Compete, Collaborate, Investigate: Exploring the Social Structures of Open Source Intelligence Investigations

Yasmine Belghith
byasmine@gatech.edu
School of Interactive Computing,
Georgia Institute of Technology
Atlanta, GA, USA

Sukrit Venkatagiri
sukrit@vt.edu
Department of Computer Science,
Virginia Tech
Arlington, VA, USA

Kurt Luther
kluther@vt.edu
Department of Computer Science,
Virginia Tech
Arlington, VA, USA

ABSTRACT

Online investigations are increasingly conducted by individuals with diverse skill levels and experiences, with mixed results. Novice investigations often result in vigilantism or doxxing, while expert investigations have greater success rates and fewer mishaps. Many of these experts are involved in a community of practice known as Open Source Intelligence (OSINT), with an ethos and set of techniques for conducting investigations using only publicly available data. Through semi-structured interviews with 14 expert OSINT investigators from nine different organizations, we examine the social dynamics of this community, including the collaboration and competition patterns that underlie their investigations. We also describe investigators' use of and challenges with existing OSINT tools, and implications for the design of social computing systems to better support crowdsourced investigations.

CCS CONCEPTS

• **Human-centered computing → Collaborative and social computing**.

KEYWORDS

investigation; open source intelligence; OSINT; competition; collaboration; experts; crowdsourcing

ACM Reference Format:
Yasmine Belghith, Sukrit Venkatagiri, and Kurt Luther. 2022. Compete, Collaborate, Investigate: Exploring the Social Structures of Open Source Intelligence Investigations. In *CHI Conference on Human Factors in Computing Systems (CHI '22), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3491102.3517526

1 INTRODUCTION

Online investigations are increasingly conducted by individuals of diverse skill levels and experience, with varying success rates. Novice investigators can be successful in uncovering crimes, finding perpetrators, and helping to deliver justice [29, 88]. They have also supported crisis response efforts [20, 51]. However, there have also been several well-known incidents involving online and in-person vigilantism [67, 91]. This includes "naming and shaming," disclosure of highly personal details (i.e., doxing), and misidentification of individuals, most notably in the 2013 Boston Marathon bombing [67] and the storming of the U.S. Capitol in 2021 [49].

Compared to novices, expert investigators have been more successful both in the court of public opinion and the court of law [51, 100]. One reason for expert investigators' comparatively greater successes and fewer mishaps may be their active participation in the community of practice known as Open Source Intelligence (OSINT) [19, 30, 58, 64]. OSINT refers to data that can be gathered from publicly and legally available sources [62]. The OSINT community has its own rules and techniques for collecting, verifying, and analyzing open source information to derive intelligence and fulfill a goal (e.g., identifying a suspect, finding a missing person, proving or disproving a statement) [97]. It has numerous applications, ranging from employee vetting [12, 77] to counter-terrorism and human rights advocacy [22, 47].

In this work, OSINT experts refers to investigators who actively participate in the OSINT community, are well-versed in its techniques, and abide by its values and ethos. These include prioritizing transparency, avoiding the use of subterfuge, and limiting investigations to passive reconnaissance. OSINT experts often come together as part of larger organizations or events, giving rise to a rapidly growing community. Novices are newcomers to the field of OSINT and often join experts' organizations to conduct investigations in a variety of domains. We consider novices as peripheral members of the community, training towards becoming experts. Experts who direct OSINT organizations or events and coordinate the investigations are referred to as *organizers*. Novices and other OSINT experts who are assisting the organizer in their investigation are considered *contributors*.

Throughout their investigations, organizers and contributors leverage two different forms of social interaction: competition and collaboration. We refer to both tactics as *social OSINT*. While prior work has focused on OSINT tools and techniques [60, 97], our work here focuses on the social aspects of OSINT. Prior work in HCI has also shown that the social, human infrastructure of an organization can be just as important as the technological infrastructure [23, 53, 92]. Our work seeks to inform future OSINT investigations, and crowdsourced investigations in general — conducted by novices and experts alike.

With this motivation, we address the following research questions in this paper:

CHI '22, April 29-May 5, 2022, New Orleans, LA, USA

ACM ISBN 978-1-4503-9157-3/22/04…$15.00
https://doi.org/10.1145/3491102.3517526

(1) RQ1: What are organizers' and contributors' motivations, experiences, and attitudes towards social OSINT investigations? How do they define success?
(2) RQ2: How do organizers plan and structure the OSINT investigations? What challenges do they face, and how do they manage them?

To address these questions, we recruited OSINT investigators from organizations and events across the social structure spectrum, ranging from purely competitive to purely collaborative social structures. Through semi-structured interviews with 14 expert OSINT investigators from nine different organizations, we describe their backgrounds, motivations, and the commonalities and differences between their social dynamics. We also describe the factors that enable their success, such as their emphasis on transparency, and solid foundation in ethics and security, and the challenges that they face, such as the unreliability of certain tools and the difficulty in gathering and verifying digital content. Upon a closer look at the social dynamics within the organizations and events, we find that there is no clear delineation between collaborative and competitive structures. Instead, we observe different social OSINT tactics at play — a blend of competitive strategies within overarching collaborative structures and vice versa. Each tactic carries different implications, such as collaboration enabling investigators to broadly share their expertise with other, while competition helping them refocus their efforts. We also find that these social structures are influenced by power dynamics outside of the organizations. For instance, the organizations that they work within dictate access to contributors and resources.

Our paper makes the following contributions:

(1) We enrich the current literature on investigations within HCI by providing an in-depth description of the OSINT investigative community as a community of practice. We present its social dynamics, practices, and key elements: a culture of transparency, the presence of an adversarial mindset, and collaboration among individuals with diverse motivations and backgrounds.
(2) We define and characterize social OSINT tactics as a combination of competitive and collaborative strategies used in structuring OSINT investigations, and their implications. Our findings also add more nuance to related work on competitions.
(3) We suggest tool design recommendations to better support OSINT, and more generally crowdsourced, investigations.

2 BACKGROUND AND RELATED WORK

2.1 Open Source Intelligence Investigations

Open source intelligence (OSINT) investigations involve the collection and analysis of publicly available data to generate intelligence that addresses a specific need [97]. More recently, the rise of social media and increasingly digitally-mediated social interaction has democratized access to large amounts of personal information, and powerful tools for analyzing it [37]. OSINT investigations of digital traces and social media are regularly conducted in domains such as journalism [41], business [e.g., 15, 75, 77, 103], counter-terrorism [69], cybersecurity [28], and human rights advocacy [22, 47].

Traditionally, the OSINT cycle consists of: content discovery, verification, preservation, and publication [97]. McKeown et al. [58] argue that the target of an OSINT investigation will generally shape the type of investigation that will be carried out, the type of data that will be gathered and analyzed, the levels of detail that will go into the investigation, the tools used, the investigators' behaviors and attitudes, and the various outcomes of that investigation (e.g., reports, forecasts, news articles, criminal proceedings).

Conducting OSINT investigations involves more than just the type of data or techniques used. According to practitioners, OSINT also comes with its own ethos [40, 97]. The OSINT ethos prioritizes transparency and accountability, frowns upon the use of subterfuge, and limits investigations to passive reconnaissance [e.g., 22, 50]. This ethos may be the reason for expert OSINT investigators' successes and reduced rate of ethical mishaps. Directly contacting law enforcement coupled with only engaging in passive reconnaissance greatly lowers the possibility of vigilantism — especially doxxing and misidentification. For example, while both novices and experts sought to use OSINT to investigate the storming of the U.S. Capitol in 2021, some novices publicly misidentified individuals [49]. On the other hand, John Scott-Railton, an OSINT expert, shared his findings directly with the FBI [31] and encouraged his collaborators and followers not to publicly tweet unconfirmed names. Scott-Railton's work directly led to two arrests [65].

The access to increasing amounts of open source data, along with the OSINT ethos, has led many OSINT experts from diverse backgrounds to form organizations in order to increase their investigations' impact. For example, OSINT experts of Amnesty International founded a Citizen Evidence Lab and Digital Verification Corps which involves crowdsourced volunteers collaborating from all over the world [7]. They published a report detailing their methodology, analysis and findings of their investigation into online abuse against women which resulted in better protections for women on Twitter [6]. Other organizations use competitive models. For example, Hackatoria is an organization that simulates OSINT investigations in the form of Capture The Flag (CTF) competitions using fabricated data [39]. Their mission is to expose individuals to the OSINT field and community by helping them to learn OSINT skills, resources, and values in a controlled and playful environment [39]. Due to the need for individuals with diverse domain expertise in the field, both collaborative and competitive organizations play an important role in building the OSINT community [66, 95].

Along with the advantages of OSINT investigations, there are also challenges [24, 43, 58]. During an investigation, issues can arise from the ephemerality of open source information online [22] or because deep fakes, dis-, and mis-information are harder to verify [22, 43]. Another challenge is the possible exposure to sensitive materials, especially when investigating violence of any kind, that can result in secondary trauma [9]. Regardless of resources, Gill [36] states that the success of an OSINT investigations depends on its social structure: its members, their roles, and their training. Our work here contributes a deeper understanding of the *social* dynamics and practices within OSINT organizations. We also highlight OSINT experts' varied backgrounds and motivations, as well as the social and technological challenges that they face during the course of their investigations.

2.2 Investigations in CSCW

Prior CSCW research has focused on top-down [e.g., 3, 72], bottom-up [e.g., 26, 42, 45], or hybrid investigations [92]. All three investigation types include similar stages, such as collecting and analyzing information towards a specific goal (e.g., the opening of a criminal case, the identification of a suspect), and have often been described as a sensemaking process [e.g., 4, 21, 93]. Generally, top-down, law enforcement-led investigations are more commonly studied within CSCW. Here, access to information is limited by law enforcement. Prior work has focused on the design of tools to support collaboration and coordination between law enforcement agents [3, 72]. For example, Alharthi et al. [4] examined Search and Rescue responders' investigations as a collaborative sensemaking activity to generate design recommendations for collaboration systems. Sometimes, these top-down investigations benefit from members of the community or neighborhood residents passively providing information [20]. For example, Lewis and Lewis [55] examined a community's use of CLEARPath, a website that enables residents to "serve as an information sharing vehicle" between the police and the community, and found that residents used the forum to strengthen their social ties and discuss collective action. Brush et al. [13] proposed augmenting the potential for crime prevention through a digital neighborhood watch. Additional research surfaced the importance of civic engagement and communication, online and offline, between the police and communities in crime prevention [26, 45, 78].

On the other hand, bottom-up, novice-led investigations are typically self-organized by crowds, usually online, who coordinate their efforts and combine their diverse knowledge to conduct the different stages of an investigation. We define these bottom-up investigations as crowdsourced investigations. CSCW researchers have examined these crowd mobilizations on social media. Crowds take on varied roles, such as information diffusion during crises [e.g., 8, 84, 99], or conducting data analysis and validation in citizen science projects [89, 96]. Daily and Starbird [21] studied emergent crowd work on social media during crises as collective sensemaking throughout which online crowds interpreted complex and uncertain data. Huang et al. [42] examined how crowds of online volunteers analyzed photos related to the 2013 Boston Marathon Bombings in the effort of identifying the perpetrators; however, this effort resulted in the infamous misidentifcation of a suspect. More recently, Arif et al. [8] studied mechanisms used by crowds to correct online information on social media about crisis events such as a rumored flight hijacking and the 2015 Paris Attacks, showing that, while crowds do share rumors, they undertake different strategies and attempts to correct them.

Additional prior work also demonstrated that coordinated and directed crowds can augment an investigation's potential [e.g., 56, 57, 92, 94]. For instance, Venkatagiri et al. [94] introduced GroundTruth, a system that enables experts and novice crowds to perform image geolocation, a complex sensemaking task often needed during OSINT investigations. Another example includes Agapie et al.'s [2] case study of crowdworkers tasked to collaboratively report on news events and engage in local information collection assignments.

Our work here contributes to the growing body of literature within CSCW focused on understanding and supporting investigations. While prior work has focused on studying top-down investigations led by experts, or crowdsourced investigations led by novices, we focus on crowdsourced investigations led by expert OSINT investigators at the core of the OSINT community of practice, and their perceptions of novices at the periphery. Additionally, prior work has focused on how investigators leverage collaboration to scale up their investigations. We extend this work to study how OSINT experts leverage both collaborative and competitive efforts to conduct their investigations. We also draw on prior work at the intersection of investigations and sensemaking to suggest design recommendations for OSINT investigations.

2.3 Competitions and the Adversarial Mindset

Hutter et al. note that there is a rich history of using contests, a form of competition, to "reach a broad audience of people with various backgrounds, skills, and expertise" [44]. Such competitions have played a major role in the development of innovations such as digital televisions and the first manned mission to Mars, and are proposed by corporations, governments, and even non-profit organizations [44].

While the role of competition in OSINT investigations has seen little research attention, prior work has looked at the use of social technologies to support various forms of competition, ranging from innovation contests and hackathons [73, 87], and games and gamification [54, 63, 74], to self-competition [61]. Researchers observe an increased level of immersion and motivation when competition is present [70, 101]. For example, gamification is commonly used as an effective and purposeful incentive mechanism for users of CSCW systems; such design examples have been used in crowdsourcing [63], innovation communities [87] and other platforms. Yu et al. [102] combined intrinsic incentives, generally associated with collaboration, and extrinsic incentives, usually associated with competition, in several experiments on a crowdsourcing platform and found that both were important in motivating participants; however, some incentives could potentially undermine others.

Similarly, Tausczik and Wang [87] examined open innovation contests on Kaggle, and found that only a small percentage of participants, mainly ones doing moderately well in the contest, shared code. They found that sharing code only improved individual, and not collective, performance. They recommend careful consideration when combining these approaches, which can lead to greater benefits than using either alone.

Another example from Hutter et al.'s work [44] focuses on the simultaneous combination of collaboration and competition in community-based design contests where contestants are encouraged to communicate with their competitors. They found that communititors (i.e., people who collaborated and competed) won the design contest and earned the most awards.

Because of the strength of online community ties, extrinsic incentives, such as winning a prize, are not the only motives for participating in competitive organizations and events. There are additional intrinsic incentives related to community building, which, in turn, increase participation and enhance the quality of work submitted. Hutter et al. name this phenomenon "communitition"

based on a similar concept in business named "co-opetition." [44] A more recent example comes from Morschheuser et al.'s work on the concept of cooperative gamification, a structure requiring positive goal interdependence between players, which they suggest could be a promising approach for crowdsourcing and other CSCW systems [63].

Another relevant aspect of competition is the adversarial nature of investigations, where two opposing sides exist [82, 83]. Prior research has shown that intelligence analysts [16], investigative journalists [1], and Information Security (InfoSec) and cybersecurity professionals [14, 68], many of whom join the OSINT community, all foster and employ an adversarial mindset in their training, analyses, and investigations. This mindset inherently lends itself to competition. A prime example is their reliance on competitions as forms of training, such as Capture The Flag (CTF) competitions [14], hackathons [76], or case exercises against enemy actors [32]. Votipka et al. found that hacking exercises can support learning and establishing a helpful online community, but organizers need to carefully consider their structure as to not let the adversarial mindset of competition to get in the way of community participation and education [95]. Chin et al. note that the adversarial mindset in intelligence analysts also leads to a distrust in their peers' analyses unless the data source is shared. They propose that intelligence analysts should forego their historically competitive culture and environment for a more collaborative setting to avoid major threats, such as the 9/11 terrorist attacks [16].

In relation to prior work focused on competition and/or collaboration, we study how the OSINT organizations' members' diverse motivations, their ethos, and the adversarial nature of investigations lead to diverse social dynamics, including different combinations of competition and collaboration. In particular, we focus on their background and motivations, investigative processes and roles and responsibilities, comparing and contrasting their training practices and regimens, and their division of labor.

3 METHODS

3.1 Recruitment and Participants

When recruiting participants, we aimed for a breadth of domain applications and basic social structures of the investigations. We identified a number of organizations and events that carry out OSINT investigations in various domains (e.g., international crime, environmental issues, national security and public safety, human rights violations, theoretical investigations) and social structures (i.e., competitive or collaborative) (see Table 1). Some of the organizations conduct real-world investigations while others create simulated ones. *Real-world investigations* provide intelligence that has the potential to affect or augment an ongoing investigation (e.g., by law enforcement, intelligence agencies, NGOs, companies) or to focus attention on world events with potential impacts on the investigation's clients or the public (e.g., lawsuit, employee termination, news article, NGO report). They can either be collaborative (e.g., O2, O3, O4) or competitive (e.g., O7) and they are often conducted in partnership with another entity (e.g., law enforcement, media, NGOs, governments). On the other hand, *simulated investigations* do not serve a real investigative purpose or have impacts on the investigations' subjects. They are, however, a common activity among this community of practice, allowing novices to join the community and provide them with minimal-risk training. Similar to real-world investigations, they can either be collaborative (e.g., O11, O12) or competitive (e.g., O1, O6, O8) in the form of Capture The Flag (CTF) contests or competitive quizzes, and use either fabricated data or real public information. While we initially divided organization based on either competitive or collaborative social frameworks, our understanding evolves during interviews, revealing a more complex intertwining between collaborative and competitive approaches.

We sought to recruit, through purposive and snowball sampling [80, 90], at least two participants with different roles (i.e., organizer or contributor) from each organization and/or event. We began recruitment with purposive sampling, through direct email invitations of multiple organizers and/or participants who publicly mentioned belonging to one of the selected organizations or events, and continued with snowball sampling to include other organizers and/or contributors within their organization or event. Participants were compensated ($50 Amazon gift card) for taking part in our study.

In total, we interviewed 14 participants (P1–P14). We consider all recruited participants to be OSINT experts. Some solely held organizer roles (n=8), some solely held contributor roles (n=2), and others held both roles either across different organizations or different investigations (n=4). The participants represented 14 different organizations and events (O1–O14). Our findings mainly focus on the participants' experiences in nine organizations for which we recruited at least two participants (O1–O9).

The participants' locations included Asia (n=1), Europe (n=4), and North America (n=9). The participants identified mostly as men (n=9, n=5 women, n=0 nonbinary), and their ages ranged from 26 to 55 years, with a majority (n=6) falling in the 46 to 55 age range.

While all participants self-identify as open source investigators or having ties with OSINT investigations (see Table 2), their backgrounds range from security consultants (n=5) to journalists (n=5), including investigative journalists (n=2), to intelligence analysts (n=2), to a geospatial analyst (n=1) and graphic designer (n=1).

3.2 Data Collection

Participants completed a consent form and a demographics presurvey, with Institutional Review Board (IRB) approval. We conducted semi-structured interviews between October 2020 and January 2021. Each interview was conducted remotely over Zoom and lasted a maximum of 60 minutes. During the interview, we asked the participant's about their professional background, their relation to OSINT, their motivations and definition of success when conducting OSINT investigations, and their investigative process, including their strategies for collecting, verifying, analyzing, and when applicable, preserving and disseminating, the information. Following that, we inquired about their investigations' social structures; we asked about the coordination of individuals during the process, their roles and responsibilities, and their typical tasks, as well as their technology usage and needs. While the main focus of our study is the social structure of these OSINT investigations, we believe that asking participants about their entire investigative process helps us understand the broader view of how different stages of the investigation are conducted and how different aspects

Table 1: Organization Codes and Descriptions *we present the overarching social framework based on our initial observations during the organizations' selection for recruitment, our understanding changes during the interviews, showing more complex frameworks, with collaborative organizations employing competitive concepts and vice versa.

Organization	Social Framework*	Investigation Type	Domain Application
O1	Competitive	Simulated with fabricated data	CTF contest with changing themes
O2	Collaborative	Real world	National security and public safety investigations
O3	Collaborative	Real world	Human rights violations investigations
O4	Collaborative	Real world	Injustices and crime investigations in Africa
O5	Collaborative	Real world	War zones, human rights violations, and criminal investigations
O6	Competitive	Simulated with real data	CTF contest investigating the lives of real volunteers
O7	Competitive	Real world	CTF contest investigating missing person cases
O8	Competitive	Simulated with real data	Daily Geo-location quizzes on Twitter
O9	Collaborative	Real world	Child trafficking and exploitation investigations
O10	Collaborative	Real world	Economic and cyber crime investigations
O11	Collaborative	Simulated with real and fabricated data	OSINT news and trainings
O12	Collaborative	Simulated with real and fabricated data	Cybersecurity and OSINT training
O13	Collaborative	Real world	Investigations for domestic violence victims
O14	Collaborative	Real world	Corporate social engineering investigations

of the investigation come into play which ameliorates our understanding of the social dynamics in action [79]. Participants P6 and P7 were interviewed simultaneously; all other participants were interviewed separately.

All interviews were audio and video recorded with participants' consent. Automated transcripts were generated by Zoom and manually corrected line-by-line. Throughout all interviews, we also maintained typed notes. All participant and organization names have been anonymized.

3.3 Data Analysis

We used a theoretical thematic approach to analyze the interview data [11]. Given that we are mainly interested in the social aspects of OSINT investigations, Braun and Clarke's qualitative methodology allows us to provide a more detailed and nuanced analysis of such themes within the data [11]. We used the Dedoose software to carry our qualitative analysis, creating a code tree based on themes extracted from our research questions and previous discussions between authors. Some initial codes included "definitions of success", "collaborative / competitive division of labor", "power dynamics within the organization", and "organizer's support for contributors". As the analysis progressed, all authors periodically discussed observations about the data and iterated through the codes to capture interesting nuances and themes. Some of the later codes added included "power dynamics outside of the organization", "community ties", and "contributors' support for other contributors".

As prescribed by Braun and Clarke's methods [11], we refined and iterated on the codes, resulting in a final code tree of 44 codes. The tree consisted of 7 main codes (organization's mission; background, motivations, and success; investigative process and division of labor; novice support from experts / organizers; skills training, contributors' support from contributors; and standout quotes), and the rest being child codes. We highlighted and annotated each interview transcript with one or more appropriate codes, resulting in a total of 1207 excerpts and 3652 code applications.

3.4 Limitations

The field of OSINT and its domain applications are vast. While we attempted to capture some of that breadth through our recruitment techniques, we were unable to capture the totality of domain applications or investigative social structures in the organizations we sampled. Despite striving for a gender balance across our participants, we were unable to recruit more female participants, reflecting the broader lack of gender diversity in the OSINT community [10]. We also recognize an imbalance in the roles of participants recruited, having more organizers, as their association with their organization is generally made public.

4 FINDINGS

4.1 OSINT Organizations as Communities of Practice

In the following sections, we analyze OSINT organizations as communities of practice. First, we detail participants' motivations and definitions of success as members of the community. We then describe how experts support newcomers joining their organizations and progressing to full membership by providing them with collaborative and/or competitive training strategies and instilling certain principles in them, such as ethical foundations, transparency, resilience, and safety. Next, we convey how the experts, often working closely with novices and once novices themselves, perceive the novices' progression in the community. We describe how newcomers learn the roles of technology, i.e., communication and information sharing, as well as experts' tool recommendations for supporting the community. Finally, we identify key tensions within the OSINT community and their attempted remedies through social OSINT tactics.

4.1.1 ***Motivations and Definitions of Success.*** Participants' motivations and definitions of success as members of the OSINT community, while encompassing diverse fields and investigations, share common themes including education, giving back to the community, policy and social change, combating criminal activity, and

Table 2: Participant Demographics. *We used an open-ended question to ask participants what gender they identified as; we received two response types: "man" (M) and "woman" (W). **O/C denotes participants who assumed both the role of an organizer and the role of a contributor, either in different organizations or across different investigations in the same organization.

Participant	Gender*	Age Range	Location	Role(s)**	Organization(s)	Occupation
P1	M	26-35	Asia	Organizer	O1	Security Consultant
P2	M	46-55	North America	Organizer	O2	Intelligence Analyst
P3	W	46-55	North America	Organizer	O3	Journalist
P4	M	-	Europe	O/C	O4/O5	Investigative Journalist
P5	M	26-35	North America	Contributor	O2/O10	Intelligence Analyst
P6	W	46-55	North America	Organizer	O6	Security Consultant
P7	M	46-55	North America	Organizer	O6	Security Consultant
P8	M	46-55	North America	O/C	O7/O11/O12	Security Consultant
P9	M	36-45	Europe	O/C	O8	Journalist
P10	W	36-45	Europe	Organizer	O8	Journalist
P11	M	26-35	Europe	O/C	O4/O5	Investigative Journalist
P12	W	36-45	North America	Contributor	O7/O8/O9/O13	Graphic Designer
P13	M	46-55	North America	Organizer	O9/O14	Security Consultant
P14	W	26-35	North America	Organizer	O3	Geospatial Analyst

the thrill of solving a case. As P8 said, while a specific OSINT investigation can yield either positive, negative, or inconclusive results, success and motivation stem from the *"reason why we're doing it"* — supporting the broader cause or purpose of the investigation. Some participants (n=4) are motivated by the desire of "giving back" to various communities by volunteering their time and skills to support vulnerable people, e.g., help victims escape their abusers, find missing people, and rescue trafficked children. More broadly, some, more experienced participants (n=3) mentioned policy and social change as driving their endeavors: *"once upon a time, I thought success would be 'you found the bad guys', now I think it's about getting people to work together on new issues, [...] something that could last two or three years and end up in policy"* (P4).

Many participants (n=8) are motivated by promoting OSINT education and awareness, and many experts make their income from a combination of practice and training. Some want to help educate the public on topics about which they are passionate, specifically cybersecurity and digital privacy and security awareness, as P6 and P7 mentioned: *"It was a fun way of trying to educate people about types of information that were out there [...] so that they have a greater awareness of what they're sharing, what their friends and family are sharing."* Others are motivated to educate fellow investigators. For example, P3 seeks to increase investigators' awareness about their physical and psychological safety when conducting investigations, and teach them to consider the ethical implications of their work; *"success to us [is] that students have all the tools, including how to take care of themselves psychologically, physically, and do it ethically".*

Some participants want to teach others how to develop their analytical and research skills. As P2 stated: *"It is always exciting to know that you're doing something that's having a contribution to national security and public safety; more exciting than that was helping these analysts develop their skills [...] as long as they develop strong analytical and research skills and come out of the program knowing how to effectively leverage social media, then I consider that to be a success."* As another example, P12 who is an administrator of a Discord server where OSINT community members conduct small investigations said: *"we'll do kind of a live walkthrough [of an investigation] so new people can see how to do it and how people who have been in OSINT a while think, and we kind of guide them along. It's almost like you're teamed up with [...] a mentor."*

Finally some participants (n=4) are excited by the dynamic nature of OSINT, per se, and the thrill of solving their investigations. P11 said *"it's like a game, sort of trying to follow [...] that chain of evidence and you get addicted to it. It's almost like a drug addiction in a way. That rush of adrenaline you get when you find something, you want to do that again."*

4.1.2 ***Legitimate Peripheral Participation.*** Strengthening the case for OSINT as a community of practice, we found participants shared many examples of behavior consistent with Legitimate Peripheral Participation [52] (LPP). Drawing on their own past experiences as novices and recent interactions with novices joining their organizations, our participants shared that newcomers start with low-risk tasks and slowly gain a level of mastery. As their tenure in an organization and knowledge of OSINT grows, they have greater opportunities to become experts in the community. *"We all started out as participants in there,"* said P9 when talking about the organizers in O8.

Throughout the investigations, experts support novice contributors by providing them with exercises designed to guide them through the investigative process and allow them to build not only the skills and mindset needed, but also the confidence to do OSINT work on their own. P11 recounted training others through case studies and *"showing them the thread of evidence, [...] how they can go step by step, both about finding the story, but also investigating it. That's really helpful because it builds confidence."* P5 shared his past experience as a novice contributor in O2, cultivating his project step-by-step and graduating to become a subject matter expert. P2 and P8 also mentioned that it is motivating for contributors to include their personal interests in those exercises and projects, a kind of constructionism [5].

We observe through participants' experiences that learning happens in both collaborative and competitive models. Five of our participants mention either learning or teaching the basic skills and techniques through formal courses that provide collaborative hands-on training. P3 explained that *"we did live election monitoring and we had 60 students and a lot of students in our class came [...] and kind of got their feet wet doing that."* Others encourage learning by participating in more competitive organizations that provide simulated investigative contests such as O6 or O8, or real-world investigative contests, such as O7, as P12 suggests, *"competing in the [O7] events [...] is good for just learning how to think outside of the box."*

Because of the wide range of OSINT-related skills and applications, all participants expressed that OSINT experts tend to be generalists. As P8 put, *"It's like mastering, you know, all of the languages in the world, there are some people that get really good at a lot of them, but most of us, you know, we pick what we need to work on and we master those as much as we can, but there's always stuff outside of our area of expertise."* To address this challenge and broaden their knowledge bases, participants reported that learning from and with others is a common training regimen. For example, P8 remembered a co-investigator sharing that a sea has a higher level on the horizon than an ocean and *"his experience helped me get better at validating and verifying [image geolocations]."* The community's culture of transparency carries into competitions during which participants still share their diverse skill sets and methodologies with other competitors. As an example, P6 spoke excitedly about a competition she and P7 organized where *"the people who were competing are standing around asking each other, 'well, how did you get that answer?'[...] They're explaining and sharing the different open source sites that they found that other people didn't know anything about."* P10 also heavily encourages people who participate in O8's quizzes to share their various approaches to finding the answer, emphasizing *"learning from others and working together with others"* as much as winning.

4.1.3 ***OSINT Community Foundations.*** Open source work can be time-consuming, frustrating, and even physically or mentally taxing. All participants emphasized several important foundations for doing OSINT work: 1) understanding the ethical and legal implications of their work, and 2) stressing transparency, resilience, and safety. These foundational principles are valued by the community, and experts attempt to instill these concepts in novices throughout their learning process. P2 recommended to train all team members in the appropriate legal guidelines, such as 28 CFR Part 23, the federal law regulating the collection of information on U.S. persons when working with law enforcement, as well as OPSEC, i.e., *"some basic operational security procedures that are meant to protect themselves as well as the work they're doing [like] crash courses on VPNs, virtual machines and the dark web."* In the case of O9's investigations into child trafficking and exploitation, P13 shared that all investigative work has to be done on their proprietary VDI (Virtual Desktop Infrastructure) software, as it is set up to safeguard the volunteers *"from getting any illegal material by mistake on their computer."* During his interview, P9 described ethical questions he wrestles with, such as: *"'Should I try to reset someone's password to find out if he's registered at this platform?'"*

Organizers emphasize the importance of safety and mental and emotional resilience through teaching patience, rotating personnel on projects, fostering strong bonds within the organization, mandating therapy sessions, or even blacklisting certain areas of the internet. While working on an investigation related to the COVID-19 pandemic, P2 said that one *"team was so busy, we started rotating people through it every week [...] it was such an intense work environment, we didn't want people in that for too long."* P3 added that *"user generated content can be dramatic and traumatic in ways just as traumatic as coming into contact with trauma firsthand in some ways because it's so intimate."* In order to reduce the exposure to such content, P4 advised to *"watch it on a phone, watch it in black and white, turn off the sound, don't get immersed into this."*

Beyond the supportive infrastructure established by the organizers, contributors of all experience levels support each other by building strong community ties and maintaining friendly relationships. P14 excitedly recounted that *"students do quite a bit of, like, getting to know each other, and when we were in person they'd go out salsa dancing."* P3 elaborated on the benefits of community building, citing it as a resiliency method that also helps foster shared ethics and norms, *"[making] everyone feel, you know, part of this team and connected and don't leave anyone behind."* P12 mentioned that the community and other contributors have been very supportive of her learning and growing as an open source investigator, and that she *"will always find somebody to bother"* for help.

4.1.4 ***Social OSINT Tools.*** Our participants suggest that many novices, when first joining the community, are attracted to the technological aspects of the OSINT field. However, according to these participants, heavily focusing on tools can prevent newcomers from fostering more essential and portable skills, such as critical and analytical thinking. At least eight of our participants shared that newcomers seemed overly focused on tools, an attitude the experts try to refocus. P12 said, *"I see these new people coming in, and they want to know all the tools, 'what are all the tools?', 'what tools should I use?', 'what do I need to know?' and they don't learn the tradecraft behind it"*. P3 added that students join O3 thinking, *"Oh, this is a tech-heavy thing' but it's really not. It's about fact-finding [...] that part of it has to be really emphasized."* While the usage of tools is still necessary, this distancing is partially due to the dynamic nature of the OSINT field and the constant changes in capabilities, restrictions, and even layouts of different online tools and platforms. For instance, P13 shared that *"APIs change so often,[...] I found tools to be less useful than doing it manually so that presents a problem cause a lot of OSINTers [...] rely on tools, which means that they get faulty or bad data."*

Despite these cautionary tales, participants also told us that as novices gain mastery, they learn that tools still have two important roles in supporting the community's social structure: 1) communication and 2) information sharing. We observe that all participants successfully employ general-purpose, usually open-source, tools that are easy to adapt to their investigative needs. Participants, including P11, P12, and P13, cited Slack, Discord, and Signal as valuable communication tools. P12 explained that it can be a beneficial way to receive quick feedback on findings, or bounce off ideas, and that she *"thrive[s] in that kind of situation."* Further, P6 and P7 shared that their CTF contestants sometimes prefer text chat over

voice conversations during time-sensitive contests, as it may allow them to stay focused: *"We had this one team of three people, [...] and they were just staring for three or four hours, all three, and I don't think they ever talked to each other... Yeah, they were really intense"* yet highly successful.

For information sharing, participants described using SharePoint, Google Drive folders, and spreadsheets. P11 described his collaboration: *"we rely quite a bit on spreadsheets ourselves. [...] For each investigation, [co-investigator] does what we call '[name] epic spreadsheet', because it's a huge spreadsheet with [...] every video of an incident [and its location, chronolocation]..."* However, cross-platform sharing, especially if investigators have to use specialized tools for data analyses, can become somewhat unmanageable. P8 explained, *"I can't tell you the number of students [...] that tell me 'hey, I have to use One Note and it sucks,' 'I have to use Microsoft Office and it sucks,' 'I use Etherpad,' 'I use a Google Docs,' 'I use a spreadsheet,' 'I use a mind map.' There's all these different ways of documenting and yet none of them is great for sharing."* Facing these challenges, P10 described building her own tool: *"I developed [a collaborative platform for the analysis and verification of digital content] with my team, and also other organizations use it. So we can also collaborate on this together."*

Asked about their"wish list" of tools that would support or improve OSINT investigations, some participants gave examples that streamlined collaboration or building on the prior work of other investigators. P8 eagerly shared his need and vision for an open-source *"case management software dedicated to open source intelligence"* helping lead investigators manage their teams. He elaborated that *"there are so many people [who wonder] 'how do I do OSINT in a team, in a group?' because... 'How do I decrease the redundancy?' [...] It's that last piece of managing the entire case that's really, really missing."* Another example is P4's idea for preserving and sharing collaborative OSINT work that has already been generated by experts. P4 described *"[a tool that would] scrape the entire Twitter for Google Maps mentions and put them on a map. [...] So that all the history of geolocation work that I've done on Twitter over the past five years could be then plotted on a map in collaboration with every other open-source investigator"*.

4.1.5 ***Challenges and Remedial Strategies***. During the pre-investigation stage, all organizers try to formulate an investigation plan based on the OSINT cycle which consists of content discovery, verification, preservation, and publication. This stage defines the involvement of different contributors and outside entities (e.g., partners or clients), the division of labor, and the rules and training investigators have to abide by. As P3 recounts:

> *[The investigation plan] involves aspects of, kind of, 'what is our objective? What are, you know, some of the risks involved with this cybersecurity-wise or resiliency-wise? [...] What's the expectation of the partner? What will the deliverables be?' And then 'What are the steps along the way to get there? What's the capacity of our team? Do we have the right language skills for this? Do we have the tech skills?'*

We observe that greater challenges arise from the content discovery and verification stages, as they often require parsing through massive amounts of data and using various tools and techniques to verify and synthesize it into actionable intelligence. As OSINT is accessible to everyone, organizations (e.g., O4, O5, and O7) try to remedy those challenges by soliciting the assistance and/or domain expertise of additional community members for these stages through avenues that attract large crowds; i.e., crowdsourcing and time-constrained competitive events. As P11 shared, for one of the investigations conducted by O4, *"we ended up bringing in 15 people all together, working, but most of them, it wasn't full time... it was quite intense but then once the findings were made, then they don't have to work on it [anymore]."* As a contributor, P12 shared her experience in O7's CTF: *"you don't get a rundown of what everyone has found afterwards, how they found it, because they just give it to law enforcement and a lot of it never gets [shared back with the contestants]."*

Bringing together contributors from diverse backgrounds creates tensions. From a broader perspective, our interviews highlight that different participants valued ethical implications, interdisciplinarity in OSINT, and online recognition on different levels. Two of the participants explicitly attributed certain values, such as the desire for online recognition, to the *"tech bro"* (P3), or more specifically, *"BrOSINT"* (P14) culture. P11 described some of the tensions that can stem from these different values colliding: *"There was like an interesting tension when we were working on [investigation title] between open-source investigators who wanted to publish [the findings] straight away [on their Twitter accounts], and obviously my boss was like, 'no, no, we can make a video about it [instead].'"* To remedy these tensions, some organizers, such as P2, P3, and P14, attempt to frame their investigations in different ways to attract contributors with more similar values. P3 elaborated, *"we found when we have classes where we get more men, and we have classes about human rights, where we get all women, so... but it's like framing is important, like, how are you framing this: is it a tech bro thing or is it a human rights thing?"*

4.2 Primarily Collaborative OSINT Organizations

The need for contributors from diverse backgrounds results in varying social structures; some more collaborative, some more competitive, and some with unique blendings of collaborative and competitive strategies (i.e., social OSINT tactics), as shown in Figure 1. As the overarching social structure of an organization, collaboration tends to be more prevalent than competition, especially in organizations that conduct real-life investigations, as we can see in O2, O3, O4, O5, O9, O10, O13, and O14. However, this social structure is also adopted by organizations that conduct simulated investigations, such as O11 and O12. Explaining the reasoning behind O2's more collaborative structure, P2 pointed to authenticity as well as diverse perspectives: *"part of it is a recognition that almost all the work done in the U.S. intelligence community now, analytic work, is done in a team-based environment, so we want [the students] to be familiar with working in a team-based environment and develop these team-working skills, but it's also just a sound analytic practice, that if you have multiple perspectives, it helps eliminate or at least counteract cognitive bias."* P3 elaborated on collaboration as a cultural aspect of OSINT: *"[the] open source community generally is super collaborative and that's what I love about it and I think anything*

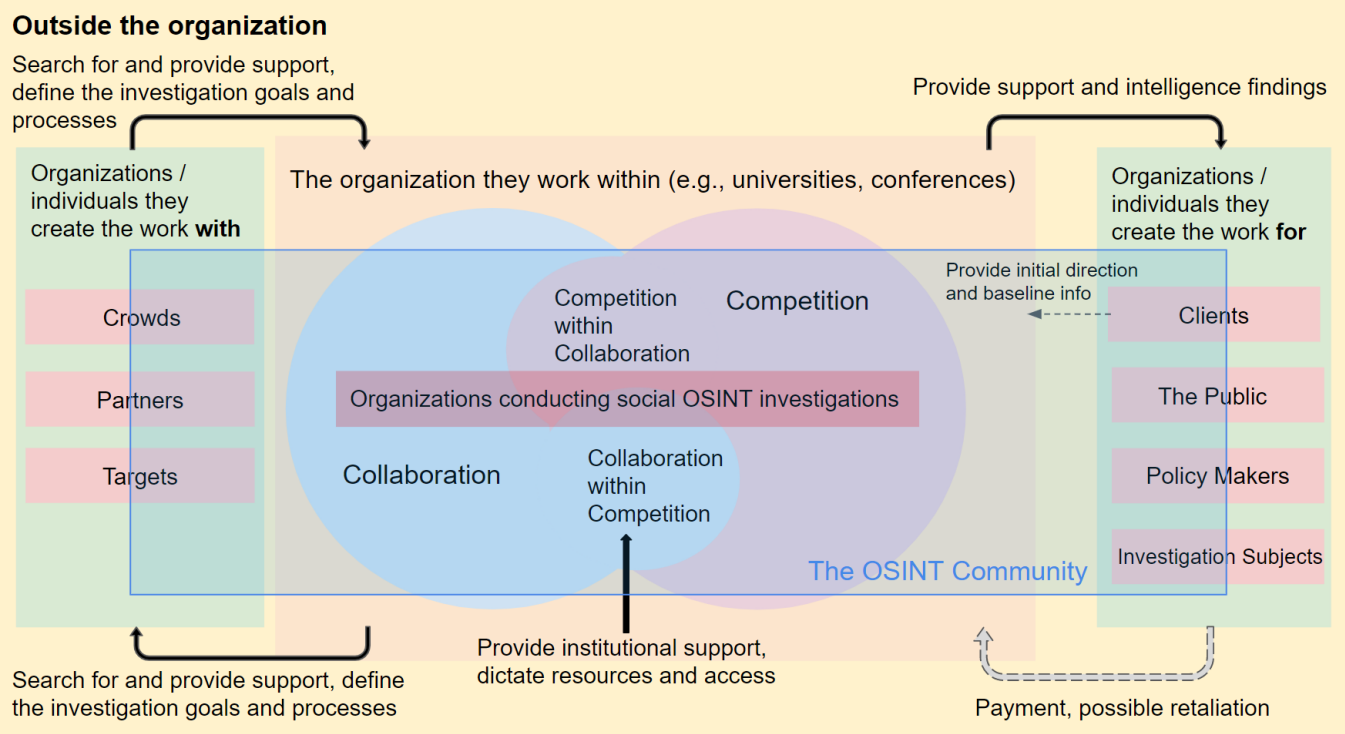

Figure 1: Diagram depicting the social dynamics within and outside the organizations conducting OSINT investigations. These organizations sit in the middle of the diagram, in an interplay between collaboration, competition, and social OSINT tactics. We present organizations and/or individuals they work within which provide institutional support (orange). We also present organization they work with (right), or for (left) and the different interactions/dynamics between them. We overlay the boundaries of the OSINT community, which encompass the entirety of the organization we study but only include a portion of the organizations they work within, with, and for. (Dashed arrows denote possible, but not certain, interactions.)

we all do in this space should be emulating that — collaborating with different partners, collaborating across disciplines, covering different sectors... etc." This practical embrace of collaboration acknowledges that the field of OSINT cannot be mastered by a single or small group of individuals, and therefore, working with others and accepting help from others leads to more successful investigations. As P11 said *"just working on your own, you end up missing a lot of information [...] you can spend hours trying to investigate the story, but [...] you talk to someone else and other open source investigators and they might have another idea that you haven't thought about."* P5 added that being able to leverage other people's subject matter expertise beyond one's own is *"a giant skill whenever it comes to open source investigation."*

Compared to competitive OSINT, this collaborative social model is characterized by a more defined structure and hierarchy in the roles and responsibilities of the members, less explicit rules for tasks, and an emphasis on transparency, communication, and strong bonds between members.

4.2.1 ***More Structure and Hierarchy.*** Our interviews found that organizations using a more collaborative structure overall tend also to employ a more rigid structure and hierarchy in their roles and responsibilities, such as having formal titles for staff positions, and team members reporting to a team leader. For example, O2, O3, O4, and O9 feature organizer positions with specific titles such as "Lab Director", "Team Coordinator", and "Executive Producer." Participants also perceived a considerable need for coordination between investigators, mainly to reduce the redundancy in effort and advance the investigation more efficiently. P14 explained that *"it usually works best when there's a professional staff member with a [graduate student] or with an undergrad to define the team and to help structure the tasks, and to make decisions about what the parameters would be."* We speculate that these organizations define a clear structure and hierarchy in order to manage and scale up the large number of individuals usually involved in their investigations. Bigger groups are often modularized into smaller teams; as P4 noted, *"When you're getting together a room of 30 people trying to document every airstrike in [country], sometimes you need to break them down in teams of five."*

While high structure is common for collaborative OSINT, it is not universal or without its drawbacks. P4 also pointed out that occasionally investigations can happen spontaneously, without much structure and/or coordination discussed: *"it's been that investigators from Twitter, that just had a mutual drive and a mutual passion and say, 'oh my god, let's get these people', and there's no roles discussed there's no hierarchy or team leaders, it really is just a group of people*

that want to do good in the world." P2 also warned that having defined hierarchical roles can sometimes create delegation challenges, such as *"a team lead who is doing all the work themselves or isn't providing sufficient direction or is not allowing people to participate as much as they should."*

4.2.2 ***Less Explicit Rules.*** On the other hand, collaborative organizations tend to feature less explicit or strict rules about how to carry out specific tasks, which tools or techniques to use, or which sources of information to explore, and rely more heavily on the expertise and creativity of the contributors. As P3 recounted: *"we were empowering the students to [be] the experts and to be the innovators and that [...] was a great, great model because the students didn't go look to us and go okay, 'help me figure this out.'"* P14 elaborates on some of the benefits of empowering contributors to be creative: *"we like that atmosphere that everyone feels like it's a little bit more free [...] by seeing what's possible they then start to realize that [the information] they're sitting on is really valuable."*

4.2.3 ***Emphasis on Transparency and Communication.*** In more collaborative settings, good communication is a requirement to enable individuals to work together effectively for lengthy investigations, especially when those individuals do not have the same domain expertise or background. In keeping with that, some participants mention that they attribute more effort to the process over the product. For example, P9 attributed more importance to contributors sharing their methods in solving the quiz than the correct answer. P3 elaborated that the importance is in showing *"these are the steps that I went through, and this is what we can show, and this is what I know and this is what I don't know. [...] That transparency is critical to the open source process."* When working with other investigators, the methodology needs to be transparent, with detailed and structured documentation in order for all investigators to be of the same mind and communicate more precisely. For example, P5 explained that his target profiles are very robust and thorough when working in a team environment, but very minimal and only comprised of *"little notes"* when he is working alone.

4.2.4 ***Strong Bonds.*** Along with robust communication, many participants value strong bonds between investigators. There is a push for individuals investigating together to foster a friendly relationship which improves the quality of their communication, of their resilience and in turn of their work and their sense of community. P4 mentioned building those strong bonds as the *"perfect way"* to work on investigations. Similarly, P5 recalled structuring the tasks of one of O2's investigations based on his teammates' preferences, strengths and weaknesses: *"I think it takes a good amount of knowledge on the people that you work with [to do that]."* P9, P10 and P12 added that contributors who communicate with others will slowly build *"some sort of relationship"* (P9) and slowly become *"part of the family"* (P10).

Some participants, including P4 and P11, mentioned that breaking down bigger groups into smaller teams aids in the creation of such bonds, and in keeping communication lines open between people. P11 shared that during one of O4's big investigations, as more contributors were added to the Slack channel, public conversations in the main chat were decreasing, while private messages were increasing. As a solution, he split this *"big collaboration"* into smaller groups so *"people are then more comfortable to talk and express."* P4 also explained his preference for smaller teams: *"you build a bond with people as well which is important, rather than just 'you do this', 'you do that',[...] it's more 'hey, we're out to do well in the world and we have a small group of dedicated people that can work together.'"* P8 adds that smaller teams can also be beneficial in harnessing the power of sole performers or lone analysts in a collaborative setting by having *"teams of one"* encompassed in a workflow with bigger teams.

4.3 Primarily Competitive OSINT Organizations

As an alternative social structure, competition is mainly present in organizations that offer simulated investigations, such as O1 and O6's CTF competitions and O8's quizzes. As a notable exception, it has also been implemented as a CTF contest for real-world investigations into missing persons by O7. In simulated investigations, this structure aims to assist novices in learning critical skills within a low-risk environment. On the other hand, in real-life investigations, these contests can harness the advantages of competition, including motivation, speed, diversity, and gamification. At least eight of our participants identified competition as a powerful motivator, keeping contributors engaged in the investigation and focused on the task at hand, and creating a sense of urgency. Using competitive strategies can also limit groupthink, and in some cases, reduce the feelings of immersion in distressing user-generated content. It is important to note that while recognizing the benefits of competitive structures, a smaller number (n=2) of participants prefer the social interactions enabled by more collaborative models. P8, while playing in O7's CTF, shared that *"from the competitor point of view, it was... it was pretty darn isolating, [...] as I already mentioned, I'm a very collaborative person,"* P10 also agreed that she is happier when collaborating with others than competing alone.

In OSINT organizations, this competitive model is characterized by a less defined structure and hierarchy in the roles and responsibilities of the members, more explicit rules about tasks, the use of gamification, and the presence of an adversarial mindset.

4.3.1 ***Less Structure and Hierarchy.*** In contrast to organizations that support a more collaborative structure, we find that those that implement a more competitive model overall tend to feature a less defined structure and hierarchy in roles and responsibilities within teams conducting investigations. For example, O1, O6 and O8 do not feature official position titles other than "organizer" and "participants" (also called "players" or "contestants"). O7 features a "judge" who verifies contributors' submissions in addition to these two roles. While organizers have defined roles and responsibilities, team members often do not have an official team leader; each team usually has a team name displayed on the scoreboard and decides on their own structure or lack thereof. P6, P7, and P12 all shared that players *"get to choose who's on their team"* (P6 and P7) and *"it's organized as far as the specific teams feel like they want to organize it"* (P12).

As team members gain experience with one another, they may adopt informal, flexible roles that change within and between events. P12, recalling her own progression as a player, elaborated, saying that *"the more seasoned teams [in CTFs] have a structure set up where*

maybe one person is digging deeper into all of the missing people and someone is just doing surface level submissions for points and I think when people have done these competitions a few times, they start to figure out that you have to have a system like that to get the big points." We speculate that this division of labor partly results from the smaller sizes of teams, ranging from two to four individuals, participating in shorter, more time-constrained, investigations. While sometimes teams of one are allowed in competitive events, according to P1, P6 and P8, they are rare.

4.3.2 ***More Explicit Rules.*** On the other hand, we observe in competitive OSINT events more explicit and strict rules about which sources of information are acceptable, which tools and techniques are allowed, how information should be submitted and how points are awarded. Rules related to acceptable sources and submission steps aim to keep the competitors focused on contributing useful information during the time-constraint, while other rules related to the point system and tools allowed strive to maintain a level playing field among contestants. For example, P8 mentioned that for O7's CTFs, *"the teams need to submit the URL and why they think it's important, [...] their reasoning or analysis behind it."* P6 and P7 also said that players *"could only have two tries"* for O6's challenges. P1, P6, P7 and P12 explain that maintaining a level playing field is important. Sometimes players will *"start, you know, just breaking the rules a little bit"* (P1) or *"hacking the game and making it unfair for the rest of the participants"* (P6). P12 adds that O7's judges may accept submissions differently if the rules are not standardized, which can create some tension during the competition.

4.3.3 ***Gamification.*** Mainly in simulated but also real-world investigations, a benefit of gamification is motivating people to learn OSINT skills who might not otherwise be interested. P6 and P7, for example, implemented competition in the form of a CTF and *"sort of gamified the education process."* P8 added that this sort of structure is *"getting a huge number of people introduced to [the] OSINT world, it's getting a lot of people interested in investigation, it's getting them into the process."* P1 also mentioned that sometimes companies or other organizations encourage their employees to participate in CTFs and acquire new skills that way. However, a number of participants, including P4, P8, and P11, were quick to warn that this kind of playful motivation does not necessarily correlate with better investigative results, and there are some things to keep in mind in order to successfully implement competitive strategies in the investigative process. For example, P1 shared that the prize of the CTF plays a role in extrinsically motivating people to participate, suggesting that some players may be more interested in the prize than the quality of the investigation, tempting them to cheat their way to the prize.

Participants, such as P1, P6 and P7, who organize investigations as simulations also encountered challenges when trying to emulate real-world investigations and techniques in a CTF-style competitive event. While P1 tries to create challenges that hone in on real-world OSINT tactics, the gamified format of competitive events often rewards a different set of strategies. P8 said that *"if [people] take that same methodology that they use to win the CTF, and they try to apply that within a business setting in a real OSINT environment they're going to absolutely fail"* because for many CTFs the winning goal is *"to submit as many flags as possible, which is different than doing an open source intelligence investigation."*

4.3.4 ***An Adversarial Mindset.*** The adversarial mindset and nature of competitive OSINT also creates a sense of urgency that might encourage contributors to work more efficiently. P11 believes that *"a healthy dose of competition can help, definitely, people move faster and... refocus at times because, also again, the open source investigation, you can go down so many rabbit holes... [competition] can definitely push you... As soon as you switch on the competitive mindset, you might be more focused and because you've got the time pressure."* This efficiency can be critical for time-sensitive investigations, such as breaking news events, missing persons cases, and criminal manhunts. However, this competitive mindset should not hinder communication. While competition is *"a wonder for projects"*, as P4 shared, *"the idea of independent competition is not so great because that's what happens in intelligence agencies, they silo information and they don't reach out to each other."* This lack of communication is sometimes used during CTFs, in order to mislead other competitors on a certain team's progress. For example, P6 and P7 mentioned that *"we've had people hold on to flags and drop them at the last minute to drive some of the other competitors crazy."* Some teams also employ *"smack talk"* (P7) in an attempt to demoralize other teams.

The adversarial nature of investigations also leads to another, more subtle, form of competition we observe in our participants' experiences: competing for attention or recognition. For instance, some contributors or organizers have the desire to be the first to publish the findings of their investigation, with journalists not wanting to *"get scooped"* (P11), or want to showcase the results of their investigations and the skills they employed, *"natural[ly] wanting to show outputs that different teams have [like stories, reports, or legal memos]"* (P14). This motivation, according to P10 and P11, is sometimes linked to the *"ego of the individual"* (P11), and whether they care for public recognition of their achievements, or can also be a personal challenge.

4.4 Social OSINT: Blending Collaboration and Competition

As previously mentioned, OSINT investigations are often challenging. They require the involvement of investigators from diverse backgrounds and with various domain expertise who are motivated to parse through massive amounts of data to extract well-grounded intelligence. Eight of the organizations we studied blend collaborative and competitive approaches within their structures to address these challenges, as shown in Figure 1. Within organizations that feature a competitive structure overall, O1, O6, and O7 implement team-based competitions where team members collaborate, stress the need for robust communication, and are often transparent about their findings and techniques with other competitors. O8, which offers competitive daily quizzes, has members who collaborate on solving them through private chats and are heavily encouraged to share their methodologies publicly. On the other hand, O3, O4, and O5 which feature more collaborative structures, encourage an adversarial mindset to create a sense of urgency within competitors and avoid groupthink. In fact, O4 also uses red-teaming, encouraging investigators to "attack" the analysis of their peers. Additionally,

O4 and O12 also set up smaller CTF contests to gamify some stages of the investigation.

4.4.1 ***Collaboration in Primarily Competitive Organizations.*** We found that in a number of organizations, collaborative strategies appeared at a smaller scale within a more competitive structure. Especially in team-based competitions, as implemented by O6, O7 and sometimes O12, members of the same team have free access to each other's skills and domain expertise, and emphasize strong and constant communication because of the contests' time constraints. For example, P12 recalled that during O7's CTF, *"they give you like seven people that you're looking into, so each one of us, [in the team], will pick one person and we'll work on them for like an hour and then, if we hit a dead end we'll switch people just to kind of keep it going."* Her team also sets up a Slack or Discord channel for each target and each teammate *"will post in all [the target] details, what they're finding and other people will kind of comment on it. So it is a collaborative environment..."*

4.4.2 ***Competition in Primarily Collaborative Organizations.*** We also found that some organizations valued competition when incorporated into real-world investigations, and more collaborative settings, as long as communication lines between "opposing" teams remain open and people continuously share their progress and skills with others. Beyond the motivational benefits, competition can help create sounder investigative arguments by having an "opponent" poke holes in the analysis of another investigator, known as *"red teaming."* P11 explained that, while O4 conducts investigations collaboratively, once the investigation is complete *"we'll bring another open source investigator who wasn't working on the story and that person will go through the story with the idea: 'I need to break that story. I need to find a hole in that story. I need to find a mistake.'"* It can also, perhaps surprisingly, help investigators cope with emotionally distressing work facilitating their progress. For example, P4's organization conducts human rights investigations using OSINT methods, and *"to keep that fun we set up little challenges like capture the flag, [...] which is terrible to think of because you're doing human rights cases and you're looking at bombings, but at the same time, if you can gamify that competition, you can get better results."*

4.5 Outside the Organizations

Having examined the social dynamics within the different organizations our participants belong to, we now turn to certain power dynamics that affect the OSINT investigations from outside the organization. First, we present our observation about organizations they work within, with and/or for and how these entities influence the investigative process and provide the OSINT community with a way for their findings to have a concrete impact, then we present certain ties with communities that receive the results of the investigation, or even in some cases with the targets of the investigations, as shown in Figure 1.

4.5.1 ***Organizations Within Organizations.*** Some participants mentioned that their organizations are hosted within an overarching institution or event. As a result, these institutions' or events' rules, regulations and structures impact the organizations' investigations and structure or sometimes dictate the resources they have access to or the contributors allowed to join (cf. Fig 1). For example, O2 and O3 are part of two different universities, O8 is hosted on Twitter, while O1, O6 and O7 are hosted by a number of different conferences. P2, P3, P5 and P14 pointed out that all staff members or organizers of O2 and O3 are employees or faculty members of their respective universities, while the contributors are recruited from a pool of qualified students (e.g., students from a specific major or students who have completed pre-requisite classes). P3 stated that, while O2 is open to students from various disciplines, it is based in a department of the university, encouraging a larger number of that department to join O2. One of the challenges surfaced by the participants is *"a lot of also quality control, because students [who join], they become great at it and then they graduate"* (P3). P11 indicated a difference in access to resources between O4 and O5, with O4 having stricter rules when it comes to crowdsourcing the help of the broader OSINT community and sharing investigative information on social media. P1, P6, and P7 all mentioned that they need to coordinate O1 and O6's events with the conference organizers and that participation is usually restricted to the conference attendees.

4.5.2 ***Organizations They Work For.*** As mentioned in a previous section, some organizations tend to conduct their investigations with or for other institutions (e.g., law enforcement, media, NGOs, government agencies). We observe a difference in relationship between entities the organizations work with, and entities they work for. In the latter case, those entities tend to be perceived as *"customers"* (P2) or clients for whom the organization is providing a product or service. These institutions may provide direction or baseline information during the pre-investigation stage; however, they are less involved in the different components, tasks, and intricacies of the investigative process. P2 shared his perspective on working for such entities:

> *In a lot of cases, consumers of intelligence regard it as a free good. It's just something that shows up magically in their inbox and they don't really give much thought to what comes behind it. So in addition to those specific taskings, we're going to spend a lot of time thinking about 'what is going on in the world that at least should be of interest to our stakeholders, even if they don't realize that it should be of interest to them?'*

4.5.3 ***Organizations They Work With.*** On the other hand, institutions that organizations work with tend to act more like *"partners"* (P3). Even though these partners will still consume the intelligence provided by the organization, they tend to be more involved throughout the investigative process, providing assistance in several stages and helping with training. P3 prefers conducting investigations with partners of O3, saying: *"[NGO name] is great and has been our best partner over time because they have researchers around the world that really need extra support. They know what they want, they sometimes come to us and say, you know 'something's happening in Cameroon, we have five videos. Can you verify these?' and then the students will take a deep look at those."* We discern that participants indicate more balance and compromise happening between the partners' needs and the organization's, than with the clients'. P14 talked about one of O3's partners providing investigative support:

"they have four — which I thought was quite a lot — four different people independently review the geolocation, which I think is good, so the pressure isn't on the students and they've got other professionals and contractors." Through their work with partners, members of O3 are able to witness the results of their investigations being used in NGO reports and even legal proceedings.

Even when organizations are not necessarily working on a certain investigation with another entity, there are community ties between contributors belonging to both institutions which encourage them to share information or provide assistance. P4 and P10, among other participants, said that they follow many other members of different organizations conducting OSINT investigations, which allows them to share or receive leads, ask for help, or even *"have quizzes during lockdown and stuff like that together"* (P4).

4.5.4 ***Subjects of the Investigation.*** In another attempt to remain transparent, participants shared that, in some cases, the subjects of the investigation are aware that an investigation is being conducted on them and provide their consent, such as in the case of O6 that recruits volunteer targets for their CTF, or O13 that is tasked to assist *"domestic violence victims"* (P12) by restricting their information online. P6 and P7 prepare their *"voluntargets"* by trying to put them at ease and explain the process in detail, while also connecting them to previous volunteers who act as references. P12 provides the victims with regular updates about the investigation, and involves them in the verification process. However, sometimes OSINT investigators cannot be transparent with their subjects in order to protect their identities, and avoid compromising the integrity of their investigations. P5, for example, pointed out that he uses alias accounts on social media to be granted access to certain Facebook groups, in which case, subjects of the investigation are not made aware that an investigation is happening. In P13's corporate investigations, while the company is aware that an investigation is being conducted on their employees, the employees themselves are not to avoid them concealing information.

4.5.5 ***The Public.*** Once the investigation is complete, a number of organizations (such as O3, O4, and O5), share their findings publicly (e.g., by publishing a news story or producing a documentary). There are a number of potential consequences, including individuals or policy makers being influenced by the findings, subjects of the investigation being placed in the limelight, other OSINT analysts trying to poke holes in the findings, or even retaliation by outside actors. P4 elaborated on some of the reasons for meticulously reviewing every step of the investigation: *"it's going to be digested by the wizards on Twitter that say, 'well, your geolocation's wrong here, your open source's wrong and your evidence is wrong.' And people in [country] have patriotic open source analysts, happens about [another country] too, [...] that will look at this stuff and say, 'I'm going to take this thing apart.'"* In an attempt to prevent negative consequences, OSINT investigators strive to present their findings in a transparent manner, allowing the public to trace the provenance of their data and results, and employ competitive strategies such as red-teaming, as mentioned in a previous section, to ensure the robustness of their analyses.

P4 added that another social aspect to consider is the invisible influence from outside actors that affects what we see and what is being investigated; when speaking about receiving a lead into an investigation, he said: *"it may have been sent to you for a reason of trying to stir the pot... to influence something that's actually already ongoing, and I think that's very dangerous because it's something that's very hard to verify with proof."*

5 DISCUSSION

Above, we described the personal, interpersonal, and organizational factors that shaped our participants' investigative process. In the following sections, we discuss the three elements that uniquely characterize the OSINT community and how many OSINT organizations blended both competition and collaboration to achieve their goals. We also discuss implications for the design of tools and ways to improve social dynamics within OSINT investigations, as well as investigations within CSCW and HCI more broadly.

5.1 Reflections on Success in the OSINT Community

In our findings, participants presented a variety of ways in which they define success and motivation for themselves when participating in the OSINT community, related to education, giving back to the community, policy and social change, combating criminal activity, and the thrill of solving a case. Sometimes the participants' definitions of success are adapted for simulated investigations that have educational or charitable purposes. However, their efforts may not directly impact or solve real investigations, suggesting that participants' definitions of success may offer limited reward in the real world. Participants also mention facing social and technical challenges, including parsing through and verifying large quantities of diverse data sets, tensions sometimes arising between individuals from various backgrounds and domains, and difficulties balancing the adversarial mindset with the collaboration needed to conduct investigations. For example, while O7 conducts real investigations, P8 mentioned how their CTF contests may duplicate effort by having competitors submitting the same information. Further, P12 was disappointed that competitors' efforts were not rewarded with any follow-up with law enforcement after the contest to know if their work has resulted in the case being solved.

Our findings showed that organizers and contributors can successfully support and expand their OSINT communities through such efforts. However, they may not have the same motivations as professionals in the OSINT field who conduct real-world investigations with the predominant goal of "solving the case." This highlights a gap between some of the OSINT communities of practice that we identified in our study and OSINT as a profession. To close this gap, social OSINT organizers should seek to align their definitions of success for an organization or event with its collaborative or competitive social structure. Primarily collaborative organizations tend to support more authentic investigations, extensive communication, and strong relationship formation, but can be prone to groupthink. Primarily competitive organizations using gamified participation models can boost participation and speed up contributions, but may be less authentic and prone to challenges such as redundancy, cheating, and conflict between teams. As we discuss below, blending the two models may offer the best success potential, allowing organizations to tailor the social dynamics to meet their unique needs.

5.2 Reflections on The Three Elements of the OSINT Community

We surfaced three elements that characterize the OSINT community: 1) the culture of transparency in their work, 2) the presence of an adversarial mindset when conducting investigations, and 3) the collaboration among individuals with diverse motivations and backgrounds.

The OSINT community emphasizes transparency in its work: all participants emphasized only using open source or publicly available data, documenting all sources of data, as well as sharing the detailed methods and analysis techniques used to verify the information and reach their conclusions. Expert members incentivize novices to ensure their documentation of the gathered data, and their verification techniques are transparent through various processes such as recording URL sources, archiving data, and preserving its metadata in order to maintain the authenticity of the evidence. For example, we found that in O9 all investigative work is logged and tracked on proprietary machines and accessible to all investigators assigned to the case. This culture of transparency also extends outside of their organizations: OSINT investigators share their detailed reports with their partners, clients, and the public. Their use of exclusively publicly available data makes it easier for them to be transparent about every step, and perhaps even necessitates that they do — because anyone can theoretically verify or debunk their claims. This rigorous and transparent documentation allows everyone to see the chain of custody when gathering information, and can lead to more trust in their reports and findings by the public, law enforcement, and courts of law [22].

As mentioned by previous research [1, 68, 68, 82], investigations often have an adversarial nature. For instance, in cybersecurity [14], there is a concept of an "attacker" and a "defender." This perspective leads many OSINT investigators with cybersecurity backgrounds to foster an adversarial mindset which inherently lends itself to competitive strategies being employed. We observed these strategies through their use of CTFs, red teaming, and gamification of repetitive or tedious tasks. This mindset can also be present in OSINT investigators with a journalism background, as a product of the meritocratic system underpinning their profession [66]. However, unlike in Chin et al.'s study [16] where intelligence analysts tended to doubt their peers' analyses, we found that OSINT investigators seem to be more confident in their community members' work due to the transparency of data source and techniques employed, even when competitive strategies were used. This finding agrees with Müller and Wiik's findings where OSINT investigators were enablers of collaboration and transparency within the field of investigative journalism [66].

Despite this adversarial mindset, we found that the sheer amount of digital information available required OSINT investigators to collaborate with each other to parse through, verify, and document their investigation in a timely manner. In addition, the wide range of OSINT skills and applications needed to conduct investigations, as mentioned by the participants, also results in a collaborative setting involving individuals with varied backgrounds and skill sets, such as cybersecurity experts, graphic designers, or journalists, and with varied motivations. Such openly collaborative investigations are seemingly made possible because of the OSINT community's culture of transparency. Considering prior research (e.g., [98]) and our findings, we suggest that increasing diversity in both demographics and domain expertise has the potential to generate more robust results for OSINT investigations. However, prior research has found team diversity can be detrimental if individuals are not able to achieve common ground [18, 81]. Similarly, our findings show that tensions can arise from having individuals who hold different values and mindsets in the same organization, such as between members of the so-called "brOSINT" culture and other investigators otherwise driven by social justice. Successful collaborations require carefully negotiating these tensions, such as through Friedman's value sensitive design framework [34] or Tatar's design tensions framework [85].

5.3 Reflections on Social OSINT: Combining Collaboration and Competition

As mentioned in our related work, combining collaboration and competition can motivate individuals to participate in innovation contests and crowdsourcing tasks, as well as enhance the quality of work submitted [44, 87]. Our findings show that OSINT organizations also employ both concepts, but in different combinations. Even in more competitive settings, we found that participants had a desire to give back to the community, or to learn from other members, motives that align with Hutter et al.'s study of collaboration in design contests [44]. However, previous research also demonstrates that competition, and some extrinsic incentives, can sometimes inhibit collaboration, but the degree to which collaboration is inhibited depends on the contest's design [87]. These studies recommend attributing an extrinsic incentive to collaboration in competitive settings, by rewarding competitors who exhibit collaborative behavior throughout the contest [44, 86], or by designing positive goal interdependence in the game, making the success of one player positively correlated with the success of another [63]. We propose that these approaches may also benefit the CTF style designs of more competitive OSINT organizations we examined, such as O1, O6, or O7, reducing the amount of duplicated effort by different teams, and incentivizing contestants to share some of their expertise and findings with other teams, increasing communication and transparency. We also suggest that fully or partially sharing the answer to a flag with the rest of the competitors after it has been found by a team can reduce the effort in deduplicating the competitors' submissions after the CTF, and discourages teams from siloing useful information — a common challenge in collaborative sensemaking [57].

Correspondingly, we propose that competitive strategies can benefit more collaborative OSINT organizations, as we observe in O2, O3 or O4, by limiting groupthink and inaccuracy blindness, reducing feelings of immersion in traumatic content, and encapsulating certain investigative tasks. Kane et al. [46] posit that prompting collaborators to "exert discriminatory thinking and analysis" towards their teammates' work could help them detect inaccurate information. For example, we found that adopting a competitor's mindset helped members of O4 generate well-grounded investigative arguments and avoid retaliation by outside actors once their investigations' results were made public.

Finally, we suggest that more crowdsourced investigations in general can benefit from establishing social ties and leveraging gamification. In the organizations we studied, We found that encouraging the establishment of strong social ties, more specifically friendships, between investigators can provide advantages beyond sensemaking and productivity by strengthening the available support systems and building resilience into investigative teams. Kessler et al. [48] posit that careful conversation with a sympathetic peer can help cope with stress, which is also a secondary trauma mitigation technique employed by other OSINT investigators who focus on human rights violations [22]. Growing a strong social support network between investigators, and even including members who are versed in therapeutic techniques, can assist in shielding members from secondary trauma. Gamifying certain stages of the investigation can also reduce feelings of immersion in user-generated content, especially when it is traumatic such as in human rights investigations. While gamification could help mitigate secondary trauma among participants exposed to upsetting content, such decontextualization risks adverse consequences, trivializing or misconstruing its meaning.

5.4 Social OSINT Tool Design Implications

Our findings present participants' attitudes towards tools and technology, emphasizing a measured wariness when approaching specialized tools but embracing their use nonetheless, especially during the more challenging stages of the OSINT cycle. However, we also report on participants' successful use and adaptation of more general-purpose, typically open-source, tools to coordinate their social OSINT efforts. Participants also expressed a need for tools that support or improve the current social structures of their organizations and events, such as a multi-user case management platform. We present a number of recommendations based on our findings.

OSINT investigations are a complex and creative sensemaking process, requiring the adaptability of a multitude of tools at various stages of the investigation. Given this requirement, we highlight the concept of appropriation in design and relate it to the domain of OSINT investigations. Gonzales et al. [38] surface the importance of designing *appropriable* tools that can accommodate changing workflows and adjust well with other tools being used. In addition, tools such as shared workspaces and collaborative sensemaking systems have been shown to increase awareness of others' activities and progress, benefiting analytical tasks [17, 71]. Taking these prior works into account, we propose that tools supporting social OSINT investigations should allow users to define their own investigative process without centralizing all tasks in one platform.

Our first recommendation is a tool that would act as a dashboard encompassing all stages of the investigation, allowing users to visualize the current activities being completed, and check their progress, and acting as a meeting point where investigators can upload their data from different tools for others to download. We also recognize that, in some cases, investigators may not want to share the information they have, as in the case of journalists concerned about "getting scooped." Therefore, we recommend that tools promote social translucence [27] into the investigative process without inhibiting the potential for competitive strategies to be implemented by the users. For example, a user would be able to see the investigative stages a competitor has completed and a summary of their findings without having access to the details of the activity they are currently working on or the exact data they have gathered. Platforms such as CrossCheck by First Draft News [33], or Check by Meedan [59] which enable journalists to collaborate on the verification of information, demonstrate that journalists can be encouraged to collaborate, especially on open source information.

Despite cautionary tales about tool obsolescence, OSINT investigators still find benefits in different specialized analysis tools dependent on the data they collect, especially during the already-challenging content discovery and verification stages. To alleviate the burden of sharing their data across tools, we suggest an open source standard for tool interoperability at different levels of abstraction [25, 35], facilitating the importing and exporting of data from one tool to another. For example, we propose allowing GPS coordinates to be exported from mapping tools and geotagged social media posts, then to import them into a flight tracking software to automatically track flights within the vicinity of those coordinates.

Our findings demonstrate that OSINT investigators rely on crowdsourcing content discovery and verification tasks when they face obstacles and they do so by recruiting outside analysts on social media platform, notably Twitter. However, social media content can be ephemeral and eclipsed by newer content, as mentioned by P4. Inspired by this finding, we suggest providing investigators with a crowdsourcing platform that would directly link them to a community of experts on Twitter, for example, while preserving and categorizing their work which would alleviate the burden of registering on a different platform and take advantage of an already thriving social network of experts.

6 CONCLUSION

In this paper, we presented a qualitative study with 14 open source intelligence (OSINT) experts to explore how they conduct and socially structure their investigations, and their attitudes towards the current social dynamics in place. We enriched the existing literature on investigations by providing an in-depth analysis of the OSINT community as a community of practice from an expert perspective, detailing the various personal, interpersonal, and organizational factors that shaped their investigations. We also defined and characterized *social OSINT* as combinations of competitive and collaborative strategies that support OSINT investigations. Finally, we drew implications for social computing systems and social structures that can empower OSINT investigators in their various motivations and domain applications, ranging from uncovering human rights violations to fighting child trafficking and exploitation.

ACKNOWLEDGMENTS

First, we would like to thank our expert participants for their valuable time and insight into the OSINT community. We would also like to thank our anonymous reviewers for their thoughtful feedback and detailed comments. This research was supported by NSF award IIS-1651969.

REFERENCES

[1] Jesse Abdenour. 2018. Inspecting the Investigators: An Analysis of Television Investigative Journalism and Factors Leading to Its Production. *Journalism &*

Mass Communication Quarterly 95, 4 (Dec. 2018), 1058–1078. https://doi.org/10.1177/1077699017733438 Publisher: SAGE Publications Inc.

[2] Elena Agapie, Jaime Teevan, and Andrés Monroy-Hernández. 2015. Crowdsourcing in the Field: A Case Study Using Local Crowds for Event Reporting. In *Proceedings of the Third AAAI Conference on Human Computation and Crowdsourcing (HCOMP-15)*. Association for the Advancement of Artificial Intelligence, 11. https://www.microsoft.com/en-us/research/publication/crowdsourcing-in-the-field-a-case-study-using-local-crowds-for-event-reporting/

[3] Joelle Alcaidinho, Larry Freil, Taylor Kelly, Kayla Marland, Chunhui Wu, Bradley Wittenbrook, Giancarlo Valentin, and Melody Jackson. 2017. Mobile Collaboration for Human and Canine Police Explosive Detection Teams. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17)*. Association for Computing Machinery, New York, NY, USA, 925–933. https://doi.org/10.1145/2998181.2998271

[4] Sultan A. Alharthi, Nicolas James LaLone, Hitesh Nidhi Sharma, Igor Dolgov, and Z O. Toups. 2021. An Activity Theory Analysis of Search and; Rescue Collective Sensemaking and Planning Practices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 146, 20 pages. https://doi.org/10.1145/3411764.3445272

[5] Morgan G. Ames. 2018. Hackers, Computers, and Cooperation: A Critical History of Logo and Constructionist Learning. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (Nov. 2018), 1–19. https://doi.org/10.1145/3274287

[6] Amnesty International. 2018. Troll Patrol Findings. https://decoders.amnesty.org/projects/troll-patrol/findings

[7] Amnesty International. 2019. Large-scale Investigations Powered by Thousands of Digital Volunteers Worldwide. https://citizenevidence.org/2019/12/11/large-scale-investigations-powered-by-thousands-of-digital-volunteers-worldwide/ Section: Crowd-sourcing.

[8] Ahmer Arif, John J. Robinson, Stephanie A. Stanek, Elodie S. Fichet, Paul Townsend, Zena Worku, and Kate Starbird. 2017. A Closer Look at the Self-Correcting Crowd: Examining Corrections in Online Rumors. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17)*. Association for Computing Machinery, New York, NY, USA, 155–168. https://doi.org/10.1145/2998181.2998294

[9] Elise Baker, Eric Stover, Rohini Haar, Andrea Lampros, and Alexa Koenig. 2020. Safer Viewing. *Health Hum Rights* 22, 1 (June 2020), 293–304. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7348432/

[10] Bellingcat Investigation Team. 2015. Diversifying OSINT: Women Experts. https://www.bellingcat.com/resources/articles/2015/12/08/women-in-osint-diversifying-the-field/

[11] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (Jan. 2006), 77–101. https://doi.org/10.1191/1478088706qp063oa Publisher: Routledge _eprint: https://www.tandfonline.com/doi/pdf/10.1191/1478088706qp063oa.

[12] Andrea Broughton, Beth Foley, Stefanie Ledermaier, and Annette Cox. 2014. The use of social media in the recruitment process. *Institute for Employment Studies* 3, 13 (2014), 81.

[13] A.J. Bernheim Brush, Jaeyeon Jung, Ratul Mahajan, and Frank Martinez. 2013. Digital neighborhood watch: investigating the sharing of camera data amongst neighbors. In *Proceedings of the 2013 conference on Computer supported cooperative work (CSCW '13)*. Association for Computing Machinery, New York, NY, USA, 693–700. https://doi.org/10.1145/2441776.2441853

[14] Tanner J Burns, Samuel C Rios, Thomas K Jordan, Qijun Gu, and Trevor Underwood. 2017. Analysis and Exercises for Engaging Beginners in Online CTF Competitions for Security Education. *USENIX Workshop on Advances in Security Education (ASE 17)* 9 (2017), 9.

[15] Jonathan L. Calof and Sheila Wright. 2008. Competitive intelligence: A practitioner, academic and inter-disciplinary perspective. *European Journal of Marketing* 42, 7/8 (Jan. 2008), 717–730. https://doi.org/10.1108/03090560810877114 Publisher: Emerald Group Publishing Limited.

[16] George Chin, Olga A. Kuchar, and Katherine E. Wolf. 2009. Exploring the analytical processes of intelligence analysts. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Boston MA USA, 11–20. https://doi.org/10.1145/1518701.1518704

[17] Gregorio Convertino, Helena M. Mentis, Mary Beth Rosson, Aleksandra Slavkovic, and John M. Carroll. 2009. Supporting content and process common ground in computer-supported teamwork. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*. Association for Computing Machinery, New York, NY, USA, 2339–2348. https://doi.org/10.1145/1518701.1519059

[18] Catherine Durnell Cramton and Pamela J. Hinds. 2014. An Embedded Model of Cultural Adaptation in Global Teams. *Organization Science* 25, 4 (Jan. 2014), 1056–1081. https://doi.org/10.1287/orsc.2013.0885 Publisher: INFORMS.

[19] Cyber Week. 2021. OSINT for good | Cyber Week 2021. https://www.cyberweek2021.austcyber.com/event/osint-good

[20] Dharma Dailey and Kate Starbird. 2014. Journalists as Crowdsourcerers: Responding to Crisis by Reporting with a Crowd. *Computer Supported Cooperative Work (CSCW)* 23, 4 (01 Dec 2014), 445–481. https://doi.org/10.1007/s10606-014-9208-z

[21] Dharma Dailey and Kate Starbird. 2015. "It's Raining Dispersants": Collective Sensemaking of Complex Information in Crisis Contexts. In *Proceedings of the 18th ACM Conference Companion on Computer Supported Cooperative Work and; Social Computing* (Vancouver, BC, Canada) *(CSCW'15 Companion)*. Association for Computing Machinery, New York, NY, USA, 155–158. https://doi.org/10.1145/2685553.2698995

[22] Sam Dubberley, Alexa Koenig, and Daragh Murray (Eds.). 2020. *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*. Oxford University Press, Oxford, New York.

[23] Michaelanne Dye, David Nemer, Josiah Mangiameli, Amy S. Bruckman, and Neha Kumar. 2018. *El Paquete Semanal: The Week's Internet in Havana*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3173574.3174213

[24] Sophie Dyer and Gabriela Ivens. 2020. What would a feminist open source investigation look like? *Digi War* 1 (April 2020), 5–17. https://doi.org/10.1057/s42984-020-00008-9

[25] Douglas C. Engelbart. 1990. Knowledge-domain interoperability and an open hyperdocument system. In *Proceedings of the 1990 ACM conference on Computer-supported cooperative work (CSCW '90)*. Association for Computing Machinery, New York, NY, USA, 143–156. https://doi.org/10.1145/99332.99351

[26] Sheena L. Erete. 2015. Engaging Around Neighborhood Issues: How Online Communication Affects Offline Behavior. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '15)*. Association for Computing Machinery, New York, NY, USA, 1590–1601. https://doi.org/10.1145/2675133.2675182

[27] Thomas Erickson and Wendy A Kellogg. 2000. Social translucence: an approach to designing systems that support social processes. *ACM transactions on computer-human interaction (TOCHI)* 7, 1 (2000), 59–83.

[28] Esteban Borges. 2019. SecurityTrails | OSINT Framework: The Perfect Cybersecurity Intel Gathering Tool. https://securitytrails.com/blog/osint-framework

[29] Europol. 2019. *Stop Child Abuse – Trace an Object*. Europol. https://www.europol.europa.eu/stopchildabuse

[30] Europol. 2021. Stop Child Abuse – Trace an Object. https://www.europol.europa.eu/stopchildabuse

[31] Ronan Farrow. 2021. An Air Force Combat Veteran Breached the Senate. https://www.newyorker.com/news/news-desk/an-air-force-combat-veteran-breached-the-senate

[32] FBI. [n.d.]. *New Agent Training*. Federal Bureau of Investigation. https://www.fbi.gov/services/training-academy/new-agent-training

[33] First Draft. 2017. CrossCheck: Our Collaborative Online Verification Newsroom. https://firstdraftnews.org:443/about/crosscheck-newsroom/

[34] Batya Friedman. 1996. Value-sensitive design. *interactions* 3, 6 (1996), 16–23.

[35] P. Ganguly and P. Ray. 2000. Software interoperability of telemedicine systems: a CSCW perspective. In *Proceedings Seventh International Conference on Parallel and Distributed Systems (Cat. No.PR00568)*. IEEE, 349–356. https://doi.org/10.1109/ICPADS.2000.857717 ISSN: 1521-9097.

[36] Peter Gill. 2018. The way ahead in explaining intelligence organization and process. *Intelligence and National Security* 33 (2018), 574–586. https://doi.org/10.1080/02684527.2018.1452566

[37] Michael Glassman and Min Ju Kang. 2012. Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior* 28, 2 (March 2012), 673–682. https://doi.org/10.1016/j.chb.2011.11.014

[38] Joseph A. Gonzales, Casey Fiesler, and Amy Bruckman. 2015. Towards an Appropriable CSCW Tool Ecology: Lessons from the Greatest International Scavenger Hunt the World Has Ever Seen. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work and; Social Computing* (Vancouver, BC, Canada) *(CSCW '15)*. Association for Computing Machinery, New York, NY, USA, 946–957. https://doi.org/10.1145/2675133.2675240

[39] Hacktoria. 2021. Hacktoria – Story Based OSINT Capture The Flag Challenges. https://hacktoria.com/

[40] Melissa Hanham and Jaewoo Shin. 2020. Ethics in the Age of OSINT Innocence. *Stanley Center for Peace and Security* (May 2020), 6. https://stanleycenter.org/publications/ethics-osint-innocence/

[41] Eliot Higgins. 2021. *We Are Bellingcat : An Intelligence Agency for the People*. Bloomsbury Publishing, London.

[42] Y. Linlin Huang, Kate Starbird, Mania Orand, Stephanie A. Stanek, and Heather T. Pedersen. 2015. Connected Through Crisis: Emotional Proximity and the Spread of Misinformation Online. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '15)*. Association for Computing Machinery, New York, NY, USA, 969–980. https://doi.org/10.1145/2675133.2675202

[43] Arthur S. Hulnick. 2002. The Downside of Open Source Intelligence. *International Journal of Intelligence and CounterIntelligence* 15, 4 (Nov. 2002), 565–579.

https://doi.org/10.1080/08850600290101767

[44] Katja Hutter, Julia Hautz, Johann Füller, Julia Mueller, and Kurt Matzler. 2011. Communitition: The Tension between Competition and Collaboration in Community-Based Design Contests. *Creativity and Innovation Management* 20, 1 (2011), 3–21. https://doi.org/10.1111/j.1467-8691.2011.00589.x _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1467-8691.2011.00589.x.

[45] Aarti Israni, Sheena Erete, and Che L. Smith. 2017. Snitches, Trolls, and Social Norms: Unpacking Perceptions of Social Media Use for Crime Prevention. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17)*. Association for Computing Machinery, New York, NY, USA, 1193–1209. https://doi.org/10.1145/2998181.2998238

[46] Aimée A Kane, Sara Kiesler, and Ruogu Kang. 2018. *Inaccuracy Blindness in Collaboration Persists,*. Association for Computing Machinery, New York, NY, USA, 9.

[47] Lachlan Kermode, Jan Freyberg, Alican Akturk, Robert Trafford, Denis Kochetkov, Rafael Pardinas, Eyal Weizman, and Julien Cornebise. 2020. Objects of violence: synthetic data for practical ML in human rights investigations. *arXiv:2004.01030 [cs]* (April 2020), 12. http://arxiv.org/abs/2004.01030 arXiv: 2004.01030.

[48] R C Kessler, R H Price, and C B Wortman. 1985. Social Factors in Psychopathology: Stress, Social Support, and Coping Processes. *Annual Review of Psychology* 36, 1 (1985), 531–572. https://doi.org/10.1146/annurev.ps.36.020185.002531 _eprint: https://doi.org/10.1146/annurev.ps.36.020185.002531.

[49] Meryl Kornfield. 2021. *The wrong ID: Retired firefighter, comedian and Chuck Norris falsely accused of being Capitol rioters.* Washington Post. https://www.washingtonpost.com/technology/2021/01/16/sleuths-falsely-identify-rioters/

[50] Trace Labs. [n.d.]. Search Party Rules. https://www.tracelabs.org/about/search-party-rules

[51] Nicolas J LaLone, Jess Kropczynski, and Andrea H Tapia. 2018. The Symbiotic Relationship of Crisis Response Professionals and Enthusiasts as Demonstrated by Reddit's User-Interface Over Time. In *ISCRAM*. 13.

[52] Jean Lave and Etienne Wenger. 1991. *Situated Learning: Legitimate Peripheral Participation*. Cambridge University Press, Cambridge, UK. Google-Books-ID: CAVIOrW3vYAC.

[53] Charlotte P. Lee, Paul Dourish, and Gloria Mark. 2006. The Human Infrastructure of Cyberinfrastructure. In *Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work* (Banff, Alberta, Canada) *(CSCW '06)*. Association for Computing Machinery, New York, NY, USA, 483–492. https://doi.org/10.1145/1180875.1180950

[54] Sunwha Lee, Sungho Lee, Yoojin Lee, Sanghoo Park, and Jinwoo Kim. 2014. Effect of competition and collaboration in social network game on intimacy among players. In *Proceedings of HCI Korea (HCIK '15)*. Hanbit Media, Inc., Seoul, KOR, 425–433.

[55] Sheena Lewis and Dan A Lewis. 2012. Examining technology that supports community policing. In *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems - CHI '12*. ACM Press, New York, NY, USA, 10.

[56] Tianyi Li, Yasmine Belghith, Chris North, and Kurt Luther. 2020. CrowdTrace: Visualizing Provenance in Distributed Sensemaking. In *2020 IEEE Visualization Conference (VIS)*. IEEE, 5.

[57] Tianyi Li, Kurt Luther, and Chris North. 2018. CrowdIA: Solving Mysteries with Crowdsourced Sensemaking. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW (Nov. 2018), 105:1–105:29. https://doi.org/10.1145/3274374

[58] Sean McKeown, David Maxwell, Leif Azzopardi, and William Bradley Glisson. 2014. Investigating people: a qualitative analysis of the search behaviours of open-source intelligence analysts. In *Proceedings of the 5th Information Interaction in Context Symposium (IIiX '14)*. Association for Computing Machinery, New York, NY, USA, 175–184. https://doi.org/10.1145/2637002.2637023

[59] Meedan. [n.d.]. Check. https://meedan.com/check

[60] Stephen C. Mercado. 2004. *Sailing the sea of OSINT in the information age*. Technical Report. American Psychological Association. https://doi.org/10.1037/e741272011-005 type: dataset.

[61] Alexander Michael and Christof Lutteroth. 2020. Race Yourselves: A Longitudinal Exploration of Self-Competition Between Past, Present, and Future Performances in a VR Exergame. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–17. https://doi.org/10.1145/3313831.3376256

[62] Michael W. McLaughlin. 2012. Using open source intelligence software for cybersecurity intelligence. https://www.computerweekly.com/tip/Using-open-source-intelligence-software-for-cybersecurity-intelligence

[63] Benedikt Morschheuser, Alexander Maedche, and Dominic Walter. 2017. Designing Cooperative Gamification: Conceptualization and Prototypical Implementation. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17)*. Association for Computing Machinery, New York, NY, USA, 2410–2421. https://doi.org/10.1145/2998181.2998272

[64] MwOsint. 2019. Unravelling the Norton Scam. https://keyfindings.blog/2019/08/28/unravelling-the-norton-scam/

[65] Greg Myre. 2021. How Online Sleuths Identified Rioters At The Capitol. https://www.npr.org/2021/01/11/955513539/how-online-sleuths-identified-rioters-at-the-capitol

[66] Nina C. Müller and Jenny Wiik. 2021. From Gatekeeper to Gate-opener: Open-Source Spaces in Investigative Journalism. *Journalism Practice* 0, 0 (May 2021), 1–20. https://doi.org/10.1080/17512786.2021.1919543 Publisher: Routledge _eprint: https://doi.org/10.1080/17512786.2021.1919543.

[67] Johnny Nhan, Laura Huey, and Ryan Broll. 2017. Digilantism: An analysis of crowdsourcing and the Boston marathon bombings. *The British journal of criminology* 57, 2 (2017), 341–361.

[68] Tj OConnor and Christopher Stricklan. 2021. Teaching a Hands-On Mobile and Wireless Cybersecurity Course. In *Proceedings of the 26th ACM Conference on Innovation and Technology in Computer Science Education V. 1*. ACM, Virtual Event Germany, 296–302. https://doi.org/10.1145/3430665.3456346

[69] Department of Homeland Security. 2010. (U//FOUO//LES) DHS Terrorist Use of Social Networking Facebook Case Study | Public Intelligence. https://publicintelligence.net/ufouoles-dhs-terrorist-use-of-social-networking-facebook-case-study/

[70] Juhong Park, Alice Oh, and Suin Kim. 2017. Analysis of the Effect of Competition on Player Immersion and Engagement in a Mobile Game. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 6.

[71] Nicholas J. Pioch and John O. Everett. 2006. POLESTAR: collaborative knowledge management and sensemaking tools for intelligence analysts. In *Proceedings of the 15th ACM international conference on Information and knowledge management (CIKM '06)*. Association for Computing Machinery, New York, NY, USA, 513–521. https://doi.org/10.1145/1183614.1183688

[72] Ronald Poelman, Oytun Akman, Stephan Lukosch, and Pieter Jonker. 2012. As if being there: mediated reality for crime scene investigation. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work (CSCW '12)*. Association for Computing Machinery, New York, NY, USA, 1267–1276. https://doi.org/10.1145/2145204.2145394

[73] Emily Porter, Chris Bopp, Elizabeth Gerber, and Amy Voida. 2017. Reappropriating Hackathons: The Production Work of the CHI4Good Day of Service. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 5.

[74] Melissa J. Rogerson, Martin R. Gibbs, and Wally Smith. 2018. Cooperating to Compete: the Mutuality of Cooperation and Competition in Boardgame Play. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3173574.3173767

[75] Daniel Rouach and Patrice Santi. 2001. Competitive Intelligence Adds Value:: Five Intelligence Attitudes. *European Management Journal* 19, 5 (Oct. 2001), 552–559. https://doi.org/10.1016/S0263-2373(01)00069-X

[76] Amy Ru and Foaad Khosmood. 2020. Hackathons for Workforce Development: A Case Study. In *International Conference on Game Jams, Hackathons and Game Creation Events 2020 (ICGJ20)*. Association for Computing Machinery, New York, NY, USA, 30–33. https://doi.org/10.1145/3409456.3409462

[77] Ryan Hunt. 2012. Thirty-Seven Percent of Companies Use Social Networks to Research Potential Job Candidates, According to New CareerBuilder Survey - Apr 18, 2012. http://press.careerbuilder.com/2012-04-18-Thirty-Seven-Percent-of-Companies-Use-Social-Networks-to-Research-Potential-Job-Candidates-According-to-New-CareerBuilder-Survey

[78] Niharika Sachdeva and Ponnurangam Kumaraguru. 2017. Call for Service: Characterizing and Modeling Police Response to Serviceable Requests on Facebook. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17)*. Association for Computing Machinery, New York, NY, USA, 336–352. https://doi.org/10.1145/2998181.2998292

[79] Matthew J. Salganik and Duncan J. Watts. 2009. Web-Based Experiments for the Study of Collective Social Dynamics in Cultural Markets. *Topics in Cognitive Science* 1, 3 (July 2009), 439–468. https://doi.org/10.1111/j.1756-8765.2009.01030.x

[80] Irving Seidman. 2006. *Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences*. Teachers College Press, New York, NY, USA.

[81] Pnina Shachaf. 2008. Cultural diversity and information and communication technology impacts on global virtual teams: An exploratory study. *Information & Management* 45, 2 (March 2008), 131–142. https://doi.org/10.1016/j.im.2007.12.003

[82] Dan Simon, Minwoo Ahn, Douglas M. Stenstrom, and Stephen J. Read. 2020. The adversarial mindset. *Psychology, Public Policy, and Law* 26, 3 (Aug. 2020), 353–377. https://doi.org/10.1037/law0000226 Publisher: American Psychological Association.

[83] Dan Simon, Doug Stenstrom, and Stephen J. Read. 2009. Adversarial and Non-Adversarial Investigations: An Experiment. *SSRN Electronic Journal* (2009), 23. https://doi.org/10.2139/ssrn.1401723

[84] Kate Starbird and Leysia Palen. 2012. (How) will the revolution be retweeted? information diffusion and the 2011 Egyptian uprising. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work (CSCW '12)*. Association for Computing Machinery, New York, NY, USA, 7–16. https://doi.

org/10.1145/2145204.2145212
[85] Deborah Tatar. 2007. The design tensions framework. *Human–Computer Interaction* 22, 4 (2007), 413–451.
[86] Yla Tausczik and Mark Boons. 2018. Distributed Knowledge in Crowds: Crowd Performance on Hidden Profile Tasks. *Proceedings of the International AAAI Conference on Web and Social Media* 12, 1 (2018), 10.
[87] Yla Tausczik and Ping Wang. 2017. To Share, or Not to Share? Community-Level Collaboration in Open Innovation Contests. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW (Dec. 2017), 100:1–100:23. https://doi.org/10.1145/3134735
[88] The Washington Post 2015. Crowdsourcing may have solved a 20-year-old cold case. *The Washington Post* (2015).
[89] Ramine Tinati, Max Van Kleek, Elena Simperl, Markus Luczak-Rösch, Robert Simpson, and Nigel Shadbolt. 2015. Designing for Citizen Data Analysis: A Cross-Sectional Case Study of a Multi-Domain Citizen Science Platform. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 4069–4078. https://doi.org/10.1145/2702123.2702420
[90] Ma Dolores C. Tongco. 2007. Purposive Sampling as a Tool for Informant Selection. *Ethnobotany Research and Applications* 5, 0 (Dec. 2007), 147–158. http://ethnobotanyjournal.org/index.php/era/article/view/126 Number: 0.
[91] Daniel Trottier. 2017. Digital vigilantism as weaponisation of visibility. *Philosophy and Technology* 30, 1 (2017), 55–72.
[92] Sukrit Venkatagiri, Aakash Gautam, and Kurt Luther. 2021. CrowdSolve: Managing Tensions in an Expert-Led Crowdsourced Investigation. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–30.
[93] Sukrit Venkatagiri, Aakash Gautam, and Kurt Luther. 2021. CrowdSolve: Managing Tensions in an Expert-Led Crowdsourced Investigation. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW1, Article 118 (apr 2021), 30 pages. https://doi.org/10.1145/3449192
[94] Sukrit Venkatagiri, Jacob Thebault-Spieker, Rachel Kohler, John Purviance, Rifat Sabbir Mansur, and Kurt Luther. 2019. GroundTruth: Augmenting Expert Image Geolocation with Crowdsourcing and Shared Representations. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW (Nov. 2019), 107:1–107:30. https://doi.org/10.1145/3359209
[95] Daniel Votipka, Eric Zhang, and Michelle L. Mazurek. 2021. HackEd: A Pedagogical Analysis of Online Vulnerability Discovery Exercises. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 1268–1285. https://doi.org/10.1109/SP40001.2021.00092
[96] Andrea Wiggins and Yurong He. 2016. Community-Based Data Validation Practices in Citizen Science. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work and Social Computing* (San Francisco, California, USA) *(CSCW '16)*. Association for Computing Machinery, New York, NY, USA, 1548–1559. https://doi.org/10.1145/2818048.2820063
[97] Heather J Williams and Ilana Blum. 2018. *Defining second generation open source intelligence (OSINT) for the defense enterprise.* Technical Report. RAND Corporation Santa Monica United States.
[98] Anita Williams Woolley, Christopher F. Chabris, Alex Pentland, Nada Hashmi, and Thomas W. Malone. 2010. Evidence for a Collective Intelligence Factor in the Performance of Human Groups. *Science* 330, 6004 (Oct. 2010), 686–688. https://doi.org/10.1126/science.1193147 Publisher: American Association for the Advancement of Science Section: Report.
[99] Volker Wulf, Kaoru Misaki, Meryem Atam, David Randall, and Markus Rohde. 2013. 'On the ground' in Sidi Bouzid: investigating social media use during the tunisian revolution. In *Proceedings of the 2013 conference on Computer supported cooperative work (CSCW '13)*. Association for Computing Machinery, New York, NY, USA, 1409–1418. https://doi.org/10.1145/2441776.2441935
[100] Elizabeth Yardley, Adam George Thomas Lynes, David Wilson, and Emma Kelly. 2018. What's the deal with 'websleuthing'? News media representations of amateur detectives in networked spaces. *Crime, Media, Culture* 14, 1 (2018), 81–109. https://doi.org/10.1177/1741659016674045
[101] Nick Yee, Nicolas Ducheneaut, and Les Nelson. 2012. Online gaming motivations scale: development and validation. In *Proceedings of the SIGCHI conference on human factors in computing systems*. Association for Computing Machinery, New York, NY, USA, 4.
[102] Lixiu Yu, Paul André, Aniket Kittur, and Robert Kraut. 2014. A comparison of social, learning, and financial strategies on crowd engagement and output quality. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing (CSCW '14)*. Association for Computing Machinery, New York, NY, USA, 967–978. https://doi.org/10.1145/2531602.2531729
[103] Lovro Šubelj, Štefan Furlan, and Marko Bajec. 2011. An expert system for detecting automobile insurance fraud using social network analysis. *Expert Systems with Applications* 38, 1 (Jan. 2011), 1039–1052. https://doi.org/10.1016/j.eswa.2010.07.143