psychoactive Substances, there was little need to argue about the minutiae (which was the problem with the drugs)[39]. It doesn't matter if you brand your cybercrime as something exotic or new – you still can still be prosecuted under one of these generic laws.

4.5 Naming scripts as a signalling tactic

Despite the fact that cybercrimes tend to be prosecuted under generic rather than specific laws (despite the innovation in technologies used or the emergence of new criminal phenomena with new names), the cybercrime underground still attempts to use names for crime types tactically to shape the response of law enforcement and the perceptions of customers.

Exemplary of this are attempts to brand Denial of Service platforms as so-called 'stresser' services. Denial of Service attacks have historically been marketed to gamers as 'booting', allowing them to 'boot' their competition offline, however there was an effort by providers to describe this activity instead as 'stressing' [82]. Here, the name stresser is used to (falsely) signal that the service is not illegal and users are not breaking the law (implying that the intended use case is for stress-testing one's own website) [54]. In this case the name both attempts to back up a legal argument (if the provider is arrested, they can claim that they were operating a legitimate service that was abused); and to persuade their customers that they were not about to use an inherently illegal services. In some cases, this was fairly successful – with some in law enforcement and academia (see [36] for a discussion of this debate) entertaining for a while the notion that these genuinely might be 'dual-use' technologies with legitimate, non-criminalised use cases (despite the attack infrastructure itself almost always involving compromising machines and using bandwidth not owned by the provider, hence constituting a CMA offence).

Similar dynamics appear in the ways that criminal services use the naming system of the Internet infrastructure itself as a form of neutralisation [14]. Cybercrime services advertising in the West have continued to try to use .com domain names rather than .ru, .su or .onion (Tor Hidden Services) domains, despite the fact that these would make them harder to take down. The use of Russian or Onion domains would send a clear signal to users that the service is criminal – and hence, provide a barrier to them using it.

This is part of the broadening and changing of the subcultures associated with cybercrime – these services aim for a much wider user base, who are less involved in the hacker subculture [22, 82]. These effects can be observed empirically – for example, in the effectiveness of law enforcement advertising campaigns that inform users searching for these services that they are illegal [24]. Several rounds of law enforcement takedowns and interventions against the use of PayPal and other mainstream transaction services have begun to shift these practices; many have switched to the shadier-seeming Bitcoin, and have started using .ru and .su domain names, which appears to have reduced their customer base [15]. We show the marked switch away from .com to .ru/.su domains in Figure 6.

In recent years, with the industrialisation of many forms of cybercrime, these dynamics have changed. The subcultural side is still there – we observe naming to create identity and self, to demarcate boundaries, to share and organise crime scripts and practices, to mark insiders and outsiders, and to serve as attachment points for moral codes and judgements, interpretations and values. We now turn to the dynamics of naming in cybercrime as an ecosystem of technological innovation – a set of markets for both harmful and protective technologies.

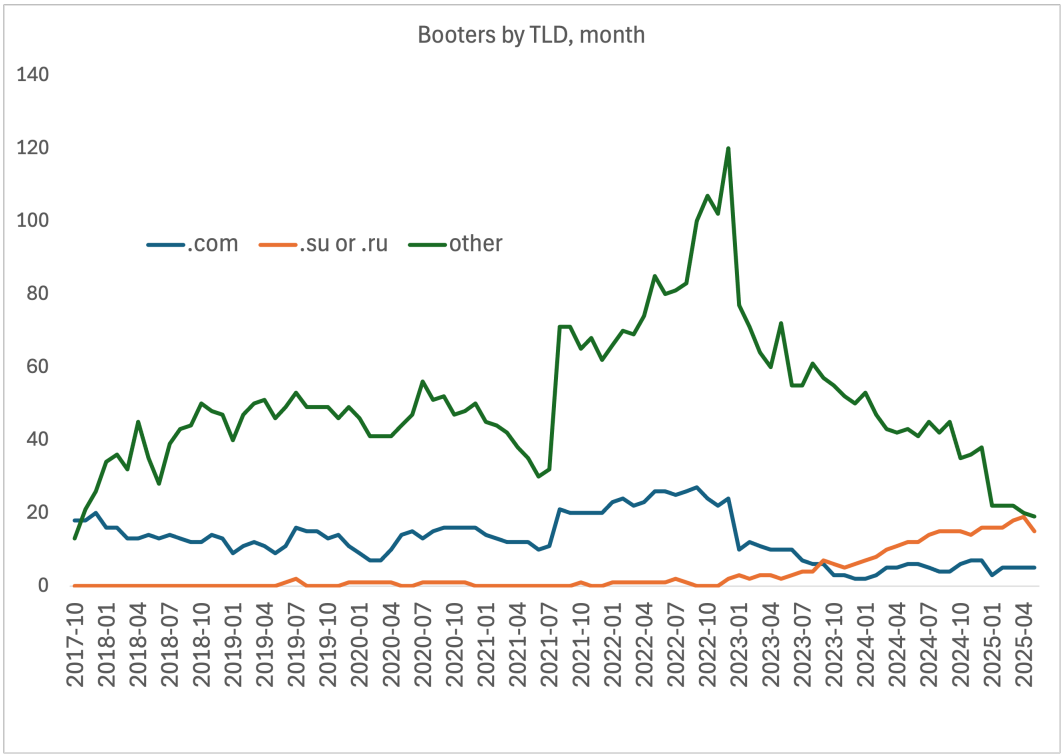

Figure 6: Number of active booters by month per Top Level Domains (TLD)

5 Names as brands in cybercrime markets

Names in cybercrime and cybersecurity clearly incorporate features of the labelling of criminal phenomena as we describe above. However, we argue, these are not only criminal markets, but markets for technological innovation. A now well-established body of scholarship in cybersecurity and cybercrime studies has developed economic accounts of cybercrime. This work initially prioritised individualistic Rational Actor perspectives [2, 79]. Further development of these engaged wider theories from behavioural economics and game theory [1, 4, 48]. More recently, a number of papers have begun to draw theory from evolutionary economics to understand the dynamics of cybercrime as a technology market or ecosystem, with features much like legitimate technology markets. These focus on the co-ordination of skills, information, forms of labour, and innovation dynamics [10, 16, 22, 44].

In comparison to criminological scholarship to date, evolutionary economics similarly frames crime as an ecosystem, but rather than focusing on subcultures, focuses on how technological products, business models, and practices evolve and diffuse within markets. While the market for defender services and products is clearly at least in part a market for tech innovation, we argue that the cybercrime ecosystem to which it is inescapably linked also has the dynamics of a tech innovation market. Apparently transformative innovations may never find a business model, may never diffuse successfully, may not compete with established products, and may not be adopted by key firms that influence the market. A new vulnerability is a technological innovation – and like other new technologies, its adoption and implementation is shaped by the dynamics of a competitive market. Much as in legitimate tech markets, names, categories, and branding play an important role in mediating these dynamics and shaping the behaviour of market actors.

5.1 Branding criminalised products

The first way in which names shape markets is the role they play in branding. In legitimate markets for products, brand names are an important way in which customers make sense of different offerings [34, 81]. Once a brand is established, it wields considerable power as a repository of consumer trust, prestige, and accumulated associations – many well-known High Street brands today are 150 years old, often carrying

the name of the company founder. Names are often chosen to be aspirational, to capture interest, to signal a place in a particular market, and to translate well internationally [25]. Changing well-established brands is both expensive and risky.

In other heavily industrialised criminal markets – such as drugs – names operate fully as branding, serving to distinguish products, imply novelty or signal quality. This is a long-standing phenomenon – for example, a study in 1983 found more than 400 different 'brand names' of heroin circulating in street markets in New York, often with their own associated logos, symbols, or coloured tape [47]. These were generally used to differentiate between products in an extremely crowded market with many competing sellers, with names usually chosen to signal potency (e.g. 'Black Death'). These facilitated an active 'street grapevine' through which purchasers informally established the highest quality offerings at any given time and then were able to seek them out directly via the branding. New customers entering the market could be directed by established buyers to seek a particular named brand.

As illicit markets have extended to digital marketplaces, naming still affords many of these functions, but with some differences. For contemporary online drug markets, branding is often used to signal the relative safety and legality of a particular product (especially where it is genuinely novel in type) [28], and for established drugs, to be eye-catching, incorporate subcultural references (especially in markets where customers identify within different drug-using subcultures), and signal potency or effect [31]. In practice, engaging with these brands (through comparing experiences, arriving at favourite, remembering particularly good or bad previous products) becomes part of the experience of using criminalised drugs – they are important material artefacts of the subculture [38].

5.2 Attempts to differentiate

While BANAL vulnerabilities are now often discovered and innovated by defenders (i.e. offensive researchers rather than those in the cybercrime communities) through primary research (with the marketing intended to get the media, customers, and researchers to 'buy in' to the new bug and take it seriously), attackers also engage in branding practices to popularise their own products and establish them in the market. Marketing and branding of malware and of small technical tweaks to existing products are important in driving action and success in underground criminal ecosystem. Most users of cybercrime services lack the technical expertise to assess the merits or novelty of different offerings, and so successful branding is generally a major factor in determining where the market moves initially [82]. We see evidence of these trivial dynamics of names-as-brands in the market for vulnerabilities and services; for example, booter services will generally attempt to distinguish themselves by advertising new 'methods' with their own names, often trivial variations on existing capabilities, but nonetheless effective in cultivating a rush of customers. When this branding is picked up by the media, it serves as free marketing for these new forms of crime, vulnerabilities, or innovations (such as using deepfakes to support frauds). Similarly, brands deployed by defenders reportedly do shape security responses – a BANAL vulnerabilty is more likely to set hares running than a plea to keep systems reliably patched.

The features that make for a compelling brand – namely, appeals to subculture, the use of humour or in-jokes, links to other successful legitimate brand ecosystems (such as anime or video games), signals of quality or qualities of the product, and links to existing and established products – are evident in both attacker and defender branding. The logo for Meltdown, for example, directly recalls the logo for Heartbleed released 4 years earlier – enabling an easy visual link between the two for the media and public. As the security press and defender industry are both directly concerned with gathering and reporting intelligence from the cybercrime underground, they also by necessity pick up and reinforce the brands that emerge there. This means that they are essentially forced to participate in the cybercrime market processes themselves; their incentives to 'market' a new vulnerability, business, or product as a threat to their consumers serve the same aims of signalling quality (in this case, level of threat and novelty), subcultural cues (to signal the criminal or foreign, and hence culturally alien nature of the threat), and to guide the customer (here, for defensive services and products) through establishing links to previous threats. Much as in the mirrored processes of labelling we describe above, both the legitimate

and criminalised sides of the ecosystem are aligned around the same process, with the same incentives, and produce the outcome together.

6 Names and information brokerage in innovation ecosystems

6.1 Directing adoption in an information-poor innovation environment

Cybercrime ecosystems are not simply a market for products – they are also markets for technological innovation. For those looking to adopt or defend against new forms of crime, the maturity and potential or novel technological innovations are difficult to assess. In technology markets, offerings are assessed by market actors through processes of social learning (especially computer technologies such as enterprise software, where on-paper documentation gives little sense of how a product will perform in practice) [107, 113]. It may take months or years of implementation work in order to assess the 'true' benefits and costs [95]. In legitimate technology innovation markets, information is often entirely lacking – or customers and users lack the skills to interpret it. Names therefore often work as important early signals to consumers – in, for example, biotechnology markets, they are strategically selected to tie perceptions of a new product or feature to those of previous successful technologies whose properties are known [9]. These processes of using names in 'anchoring' [106] innovation draw horizontal and vertical connections with other technologies. Beyond the naming of individual technologies, products, or innovations, markets generally over time group products together as 'classes' or 'categories' of technology. The names which emerge for these also play an important role in branding, marketing, and market shaping; existing categories provide a 'bucket' that can be used to make sense of emerging products and capabilities, while new category names signal breaks in a technological ecosystem [96].

These have analogies in cybercrime technologies, many of which can be seen in the discussion above. Vulnerabilities, bugs, and malware can all be understood usefully as innovations within a technological ecosystem, with many analogous features to 'legitimate' technological innovations. In illicit ecosystems, the same dynamics of frontline research, implementation, diffusion, and adoption apply; and these are similarly shaped by the availability of information in the market. Some new vulnerabilities or business models will be paradigm shifts or 'new science'; others will be incremental – small changes and improvements to existing technologies or practices [20].

Actors in cybercrime ecosystems need to decide where to spend their time. For those running an established business, it may be more economic to adopt an incremental improvement rather than risk switching to a new business model or paradigm [10]. For those engaged in frontline experimentation and innovation, there are large incentives to exaggerate the threat of esoteric or complex innovations that are by their nature extremely difficult to mature or exploit in practice (for models of how actors actually develop the technical beginnings of exploits into real capabilities, see, e.g. [13]). Thus, actors need to evaluate how mature a 'product' actually is – is this simply hype, or is it something that needs to be reckoned with immediately? This is also the case for defenders – is implementation likely to be within the reach of only the skilled and highly-resourced few, or is it something that will quickly be picked up? Is there a coherent business model that suggests the potential for mass exploitation, or is it likely to remain a rare and specialist threat?

6.2 Innovation intermediaries

Making sense of all this is a question of information circulation in the market – much as for a legitimate technology innovation market. In general, evolutionary economics assumed that these larger-scale categories and their attendant names were arrived at in a communitarian fashion; categories would be established over time via processes of market consensus-forming as offerings were assessed and clusters of innovation came together around broad product types [96]. However, more recently, scholarship has identified key 'innovation intermediaries' [74, 26] as playing a role in shaping markets – partly through the generation and management of categories and names. These are 'promissory' organisations [94] that act as information brokers and hence play a major role in structuring the market and directing activity. Pollack and

Williams [96] argue that, in the legitimate technology innovation ecosystem, consultancies like Gartner play an important role in naming new classes of technology and in categorising emerging products within older ones. Actors with perceived authority, like Gartner, can use the power of naming to co-ordinate the market and the landscape in which solutions are branded – they focus attention by signalling what the upcoming new developments to be reckoned with are. These intermediaries work to assess the ecosystem, identify clusters of innovation, and give a name to new categories of technology or product – which might not themselves realise that they are 'novel'. This name serves to draw a box around a new potential market, with players aligning themselves around these structures of naming and categorisation, identifying niches to exploit and markets to dominate [96].

Gartner (and similar intermediaries) produce a number of products that help markets overcome information deficits and evaluate claims made in the branding of novel innovations. Two notable Gartner products are well-known in the private sector, namely the Hype Cycle and the Magic Quadrant. The hype cycle hypothecates a characteristic curve (seen in Figure 7) associated with new innovations. To sustain a novel innovation to market maturity its promoters (and early adopters) need to set an enticing vision to secure investment. This also serves to work against Fear, Uncertainty, and Doubt – a strategy deployed by established powerful actors in an ecosystem to avoid disruption of their entrenched position by innovative newcomers [90]. However, this hype follows a curve – moving through the 'peak of inflated expectations', to the 'trough of disillusionment' as the bubble bursts, and through the 'slope of enlightment' as the true value is realised [111].

Analogous dynamics apply to new vulnerabilites or other innovations in cybercrime – the discoverer (either criminal or legitimate) needs to generate hype to push actors to adopt (either by buying a service, incorporating the innovation in their own scripts or technologies, or 'adopting' it as a defender by taking it seriously enough to mitigate it). For example, despite a rush of experimentation caused by a few successful cases, using generative AI to conduct email fraud may well not prove to provide any savings or benefits to attackers in the short term – but it may slowly become a feature of the wider ecosystem after the hype subsides. Gartner produces hype cycles for many classes of technology innovation – assessing where they currently are on this pathway.

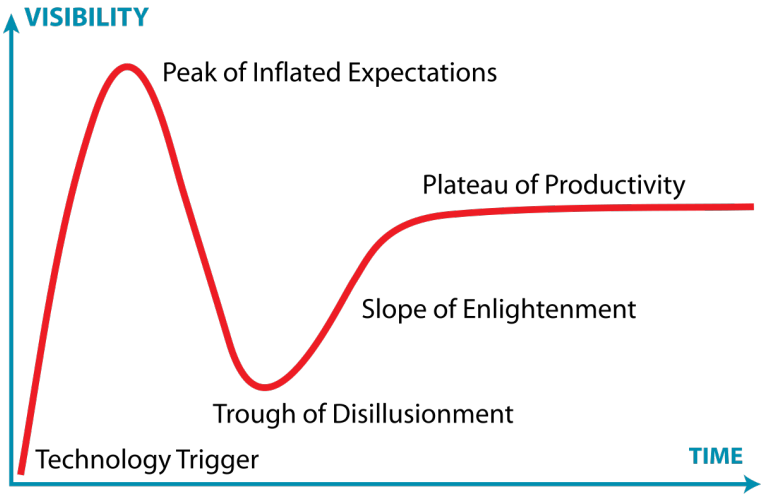

Figure 7: The Gartner Hype Cycle (Gartner, 2024).

The Gartner Magic Quadrant (see Figure 8) similarly assesses the maturity and market position of different innovation actors (and their associated technologies) [93]. Along axes of 'completeness of vision' and 'ability to execute', it places actors in four quadrants – challengers, who execute well but currently lack alignment with the landscape and direction of the overall ecosystem; visionaries, who understand where the market is heading but lack the ability to consistently deliver; niche players, who focus fairly well within a narrow area; and leaders, who both have capability in the present and are strategically aligned

with the ongoing long-term trends. Gartner develops both these products for the defence side of the cybercrime ecosystem – but crucially, not for the attackers.

Figure 8: The Gartner Magic Quadrant (Gartner, 2024).

6.3 Information asymmetries

In understanding the cybercrime ecosystem, information diffusion is a real problem; the desired outcome for both attackers looking to invest their time in developing effective exploits and defenders looking to mitigate them is to have an accurate assessment to hand of the threat, potential scale, current maturity, and pathways to exploitation of a new innovation (be it in the technology, business model, or associated practices).

Currently, the incentives are for attackers (if they are service providers) to rebrand trivial new capabilities as transformative, or (if they are innovators) to waste their time on exploring exotic exploits in niches that may never reach maturity, thus in both cases stifling innovation and stagnating the market around a few lucrative offerings such as ransomware and fraud. In the absence of venture capital funding to protect nascent innovations in niches and shepherd them to maturity and markets (except possibly for some state-aligned groups), it appears that scalable and transformative endogenous innovation is likely to continue to be rare.

For defenders, this information asymmetry also has negative effects. Effective communitarian forms of assessing, categorising, and naming vulnerabilities are frustrated by commercial incentives – companies will not share their experiences with one another except in extremis. In the absence of effective and authoritative information brokerage or communitarian knowledge-making within the ecosystem, cybersecurity companies are also attempting to function as innovation intermediaries, by deploying their power and authority to name new kinds of threat, then using these to co-ordinate, brand, and market that threat to defenders. For well-established security companies, their visibility of the ecosystem across several clients may give them a genuinely wide view of the threat landscape and the relative severity of a given development. However, as demonstrated by our BANAL vulnerabilities, their incentives to communicate this accurately to their customers, police, policymakers, the media, and the public are mismatched. Moreover, while BANAL vulnerabilties may get a threat board-level attention and support within a company, periodically

forcing cybersecurity teams to break their normal routines of threat assessment, patching, and mitigation simply because their boss has seen a news report can also lead to negative outcomes. Not least, this risks producing a form of 'alert/alarm fatigue' [110, 60] in teams over time.

6.4 Economics and performativity in cybercrime innovation ecosystems

In this paper, we have documented a range of functions performed by the names and brands which circulate in the cybercrime ecosystem, drawing on different bodies of theory from criminology, cybersecurity, innovation theory, and evolutionary economics. But what happens when you bring these bodies of theory together – names as cultural labels, names as an organising structure for practices, names as brands for marketing novel products, and names as a mechanism for assessing and managing innovation? We can observe the *symbolic* acts of naming as labelling and branding bleeding into the *practical* co-ordination of practices and information brokerage. But what does this tell us about the economics of cybercrime and cybersecurity?

Each of these forms of naming and branding which we describe are ways in which different actors attempt to influence the production and circulation of knowledge which forms the information economy of the cybercrime ecosystem. It is this economy which shapes much of the activity of actors – what they prioritise, how they position themselves, and how they make sense of the costs and benefits of different decisions. It also shapes the evolutionary dynamics of the ecosystem over time – which niches emerge, which strategies succeed, and how the landscape changes. Within this environment, dynamics emerge which are recognisable from accounts of more mainstream economic scenarios, namely, attempts at naming, modelling, measuring, and categorising become *performative*, in that they shape the very reality which they describe.

A well-known example of performativity in economics are the Black-Scholes-Merton equations for the dynamics of derivatives in a financial market. As described by Mackenzie [69], this was initially not necessarily a particularly *accurate* measure of risk, however it proved a popular way of quantifying forms of uncertainty that had previously been unmeasurable, and the more who adopted it, the more the market behaved *as though it were true*. Hence, the method used for measuring the system shaped the system itself. Attempts to impose order on information in the cybercrime ecosystem – whether they be through names, models, or measurements – all shape the actions of the actors therein, and hence the dynamics of the ecosystem. The characterisation of threats and threat groups as numerous, frightening, transformative, and sophisticated changes what law enforcement and defenders do [20] which can in turn, lead to de-prioritising the more mundane, everyday 'basics' of cybersecurity which protect against the vast majority of attacks (and hence contribute to the self-fulfilling prophecy of cybercrime as a terrifying problem that is escalating in severity as more and more critical services fall victim to major public breaches). The careless, organic, or partial production of apparently-objective metrics and measurements can, as we have documented, lead to incentives to simply game these – a practice which we observe both on the adversary and defender sides of cybersecurity.

Mackenzie also documents the opposite case, namely that some forms of measurement and modelling can make themselves *less* true when adopted (which he terms counter-performativity) – for example, when a Google Maps model suggests that a route will have very little traffic on it to hundreds of thousands of car drivers who immediately flock there. This can also be observed in cybercrime ecosystems – namely, that if law enforcement measure the number of attacks committed by various DDoS services, create a ranked list, and prioritise the arrests of the top X biggest booter providers in the world, then being slightly less successful (i.e. X+1 on the list) might well be a recipe for far better long-term performance.

In an ecosystem model, attention to the *performative* dynamics of information helps us understand the strategic incentives at play for different actors – not only in how they make decisions about what they do, but in terms of how they signal information to the wider ecosystem through tactics like naming and branding. In addition to seeking out and occupying key niches and competing with their contemporaries, both attackers and defenders are also shaping the information environment directly, creating second-order co-ordination effects which cannot be captured through an individual rational-actor decision model.

Performative dynamics in economic ecosystems exhibit many of the 'bootstrapping' functions that criminologists have documented in criminal labelling – namely, the alignment of small-scale incentives over time can create large-scale structural change. As the consequences of these strategies and incentives aggregate over time, they have boxed much of the defender ecosystem into fruitless competitions over signalling rather than a co-ordinated assessment of risk.

To summarise: a core information brokerage function is being turned to the services of a moral panic and marketing for cybersecurity companies; labelling functions are predominating over brokerage ones due to misplaced incentives, and this is leading to perverse outcomes. This is producing cascades of labelling that threaten to push more people into cybercrime and misrepresents the issues to law enforcement and victims in ways that misdirect resources. Branding is exploding the cybercrime space rather than integrating it.

7 Practical concerns

There is a clear need for better information brokerage and 'promissory work' in the cybersecurity market ecosystem. Agencies like Gartner do in fact assess Threat Intelligence, Security Technology companies and software portfolios, but these analyses are focused entirely on enterprise and managed services for defenders. Cybersecurity is a fairly unique innovation market because it is adversarial – joined by definition to a competitor innovation market for emerging technologies created by attackers. We argue that a 'market analyst' function is sorely lacking for this second half of the security ecosystem; the proliferation of often-unhelpful practices of naming is an attempt by the market to fill this vacuum. The utility of products like the Hype Cycle and Magic Quadrant is partly that they provide communities something to argue over – they have the authority of a trusted intermediary which is heavily incentivised to attempt to be objective, but provide an infrastructure around which market participants can develop and contest a communal perspective. Conversely, one can also see the negative effects that the production of a Hype Cycle and Magic Quadrant for vulnerabilities and crime groups might have in stimulating innovation and competition for attackers – becoming a de facto leaderboard.

7.1 The role of academia

Academics and researchers might also consider themselves as fairly objective information brokers. A common complaint by academics themselves is the time lag associated with formal publication – though there is a well-established culture of responsible disclosure and the use of pre-prints to signal the wider ecosystem, although this can lead to issues where some venues insist that this undermines their double-blind review system [12]. There are also clearly some perverse incentives for academics – who much like security companies and the press are encouraged to make things seem novel or important. Having a BANAL bug in the mainstream press is direct evidence of impact, and hence a driver for funding and promotion. The main nominal sites of knowledge production in cybersecurity – the academy, private practitioners, major security conferences, and the media (and to some extent state security services) are part of the same ecosystem of attention and prestige; their incentives often align.

There is evidence of changes in recent years – researchers used to write papers about very specific cybercrimes (particularly new groups, business models, tools or activities) while over the last few years they have moved towards producing SoK papers which integrate knowledge across the existing literature. However, it might be argued that this is merely documenting a very scattered literature to help people catch up. Writing an SoK paper is a lot of work so is often suggested to first year PhD students, who may well have finished it by their final graduation. Academics also lack data on the reality of cybercrime (despite initiaitves like the Cambridge Cybercrime Centre's CrimeBB database [89]).

While academics and researchers have clear strengths in lab-based research and the discovery of new vulnerabilities, this is only one part of a cybercrime phenomenon – which incorporates these methods into underground tools, practices, business models, and processes. It is this holistic view which reflects the 'maturity' of a particular cybercrime threat. Information on these is far more available to state security agencies, the private companies being attacked and the security companies defending them; the incentives

are overwhelmingly not to share this information (as it is a core product for many security companies, makes attacked companies look bad, and falls under national security protections for the state).

7.2 Existing initiatives

Two ongoing sets of initiatives suggest fruitful avenues for development. The first involves various state and institutional authorities that have been emerging to take this role focused around government and often similarly co-ordinating a range of private, law enforcement, and academic players. These include in the UK the National Technical Authorities (for cybersecurity, GCHQ's National Cyber Security Centre) who have also done much – in some cases but not others – to puncture the hype around novel but arcane vulnerabilities and groups [80] (see for example, Ian Levy's comments on 'magic amulets' [66]). In the US, this function is carried out by the Cybersecurity and Infrastructure Security Agency (CISA). A recent example of this is the NCSC guidance on assessing 'forgivable' versus 'unforgivable' vulnerabilities [83]. The NCSC has also put significant work into developing information sharing about threats and attacks with and between private sector Critical National Infrastructure providers via Information Exchanges.

Another UK intervention is the recent 'Hurricane' rating system for attack severity, which proposes that a newly created Cyber Monitoring Centre work to assess attacks hitting the UK [33]. Over a one-month period, the CMC collates and analyses a range of data sources, placing the attack on a scale with x-axis being affected population and y-axis financial impact. The square where the attack meets on these two axes corresponds to its 'hurricane category'.[10]

There are some issues with this, particularly that it is retrospective rather than prospective and it often takes several months for forensics and accounting of actual damage and effects; not all of which can be easily financially quantified. A broader issue with official rankings more broadly is that they become performative – they shape the reality that they are measuring. As Richard Hamming (of the Hamming code) argued, "you get what you measure" [51]. Companies' stock prices go up or down and individual careers are made on small movements in Gartner's assessments of their fortunes. Any ranking or assessment system creates enormous incentives for gaming – to inflate severity to enrol the interest of the FBI or NCA in investigation, or to deflate it to bring it under the level at which it needs to be reported at all.

The wider context does create some incentives for government-centred projects to overstate (or mis-state) the inevitability and threats of major new technologies, such as quantum computing, artificial intelligence, and blockchain, in the new context of techno-nationalism and the return of national industrial strategies. Concretely, boosterism of these sectors and the potentials of associated immature tech may well be important to ministers who have just green-lit millions of pounds of investment in data centres or Stargate technologies.

A second approach might be found in the growth of multi-agency working groups, incorporating infrastructure providers, law enforcement, and academics. In these, commercially disinterested parties such as researchers (who do admittedly have their own incentives to inflate the severity of new threats) can play a role in collectively assessing what new threats or groups are worth worrying about in partnership with frontline law enforcement and defenders, using this to organise communal action.

In theory, these groups have design elements which could serve to mitigate the perverse incentives we describe above. By carefully incorporating both informal and formal protections around information sharing, 'TLP Red' information can be passed between participants within the context of the group against the grain of incentives that usually prohibit information sharing between law enforcement and private companies. This framing permits fast diffusion of information, about a shared 'problem' (for example, a new style of DDoS). The intent is for this heterogeneous group – with many different kinds of

[10]The NCSC is merely rating each issue on a scale of Cat1 to Cat5, they are not naming them. Interestingly, the UK Met Office started naming storms in 2015 (the US has been naming hurricanes since 1953 [119]) with a view to simplifying communications and making the public more aware of imminent danger [117].

expertise – to come to a balanced communal perspective, rather than one based only on the concerns of their individual parent organisations. Thus, if conflicts, egos, and incentives can be managed, when a new issue arises a working group perspective should develop (and be tested and evaluated in an ongoing fashion) rather than merely a law enforcement, security company, or academic one.

This approach has seen some recent successes, for example, in the Big Pipes group described by Greenberg in the popular press [49], in innovative activities led by law enforcement to disrupt the DDoS-as-a-service ecosystem [24] and in the mobilisation of action at scale in the Internet peering landscape [21]. A 2008 group who focussed solely on tackling the Conficker malware threat, disbanding thereafter, documented the lessons they had learnt from their project [27]. However, although this working group approach can be productive, it generally involves small groups of elite trusted actors working largely in secret to achieve major change or disruption – it does not diffuse information to the wider ecosystem.

8 Conclusions

We started by considering BANAL bugs (with names and logos) and provided a brief account of the naming of malware. We then considered how cybercrime groups are named and the dual role of Law Enforcement (and military) naming of operations to both obscure detail and to provide PR for their activities.

We noted that one of the problems that occurs is that a plethora of names arise for the same group or program. One of this paper's authors is fond of observing that threat actor groups aren't really dangerous unless they have more than three names – just like the rule of thumb from 20+ years ago that malware was only common enough to be interesting (and a threat) if it had been given more than one name. The reality behind this aphorism is that groups that get identified independently by different sets of investigators are probably operating at considerable scale.

It is clear that names play a wide variety of roles in cybercrime ecosystems; we discussed in turn the scholarship on each of these from criminological and economic perspectives, linking them to particular examples. Within both bodies of theory, we see names playing a cultural or signalling function – whether for group identity or consumer branding – and note that criminalised groups and security professionals essentially work to the same ends. They are both incentivised to buy into and reproduce the same labels and the same brands.

In both economic and criminological scholarship, alongside these cultural functions, there are a range of more practical, material functions of naming – names materially organise criminalised practices through cohering crime types and scripts, and they are a crucial mediator for information flow in the innovation ecosystems of cybercrime and cybersecurity. Here, incentives for attackers and defenders do differ. However, we argue that the lack of strong intermediaries to structure this landscape is creating a gap. This gap is predominantly being filled by the cultural functions of naming; these are bleeding over, allowing labelling and marketing to distort the information functions of cybercrime and cybersecurity markets. Often, individual names are playing both functions – they simultaneously operate as cultural and ideological features of the market, and also material structures of the underlying economy.

The issues of branding, naming, and marketing which we identify in this paper are well-known in industry; we attempt here to develop a systematic framework, with empirical examples, to make sense of this at scale. We also innovate by proposing our own brand name (BANAL bugs) and logo to market this concept, as something of an experimental intervention. If we are accurate in arguing that branding plays this outsize role, the deployment of our own branding may hopefully function as a corrective. For future research, we believe that there is significant theoretical and empirical ground to be developed in treating cybercrime and cybersecurity as linked innovation ecosystems – the tools and concepts of evolutionary economics and an attention to the *performative* characeristics have real promise for making sense of these dynamics and intervening further.

Figure 9: Our tentative marketing campaign for BANAL bugs

References

[1] Tansu Alpcan and Tamer Başar. *Network security: A decision and game-theoretic approach*. Cambridge University Press, 2010.

[2] Ross Anderson. Security economics: a personal perspective. In *Proceedings of the 28th Annual Computer Security Applications Conference*, pages 139–144, 2012.

[3] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, Alex J Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. Understanding the Mirai botnet. *USENIX Security Symposium*, pages 1093–1110, 2017.

[4] Michelle Baddeley. Information security: Lessons from behavioural economics. In *Workshop on the Economics of Information Security*, 2011.

[5] BBC. How do police operations get their names?, 2008. URL: `http://news.bbc.co.uk/1/hi/magazine/7288489.stm`.

[6] Howard S Becker. Outsiders. *Studies in the Sociology of Deviance*, 1, 1963.

[7] Valerie Bell, Craig Hemmens, and Benjamin Steiner. Up skirts and down blouses: A statutory analysis of legislative responses to video voyeurism. *Criminal Justice Studies*, 19(3):301–314, 2006.

[8] Victoria Bernal. The cultural construction of cybersecurity: Digital threats and dangerous rhetoric. *Anthropological Quarterly*, 94(4):611–638, 2021.

[9] Reginald Boersma, P Marijn Poortvliet, and Bart Gremmen. The elephant in the room: How a technology's name affects its interpretation. *Public Understanding of Science*, 28(2):218–233, 2019.

[10] Rainer Böhme, Richard Clayton, and Ben Collier. Silicon den: cybercrime is entrepreneurship. In *Workshop on the Economics of Information Security*, 2021.

[11] Martin Booth. *Cannabis: a history*. Macmillan, 2015.

[12] Nicholas Boucher and Ross Anderson. Talking trojan: analyzing an industry-wide disclosure. In *Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses*, pages 83–92, 2022.

[13] Sergey Bratus, Michael E. Locasto, Meredith L. Patterson, Len Sassaman, and Anna Shubina. Exploit programming: From buffer overflows to "weird machines" and theory of computation. *;login:*, 36(6), 2011.

[14] Russell Brewer, Sarah Fox, and Caitlan Miller. Applying the techniques of neutralization to the study of cybercrime. *The Palgrave handbook of international cybercrime and cyberdeviance*, pages 547–565, 2020.

[15] Ryan Brunt, Prakhar Pandey, and Damon McCoy. Booted: An analysis of a payment intervention on a DDoS-for-hire service. In *Workshop on the Economics of Information Security*, pages 06–26, 2017.

[16] Michele Campobasso, Radu Radulescu, Sylvan H.J.P. Brons, and Luca Allodi. You can tell a cybercriminal by the company they keep: A framework to infer the relevance of underground communities to the threat landscape. In *Workshop on the Economics of Information Security*, 2023.

[17] Catalin Cimpanu. There's a 120,000-strong IoT DDoS botnet lurking around, 2016. URL: https://news.softpedia.com/news/there-s-a-120-000-strong-iot-ddos-botnet-lurking-around-507773.shtml.

[18] Stanley Cohen. *Folk devils and moral panics*. Routledge, 2011.

[19] Gabriella Coleman. *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. Verso books, 2015.

[20] Ben Collier and Richard Clayton. A "sophisticated attack"? innovation technical sophistication and creativity in the cybercrime ecosystem. In *Workshop on the Economics of Information Security*, 2022.

[21] Ben Collier and Richard Clayton. Peer (ing) pressure: Achieving social action at scale in the internet infrastructure. In *Workshop on the Economics of Information Security*, 2024.

[22] Ben Collier, Richard Clayton, Alice Hutchings, and Daniel R. Thomas. Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies. In *Workshop on the Economics of Information Security*, 2020.

[23] Ben Collier, Daniel R Thomas, Richard Clayton, and Alice Hutchings. Booting the booters: Evaluating the effects of police interventions in the market for denial-of-service attacks. In *Proceedings of the Internet Measurement Conference (IMC)*, pages 50–64. ACM, 2019.

[24] Ben Collier, Daniel R Thomas, Richard Clayton, Alice Hutchings, and Yi Ting Chua. Influence, infrastructure, and recentering cybercrime policing: evaluating emerging approaches to online law enforcement through a market for cybercrime services. *Policing and Society*, pages 1–22, 2021.

[25] Leslie Collins. A name to compare with: A discussion of the naming of new brands. *European Journal of Marketing*, 11(5):337–363, 1977.

[26] Ana Colovic, Annalisa Caloffi, Federica Rossi, Stefania Paladini, and Mehdi Bagherzadeh. Innovation intermediaries and emerging digital technologies, 2024.

[27] Conficker Working Group. Lessons learned. White Paper, 2011. URL: https://www.senki.org/wp-content/uploads/2020/11/Conficker-Working-Group-Lessons-Learned-June-2010-Published-January-2011-whitepaper_76813745321.pdf.

[28] Ornella Corazza, Giuseppe Valeriani, Francesco Saverio Bersani, John Corkery, Giovanni Martinotti, Giuseppe Bersani, and Fabrizio Schifano. "Spice,","kryptonite","black mamba": an overview of brand names and marketing strategies of novel psychoactive substances on the web. *Journal of Psychoactive Drugs*, 46(4):287–294, 2014.

[29] Derek B Cornish. Crimes as scripts. In *Proceedings of the International Seminar on environmental criminology and crime analysis*, volume 1, pages 30–45. Florida Department of Law Enforcement Tallahassee, 1994.

[30] Tom Cotterill. M&S cyber attack is linked to gang of teenage hackers called 'Scattered Spider' who also targeted casino giant MGM. *Daily Mail*, 2025.

[31] Nicolae Eduard Craciunescu. Drugs, brands and consumer culture: the sign-value of the products sold on the darknet marketplaces. *Drugs and Alcohol Today*, 21(2):124–134, 2021.

[32] Sean Creaney. Targeting, labelling and stigma: challenging the criminalisation of children and young people. *Criminal Justice Matters*, 89(1):16–17, 2012.

[33] Cyber Monitoring Centre. Event categorisation methodology, 2025. URL: https://cybermonitoringcentre.com/wp-content/uploads/2025/02/CMC-Methodology_5Feb2025.pdf.

[34] Melissa Davis and Jonathan Baldwin. *More than a name: An introduction to branding*, volume 11. AVA publishing, 2005.

[35] Thomas E Dearden and Katalin Parti. Cybercrime, differential association, and self-control: knowledge transmission through online social learning. *American Journal of Criminal Justice*, 46(6):935–955, 2021.

[36] David Douglas, José Jair Santanna, Ricardo de Oliveira Schmidt, Lisandro Zambenedetti Granville, and Aiko Pras. Booters: can anything justify distributed denial-of-service (DDoS) attacks for hire? *Journal of information, communication and ethics in society*, 15(01):90–104, 2017.

[37] David Downes. *The Delinquent Solution (Routledge Revivals): A Study in Subcultural Theory*. Routledge, 2013.

[38] Micheline Duterte, Camille Jacinto, Paloma Sales, and Sheigla Murphy. What's in a label? ecstasy sellers' perceptions of pill brands. *Journal of psychoactive drugs*, 41(1):27–37, 2009.

[39] Lilian Edwards, Judith Rauhofer, and Majid Yar. Recent developments in UK cybercrime law. *Handbook of Internet Crime*, pages 413–436, 2013.

[40] Electronic Transactions Development Agency (Thailand). Threat group cards: A threat actor encyclopedia, 2024. URL: https://apt.etda.or.th/cgi-bin/aptgroups.cgi.

[41] Finn-Aage Esbensen, L Thomas Winfree Jr, Ni He, and Terrance J Taylor. Youth gangs and definitional issues: When is a gang a gang, and why does it matter? *Crime & delinquency*, 47(1):105–130, 2001.

[42] F-Secure. Virus:Boot/Stoned, 2010. URL: https://www.f-secure.com/v-descs/stoned.shtml.

[43] Bob Fine. Labelling theory: An investigation into the sociological critique of deviance. *Economy and Society*, 6(2):166–193, 1977.

[44] Vaibhav Garg and L Jean Camp. Why cybercrime? *ACM SIGCAS Computers and Society*, 45(2):20–28, 2015.

[45] Alisdair A Gillespie. "Up-skirts"and"down-blouses": Voyeurism and the law. *Criminal Law Review*, 5:370, 2008.

[46] Matt Goerzen and Gabriella Coleman. Wearing many hats. *Data and Society*, 2022.

[47] Paul J Goldstein, Douglas S Lipton, Edward Preble, Ira Sobel, Tom Miller, William Abbott, William Paige, and Franklin Soto. The marketing of street heroin in New York City. *Journal of Drug Issues*, 14(3):553–566, 1984.

[48] Cleotilde Gonzalez. From individual decisions from experience to behavioral game theory: lessons for cybersecurity. In *Moving Target Defense II: Application of Game Theory and Adversarial Modeling*, pages 73–86, 2012.

[49] Andy Greenberg. The team of sleuths quietly hunting cyberattack-for-hire services. *Wired*, 2023. URL: https://www.wired.com/story/big-pipes-ddos-for-hire-fbi/.

[50] Ben Grubb. Heartbleed disclosure timeline: who knew what and when. *Sydney Morning Herald*, 2014. URL: https://web.archive.org/web/20141125191721/http://www.smh.com.au/it-pro/security-it/heartbleed-disclosure-timeline-who-knew-what-and-when-20140415-zqurk.html.

[51] Richard Hamming. You get what you measure, 1995. URL: https://www.youtube.com/watch?v=LNhcaVi3zPA.

[52] Alan Harding. UK military operation names, 2010. URL: http://www.alanharding.com/Military/codenames/operations.html.

[53] Thomas J Holt. Examining the role of technology in the formation of deviant subcultures. *Social Science Computer Review*, 28(4):466–481, 2010.

[54] Thomas J Holt, Jin R Lee, and Olga Smirnova. Exploring risk avoidance practices among on-demand cybercrime-as-service operations. *Crime & Delinquency*, 69(2):415–438, 2023.

[55] Jack Hughes, Seth Aycock, Andrew Caines, Paula Buttery, and Alice Hutchings. Detecting trending terms in cybersecurity forum discussions. In Wei Xu, Alan Ritter, Tim Baldwin, and Afshin Rahimi, editors, *Proceedings of the Sixth Workshop on Noisy User-generated Text (W-NUT 2020)*, pages 107–115. Association for Computational Linguistics, 2020.

[56] Alice Hutchings. The amplification of online deviancy through the language of violent crime, war, and aggression. *IEEE Security & Privacy*, 22(2):81–84, 2024.

[57] Alice Hutchings and Richard Clayton. Exploring the provision of online booter services. *Deviant Behavior*, 37(10):1163–1178, 2016.

[58] Alice Hutchings and Thomas J Holt. A crime script analysis of the online stolen data market. *British Journal of Criminology*, 55(3):596–614, 2015.

[59] Alice Hutchings and Sergio Pastrana. Understanding ewhoring. In *IEEE European Symposium on Security & Privacy (EuroS&P)*, pages 201–214, 2019.

[60] Paul Kearney, Mohammed Abdelsamea, Xavier Schmoor, Fayyaz Shah, and Ian Vickers. Combating alert fatigue in the security operations centre. *Available at SSRN 4633965*, 2023.

[61] Yoongu Kim, Ross Daly, Jeremie Kim, Chris Fallin, Ji Hye Lee, Donghyuk Lee, Chris Wilkerson, Konrad Lai, and Onur Mutlu. Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors. In *Proceedings – International Symposium on Computer Architecture*, 06 2014.

[62] Malcolm Klein. The eurogang definition. *The Oxford Handbook of Gangs and Society*, page 15, 2024.

[63] Paul Kocher, Jann Horn, Anders Fogh, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom. Spectre attacks: Exploiting speculative execution. In *IEEE Symposium on Security & Privacy*, pages 1–19, 2019.

[64] Andrew Kwong, Daniel Genkin, Daniel Gruss, and Yuval Yarom. Rambleed: Reading bits in memory without accessing them. In *IEEE Symposium on Security & Privacy*, pages 695–711, 2020.

[65] Eric Rutger Leukfeldt and Majid Yar. Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, 37(3):263–280, 2016.

[66] Ian Levy. National scale cyber security. In *USENIX Enigma*, 2017. URL: https://www.usenix.org/conference/enigma2017/conference-program/presentation/levy.

[67] Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Anders Fogh, Jann Horn, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg. Meltdown: Reading kernel memory from user space. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 973–990, 2018.

[68] Jonathan Lusthaus. Trust in the world of cybercrime. *Global crime*, 13(2):71–94, 2012.

[69] Donald MacKenzie. Is economics performative? option theory and the construction of derivatives markets. *Journal of the history of economic thought*, 28(1):29–55, 2006.

[70] Mandiant. APT1: Exposing one of China's cyber espionage units, 2013. URL: https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf.

[71] Lesley McAra and Susan McVie. Youth crime and justice: Key messages from the Edinburgh study of youth transitions and crime. *Criminology & Criminal Justice*, 10(2):179–209, 2010.

[72] Lesley McAra and Susan McVie. Negotiated order: The groundwork for a theory of offending pathways. *Criminology & Criminal Justice*, 12(4):347–375, 2012.

[73] J Stanley Metcalfe. Evolutionary economics and technology policy. *The economic journal*, 104(425):931–944, 1994.

[74] Morgan Meyer and Matthew Kearnes. Introduction to special section: Intermediaries between science, policy and the market. *Science and public policy*, 40(4):423–429, 2013.

[75] Robert A Mikos and Cindy D Kam. Has the "m" word been framed? marijuana, cannabis, and public opinion. *PLoS One*, 14(10):e0224289, 2019.

[76] Paweł Miśkowiec. Name game: the naming history of the chemical elements—part 3—rivalry of scientists in the twentieth and twenty-first centuries. *Foundations of Chemistry*, 25(2):235–251, 2023.

[77] Steve Mizrach. Iterative discourse and the formation of new subcultures. *Anthropology of Consciousness*, 8(4):133–143, 1997.

[78] Norma Möllers. Making digital territory: Cybersecurity, techno-nationalism, and the moral boundaries of the state. *Science, technology, & human values*, 46(1):112–138, 2021.

[79] Tyler Moore, Richard Clayton, and Ross Anderson. The economics of online crime. *Journal of Economic Perspectives*, 23(3):3–20, 2009.

[80] Adrian Moss. Telecoms breaches & attacks (or how advanced is APT?), 2021. URL: https://niccstandards.org.uk/wp-content/uploads/2021/11/08-NICC-Breaches-and-Attacks.pdf.

[81] John Murphy. Branding. *Marketing Intelligence & Planning*, 6(4):4–8, 1988.

[82] Roberto Musotto and David S Wall. More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime. *Trends in Organized Crime*, pages 1–19, 2020.

[83] National Cyber Security Centre. A method to assess 'forgivable' vs 'unforgivable' vulnerabilities, 2025. URL: https://www.ncsc.gov.uk/report/a-method-to-assess-forgivable-vs-unforgivable-vulnerabilities.

[84] Jessica Neicun, Andres Roman-Urrestarazu, and Katarzyna Czabanowska. Legal responses to novel psychoactive substances implemented by ten European countries: An analysis from legal epidemiology. *Emerging trends in drugs, addictions, and health*, 2:100044, 2022.

[85] Lars Öhrström and Norman E. Holden. The three-letter element symbols: Lars öhrström talks to Norman E. Holden about unnilhexium, and other periodic table ghosts of the cold war. *Chemistry International*, 38(2):4–8, 2016.

[86] Emmanuela Onyilofor. The effectiveness or otherwise of the Computer Misuse Act 1990: Technological development and technology neutrality. *Available at SSRN 2760024*, 2014.

[87] Mary Virginia Orna. On naming the elements with atomic number greater than 100. *Journal of Chemical Education*, 59(2):123, 1982.

[88] Tim Parisi. Not a SIMulation: CrowdStrike investigations reveal intrusion campaign targeting telco and BPO companies, 2022. URL: https://www.crowdstrike.com/en-us/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/.

[89] Sergio Pastrana, Daniel R Thomas, Alice Hutchings, and Richard Clayton. CrimeBB: Enabling cybercrime research on underground forums at scale. In *Proceedings of the 2018 World Wide Web Conference*, pages 1845–1854, 2018.

[90] Bryan Pfaffenberger. The rhetoric of dread: Fear, uncertainty, and doubt (FUD) in information technology marketing. *Knowledge, Technology & Policy*, 13(3):78–92, 2000.

[91] Fred Plan, Van Ta, Michael Barnhart, Jeff Johnson, Dan Perez, and Joe Dobson. APT43: North Korean group uses cybercrime to fund espionage operations, 2023. URL: https://cloud.google.com/blog/topics/threat-intelligence/apt43-north-korea-cybercrime-espionage.

[92] Kevin Poireault. What's in a name? understanding threat actor naming conventions. *Infosecurity Europe*, 2023. URL: https://www.infosecurityeurope.com/en-gb/blog/threat-vectors/understanding-threat-actor-naming-conventions.html.

[93] Neil Pollock and Luciana D'Adderio. Give me a two-by-two matrix and i will create the market: Rankings, graphic visualisations and sociomateriality. *Accounting, Organizations and Society*, 37(8):565–586, 2012.

[94] Neil Pollock and Robin Williams. The business of expectations: How promissory organizations shape technology and innovation. *Social Studies of Science*, 40(4):525–548, 2010.

[95] Neil Pollock and Robin Williams. Who decides the shape of product markets? the knowledge institutions that name and categorise new technologies. *Information and Organization*, 21(4):194–217, 2011.

[96] Neil Pollock and Robin Williams. *How industry analysts shape the digital future*. Oxford University Press, 2016.

[97] Rosemary Purcell, Michele Pathé, and Paul E Mullen. Stalking: Defining and prosecuting a new category of offending. *International journal of law and psychiatry*, 27(2):157–169, 2004.

[98] Quorum Cyber. Understanding the dragonforce 'cartel': The cybercriminals targeting retailers with ransomware, 2025. URL: https://www.quorumcyber.com/insights/understanding-the-dragonforce-cartel-the-cybercriminals-targeting-retailers-with-ransomware/.

[99] Peter Reuter and Bryce Pardo. Can new psychoactive substances be regulated effectively? an assessment of the British Psychoactive Substances Bill. *Addiction*, 112(1):25–31, 2017.

[100] José Jair Santanna, Roland van Rijswijk-Deij, Rick Hofstede, Anna Sperotto, Mark Wierbosch, Lisandro Zambenedetti Granville, and Aiko Pras. Booters – an analysis of DDoS-as-a-service attacks.

In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pages 243–251, 2015.

[101] Molly Sauter. '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, 2013.

[102] Molly Sauter. *The coming swarm: DDoS actions, hacktivism, and civil disobedience on the Internet*. Bloomsbury Publishing USA, 2014.

[103] Robin Seggelmann, Michael Tüxen, and Michael Williams. Transport layer security (TLS) and datagram transport layer security (DTLS) heartbeat extension. RFC 6520, 2012.

[104] Tracy Shildrick. Youth culture, subculture and the importance of neighbourhood. *Young*, 14(1):61–74, 2006.

[105] Gregory C Sieminski. The art of naming operations. *The US Army War College Quarterly: Parameters*, 25(1):32, 1995.

[106] Ineke Sluiter. Old is the new new: The rhetoric of anchoring innovation. *The Language of Argumentation*, pages 243–260, 2021.

[107] Knut H Sørensen. Learning technology, constructing culture. socio-technical change as social learning. *Trondheim: Norwegian Universitu of Science and Technology*, page 22, 1996.

[108] Alex Stamos. Keynote: Tackling the trust and safety crisis. In *USENIX Security '19*, 2019.

[109] David Stang. Information on the brain virus and variants, 1989. URL: http://www.textfiles.com/virus/braininf.vir.

[110] Brian Stanton, Mary F Theofanos, Sandra Spickard Prettyman, and Susanne Furman. Security fatigue. *IT Professional*, 18(5):26–32, 2016.

[111] Martin Steinert and Larry Leifer. Scrutinizing Gartner's hype cycle approach. In *Picmet 2010 technology management for global economic growth*, pages 1–13. IEEE, 2010.

[112] Francesca Stevens, Leonie M Tanczer, Frances Ridout, and Shane D Johnson. *The Applicability of the UK Computer Misuse Act 1990 onto Cases of Technology Facilitated Domestic Violence and Abuse*. UCL, 2021. URL: https://www.ucl.ac.uk/computer-science/sites/computer_science/files/the_applicability_of_the_uk_computer_misuse_act_1990_onto_cases_of_technology_facilitated_domestic_violence_and_abuse.pdf.

[113] James Stewart and Sampsa Hyysalo. Intermediaries, users and social learning in technological innovasion. *Perspectives On User Innovation*, 16:57, 2010.

[114] Edwin H Sutherland. The theory of differential association. In *Readings in criminology and penology*, pages 365–371. Columbia University Press, 1972.

[115] Will Thomas. Defending against SCATTERED SPIDER and The Com with cybercrime intelligence, 2024. URL: https://www.sans.org/blog/defending-against-scattered-spider-and-the-com-with-cybercrime-intelligence/.

[116] Chrissy Thompson. Skirting around the issue: Misdirection and linguistic avoidance in parliamentary discourses on upskirting. *Violence against women*, 26(11):1403–1422, 2020.

[117] UK Met Office. UK storm centre, 2024. URL: https://www.metoffice.gov.uk/weather/warnings-and-advice/uk-storm-centre/index.

[118] Rolf Van Wegberg, Fieke Miedema, Ugur Akyazi, Arman Noroozian, Bram Klievink, and Michel van Eeten. Go see a specialist? predicting cybercrime sales on online anonymous markets from vendor and product characteristics. In *Proceedings of the web conference 2020*, pages 816–826, 2020.

[119] World Meteorlogical Organisation. Tropical cyclone naming, 2023. URL: https://wmo.int/resources/wmo-fact-sheets/tropical-cyclone-naming.

[120] Majid Yar and Kevin F Steinmetz. *Cybercrime and society*. SAGE Publications, 2019.