The emotional infrastructure of a cybercrime collective

The Emotional Infrastructure of a Cybercrime Collective: Evidence from Dark0de

Authors:

Maja Sawicka[1] (Corresponding author);

https://orcid.org/0000-0002-7198-8349

Angus Bancroft[2]

https://orcid.org/0000-0001-5795-628X

Irene Rafanell[3]

https://orcid.org/0000-0002-9349-3478

[1]University of Warsaw;

Department of Sociology, Karowa 18 00-324 Warsaw, Poland; tel/fax: +48 22 55 20 706; m.sawicka@is.uw.edu.pl

[2]University of Edinburgh, Old College, South Bridge, Edinburgh EH89YL, + 44 131 6506642; angus.bancroft@ed.ac.uk

[3]University of the West of Scotland, *institutional and email addresses, telephone and fax numbers*

Authors' short biographical notes:

Dr. Maja Sawicka is Assistant Professor at the Chair of Digital Sociology, Department of Sociology, University of Warsaw. Her research focuses on emotions and (digital) social interactions.

Professor Angus Bancroft is Chair in Sociology at the University of Edinburgh. He studies illicit markets, cybercrime groupings and intoxication.

Dr. Irene Rafanell is Lecturer in Sociology at the University of the West of Scotland. Her work explores the connections between social theory, social constructionism, sociology of knowledge and the body.

Word count (manuscript with references and tables): **8820**

Abstract

Complex cybercrime markets face collective action problems. As they involve disparate networks of individuals they cannot use in person persuasion or coercion to ensure cooperation. They face a tension between being open to new members and opportunities, and regulating participation. We propose that collective emotional regulation plays a crucial part in managing members' behaviours within illicit marketspaces.

We take one critical case, Dark0de, which was a leading English language cybercrime market. Drawing on a publicly available dataset of internal discussions we use Qualitative Thematic Content Analysis and Conversational Analysis to investigate how through mutual emotion regulation this cybercrime collective managed collective action dilemmas deriving from the context of its activity, containing conflict among members and fostering cooperation along with competition. We conclude that emotional micro-dynamics are key to maintaining cyber-criminal marketplaces as relatively stable communities, circumscribing individuals' actions and aligning them with emergent normative orders, enabling those communities to remain operable in adverse environments. Dark0de can be seen as a representative case for a category of digital environments where the community develops its own emotional ethnopsychology, which uses displays of semi-ironic abuse and attack along with cooperation on emerging projects.

Key words: cybercrime; online community; emotions; social interactions; Conversational Analysis; Dark0de

Introduction

Cybercriminal activity is increasingly mediated, coordinated and channelled through a range of underground markets, communities and other associational networks which along with growing 'families' of technologies such as ransomware form a complex and effective criminal ecosystem (Ahn et al., 2016; Grabosky, 2016). These developments have increased the threat effect, so sophisticated attacks can be deployed by technologically relatively unsophisticated threat actors (Holt, 2013). The socio-economic organisation is marked by a more demarcated division of labour (Dupont et al., 2016), the emergence of economic service models (Hutchings & Clayton, 2016), and market or market-mimicking infrastructures (Barratt et al., 2014) that are more responsive to demand (Barratt & Aldridge, 2020). In terms of personnel there is changed sociological sorting and self-identification (Holt & Kilger, 2008) and social-psychological feeling structure (Collier et al., 2021). That represents a cultural shift from the formerly predominant hacker subcultures with their 'crafty' deep knowledge and skill and celebration of transgression (Steinmetz, 2015), instead emphasising a combination of longevity, activity and interpersonal networking (Décary-Hétu & Dupont, 2013).

That also represents a challenge in terms of how we theorise these groupings as effective communities of practice. They cannot rely on a shared deep cultural and technical knowledge, meaning the relationship between cybercriminal participants and their technology is increasingly mediated by other factors. Whereas coherent, internally organised groupings such as the Russian language CarderPlanet exhibit professionalism and a formal, role defined structure (DeSombre & Byrnes, 2018), others are looser, permissive and more porous, and open to new participants. Cybercrime groupings that operate in an open way face several interlinked problems with valuation, coordination and cooperation (Bakken et al., 2018; Beckert and Wehinger, 2012). Their internal social ordering is uncertain (Tzanetakis, 2018). These networks must regulate their members without easy access to in person modes of coercion, persuasion or

trust building, and where retaliation against bad actors is difficult or useless (Bergeron et al., 2021). Managed competition is used to maintain a high quality of valued cybercriminal assets, personnel and opportunities, but it faces two challenges: conflict has to be contained, and competition can only work alongside cooperation (Vu et al., 2020).

Such collective action problems are usually thought to be resolved through a combination of informationalisation (Bakken et al., 2018), trust (Lusthaus, 2012), the circulation of reputational capital (Przepiorka et al., 2017) and reputational or dispute governance processes (Dupont & Lusthaus, 2021; Odabas et al., 2017). Security specialists and sometimes participants tend to refer to technological solutions when assessing or disrupting these systems. There are challenges when resorting to technological solutionism. Reputation systems are limited in their effect and trust requires repeated interaction (Dupont & Lusthaus, 2021; Munksgaard, 2022). Centralised market systems pioneered in the darknet cryptomarkets provide a partial solution, allowing for rapid innovation in response to policing action (Ladegaard, 2020) and the creation of trust and price-setting mechanisms (Moeller & Sandberg, 2015). Administrators of cybercrime forums attempt to use similar innovations in forum design to create a hierarchy of access, defining some areas as having top level access, with special access to tools and other privileged users (Langel et al., 2022). These attempts to embed a hierarchy, however, are often ineffective (Dupont et al., 2017). Many function with minimal or no trust mechanisms, relying instead on interpersonal dynamics. As Maddox et al. (2016) discuss in the context of the original Silk Road, these are mutually engineered digital realities.

We take one case that combines some of these features, Dark0de (also called Darkode), which was part of the exploit kit ecosystem (Suren & Angin, 2019). It was an invitation based forum with a sparse market infrastructure and limited market identity but it became highly successful. The FBI characterised Dark0de as a ‘one-stop, high-volume shopping venue for some of the world’s most prolific cyber criminals’ (FBI, 2015) and Europol rated it as the

highest ranked English speaking hacking forum, an area usually dominated by Russian language sites (Europol, 2015). In its initial form the site ran from 2008 until coordinated policing action closed it down in 2015. A new version was launched with some of the original members some time afterwards (Cox, 2016).

Like other cybercrime focused markets, Dark0de suffered a classic valuation and coordination problem which is brought into being by several layers of opacity. Members had difficulty assessing the effectiveness of products sold and used, they did not have very effective feedback mechanisms, and they had little knowledge of each other. That is in contrast to longer lasting drug focused cryptomarkets where engagement is much richer. There, identities are more stable as they can be confirmed by PGP keys and the attestations of members in good standing (Norbutas et al., 2020).

In order to understand how Dark0de resolves collective action problems for its members we draw on the insight that emotions are an effective informal social control and regulation mechanism (Sawicka, Rafanell & Bancroft, 2022). Following interactionists' accounts of emotions we hypothesise that informal social control operates through emotions of shame and pride (Scheff, 1988; Shott, 1979). Shame and pride are triggered by a sanctioning process and can be deployed to bring deviant behaviours - including emotionally deviant acts - back in line with internal norms, or to praise and further normative, compliant behaviours. The process of emotion sanctioning has been theorized mainly by Scheff (1988, 2000) in the theory of 'deference-emotion system'. Scheff argues that two key emotions of shame and pride are at the core of the generation of community consensus and patterned behaviour and as such should be understood as profoundly social in that they intersubjectively link individuals within a collective. According to Scheff shame in particular should be seen as the 'master' emotion in that it regulates all sorts of social bonds generating the self-monitoring which ensures compliance with internal community norms. Shame and pride are crucial social emotions as

they perform a key signalling function pertaining to belonging to a community or collective: shame signals a loss of status, including the most basic status of being a member of a community, and its power derives from fear of social exclusion. Pride, on the contrary, signals a firm social standing, a rise in status, and informs an individual that their belonging to a community is secured (Turner & Stets, 2006).

To expand on existing analyses of emotions in cybercrime contexts, this study aims to uncover emotional mechanisms embedded in digital interactions which underpinned how the Dark0de community managed collective action dilemmas, in particular the collaborative process of knowledge production and sharing. In this study we investigate how Dark0de with its particular features solves challenges embedded in collective action in the cybercrime context and employs emotional regulation based on feelings of pride and shame, thus developing its own feeling structure which enables both competition and collaboration.

Methods and Data

The crucial challenge which Dark0de had to address to maintain operability derived from the opacity of the digital environment in which the community operated, further magnified by constant pressure exercised by the law enforcement agents attempting to infiltrate the group. Simultaneously, the forum (a communication space accompanying the marketplace), although it triggered a variety of security concerns, was in itself established as a response to the challenges of collective action embedded in cybercrime activity. This unique feature renders Dark0de a laboratory-like environment well-suited to investigate the processual dynamics of collective action, offering insights into the underlying emotional regulation.

To investigate emotion-based, informal social control mechanisms operating in the Dark0de community, we used naturally occurring data - a repository of interactions in the forum in the years 2008-2013. The data had been scraped and leaked by a cybersecurity researcher Xylitol as part of an ongoing though ineffective effort to monitor and disrupt them (Dupont et

al., 2017). As the effort was ineffective the data does not cover the whole period of operation. Currently the rich database of discussion threads constitutes a unique source allowing for in-depth analysis of interaction dynamics in this cybercommunity. The data is publicly available under the link: http://darkode.cybercrime-tracker.net. The data is organised into folders reflecting the forum's structure: three levels of advancement: 'Fresh Fish', that is, newcomers to the community; 'Level 1', that is, regular members; and 'Level 2', that is, senior members. Within each level, the threads are grouped in thematic sections: for instance, 'Questions and problems' 'Programming', 'Challenges' etc. Each section folder contains screenshots of conversations. This feature of the data is analytically significant, because it enables following the natural dynamic of interactions, and analysing particular actions and reactions (interaction participants' utterances) in the context in which they originally nested.

This study is based on analysis of 2,135 screenshots of conversations stored in three main folders: Fresh Fish, Level 1 and Level 2, in all the thematic sections within them, excluding the 'Offtopic' folders. Each quote cited in our analysis is located within the data set with an attribution to the Level folder (FF for Fresh Fish, L1 for Level 1, and L2 for Level 2), thematic folder (C: for 'category' followed by the folder name), and individual thread name (three first words of the name).

The data is a publicly available archive. Generally the research community considers use of data produced in this way to be ethical, within limits (Christin, 2013; Martin & Christin, 2016). Participants pseudonymise themselves and are conscious of security threats. Research ethical obligations extend to secondary data analysis and means ensuring that the data analysis cannot be used to deanonymize individuals concerned or to assist in prosecution. We approached that by sampling from the data and only presenting limited quotes in the final document.

We approached the data using an analytical procedure combining qualitative thematic content analysis (QTCA) (Braun & Clarke, 2022) and Conversational Analysis (CA) for digital data (Meredith, 2019; Meredith & Potter, 2014). In the first step, we mapped the data, reconstructing key themes, and semantic relations between them (Braun & Clarke, 2022). The aim of this analytical step was to provide a feel for Dark0de's shared reality: focal point of interests (what – which topics – are discussed?); modes and practices of communication (how do participants engage with each other?); emotions in general (which feelings are expressed throughout the discussions? How are they expressed?). At this stage we grouped extracts of the data under labels (codes) pertaining to meanings identified in the data, and related the labels (codes) to each other using a semantic mapping tool to reveal themes. In order to do so we repeatedly revisited the data to discuss and collaboratively interpret and reinterpret emerging themes as we advanced further into the dataset.

Key themes revealed through QTCA are: Digital infrastructure perceptions: Dark0de's realm of activity and how it is understood by the forum members; Community aims: the perception of Dark0de, its goals, and usability; Community management: regulating Dark0de's activity, and particularly, knowledge sharing among its members; Emotions: feelings expressed explicitly and implicitly by interactants and the objects of these feelings; Inter-group rivalry/boundary work: processes and mechanisms of differentiation between Dark0de and other hacking forums; In-group rivalry/hierarchies: tensions within the community. Relations and intersections between these themes, along with interpretation of quotes encompassed by them, provided us with key insights for this study.

In the second step, we located interaction extracts within the identified themes which involved shaming and priding operations and we subjected them to a CA-based investigation. Detecting shame and pride in a textual record of interactions is a challenging task, as these two emotions are simultaneously ubiquitous and evasive, eluding traditional methods of social

research (Scheff, 1988). To operationalise shaming and priding for this study, we combined the symbolic interactionists' account of shame and pride according to which these two emotions convey evaluations of the self of the actor (Scheff, 1988; Shott, 1979), and ethnomethodological focus on 'methods' permeating everyday communication (Garfinkel, 1999; Rawls, 2003). As a result, we defined shaming and priding as communicative acts performed in interactions and perpetuated in their record through which individuals attempt to evoke shame and pride in their interactants by evaluating the interactants' selves to achieve successful internal social ordering.

In the course of the CA we identified sequences of adjacency pairs in the data extracts encompassing shaming and priding operations understood in the way outlined above. By 'adjacency pairs' we mean related turns of utterances (Meredith, 2019) composed of utterances (entries) seen as actions consequential for the dynamic of the interaction in which they occur, and responses elicited by these utterances, seen as reactions brought about by the entries. Thus, we documented through which sequences of actions and reactions informal social control through shaming and priding was exercised, and to which effects.

Combining QTCA with CA allowed us to achieve a twofold result: firstly, through QTCA, to understand Dark0de's idiosyncratic, localized culture and its members' shared reality, and – thus – identify specific challenges which the community had to face to remain operable. Secondly, to locate emotion-based sanctioning operations within this particular socio-cultural context to shed light, through CA, on how the deployment of emotions in mutual regulation contributed to the constitution of internal structures of Deark0de essential for its successful operability as a cybercrime community.

Findings

In this section we present key challenges faced by Dark0de in its struggles to remain operable, and how they were addressed by the community. To construct the account, we draw from the evidence provided both by QTCA and CA. We begin by investigating through QTCA how

forum members perceive the main realm of their activity, that is, the digital infrastructure. In the second step, still drawing from QTCA-generated insights, we identify key tensions connected with collaborative production of knowledge about the digital infrastructure within Dark0de's community. Next, we turn to CA to document how priding and shaming were employed in mutual regulation of behaviours, and how they – thus – contributed to managing the tensions identified in preceding sections. In the last step, we identify conditions in which shaming and priding can be deployed as means of informal social control. Through QTCA we map emotion-related processes fostering belonging and consolidating the we-identity among Dark0de members, and those which disrupt it. CA serves us to document how the feelings towards the forum and towards fellow members were regulated within the collective.

Infrastructural Context

As revealed by the QTCA, the general area of action for Dark0de members was the target software which could be exploited, and malware which could be employed for exploits. The extent to which this digital environment was obscure to forum members is revealed by the profusion of threads based on questions and assumptions about digital infrastructures. There are two key areas of doubt which emerge from those conversations, which together constitute the theme 'Digital infrastructure perceptions' identified in the analysis. Firstly, forum users were aware that they did not have full knowledge on how certain digital tools and elements of digital infrastructure function, most importantly, those crucial for their cybercrime activity, such as encryption, bullet-proof hosting or cryptocurrencies. Secondly, and in a close connection, the users were unsure how to financially profit from their ability to exploit the digital infrastructure: in the community language, 'monetize their installs'.

These uncertainties were both technical and business-related, for example, whether the best business model was pay-per-install (PPI) or a shared revenue partnership. Questions addressing these doubts generated numerous answers and lively discussions which document

that the primary use of this forum was to 'crowdsource' knowledge. The theme 'Digital infrastructure perceptions' and the practice of crowdsourcing knowledge reveal, thus, crucial characteristics of knowledge about digital infrastructures. It is fragmented, so that expertise in one aspect does not translate into in-depth understanding of other aspects of the digital environment and of cybercrime activity. Knowledge in this context is volatile, ephemeral. A 'handbook' of knowledge on critical digital infrastructures does not exist, as revealed in one of the conversations about cryptocurrencies. User Paradox noted: *I've not heard anyone mention bitcoin in several months so either people are getting rich off it and keeping it quiet, or you would be wasting your time* (L1, C:General, T:Rouge AV gang). As further discussions about cryptocurrencies indicate, sometimes no consensus was attained on the technicalities and profitability of certain digital products (e.g., running a bitcoin miner). This is not to say that participants necessarily sought consensus. They joined those discussions to verify or invalidate what they knew about cryptocurrencies. In the perspective of the forum members, knowledge pertaining to digital infrastructures is either experiential or must be inferred from implicit, ambiguous cues, and - therefore – is validated in interactions with individuals sharing the same field of interests and expertise. Those interactions, thus, become the actual 'construction site' of essential knowledge on how to conduct efficient, at least to some extent secure, and profitable, cybercrime activity.

In the following sections we investigate how the process of knowledge production and sharing which we see as the key area of collective action for forum members was ordered within Dark0de collective.

Top-down Regulation: the 'Activity' Principle

QTCA further revealed that forum members were aware that knowledge sharing is crucial for the operability of Dark0de as a collective, as evidenced by the theme 'Community aims'. This awareness is reflected in the forum design - particular forum sections were set up to foster

knowledge and competence sharing, and to accommodate collaborative effort aiming at the development of shared resources. Such an attitude is clearly visible in the introduction to the 'Challenges' section:

> the idea of the section was for people to learn, so if you could post a walk through (as detailed as you can be bothered & as if you were explaining to a child) (FF, C:Challenges, T:CrackMe).

And it is reflected in individual utterances in which members declare their interest in joining this effort, for instance:

> There's many things to talk about. I understand that almost everyone here have his own ways to make his money per month, but there's many things we could explain to each others, getting mutual benefits from it (L1, C:General, T:Darkode 2.0).

This quote shows that the users perceived personal development and financial advancement in the realm of illicit digital activities as in essence collective and collaborative. This is not to say that they renounced their individual goals and interests; on the contrary, the tension between individualistic orientations and the emphasis on collaborative strategies with which to attain those goals permeated interactions within the forum.

To resolve the tension the forum's boss attempted to nudge sharing of knowledge (experiential, up-to-date) and solutions (competences) within the collective by enforcing a semi-formal rule prescribing activity. Discussions about this rule fall within the theme 'Community's management' and its sub-theme 'Knowledge sharing'. The rule was an attempt to regulate members' behaviour by introducing an obligation to participate in the interactions on the forum. According to the rule, all members were repeatedly required to actively participate in interactions on the forum under the threat of a 'purge' if they did not.

The attempt to impose the activity principle was, however, opposed by some members of the community. To contest it, a representation of a 'quiet Russian businessmen' was invoked.

‘Businessmen’ in the forum language were actors with particular needs and financial means to invest who entered Dark0de to meet ‘authors’, that is, coders who designed digital tools such as malware and provided solutions to ‘businessmen’s’ needs. In one of conversations which started with the ‘boss’ threatening to remove inactive accounts to enforce members’ activity, users reacted:

> uid0: yea you cant do that cause some ppl only post if they are selling or buying, cant punish them for not being a troll or not posting that/ [selling and buying] is what this place is for anyway;
>
> void: and if they are russians they come here even less (cant read most of bullshit anyway) (FF, C:Announcements, T:Removed invites)

The rationale behind the opposition to the activity principle was that this rule directly endangered the market potential of Dark0de. Interactions in which activity principle was discussed reveal, thus, that the key challenge which the community had to face was how to combine two logics that were divergent, at least to some extent: a community-oriented logic which advocated sharing knowledge and other resources, and an individually-oriented market logic which advocated selling them. All this within one socio-technical assemblage: one group of people and one digital space they inhabited.

This case also indicates that the normative structure of the community was open-ended and emerged in and through interactions: norms of participation were negotiated, contested, and agreed upon in conversations between members. As we demonstrate in the next section, informal, constantly exercised peer pressure became the mechanism through which sharing was elicited and regulated, and the ‘sharing versus selling’ dilemma navigated.

Granting the Honour of Belonging: mutual emotional Regulation

Peer pressure was deployed to regulate sharing and resolve collisions between a community-oriented logic of action, and an individualistic market-oriented one. It operated based on two

key emotions: evoking pride to reward the willingness to share or to acknowledge particularly strong contributions, and evoking shame to negatively sanction misplaced contributions and other acts which endangered the fragile selling vs sharing balance.

CA-based interpretation of interaction extracts within 'Knowledge sharing' theme reveals that priding occurred when respect or gratitude was expressed in a way which conveyed a positive evaluation not only of the act of sharing, but also of the self of the sharer. An example of priding is evidenced in a conversation in which MrGold asked for a hand with a problem he encountered (Table 1.)

[Table 1. Around here]

Priding of sharing acts contributed to the reinforcement of the sharer's belonging to the community, and the establishment of a twofold reputation: as a member both valuable (someone who contributes to the community, a member in the full right), and skilled/competent (one who has enough technical competence to contribute meaningfully). The dynamic of priding, thus, brought about two effects. It set in motion micro-structuring processes, as recognition accumulated in the form of internal hierarchies of reputations, and it contributed to the emergence and consolidation of a norm prescribing sharing.

Sharing, however, needed not only to be stimulated, but also regulated. The community aimed to elicit strong contributions, because only such contributions added value to a shared resource of knowledge owned by the community. Secondly, the community had to harmonize collaborative community and individualistic market logics. On the one hand, make members share valuable pieces of knowledge which were produced with some effort, but, on the other, simultaneously, secure space for selling such products. This was a key dilemma of Dark0de, and a complex task which was accomplished through the use of shaming operations.

Practices of shaming ranged from quite benign reproofs towards generally respected members who committed mild transgressions, to strictly aggressive ones, in which any value

of a ‘project’ or its author was negated. CA of the following conversation documents how shaming was deployed to regulate members’ behaviours, and harmonize sharing and selling logics. In this case, Fcorp committed a serious transgression of the sharing norm, asking for the source code of Conficker, Dark0de’s flagship product. Access to the source code would allow rivals to design and market their own product and also help security researchers find and close vulnerabilities in their products. The selling logic was protected and reaffirmed through shaming (Table 2.).

[Table 2. Around here]

The transgression and the threat to the market logic were in this case so significant, that Fcorp's attempts to evade sanctioning through humouring the embarrassment, and save face, failed. Their withdrawal under the pressure of shaming, however, remained consequential for the community’s normative order - through it the balance between sharing and selling was reaffirmed.

Both shaming and priding could be used as effective methods of furthering the sharing logic (by blocking low quality contributions) and protecting the market logic (by blocking transgressive shares) only insofar the members of the collective care for their reputation within the community and wish to belong to it. The effectiveness of priding and shaming operations as means of social control depends on the community’s ability to develop a sense of affiliation among members and control conflicts and rivalry for top positions in internal hierarchies. In the concluding section of the empirical analysis we look in detail into emotional structures constructed within Dark0de which enabled the use of shame and pride as internal social control mechanisms.

Collective Action and the Emergence of emotional Structures

Emotion norms regulate how certain emotions are experienced and expressed within a collective. In the case of Dark0de, as revealed by the theme ‘Emotions’ which emerged from

the QTCA, two types of feelings were explicitly regulated: those pertaining to the community as a social entity, and those towards fellow members. Collective regulation of these emotions was a crucial precondition of an effective collaboration in the adverse, opaque environment of digital infrastructures and illicit activities.

Feelings towards Dark0de as a collective were regulated through identity-related boundary work through which members framed Dark0de as an 'exceptional' digital space. Members participated in this boundary work by engaging in positive evaluations of Dark0de. This process can be seen as 'collective self-priding' through which Dark0de was presented as a community of highly skilled coders, meriting high respect. This practice can be exemplified by the following quote in which user Paradox made a comparison between members of Dark0de and users of other hacking forums: *I don't know about you but the people I know on-line that aren't on DK are pretty retarded* (...). (FF, C:Announcements, T:Invites, trusted section). The expression 'retarded' and its derivatives ('retard' or 'retardness') were usually employed in the forum to denote low intellectual abilities of coders belonging to forums for 'whitehats' and less skilled hacking or malware communities. Their usage, thus, as revealed by the theme 'Inter-group rivalry: boundary work' contributed to the delineation of a symbolic boundary between the 'useless' hacking scene, and Dark0de - the true 'black-hat' community, where highly skilled individuals are committed to support each other in the process of mutual growth and benefit. A sense of mutual identification with other members fostered by contempt towards other hacking collectives permeated all the entries in which members explained why Dark0de is special in their view, for instance:

> Gonzo: This is the only place on the net where people actually give a shit, they go out of there way to help you. Since i joined dk i have learned about things i had no idea existed. This place is a learning ground (...). (FF, C:Announcements, T:Respect).

Through such entries an emotion norm was constructed which prescribed respect towards Dark0de, and, thus, encouraged self-ascription to the community and affiliation with this particular socio-technical assemblage. The intersection of themes 'Sharing knowledge', 'Emotions', and 'Inter-group rivalry: boundary work' reveals how the norm of respect emerged from the practices of Dark0de self-priding, and how it operated in enabling collaboration between members as it stimulated the willingness to share one's own knowledge and resources, and invest in the community.

A similar dynamic of collective self-priding was employed to regulate feelings towards fellow forum members, that is, construct the norm of internal trust. The theme 'Security concerns' evidences that although security issues remained one of the community's primary concerns, Dark0de was presented as an enclave of trust among other digital spaces where people cannot be trusted. The norm of internal trust can be traced in conversations in which the members debated on how to increase activity (market potential) of the forum. Solutions such as advertising membership on other forums or opening it for anyone willing to pay an admission fee were intensely criticised for going *against everything DK stands for* (FF, C:Announcements, T:More activity), and aggravating security concerns. One of those conversations was concluded with the following entries:

> Genadi: For me its good as it is, you learn to know people here and do business on jabber [internal IM communicator], thats how its supposed to be. From the people i learned to know here the percentage of fags was a trillion time smaller than the fagpercentage on other boards.
>
> Jumbie: Welcome to Darkode where "fagpercentage" is Krab [a colloquial reference to Brian Krebs, a famous security researcher] to knone. (FF, C:Announcements, T:More activity)

Through such positive evaluations Dark0de was constructed by the members as a secure and trusted space, a special character of which derives from strong bonds between members.

The we-identity constructed through the regulation of feelings towards the collective and fellow members rested on a strong sense of identification with other members of the group and its framing as a collaborative *learning ground* (FF, C:Announcements, T:Respect). Crucial in this regard was the practice of sharing: sharing strengthened bonds among members, and enhanced the wish to belong to the community as membership was perceived as a condition of access to the common resource of up-to-date, validated knowledge on digital infrastructures and cybercrime activity.

Sharing, however, could be endangered by displays of negative emotions and rivalry among fellow members, disruptive for group coherence. As revealed by the theme 'In-group rivalry: hierarchies', non-productive displays of anger generated by rivalry, such as 'flaming', were problematic for the community, in contrast to anger expressions through which shaming was performed in cases presented in previous sections. Flaming directly endangered the community-oriented logic as it undermined the collaborative character of threads designed to encourage sharing. Therefore, a substantial effort was invested into managing anger through shaming, and particularly – ridiculing displays of anger. CA of the following extract provides an insight into how anger was managed through shaming (Table 3.).

[Table 3. Around here]

Irony and performances of abuse can be considered emotional practices (Scheer, 2012) typifying underground groupings, which in this case bring about the effect of shaming. As ethnomethodologists argue, certain actions performed in interactions count as methods as long as they bring about particular effects for the restoration and maintenance of social order (Garfinkel, 1999). In the case of Dark0de, interventions based on ridiculing anger and flaming such as the one presented in Table 3. contributed to the restoration of emotional coherence within the community. Simultaneously, through shaming, sharing was protected from flaming, and cooperation from rivalry. Crucially, shaming was consequential for anger regulation -

through it an emotional norm emerged which disallowed anger displays towards constructive shares, and allowed them only in the case of misplaced shares which endangered 'sharing vs selling' balance.

Discussion

Through interaction-based dynamics of emotional regulation, emotion norms were constructed which themselves became a crucial affordance for Dark0de, enabling it to navigate collective action dilemmas specific to this group. Collective action problems manifested in knowledge production and sharing, and maintaining the balance between sharing and selling of knowledge and solutions produced within this community. Through peer-pressure operating through shaming and priding an emotional structure - a local 'ethnopsychology' (Thoits, 1989) - specific for this group emerged.

Dark0de can be seen as a representative case for a category of digital environments where the community develops its own emotional ethnopsychology and discourse, which uses displays of semi-ironic abuse and attack along with cooperation on emerging projects. There are online communities with similar dynamics, and often sharing some demographic features such as 4Chan/8Kun, extremism forums and incel worlds (Vu, 2020, 2022). They tend to be technologically basic but with sophisticated internal norms that maintain the group culture, expression and purpose. They are characteristic of what Abidin (2021) calls refracted publics, communities focused on practices of circumvention operating 'below the radar' that need to be opaque but also connected, discoverable and hidden, obfuscated but knowable, given the right cultural knowledge.

We argue that these internal norms shaping emotional structures within a community are best understood as an ethnopsychology. Ethnopsychology is traditionally conceptualised (Hochschild, 2003; Thoits, 1989; for an anthropologist account see also: Wikan, 1990) as a set of emotion rules which are collective in nature and circumscribe and shape individual subjective

psycho-physiological phenomena (Rafanell & Sawicka, 2020). Based on the empirical analysis presented above, we claim that an ethnopsychology should be understood as a collective achievement of a particular group insofar it emerges from the constant negotiation, in interaction, between members of a collective in pursue of specific goals and interests.

Dark0de's particular ethnopsychology which we identified in our investigation has to be seen as functional and instrumental for this cybercrime community because it regulated emotions directed to encourage belonging – respect and trust – and in the process it fostered coherence within the group. It also regulated anger, a potentially disruptive emotion, which, uncontrolled, could endanger collaboration on joint projects within the group. Anger was allowed in certain circumstances where it can be employed in shaming and result in bringing members' behaviours back in line with internal norms, and disallowed when its displays disrupted internal coherence. Regulation of emotions pertaining to belonging was crucial to Dark0de because of its focus on joint production and validation of knowledge about digital infrastructures. The ephemeral, 'no-handbook' like character of what counts as valid knowledge about digital technologies in this group highlights a key aspect of epistemic dynamics which can be clearly observed in the case of Dark0de: that individuals are mutually susceptible to one another when attempting to validate their individual pools of knowledge. Knowledge in general, and knowledge about ever changing digital technologies in cybercrime activity in particular, is always negotiated case by case in reference to specific local determinants. For knowledge to be counted as valid, it needs to be sanctioned by the other members of the collective, that is, receive their approval (Barnes, 1977, 1983; Bloor, 1997). This can only happen in interaction and when individuals are compelled by the desire to belong to a collective.

In this sense, knowledge is a collective good, not an individual property. This is not to say that all knowledge was subjected to the sharing obligation. There are different kinds of knowledge, for instance knowledge pertaining to how to monetise a product which must be

shared in order to attract users to the product. Then there is the closely guarded knowledge about how it works (e.g., the source code) which is tightly defended. Within those broad categories, however, we can observe in this group how what can and cannot be shared was negotiated case by case. The 'working' categorization of knowledge as sharable and non-sharable was constructed in interactions. Those negotiations and categorizations which stemmed out of them were crucial because they addressed the key tension underlying Dark0de between community-oriented and individualistic interests. For the Dark0de community the sharing of knowledge became a crucial mechanism, transforming a group of heterogeneous individuals into a community bounded by validated knowledge, concerns and goals.

Crucial in this process was the illicit context of their activity, and the pressures under which they operated. Lack of validated, up-to-date knowledge on how digital technologies function could endanger safety and generate security risks (due to law enforcement pressures), or lead to serious economic losses (as, for instance, issues with cryptocurrencies). Thus, Dark0de members could be described as being epistemically co-dependent – this community brought together individuals who depended on one another to make sense of their individual experiences in the realm of cybercrime. Knowledge sharing and norming became a crucial part of identity work necessary to acquire the status of a valued member of the community and an obligation towards the community.

Epistemic co-dependence brought Dark0de members together to form a social constellation which can be seen as a community of practice. Communities of practice are traditionally understood as grouping individuals who 'share a concern or a passion for something they do and learn how to do it better as they interact regularly' (Wenger & Wenger-Trayner, 2015). In our application of this concept to Dark0de we emphasize that a community of practice should be seen as an interacting collective coalescing around knowledge sharing and producing, and, therefore, fulfilling both individual and collective goals. Traditionally, studies

of communities of practice focus on those practices which enhance learning and development (Hara et al., 2009). Our investigation into Dark0de highlights the importance of the community for knowledge validation. In this case it was clearly observable that a sense of community and the wish to belong enabled emotion-based informal social control, which in turn fostered knowledge production and sharing.

Existing research into emotions in digital environments is underpinned by an assumption that digital interactions are to some extent liberated from social constraints and behavioural norms (Blumer & Döring, 2012). Emotions are either reduced to negative, harmful actions, as in the discourse of cyber hate, or to an excessive positive emotionality, both perceived as resulting from the 'online disinhibition effect' (Lapidot-Lefler & Barak, 2012, 2015). Our research indicates that understanding emotional dynamics operating in online illicit contexts requires considering localized settings and community processes occurring within them, and resisting a reductionist understanding of the individual. Emotions are critical to offender motive and the regulation of their behaviour during the criminal activity. Emotions both enable and place limits on offending, setting boundaries that will not be crossed. For offenders, emotions can manifest in terms of the thrills and effervescence of the 'crime moment', the seductions of transgression (Katz, 1988) and the emotional rewards of status performance (Holt, 2020).

We further this approach by defining emotions as emergent motivational and evaluative processes attaching to experience and justifying action. Therefore, emotional dynamics should be analysed as distinct from organisational or algorithmic judgements but also necessary to a cybercrime community. Emotions are central to how technology is designed and used, in particular to how digital platforms evolve and compete. Digital technology affordances invite and promote particular behaviours, emotional engagements and performances, including in illicit contexts (Goldsmith & Wall, 2019). Collective emotional regulation plays a critical part

both in creating an incentive/reward structure, channelling and giving valence to communication, and signalling hierarchy.

The analysis presented here enables us to grasp not just which emotions operate in this cybercrime community but, most importantly, how they work to support the collective's functioning. Crucial in this regard are shaming and priding activities which permeate interactions within Dark0de forum. Our analysis proves that emotional regulation deploying shame and pride underpins the emergence of local norms governing people's behaviours..

Focusing on emotional micro-processes operating in and through localized digital interactions calls for adoption of methodologies which enable an in-depth investigation of dynamics operating between individuals in digital contexts. The use of Conversational Analysis (CA) for digital interactions (Meredith, 2019; Meredith & Potter, 2014) is a solution to the problem of research methods emotionally flattening digital contexts, such as those using Big Data sets, or viewing emotional performances purely as products of the environment, rather than structuring elements which enable particular types of action and organisation. The CA approach also provides analytical tools to investigate the ways in which particular functionalities of digital techno-spaces afford for certain actions by their users (Hutchby, 2001). We argue that the localized ethnopsychology which characterized Dark0de acted as a crucial affordance for this community, promoting, circumscribing and shaping participants' behaviours. Therefore, it contributed to the coordination and effectiveness of the cybercriminal cooperation within this specific socio-technical assemblage, enabling the community to resolve collective action dilemmas inherent in its scope of activity.

This study demonstrates how a shared culture, an ethnopsychology, is used to resolve critical tensions that are inherent to cybercrime communities of this type, and how that culture is supported and recreated through repeated interactions within the community. Interactions are key to social sorting, norming and regulating participants. We have shown how localized

ethnopsychologies emerge in digital communities in response to collective action problems they have to resolve. One of the challenges they repeatedly turned to is the opacity of digital and market infrastructures. Malware is often an unknowable black box to its users, and hence a risk to the user even as they use it to exploit others. Epistemic co-dependence is, thus, key to these communities. There is also a large shadow population in malware markets, symbolized by the 'silent Russian' referred to in the Dark0de forum. Our research points to how the malware community of Dark0de act towards these silent actors, regulating participants' activity through shaming and priding operations.

The kind of community Dark0de typifies has two key tensions running through it, first between the need for cooperative practice, and the need to maintain a competitive and hierarchal worldview, and second, the challenge of operating as a generic cybercriminal assemblage in an opaque infrastructure, rather than one working within a specific project or business type such as ransomware. Many of the problems faced by members arose from these tensions, and the need to resolve them drove the emergence of a specific ethnopsychology that we have described. We therefore contribute to a growing understanding in cybercrime research that reliable illicit market exchanges are generated through repeated interaction and social ties rather than sophisticated infrastructural devices such as rating and review systems (Munksgaard, 2022). Emotional micro-dynamics should be seen as key to maintaining cyber-criminal marketplaces as relatively stable communities, circumscribing individuals' actions and aligning them with emergent normative orders, enabling those communities to maintain operability in adverse environments.

Acknowledgements

We are grateful to Samuel Rafanell-Williams for suggesting the concept of epistemic co-dependence which we applied to highlight a key dynamic within Dark0de.

Declaration of Interests Statement

The authors declare no conflict of interests.

References

Abidin, C. (2021). From "Networked Publics" to "Refracted Publics": A Companion Framework for Researching "Below the Radar" Studies. *Social Media + Society*, *7*(1), 205630512098445. https://doi.org/10.1177/2056305120984458

Ahn, G.-J., Doupe, A., Zhao, Z., et al. (2016). Ransomware and cryptocurrency: partners in crime. In T. J. Holt (Ed.), *Cybercrime Through an Interdisciplinary Lens* (pp. 119–140). Routledge.

Bakken, S.A., Moeller, K., & Sandberg, S. (2018). Coordination problems in cryptomarkets: Changes in cooperation, competition and valuation. *European Journal of Criminology, 15*(4), 442–460. https://doi.org/10.1177/1477370817749177.

Barratt, M. J., & Aldridge, J. (2020). No magic pocket: Buying and selling on drug cryptomarkets in response to the COVID-19 pandemic and social restrictions. *International Journal of Drug Policy 83*, 102894. DOI: 10.1016/j.drugpo.2020.102894.

Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2014). Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States. *Addiction 109*(5), 774–783. DOI: 10.1111/add.12470.

Barnes, B. (1977). *Interests and the Growth of Knowledge.* Routledge & Kegan Paul.

Barnes, B. (1983). On the Conventional Character of Knowledge and Cognition. In K. D. Knorr-Cetina & M. Mulkay (Eds.), *Science Observed: Perspectives on the Social Study of Science* (pp. 19–51). Sage.

Beckert, J., & Wehinger, F. (2012). In the shadow: illegal markets and economic sociology. *Socio-Economic Review, 11*, 5–30.

Bergeron, A., Décary-Hétu, D., & Ouellet, M. (2021). Conflict and Victimization in Online Drug Markets. *Victims & Offenders 0*(0), Routledge, 1–22. DOI: 10.1080/15564886.2021.1943090.

Bloor, D. (1997). *Wittgenstein, Rules and Institutions*. Routledge.

Blumer, T., & Döring, N. (2012). Are we the same online? The expression of the five factor personality traits on the computer and the Internet. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *6*(3), Article 5. https://doi.org/10.5817/CP2012-3-5

Braun, V., & Clarke, V. (2022). Conceptual and design thinking for thematic analysis. *Qualitative Psychology, 9*(1), 3–26. https://doi.org/10.1037/qup0000196

Christin, N. (2013). Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace. In *Proceedings of the 22nd international conference on the World Wide Web*, Rio de Janeiro, Brazil, 2013, pp. 213–224. WWW 2013.

Collier, B., Clayton, R., Hutchings, A., et al. (2021) Cybercrime is (often) Boring: Infrastructure and Alienation in a Deviant Subculture. *The British Journal of Criminology* (online early). DOI: 10.1093/bjc/azab026.

Cox, J. (2016). Malware Exchange Busted by the Feds Relaunches, At Least in Name. *Vice*. Available at: https://www.vice.com/en/article/pgkwvv/darkode-brand-relaunches

Décary-Hétu, D., & Dupont, B. (2013). Reputation in a dark network of online criminals. *Global Crime*, *14*(2-3), 175-196.

DeSombre, W., & Byrnes, D. (2018). *Thieves and Geeks: Russian and Chinese Hacking Communities*. Recorded Future.

Dupont, B., & Lusthaus, J. (2021). Countering Distrust in Illicit Online Networks: The Dispute Resolution Strategies of Cybercriminals. *Social Science Computer Review*. SAGE Publications Inc: 0894439321994623. DOI: 10.1177/0894439321994623

Dupont, B., Côté, A. M., Boutin, J. I., & Fernandez, J. (2017). Darkode: Recruitment patterns and transactional features of "the most dangerous cybercrime forum in the world". *American Behavioral Scientist, 61*(11), 1219–1243.

Europol, (2015). *Cybercriminal Darkode forum taken down through global action*. Europol. Available at: https://www.europol.europa.eu/media-press/newsroom/news/cybercriminal-darkode-forum-taken-down-through-global-action

FBI, (2015). *Cyber Criminal Forum Taken Down*. Federal Bureau of Investigation. Available at: https://www.fbi.gov/news/stories/cyber-criminal-forum-taken-down

Garfinkel, H. (1999 [1967]). *Studies in Ethnomethodology*. Polity Press.

Goldsmith, A., & Wall, D. S. (2019). The seductions of cybercrime: Adolescence and the thrills of digital transgression. *European Journal of Criminology*: 1477370819887305. https://doi.org/10.1177/1477370819887305

Grabosky., P. (2016). The evolution of cybercrime, 2006–2016. In T. J. Holt (Ed.) *Cybercrime Through an Interdisciplinary Lens.* London: Routledge.

Hara, N., Shachaf, P., & Stoerger, S. (2009). Online communities of practice typology revisited. *Journal of Information Science*, *35*(6), 740–757. https://doi.org/10.1177/0165551509342361

Hochschild, A. R. (2003). *The Managed Heart. Commercialization of Human Feeling*. University of California Press.

Holt, T. J. (2013). Examining the Forces Shaping Cybercrime Markets Online. *Social Science Computer Review 31*, 165–177. DOI: 10.1177/0894439312452998.

Holt, T. J. (2020). Computer Hacking and the Hacker Subculture. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 725–742). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_31

Holt, T. J., & Kilger, M. (2008). Techcrafters and Makecrafters: A Comparison of Two Populations of Hackers. In *2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing*, April 2008, pp. 67–78. DOI: 10.1109/WISTDCS.2008.9.

Hutchby, I. (2001). Technologies, texts and affordances. *Sociology*, *35*(2), 441–456. https://doi.org/10.1177/S0038038501000219

Hutchings, A., & Clayton, R. (2016). Exploring the Provision of Online Booter Services. *Deviant Behavior 37*(10), 1163–1178. DOI: 10.1080/01639625.2016.1169829.

Katz, J. (1988). *Seductions Of Crime: Moral And Sensual Attractions In Doing Evil*. Basic Books.

Ladegaard, I. (2020). Open Secrecy: How Police Crackdowns and Creative Problem-Solving Brought Illegal Markets out of the Shadows. *Social Forces 99*(2), 532-559. DOI: 10.1093/sf/soz140.

Langel, S., Décary-Hétu, D., Beaudet-Labrecque, O., et al. (2022). Private Clubs For Hackers: How Private Forums Shape The Malware Market. *The Journal on Cybercrime and Digital Invesigations, 7*(1), 13.

Lapidot-Lefler, N., & Barak, A. (2012). Effects of anonymity invisibility and lack of eye contact on toxic online disinhibition. *Computers in Human Behavior*, 28, 434–443. https://doi.org/10.1016/j.chb.2011.10.014.

Lapidot-Lefler, N., & Barak, A. (2015). The benign online disinhibition effect: Could situational factors induce self-disclosure and prosocial behaviors? *Cyberpsychology:*

Journal of Psychosocial Research on Cyberspace, 9(2), Article 3. https://doi.org/10.5817/CP2015-2-3.

Lusthaus, J. (2012). Trust in the world of cybercrime. *Global Crime, 13*, 71–94. https://doi.org/10.1080/17440572.2012.674183

Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2016). Constructive Activism in the Dark Web: Cryptomarkets and Illicit Drugs in the Digital 'Demimonde'. *Information, Communication & Society*, *19*(1), 111–126. https://doi.org/10.1080/1369118X.2015.1093531.

Martin, James, and Nicolas Christin. 2016. "Ethics in cryptomarket research." International Journal of Drug Policy 35: 84-91. https://doi.org/https://doi.org/10.1016/j.drugpo.2016.05.006

Meredith, J., & Potter, J. (2014). Conversation analysis and electronic interactions: Methodological, analytic and technical considerations. In H. L. Lim & F. Sudweeks (Eds.), *Innovative methods and technologies for electronic discourse analysis* (pp. 370–393), IGI Global.

Meredith, J. (2019). Conversation Analysis and Online Interaction. *Research on Language and Social Interaction, 52*(3), 241–256. https://doi.org/10.1080/08351813.2019.1631040

Moeller, K., & Sandberg, S. (2015). Credit and Trust: Management of Network Ties in Illicit Drug Distribution. *Journal of Research in Crime and Delinquency,* 52(5), 691–716. https://doi.org/10.1177/0022427815583912

Munksgaard, R. (2022). Building a case for trust: reputation, institutional regulation and social ties in online drug markets. *Global Crime, 0*(0), 1–24, Routledge. https://doi.org/10.1080/17440572.2022.2156863

Norbutas, L., Ruiter, S., & Corten, R. (2020). Reputation transferability across contexts: Maintaining cooperation among anonymous cryptomarket actors when moving between

markets. *International Journal of Drug Policy,* 76, 102635. https://doi.org/10.1016/j.drugpo.2019.102635

Odabas, M., Holt, T. J., & Breiger, R. L. (2017). Governance in online stolen data markets. In J. Beckert & M. Dewey (Eds.) *The Architecture of Illegal Markets: Towards an Economic Sociology of Illegality in the Economy*. Oxford University Press.

Przepiorka, W., Norbutas, L., & Corten, R. (2017). Order without Law: Reputation Promotes Cooperation in a Cryptomarket for Illegal Drugs. *European Sociological Review 33*(6), 752–764. https://doi.org/10.1093/esr/jcx072

Rafanell, I., & Sawicka, M. (2020). *Emotions in Digital Interactions. Ethnopsychologies of 'Angel's Mothers' in Online Bereavement Communities*, Palgrave Macmillan Pivot.

Rawls, A. (2003). Harold Garfinkel. In G. Ritzer (Ed.), *The Blackwell Companion to Major Contemporary Social Theorists* (pp. 89–124), Blackwell Publishing.

Sawicka, M., Rafanell, I., & Bancoft, A. (2022). Digital localisation in an illicit market space: interactional creation of a psychedelic assemblage in a darknet community of exchange. *International Journal of Drug Policy*, 103514. https://doi.org/10.1016/j.drugpo.2021.103514

Scheer, M. (2012). Are emotions a kind of practice (and is that what makes them have a history)? A Bourdieusian approach to understanding emotion. *History and theory*, *51*(2), 193-220.

Scheff, T. J. (1988). Shame and Conformity: The Deference-Emotion System. *American Sociological Review, 53*, 395–406.

Scheff, T. J. (2000). Shame and the Social Bond: A Sociological Theory. *Sociological Theory, 18*(1), 84–99.

Shott, S. (1979). Emotion and Social Life: A Symbolic Interactionist Analysis. *American Journal of Sociology, 84*(6), 1317–1334. Retrieved from https://www.jstor.org/stable/2777894.

Steinmetz, K. F. (2015). Craft(y)nessAn Ethnographic Study of Hacking. *The British Journal of Criminology 55*(1), 125–145. DOI: 10.1093/bjc/azu061.

Suren, E., & Angin, P. (2019). Know Your EK: A Content and Workflow Analysis Approach for Exploit Kits. *Journal of Internet Services and Information Security, 9*(1), 24–47.

Thoits, P. A. (1989). The Sociology of Emotions. *Annual Review of Sociology, 15*, 317–342. https://doi.org/10.1146/annurev.so.15.080189.001533.

Turner, J., & Stets, J. (2006). Moral Emotions. In J. Stets & J. Turner (Eds.), *Handbook of the Sociology of Emotions*, Springer.

Tzanetakis, M. (2018). Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time. *International Journal of Drug Policy 56*, 176–186. https://doi.org/10.1016/j.drugpo.2018.01.022

Vu, A. V. (2020). *The Shift of Incel Topics During the Pandemic*. Cambridge Cybercrime Centre.

Vu, A. V. (2022). ExtremeBB: Supporting Large-Scale Research into Misogyny and Online Extremism | Light Blue Touchpaper. *Light Blue Touchpaper*. Available at: https://www.lightbluetouchpaper.org/2022/09/02/extremebb-supporting-large-scale-research-into-misogyny-and-online-extremism/

Vu, A. V., Hughes, J., Pete, I., et al. (2020). Turning Up the Dial: the Evolution of a Cybercrime Market Through Set-up, Stable, and Covid-19 Eras. In *Proceedings of the ACM Internet Measurement Conference*, Virtual Event, USA, 27 October 2020, pp. 551–566. IMC '20. Association for Computing Machinery. DOI: 10.1145/3419394.3423636.

Wenger-Trayner, E., & Wenger-Trayner, B. (2015). *An introduction to communities of practice: a brief overview of the concept and its uses*. Available from authors at https://www.wenger-trayner.com/introduction-to-communities-of-practice.

Wikan, U. (1990). *Managing turbulent hearts: A Balinese formula for living*. University of Chicago Press.

Tables

Table 1. An example of priding (OpenVPN traffic x1, Problems and Questions, FF)

Participants	**Utterance (text of the message)**	**Action**
MrGold:	Can anyone help me how to allow traffic to only go over VPN?	sharing trigger
Other users:	*Reply, but are unable to offer a solution to the problem*	sharing attempts
Doksh:	you guys should learn to know how to use the fucking windows :D you can do that without any need of a standalone firewall software or any shit , you can make it with the windows firewall with advanced security . and for lazy dudes i will explain in details how to do it . [*the explanation in steps follows*] That's it , stay safe and enjoy :P.	sharing
core64x:	@Doksh - simple, and beautiful	priding
dice:	Thanks Dokshy, good solution :)	
Sana:	pure Dokshode	
wesTThug:	Doks has spoken ! :D	
Doksh:	Thanks guys, i'm glad to help :D	acknowledgement

Table 2. An example of shaming (L1, Programming, Need conficker source)

Participants	**Utterances (text of the message)**	**Action**
Fcorp:	Hi, iam a noob in c [*a beginner in a programming language*], and would like see conficker source, for know how it's work (...) can someone send me a pm with link to it? thank's	sharing trigger / attempt to evoke the community logic of action / transgression of the market logic of action
D0ktor H0rrible:	If I was a mod I would ban you where you stand	shaming
nutter:	i hope to god you are joking… but send me 10K LR First, then i will give it to you, sound good? :D	
skier_:	lol'd…	
Fcorp:	lol, sorry, was stupid question	withdrawal / market logic of action overrides community logic
mafi (Boss):	ok, you've been placed in the 'Introduction section of shame hall' for a while/ i'll let you in again once you have written on the blackboard 'I will not ask for Conficker source again' 100 times. locked topic	shaming / ostracism / market logic of action confirmed

Table 3. Shaming anger (L1, C:Programming, T:Javascript system working)

Participants	**Utterances (text of the message)**	**Action**
success:	*criticises a solution to a programming problem formulated by CodeCompiler*	criticism / anger trigger
CodeCompiler:	You know as much as you try to troll me success i think you secretly trying to tell me you want to suck my dick… I mean seriously… What are you putting out to do anything for CPA and PPI? nothing… cute… so unless your trying to tell me something quit riding my dick so hard you fucking faggot!	anger display
xtension:	you two make me lol so hard	shaming
Junib3r:	hahahahh i looooled so fucking hard :) you guys should make a comedy movie !	
solotech:	heheheh how i miss this post before ? :D	
success and CodeCompiler quit the conversation		reaction to shaming / withdrawal