IL WEB DELL'ODIO DECENTRALIZZATO

CHI SOSTIENE LA SUPREMAZIA BIANCA STA INIZIANDO A USARE LA TECNOLOGIA PEER-TO-PEER.

SIAMO PREPARATI?

UN REPORT DI:
EMMI BEVENSEE
&
REBELLIOUS DATA LLC

SETTEMBRE - 2020

Appartengo ad una comunità chiamata Scuttlebutt[1] che usa la tecnologia Peer-to-Peer. Questa è una tecnologia che funziona in modo radicalmente diverso da internet come lo conosciamo ora e offre un'idea potente per un futuro resiliente e sostenibile per la tecnologia e i movimenti sociali. Una sera, una persona che sviluppa per Scuttlebutt e che ha identità emarginate come me, con grande preoccupazione ha mandato un messaggio a me e a poche altre scrivendo:

" Ok - allora abbiamo già dei nazisti che usano scuttlebutt. Quando ci sono state le sparatorie in Nuova Zelanda ho sognato che nel notiziario veniva annunciato che avevano usato un'enclave di scuttlebutt per organizzarsi e radicalizzarsi. Sembra che questo sia inevitabile ... "

È seguita una lunga conversazione sui rischi creati da queste tecnologie radicali. Questa persona era sinceramente spaventata. Lo ero anch'io e lo sono ancora. Come molte altre persone, aveva lavorato sodo per curare sia la comunità che la tecnologia. Aveva paura che il frutto dell'amore di così tante persone sarebbe potuto diventare un aiuto fondamentale nell'organizzazione per la supremazia bianca e che la comunità non fosse pronta ad affrontare le conseguenze di un tale "incubo".

Nella maggior parte delle comunità Peer-to-Peer è impossibile sorvegliare o sapere quante persone le stanno usando perché per loro progettazione sono sicure e spesso private. L'unico modo per dare un'occhiata alle dimensioni di quanto questi stumenti siano utilizzati da chi sostiene la supremazia dei bianchi è quando queste persone scrivono su forum o siti web pubblici. Altrimenti, a

meno che non ci si infiltri nelle loro conversazioni, possiamo solo vedere la punta dell'iceberg della violenza (o del buono!) facilitata da queste tecnologie. Possiamo vedere il post iniziale che incoraggia le persone a passare al servizio di messaggistica criptata P2P, ma non possiamo sapere l'uso che poi ne viene fatto, a meno che le persone antifasciste non si infiltrino e lo denuncino. Possiamo vedere quando le persone ammettono di aver postato i manifesti di un cecchino sostenitore della supremazia bianca su servizi di file hosting resilienti, ma è difficile trovarli e anche se ce ne occupiamo non possiamo rimuoverli ovunque. Possiamo vedere i post che mostrano alle persone come raccogliere efficacemente fondi e comprare kit per la stampa 3d di armi da fuoco o materiali per fabbricare bombe con le criptovalute, ma non possiamo sapere quante persone lo hanno fatto; finché non è troppo tardi.

Molte persone nelle comunità si riconoscono nel fine comune di seminare per un futuro positivo grazie alle tecnologie p2p e contemporaneamente cercano di ridurre i rischi che ci spaventano. Questo documento tenta di coltivare quella speranza e di essere realistico riguardo i rischi in uno spirito di emergenza e di ottimismo[2] per il futuro del web decentralizzato.

RIEPILOGO

Le persone che sostengono la supremazia bianca hanno iniziato a cercare più servizi alternativi online, compresa la tecnologia Peer-to-Peer (P2P), poiché è in atto una crescente pressione per mitigare la rapida crescita dei sostenitori della supremazia bianca che si organizzano via Internet con forme e provider più tradizionali e centralizzate. In questo rapporto descrivo il sistema P2P per un pubblico non del settore, spiego come e perché le persone che sostengono la supremazia bianca lo stanno usando e mostro come possiamo utilizzare i punti di forza dei sistemi P2P per un impatto sociale positivo. I principali sistemi P2P usati dai sostenitori della supremazia bianca sono: archiviazione di file, forum, comunicazione e finanziamento. Le principali minacce dell'uso della tecnologia P2P per diffondere l'odio sono l'organizzazione di violenza basata sull'odio, molestie organizzate o sparpagliate e la facilitazione della diffusione di contenuti di odio dannosi o illegali. Molti nella comunità P2P stanno prendendo provvedimenti per ridurrne il potenziale abuso. La tecnologia P2P offre un incredibile potenziale per la collaborazione umana, ma pone anche alcune sfide che sono intrinseche. Questo articolo pone una domanda critica: come possiamo navigare nel terreno inesplorato della tecnologia P2P senza rinunciare ai suoi potenziali benefici o minimizzare i rischi inerenti?

Affrontare la radicalizzazione sta diventando più difficile. Le grandi piattaforme come YouTube usano algoritmi imperfetti sia per le raccomandazioni che per la moderazione automatica dei contenuti. Ospitano comunità che possono disinformare e radicalizzare[3] persone suggestionabili. La "radicalizzazione" si riferisce

ai canali in cui le persone nel tempo sono esposte a forme più estreme di ideologie e comportamenti razzisti. Gli approcci alla moderazione centralizzati, come una moderazione dall'alto o un team di sicurezza, non funzionano per la tecnologia P2P perché la tecnologia stessa si basa sulla decentralizzazione dell'autorità. Poiché sempre più persone che sostengono la supremazia bianca continuano a migrare verso la tecnologia P2P, aumenta anche il rischio che organizzino la violenza attraverso questi strumenti.

L'odio moderno non è così reattivo alla deterrenza dall'alto. Come altre persone anche chi sostiene la supremazia bianca espande l'uso di tattiche "senza leader", stanno diventando più agili nell'aggirare gli approcci centralizzati per contrastare i loro sforzi, come la politica, la moderazione automatica dei contenuti o gli arresti di aggressori "lupo solitario". La decentralizzazione dei gruppi sostenitori della supremazia bianca è sempre più facilitata da una tecnologia P2P irreprimibile e criptata. Come tale, molti metodi dei tipici sistemi e strutture governative, come la legislazione o la sorveglianza, si stanno dimostrando meno efficaci nel più moderno panorama delle minacce. Solo una rete può sconfiggere[4] una rete.

Stanno emergendo soluzioni decentralizzate. Alcuni strumenti P2P hanno introdotto nuove idee per combattere i contenuti lesivi. Alcune piattaforme hanno chiarito gli accordi con chi le usa e hanno esortato le loro comunità a bloccare il supporto per gli strumenti problematici. Altre piattaforme hanno introdotto "audit sugli abusi" per identificare e mitigare potenziali minacce per le persone. A causa della natura tecnica e sociale dei problemi

che dobbiamo affrontare, anche le nostre soluzioni devono essere ampiamente decentralizzate.

La decentralizzazione aiuta a risolvere molti problemi, ma solleva anche nuove sfide. Le tecnologie P2P possono far progredire molti dei più grandi problemi di coordinamento della società, dai trasporti pubblici e dalle catene di approvvigionamento a una positiva connessione e collaborazione sociale. Tuttavia, le sfide che ci chiedono di affrontare non hanno soluzioni facili.

INDICE

Introduzione

Il boom dei dot-comer dei primi anni novanta ha visto una rapida ed esponenziale esplosione dei tipi di contenuti condivisi. Il social web impersonato dai social media, a cui ci riferiamo come web 2.0, ha visto una rapida espansione d'uso circa un decennio dopo. In entrambi i casi, la proliferazione di contenuti lesivi e persino illegali ha colto gran parte dei progettisti di sorpresa. Questo è in parte dovuto alla mancanza di lungimiranza nella governance degli standard e dei contenuti della rete che potevano evitare che fosse utilizzata per facilitare movimenti d'odio ed estremisti. L'uso del crowdfunding a sostegno della supremazia bianca[5] mette in evidenza le sfide poste dall'infrastruttura social del web 2.0 con cui continuiamo a confrontarci oggi.

Ora siamo diretti verso una nuova era di Internet - il web 3.0[6] - che utilizza una tecnologia più decentralizzata e meno agevolmente controllabile. Mentre chi sostiene la supremazia bianca già raccolglie fondi[7] con le criptovalute, le affordance tecnologiche come l'irreprimibile archiviazione di file Peer-to-Peer (P2P) e la comunicazione criptata, stanno appena iniziando a essere utilizzate per organizzare e propagandare gli attacchi. In particolare, le proposte politiche esistenti che tentano di affrontare i contenuti illegali di odio online avranno poco o nessun potere nell'affrontare gli stessi contenuti su una rete P2P. Diverse volte i sostenitori della supremazia bianca hanno già tentato, utilizzando la tecnologia P2P, di organizzare gli attacchi e la diffusione della violenza suprematista. Tuttavia, le intuizioni che otteniamo e le misure che raccomandiamo in questa prima fase dell'Internet decentralizzato determineranno la misura in cui

saremo in grado di mitigare gli attacchi futuri attraverso l'utilizzo della rete P2P da chi sostiene la supremazia bianca.

Speriamo, anche attraverso questo rapporto, di sottrarci alla curva di odio del web 3.0 e fare luce su questi problemi, riconoscendo e capitalizzando l'incredibile valore offerto dagli strumenti stessi.

Internet centralizzata

È importante capire la quasi onnipresente natura centralizzata della maggior parte della tecnologia online per comprendere l'ascesa e l'attrattiva delle reti P2P decentralizzate. Semplificando, Internet attualmente funziona in questo modo, il tuo computer invia una richiesta di informazioni ad un computer più grande chiamato server che memorizza le informazioni di uno o più siti web. Quel server ti invia il sito web e qualsiasi informazione tu abbia richiesto. Il server memorizza tutte le informazioni di quel sito in un unico posto (più o meno), il che rende più facile per loro rimuovere il contenuto e verificare chi lo usa. D'altra parte, questa centralizzazione della tecnologia centralizza anche il potere.

Che cos'è il P2P?

Capire la tecnologia P2P richiede innanzitutto comprendere la decentralizzazione[8]. Decentralizzare la tecnologia significa cambiare radicalmente[9] il modo in cui funziona distribuendo l'autorità piuttosto che privilegiare una parte del sistema (come i server centralizzati di cui sopra). Decentralizzare significa prendere le parti di un sistema e distribuire la responsabilità, la fiducia e il potere in tutto il sistema invece di concentrare tutto in un'unica parte. Generalmente la decentralizzazione evita singoli punti di errore(SPOF), tipo un server, in modo che anche se un centro di alimentazione venisse attaccato non venga compromesso l'intero sistema. Questo estende la responsabilità della rete a più parti in modo più orizzontale. Per illustrare questo concetto rendendolo più accessibile, possiamo confrontare metodi di amministrazione - una dittatura ricorda l'iper-centralizzazione, mentre un sistema più orizzontale e democratico fatto di consigli di

amministrazione locale assomiglia alla decentralizzazione.

La decentralizzazione della tecnologia, come altri software, generalmente si basa su protocolli che permettono ai sistemi di funzionare. Un protocollo è un insieme di standard che permettono ai computer di eseguire software o comunicare tra loro. Poiché un protocollo, in questo caso, è solo un linguaggio per la comunicazione, qualsiasi cosa può essere compilata per circolare tra i computer in quel linguaggio. La posta elettronica è un esempio di protocollo. Un protocollo decentralizzato è un linguaggio per una tecnologia decentralizzata per eseguire alcune azioni come trasmettere informazioni. Un client è un tipo di interfaccia utente che consente ad un utente di utilizzare un protocollo. Protonmail e Gmail sono esempi di client che utilizzano il protocollo di posta elettronica.

L'importanza della decentralizzazione, dei protocolli e dei client per la tecnologia P2P avrà più senso se si guarda a cosa sia effettivamente la tecnologia P2P. Il sito web Tech Terms[10] definisce P2P dicendo:

In una rete P2P, i "peer" sono sistemi di computer che sono collegati tra loro via Internet. I file possono essere condivisi direttamente tra i sistemi della rete senza la necessità di un server centrale. In altre parole, ogni computer su una rete P2P diventa un file server[11] e un client.

Per accedere a Facebook il tuo computer chiede a Facebook i dati di qualche pagina e loro te li rimandano da un server centralizzato. Su una rete P2P è possibile ospitare e condividere contenuti

direttamente con altri computer. C'è una vasta gamma di tecnologie costruite in questo modo, vanno dai forum P2P alle blockchain di criptovalute. Le comunità di chi sviluppa e usa il P2P comprendono molti movimenti e sistemi d'opinione diversi, dai modelli di economia P2P alle comunità più focalizzate sul web decentralizzato, spesso indicato come il dweb (pronunciato Dee-web)[12]. Il Dweb è sostenuto da chi ha posizioni conservatrici sulla libertà di parola alle comunità con basse spese generali e resilienti che usano la rete P2P con dispositivi comuni attraverso un protocollo condiviso noto come "reti-mesh". Ci sono tensioni non solo a livello di opinione, ma anche di codice, tra la libertà di parola e chi aderisce a dweb impegnati nella rimozione di contenuti dannosi o illegali.

In generale, le tecnologie P2P e decentralizzate tendono anche a essere open-source. Secondo il dictionary.com[13] open source è "relativo o denota un software il cui codice sorgente è disponibile gratuitamente al pubblico per l'uso, la copia, la modifica, la sub-licenza o la distribuzione".

L'esempio più noto di tecnologia decentralizzata P2P e open-source si può trovare nella tecnologia della blockchain e delle criptovalute. Una blockchain[14] è fondamentalmente un libro mastro digitale che tiene traccia di chi ha inviato cosa a chi. Il libro mastro è decentralizzato nel senso che qualsiasi computer pubblico o privato può memorizzare i registri delle transazioni della valuta e può prendere parte al processo di verifica matematica dell'accuratezza delle transazioni, che sono anche disponibili pubblicamente. Le criptovalute sono uniche e si basano sulla

tecnologia decentralizzata perché si fondano su un trust pubblico che è visibile dalle stesse transazioni e prove matematiche archiviate su diversi computer contemporaneamente e disponibili per la revisione da parte di chiunque, ovunque. Le criptovalute sono molto spesso forme di denaro digitale su una blockchain. Non tutti i progetti blockchain riguardano le valute, ma è l'uso più comune. Quindi il protocollo di una data criptovaluta è il modo in cui funziona, mentre il client sarebbe un portafoglio che ti permette di scambiare quella valuta.

La tecnologia P2P e decentralizzata è così popolare che anche una piattaforma di social media mainstream come Twitter sta investendo[15] in un progetto chiamato BlueSky per sviluppare standard di social media decentralizzati e open-source. Nonostante l'utilizzo di infrastrutture centralizzate, Twitter, Facebook e simili non sono stati in grado di arginare completamente l'ondata di contenuti di odio e disinformazione e sembrano guardare alla decentralizzazione come a una possibile soluzione. Non sorprende che con tutta questa popolarità, anche i protagonisti cattivi ne stiano prendendo nota.

Centralizzazione o decentralizzazione?

Il dominio P2P espone tensioni tra diritti opposti. Le reti decentralizzate per rimanere operative hanno una configurazione unica che si basa su più computer/server. Quindi è generalmente tecnologicamente impossibile per un'autorità centrale imporre l'impostazione del discorso e la condotta di chi la usa che si tratti di chi modera il forum, un team per l'applicazione delle politiche della piattaforma, di un host del dominio o delle forze dell'ordine.

Sarah Jamie Lewis di Field Notes in Resistant Tech scrive[16], "la decentralizzazione è il grado in cui un'entità all'interno del sistema può resistere alla coercizione e funzionare ancora come parte del sistema". Definizioni come queste mostrano come le dimensioni politiche del P2P e della decentralizzazione si intreccino con le specifiche tecniche. In confronto, le reti centralizzate non hanno questi limiti dovuto alla centralizzazione della loro infrastruttura, controllo e protocolli.

Da un punto di vista tecnico, si potrebbe sostenere che la totale libertà di parola non richiederebbe alcuna autorità centralizzata che rimuova o moderi i contenuti. Tuttavia, la possibilità di rimuovere contenuti pericolosi o illegali crea probabilmente uno spazio più aperto e inclusivo per individui emarginati che possono percepire che il loro discorso sia smorzato dall'interfacciarsi con minacce odiose. Pertanto, la moderazione potrebbe anche essere considerata centrale per vivere in un mondo libero dalla violenza fondata sull'odio e per promuovere il dialogo.

Le tecnologie P2P possono proteggere il diritto di organizzarsi[17] delle persone emarginate per i loro diritti umani, ma quella stessa tecnologia rende possibile a chi sostiene la supremazia bianca di sfruttare la privacy e i sistemi senza censura per promuovere i loro ideali bigotti e razzisti. La stessa tecnologia che rende la tecnologia P2P resiliente contro i censori, la rende anche resiliente contro cose come i disastri naturali e la scarsa connettività Internet. In paesi dove il governo reprime la condivisione delle informazioni o l'accesso a Internet è bloccato, le tecnologie P2P possono aiutare le persone a connettersi.

La centralizzazione, tipo un server controllato da una società, consente di rimuovere rapidamente i contenuti pericolosi, ma mette nelle mani di pochi privilegiati il controllo di ciò che viene definito "pericoloso".

Il compito importante dell'era P2P è la democratizzazione radicale della responsabilità di mantenere Internet aperta ad argomentazioni problematiche, alla libertà di parola e ai diritti delle persone emarginate alla loto sicurezza online.

Man mano che le tecnologie decentralizzate matureranno, probabilmente occuperanno porzioni sempre maggiori del nostro uso quotidiano di Internet. Pertanto, le tensioni poste dalle scelte dell'architettura tecnologica - come costruiamo un sito Web o un software - riflettono le tensioni delle diverse libertà.

Perché chi sostiene la supremazia bianca sta migrando verso la tecnologia P2P?

I moderni movimenti di chi sostiene la supremazia bianca hanno un flusso internazionale di finanziamenti e supporto materiale da parte di individui, stati e corporazioni[18] . Hanno anche un simile supporto dall'alto verso il basso da personalità[19] e luoghi di rilievo[20]. Contemporaneamente, questi movimenti presentano un sistema di base di auto-organizzazione senza leader e flussi di finanziamento[21]. Questa capacità dal basso di muoversi a frotte[22] e in piccoli gruppi è simile agli ideali di Resistenza senza Leader[23] che molte bande naziste degli anni '80 e '90 hanno integrato[24] dopo

averne visto l'efficacia nei movimenti di sinistra. Questo movimento senza leader si è ulteriormente potenziato via Internet.

Questa struttura di movimenti orizzontali senza leader si adatta perfettamente alla tecnologia P2P, rendendo gli strumenti decentralizzati più attraenti per coloro che sostengono la supremazia bianca e singole persone. È spesso difficile per chi sostiene la supremazia bianca fare rete o creare fiducia perché sono sotto costante sorveglianza da parte di militanti e delle forze dell'ordine e la stragrande maggioranza delle persone è contraria alle loro opinioni. Come tale, la privacy e la capacità di creare fiducia senza esporsi rende utile la tecnologia P2P. Spesso chi sostiene la supremazia bianca affronta una tiritera con ramificazioni legali[25] e sociali[26] come l'arresto e la perdita del lavoro. Questo pone l'intera responsabilità del mantenimento di un'organizzazione in poche mani elette, creando una struttura ad alto rischio, perché se cadono, l'organizzazione cade con loro[27]. Poiché i sistemi P2P in generale non sono troppo centralizzati intorno a sigole persone, la loro struttura risulta più resiliente sia per militanti che per chi sostiene la supremazia bianca, cercando di evitare questi singoli punti di errore (SPOF).

Le tecnologie decentralizzate e open-source giocano un ruolo importante nel mantenere Internet florido. Ma come ogni tecnologia, possono anche essere sfruttate da cattivi personaggi - e impiegate per rendere Internet un posto meno salubre e più pericoloso.

Alcuni esempi di come gruppi negli Stati Uniti stiano usando le

tecnologie P2P per diffondere disinformazione, amplificare i contenuti tossici e incitare alla violenza saranno evidenziati nella prossima sezione. Poiché piattaforme online popolari come Twitter e YouTube hanno iniziato a reprimere chi sosstiene la supremazia bianca in seguito all'attivismo e alla denuncia delle organizzazioni per i diritti civili[27], queste comunità online non è che se ne vanno e basta. C'è stato invece un esodo verso spazi che sono più difficili da controllare e moderare, ma che hanno ancora il potenziale per raggiungere un pubblico di massa. Gli sforzi che sono riusciti a contrastare il terrorismo online della supremazia bianca hanno fatto cose tipo spingere l'organizzazione neonazista American Identity Movement[28], precedentemente conosciuta come "Identity Evropa"[29], a ridurre l'azione e il reclutamento attraverso una serie di denunce e fughe di notizie di conversazioni private, facendo rimuovere chi sostiene la supremazia bianca dalle piattaforme a pagamento[30], respingendo[31] i media e i pubblicitari che traggono profitto dalla supremazia bianca e interrompendo il servizio su 8chan. Tuttavia, con questo cambiamento, chi sostiene la supremazia bianca sta sempre più migrando verso metodi privati, di collaborazione decentralizzata e più a 'prova di censura' come le tecnologie P2P. Nel frattempo è nato del disaccordo su questo metodo nelle comunità P2P poiché alcune persone di primo piano iniziano ad adottare l'ideologia "anti-social justice warrior" nonostante le critiche e gli appelli al dialogo di altre persone nel movimento.

La tecnologia P2P può aiutarci a costruire un mondo migliore, ma è difficile.

I sistemi Peer-to-Peer possono contemporaneamente risolvere una

vasta gamma di problemi di coordinamento e anche diffondere senza sosta contenuti web dannosi. Chi sostiene la supremazia bianca sta già usando molto questi protocolli, ma c'è anche molto lavoro creativo per minimizzare il danno senza dover rinunciare al radicale potenziale di questi sistemi. Poiché il futuro dei movimenti d'odio sembra sempre più decentralizzato, le tattiche anti-odio si devono assestare su questo terreno in rapido cambiamento.

Per questo progetto, ho intervistato 6 esperti, tenuto 4 workshop, partecipato ad altri 3 workshop sull'argomento, ho avuto innumerevoli conversazioni informali con persone impegnate in questo campo e tenuto un processo di revisione aperto a tutta la comunità. Contemporaneamente stavo anche lavorando[32] su questi temi nell'ambito P2P e contro l'odio come Mozilla Open Web Fellow e come Doctoral Fellow[33] al Centre for Analysis of the Radical Right. Inoltre, gestisco una piattaforma open-source di analisi dei social media chiamata SMAT[34] e una società di consulenza di social good data science chiamata Rebellious Data LLC[35]. Questo è uno studio esplorativo che utilizza metodi di ricerca qualitativi ed etnografici incorporati, poiché i metodi quantitativi sono in gran parte ostacolati dalla natura delle tecnologie.

Uso della tecnologia P2P da parte di chi sostiene la supremazia bianca

Ci sono tre aree chiave nelle quali chi sostiene la supremazia bianca sta già utilizzando e sviluppando tecnologie P2P, tuttavia ognuna di queste aree a rischio è bilanciata dai loro potenziali usi positivi.

Archiviazione dati

Strumenti come Inter-Planetary File System[36] e Bitchute sono utilizzati per ospitare contenuti d'odio in modi estremamente difficili da censurare. L'Internet Archive sta lavorando per creare una versione[37] P2P dei sui archivi che a loro volta ospiteranno contenuti di gruppi d'odio. Se la prospettiva di un'archiviazione resiliente di documenti come manifesti e guide al terrorismo spaventa, strumenti come IPFS (InterPlanetary File System) e una versione P2P dell'Internet Archive si adattano anche a essere usati per la conservazione di prove di crimini di guerra o la possibilità di fare attivismo e giornalismo civico in contesti di governi repressivi.

Rob Monster, che si guadagna da vivere[38] proteggendo siti web dell'alt-right (alternative right) come Gab attraverso la sua società Epik[39], ha caricato il manifesto dell'attacco di Christchurch su InterPlanetary File System (IPFS). Allo stesso modo, il neo-Nazi Weev dell'infame DailyStormer ha detto[40] che ora pubblicherà tutti i suoi contenuti scritti e video su IPFS dopo che GoDaddy, Google e Cloudflare hanno rifiutato di sostenere i suoi progetti neonazisti. BitChut è stata ripresa pubblicamente[41] per aver dato ospitalità a una vasta gamma di vlogger (video-blogger) che sostengono la supremazia bianca.

Forum

Sono disparati i vari forum e social media che utilizzano la tecnologia P2P. Il potenziale dei social media P2P è articolato, come lo è per le infrastrutture di comunicazione resilienti di emergenza[42] in aree con bassa penetrazione di Internet. Tuttavia, qualsiasi strumento utilizzato per la connessione, specialmente quelli che sono più privati e sicuri, viene utilizzato in modo fazioso da coloro che sostengono la supremazia bianca e da altre individualità ostili. In questo caso, molti che sostengono la supremazia bianca stanno usando, hanno tentato di usare o stanno sviluppando sistemi di social media P2P.

Dopo che individualità terroriste si sono radicalizzate su 8chan usandolo per promuovere e gamificare[43] sparatorie di massa legate al fanatismo razzista e dopo una campagna contro di loro sostenuta da militanti[44] e con loro dal creatore primo di 8chan, finalmente sono stati abbandonati dai vari provider e trascinati davanti al Congresso[45]. Poiché il servizio veniva abbandonato, cominciò a essere pubblicizzato un clone su un servizio distribuito chiamato ZeroNet. Il vantaggio di Zeronet è che non poteva essere censurato o abbattuto se un servizio di protezione DDoS o un server decideva che 8chan fosse una responsabilità e lo eliminava.. Ron Watkins, il web manager della piattaforma 8chan teorico del fanatismo razzista, ha affermato di non sapere nulla di questo clone, anche se vi aveva creato il suo forum P2P proof-of-concept (PoC)[46]. Questi tipi di metamorfosi come ZeroNet non richiedono un'autorità centrale, così come non rispondono ad esempio ai mandati di comparizione. Anche se non hanno ancora rilasciato tutte le informazioni, Ron Watkins - in cooperazione con

"LimTheNick"[47], Vanwa Tech e Is It Wet Yet - stanno lavorando a qualcosa chiamato "Project Odin"[48] che sostiene di essere una rete P2P Content Delivery Network che potrebbe aiutare a proteggere 8chan e il suo discendente 8kun[49] dalla costante cancellazione di contenuti, pofili o pagine (deplatforming) lasciando che siano le persone ad aiutare ospitando i dati del sito web sui loro computer.

Canali di comunicazione

Inoltre, molti network terroristici di chi sostiene la supremazia bianca[50] si sono spostati verso tecnologie di comunicazione decentralizzate come Riot[51] costruita su Matrix[52](ribattezzate rispettivamente Element e Element Matrix Services) per la capacità di gestire i messaggi diretti in modo criptato. Mentre questa tecnologia fornisce anche infrastrutture fondamentali per gli attivisti dei diritti umani in tutto il globo, è anche usata da chi sostiene la supremazia bianca, come la Feuerkrieg Division[53], che aspirano all'insurrezione armata per la supremazia bianca usando esplosivi e armi da fuoco illegali e prendendo di mira le principali infrastrutture come le reti elettriche. Questa organizzazione nasce successivamente alla loro organizzazione sorella The Base, che si sta rimescolando[54] dopo una serie di arresti e denunce di alto profilo in seguito a vari omicidi correlati[55], progetti di attacchi con ordigni esplosivi e tentativi di omicidio. I loro sforzi includono un tentativo di iniziare una guerra razziale[56] protratta su larga scala, sventata per un pelo da gruppi antifascisti e dall'FBI, e si organizzano[57], in parte, anche su Riot.

Autofinanziamento

Chi sostiene la supremazia bianca e i forum delle community

collegate agli omicidi sta usando[58] criptovalute incentrate sulla privacy per raccogliere fondi non rivelando alle autorità l'identità di chi dona ma anche all'interno delle community stesse. L'anonimato delle criptovalute non è fondamentalmente diverso da quello dei contanti ed è legale finanziare chi è contro la sorveglianza. Tuttavia, il fatto che le persone raccolgono fondi per le organizzazioni terroristiche neo-naziste senza alcuna conoscenza l'uno dell'altro, solleva domande delicate.

Dopo il raduno dei nazionalisti bianchi a Charlottesville, dove è stata uccisa Heather Heyer, un donatore anonimo[59] ha donato 14,88 bitcoin all'infame sostenitore della supremazia bianca, e fondatore del Daily Stormer, Andrew Angli. Questo importo è un'allusione alle 14 lettere della parola white supremacy" e 88 che sta per 'Heil Hitler'. Guardando il valore dei bitcoin, questa donazione vale quasi 300.000 dollari. Un altro dei portafogli di Anglin[60] per Daily Stormer mostra che ha inviato e ricevuto 10 Bitcoin in oltre 1300 transazioni. Analogamente, molti sostenitori della supremazia bianca condividono il link alla propria pagina sul social network Minds[61], che offre micropagamenti decentralizzati integrati. Tutto questo mostra sia la capacità di raccogliere fondi attraverso piccoli pagamenti che di spendere il denaro per fini sconosciuti. Questo non è un evento particolarmente insolito. La maggior parte dei siti web fascisti oramai danno la possibilità di donare in varie criptovalute come Bitcoin o Ethereum, ma anche valute intrinsecamente più anonime come Monero. L'account Twitter @NeonaziWallets[62] traccia il saldo del portafoglio degli account conosciuti, ma la maggior parte di tutto ciò sta accadendo senza che sia possibile rendersene conto.

Cosa si può fare?

L'odio nel dominio P2P è una minaccia enorme, ma affrontarla richiede di estendere le nostre pratiche, menti e codici in modi nuovi.

Alcune delle principali minacce di alto livello dei gruppi d'odio nello spazio P2P sono:

-Organizzare la violenza basata sull'odio

-Molestie organizzate o sparpagliate

-Facilitare la diffusione di contenuti dannosi o illegali legati all'odio

Etica in ambito P2P

C'è una versione della Legge di Conway[63] che suggerisce che gli strumenti che sviluppiamo riflettano i nostri valori e stili di comunicazione nelle organizzazioni in cui lavoriamo. Nella codifica, una "affordance" è il modo in cui il software viene usato indipendentemente da come è destinato ad essere usato. La nostra tolleranza per certe affordance a livello di codice è un riflesso dei nostri valori nel processo. La diversità dei valori etici e politici, così come le motivazioni ideologiche, nello spazio P2P hanno un impatto sui tipi di strumenti che vengono sviluppati e su come vengono implementati. Ciò che viene costruito e come, è influenzato dal fatto che i suoi progettisti pensano che il bene potenziale di uno strumento sia controbilanciato dai suoi rischi potenziali come l'uso da parte dei sostenitori della supremazia bianca.

Per molti nello spazio P2P, in particolare quelli influenzati da

ideologie politiche come il tecno-liberismo, un credo in una combinazione di libertà massimizzata attraverso il libero mercato e la tecnologia, la possibilità di un uso malevolo dei loro strumenti è intesa come un rischio necessario per promuovere obiettivi come la libertà di parola e limitare l'eccesso di potere statale. Per quelli nello spazio P2P più influenzati dalle ideologie di sinistra e di giustizia sociale, le opportunità come l'uso di una tecnologia da parte dei sostenitori della supremazia bianca sono qualcosa da contrastare il più possibile, pur cercando di sfruttare il potenziale dello strumento. Inoltre, c'è una sub-popolazione di persone nello spazio di sviluppo del P2P che si identificano con le ideologie della supremazia bianca, anche se possono assumere la maschera di altre ideologie politiche o "dogwhistle" (dissimulate).

Ci sono anche quelli nello spazio P2P che sono spinti non tanto dall'ideologia politica o morale quanto dalla curiosità delle possibilità tecniche e matematiche. Per questo gruppo, argomenti come dimostrazione a conoscenza zero[64] - un sistema matematico e tecnico che può provare che una transazione è avvenuta senza rivelare informazioni su nessuna delle parti - sono interessanti di per sé, per il loro ruolo, in cose come la crittografia e le transazioni sicure. Questo gruppo è meno preoccupato del fatto che un dato gruppo, odioso o meno, usi i suoi strumenti ma piuttosto che possa far progredire la tecnologia e la teoria.

A seconda dei valori di una persona nel costruire o utilizzare la tecnologia P2P, lo strumento può rappresentare possibilità molto diverse. Uno sviluppatore di un progetto P2P chiamato Secure Scuttlebutt ha menzionato un esempio di questa tensione nella

comunità quando ha discusso "se i livelli più bassi del codice e dei protocolli debbano essere influenzati da preoccupazioni umane o se debbano essere 'neutrali'". Lui, e chi ha più interesse nelle implicazioni sociali e ai contesti di queste tecnologie, tende a vedere la tecnologia come intrinsecamente politica per i modi in cui interagisce ed è formata dai pregiudizi della politica in generale. Chi si concentra su preoccupazioni puramente tecniche o ideali tecno-libertari nello spazio delle criptovalute, tendono a sottolineare l'importanza della "neutralità" a livello di codice come una forma di purezza P2P. Se si pensa che il codice possa essere neutrale o meno, si influenza le affordance considerate accettabili nella tecnologia sviluppata.

Le persone guidate da ideologie di destra nello spazio P2P tendono a concentrarsi maggiormente su cose come le criptovalute e strumenti di libertà di parola estremamente incentrati sulla privacy, che hanno maggiori probabilità[65] di essere abusati da gruppi di odio, indipendentemente dall'intenzione di chi sviluppa. Ci sono potenti implicazioni positive sia negli strumenti di privacy P2P che nelle criptovalute, tuttavia è importante riconoscere questo potenziale insieme alle loro possibilità intrinseche.

Chi si concentra maggiormente sulla tecnologia liberatoria influenzata dalla giustizia sociale tende a concentrarsi maggiormente sulla tecnologia P2P orientata a connettere le persone cercando di costruire più protezioni per proteggere dagli abusi. A causa dell'enfasi sulla "neutralità" in gran parte dello spazio blockchain, tendono ad esserci persone più liberali o orientate alla giustizia sociale che gravitano verso i progetti non

strettamente basati sulla blockchain come SSB[66], il protocollo Hypercore (ex Dat)[67] o Holochain[68]. Questi sistemi sono fondamentalmente diversi dai progetti blockchain perché si affidano al potere delle reti di persone umane per definire cosa fa il protocollo piuttosto che affidarsi alla sola matematica.

La realtà di queste comunità, però, è che molte ideologie e motivazioni si sovrappongono e la maggior parte delle persone con cui ho parlato hanno opinioni diverse e complesse su una serie di questi problemi. Le tensioni a livello di codice sono incorporate nel contesto sociale che le crea. La libertà di parola rappresentata da un protocollo P2P non censurabile interagisce con la libertà di non sperimentare la violenza razzista organizzata attraverso lo stesso protocollo. Perciò è importante indagare come alcuni attori stiano respingendo l'odio in uno spazio tecnologico che è, per progettazione, difficile da censurare.

Il curioso caso di SSB

Secure-Scuttlebutt (SSB) è un protocollo P2P che aiuta i dispositivi a comunicare ma non dice loro di cosa parlare. Questo significa che sopra ci si può costruire qualsiasi cosa, da un forum a un gioco degli scacchi[69]. Gran parte della comunità per la salvaguardia delle sementi ('seeds issue') della rete SSB è influenzata da ideologie solarpunk e "walkaway" romanzo di C. Doctorow[70] sulla tecnologia sostenibile ed equa. Una parte consistente della comunità spera nei modi in cui SSB può aiutare come ad esempio per la connettività rurale nella giungla amazzonica, aiutando il coordinamento in mezzo ai disastri naturali e fornendo il controllo autonomo delle infrastrutture di comunicazione a comunità

altrimenti emarginate. Tuttavia, secondo le mie interviste, ci sono già molti problemi come la presenza di alcune persone neo-naziste nonostante l'impegno contro di loro. Diverse persone che sviluppano, con cui ho parlato, sono anche preoccupate che se la piattaforma divenisse ampiamente utilizzata, come c'è chi lo spera, porterebbe una marea di individui che tentano di organizzare campagne di terrore o molestie. Per mitigare questo hanno tentato una serie di diverse strategie:

Diversificare le conversazioni: Chi principalmente sviluppa riconosce il bisogno di intuizioni politiche e sociali nel processo di sviluppo. Per queste ragioni hanno fatto degli sforzi per portare avanti conversazioni su cosa viene fatto e come all'interno di diversi gruppi di persone e voci.

Comunità come immunità: Visto il modo in cui funziona SSB, la moderazione e ciò che viene amplificato è deciso dalla fiducia e da quanto si è connessi alla rete, piuttosto che da un algoritmo ottimizzato per il coinvolgimento come su Twitter o Youtube. Affinché un messaggio si diffonda nella rete, la persona deve essere fidata. Secondo lo sviluppatore André Staltz[71], questo la rende meno attraente per chi cerca di amplificare l'odio o la disinformazione. Inoltre, quando si blocca una persona, oltre a rifiutare di propagare i suoi messaggi, il blocco è pubblico, quindi invia un segnale che questa persona non è degna di fiducia per alcuni aspetti. In questo senso, SSB si basa in qualche misura sulle reti di reputazione[72] per isolare le persone malintenzionate.

Abuse Audit: Il canale #abuse-audit e i processi che lo

accompagnano sono stati un tentativo di mappare i possibili vettori di abuso nella rete. Usando i risultati collettivi di questo processo, sono state sviluppate strategie di mitigazione per una serie di scenari.

L'approccio Planetary: Planetary[73] è un client iOS costruito utilizzando il protocollo SSB ed è orientato verso l'adozione di massa. Planetary ha fatto uso di un controverso Capitale di Rischio/Venture Capital nel tentativo in buona fede di costruire un client ampiamente accessibile che affronta anche alcuni dei pericoli della tecnologia P2P attraverso decisioni a livello di come funziona il codice. C'è preoccupazione per l'uso di Venture Capital da parte di Planetary perchè potrà fornire un incentivo per una pericolosa adozione di massa, mentre altri sostengono che fornirà i fondi necessari per creare una sana mitigazione e strutture di conformità.

Scelte estetiche e segnalazione: SSB non si è mai pubblicizzata come una piattaforma per la libera espressione, sebbene abbia molte di queste qualità a livello tecnico. Inoltre la scelta di design è stata quella di perseguire una serie di opzioni estetiche volte ad attrarre o respingere certi tipi di persone. Per esempio, i client e la pagina web ufficiale spesso usano colori pastello, sulla homepage c'è un cartone animato di una storia d'amore interrazziale queer che spiega come funziona scuttlebutt, e molti client hanno implementato avvisi sui contenuti. Nelle interviste si spiega che questo è del tutto intenzionale al fine di allontanare le persone razziste.

Gab vs Mastodon

Gab è propagandato come una "piattaforma per la libertà di parola", ma è diventato rapidamente[74] uno spazio per la white-supremacist-echo-chamber. Quando Gab ha iniziato ad essere oscurato da vari provider, compresi gli app store di Apple e Google, hanno deciso di cambiare la loro struttura per diventare un'istanza di Mastodon, che è una forma più decentralizzata di server federati. Una federazione di server significa che puoi ricompilare il tuo server e la tua comunità nel modo che vuoi e permettergli di comunicare con altri server attraverso il protocollo Mastodon. Quando Gab ha tentato questo passaggio a Mastodon ha incontrato molte forme di resistenza[75] da gran parte della comunità Mastodon (alcune forme più efficaci di altre). Il team di sviluppo di Mastodon ha rilasciato una dichiarazione che dice:

"Mastodon si oppone completamente al progetto e alla filosofia di Gab, che cerca di monettizzare e di diffondere contenuti razzisti nascondendosi dietro la bandiera della libertà di parola. Mastodon rimane impegnata a lottare contro i discorsi razzisti; per esempio, il nostro nuovo patto tra server significa che elenchiamo su joinmastodon.org solo i server che sono impegnati a una moderazione attiva contro il razzismo, il sessismo e la transfobia. La comunità Mastodon non approva il loro tentativo di dirottare la nostra infrastruttura e ha già preso provvedimenti per isolare Gab e tenere il linguaggio razzista fuori dal fediverso".

Hanno incoraggiato tutte le istanze Mastodon a bloccare la federazione con Gab e hanno codificato i blocchi di Gab in molte delle applicazioni. Questo ha funzionato in una certa misura. Gab è ancora vivo ma è in gran parte isolato. Mentre è in gran parte impossibile bloccare l'uso improprio nei punti di

decentralizzazione, molte organizzazioni hanno perseguito deterrenti nei punti di centralizzazione come i loro normali siti web, client e portali principali.

Le prove di Ethereum

Ethereum[76] è una "piattaforma globale, open-source per applicazioni decentralizzate". Si tratta di una blockchain e di un protocollo di criptovaluta attraverso il quale è possibile costruire tutti i tipi di valute, applicazioni e anche Organizzazioni autonome decentralizzate (DAO)[77]. Uno dei fondatori di Ethereum, Vinay Gupta ha parlato pubblicamente contro il nazionalismo bianco e l'alt-right nello spazio P2P incoraggiando le persone a non dare[78] "nemmeno un centesimo" e a non sostenere i loro progetti. Successivamente è stato attaccato dal blogger neo-nazista Andrew Anglin. In risposta, Gupta ha twittato:

"Dovresti sganciarti. Non saremo buoni padroni di casa.... Combatteremo contro di voi. Renderemo le vostre vite miserabili. Troveremo... modi subdoli ma etici per far fallire il vostro progetto... In ogni caso, mettete il lavoro di tutta la vostra vita nelle mani di persone che vi odiano... Noi facciamo infrastrutture. Voi dipendete da noi".

In una certa misura, la dichiarazione di Gupta è un bluff ambizioso perché c'è poco che Ethereum possa fare per impedire ai neo-nazisti di usare la loro tecnologia. Siti web come Fascist Forge[79] hanno pulsanti di donazione Ethereum e buona parte della comunità delle criptovalute ha preso le parti del Daily Stormer in questo dibattito[80]. Tuttavia, è fondamentale che uno dei più importanti progetti blockchain abbia preso una posizione veemente e pubblica contro chi sostiene la supremazia bianca

quando spesso si fanno semplicemente spallucce e si ignora il problema.

TrustNet

TrustNet è un nuovo ed eccitante sistema[81] sviluppato da Alexander Cobleigh progettato per essere una formalizzazione Peer-2-Peer della moderazione soggettiva attraverso reti di fiducia. Il sistema è stato proposto nella sua tesi per il Master recentemente pubblicata, che descrive anche la moderazione soggettiva. La moderazione soggettiva in questo caso è il concetto che ogni partecipante alla chat può designare soggettivamente di chi si fida per moderare il contenuto per suo conto, delegando così il potere di nascondere l'abuso e bloccare i troll.

Egli descrive TrustNet come: un sistema per interagire con e gestire la fiducia. Alla base del sistema c'è un algoritmo di fiducia transitiva. Il sistema nel suo complesso è stato originariamente pensato per l'uso in combinazione con sistemi di chat peer-to-peer distribuiti, dove i peer assegnano la fiducia (un valore tra 0,0 e 1,0; 1,0 è la fiducia completa, 0,0 la completa assenza di fiducia) ad altri peer.

Egli sprona l'assegnazione della fiducia attraverso etichette significative per le persone, come l'uso dell'etichetta amico per rappresentare il valore di fiducia 0,75. TrustNet utilizza l'algoritmo Appleseed per tracciare il grafico della fiducia, utilizzando la fiducia transitiva, al fine di calcolare una classifica di assegnazione soggetiva di fiducia tra chi partecipa. Questa classifica viene poi raffinata utilizzando una tecnica di clustering, ottenendo un

gruppo dei peer più affidabili.

Il risultato di tutto questo è che il sistema può essere usato per fare cose come suggerire nuovi amici o anche moderare contenuti discutibili. Poiché TrustNet lavora in modo transitorio attraverso i peer, si può anche dire che aiuta a diffondere la fiducia attraverso una rete. Questo processo funziona in modo simile a tecnologie come Scuttlebutt e quindi funziona bene con sistemi di chat P2P progettati in modo simile.

La questione scalare

I molti tentativi e le difficoltà di coloro che lavorano per la giustizia sociale attraverso la tecnologia P2P ci danno un'idea di come possiamo utilizzare questi strumenti per costruire un mondo migliore e di cosa potrebbe ostacolare il cammino. Ma P2P significa anche avvicinare la tecnologia al comportamento umano, il che ci chiede di rispondere a più fondamentali domande su cosa vogliamo dal social networking, cosa è possibile e, soprattutto, come interagisce con il mondo reale.

Le strutture di governance della comunità sono una parte fondamentale di qualsiasi approccio di gestione dei beni comuni[82] e questo vale anche per Internet. Questo è il motivo per cui alcuni sviluppatori P2P come Dario Kazemi[83] incoraggiano le persone a costruire in piccolo, piuttosto delle dimensioni di larga scala incoraggiata dalla Silicon Valley. Robert Caplan di Data & Society sottolinea tre diversi approcci alla moderazione:

-Artigianale: Un piccolo team di moderatori di solito in-house

-Affidato alla comunità: Modelli come Mastodon, Wikipedia o

Reddit che permettono alle comunità di auto-monitorare i contenuti dannosi con autorità locali di fiducia
-Industriale: Questo di solito comporta sia l'apprendimento automatico (machine-learning) che l'esternalizzazione[84] della visione dei contenuti dannosi a persone emarginate.
Altri approcci correlati sono i filtri locali come la "glasses moderation"/"occhiali da moderatore"[85] in cui si decice individualmente quali tipi di contenuto si vorrebbe filtrare personalmente. Esempi non-P2P di questo includono l'Opt-Out[86] che filtra la misoginia con il componente aggiuntivo del browser.

Ad ogni nuovo livello di scala, una comunità deve utilizzare misure generali di accettabilità e metodi di applicazione sempre più difficili e politicamente complicati. Questo è il motivo per cui gran parte di come la riduzione del danno via P2P si basa effettivamente su soluzioni più umane a problemi tecnici piuttosto che soluzioni semplici, dall'apprendimento automatico o simili, che presentano molte insidie.

Soluzioni sociali a problemi sociali

La tecnologia P2P, come la società nel suo complesso, ha tensioni di base tra la fiducia che diamo a un ente centralizzato - la Modalità Autorità - e la fiducia che diamo agli altri, che potrebbe essere chiamata Modalità Libertà. La Modalità Autorità in qualche modo è più facile e conveniente perché un individuo non ha bisogno di pensare tanto per assicurarsi il proprio benessere e quello della sua comunità. Tuttavia, come dimostrato dalle principali piattaforme di social media, anche la centralizzazione totale non è una garanzia della capacità di eseguire un'efficace moderazione dei contenuti su larga scala. La Modalità Libertà è molto più difficile perché ci chiede di assumerci la responsabilità del nostro ambiente, ma può essere più democratica e più liberatoria in definitiva. La tecnologia P2P sta introducendo paradigmi di scelta molto più significativi e come tale inquadra in modo unico questa relazione tra libertà e responsabilità. Così, quando l'odio comincia a spuntare fuori da una tecnologia che potrebbe dare a tutti noi più libertà, come reagiamo? Questi problemi si dispiegano simultaneamente a livello di scelte individuali e politiche.

La legislazione ha una capacità estremamente limitata di reprimere la proliferazione della tecnologia decentralizzata, come si è visto con il fallimento[87] delle leggi anti-torrenting progettate per frenare la pirateria online. Come con le armi stampate in 3d[88], chiunque può postare il codice ovunque e poi chiunque può scaricarlo. È impossibile reprimere completamente questa tecnologia a meno che non si elimini l'intera Internet o la si accentri ulteriormente al di là di quanto previsto dalla Cina[89] o

dalla Russia[99]. I limiti delle soluzioni tecniche e legislative implicano la necessaria sovrapposizione di approcci multipli per mitigare la violenza basata sull'odio in senso più ampio. In quanto tale, dobbiamo lavorare per allineare le tecnologie P2P con i valori sociali il più possibile e prepararci nel frattempo a conseguenze negative non volute.

Le profonde e pervasive radici del razzismo e della violenza strutturale contro le minoranze influenzano il percorso e le probabili strade di ogni nuova tecnologia. Dato che ideologie come il razzismo strutturale e la supremazia bianca esistono già nel mondo, le tecnologie P2P possono accelerare il coordinamento pro-sociale anti-razzista o l'odio stesso a seconda dei modi in cui scegliamo di impegnarci a vari livelli. I sistemi P2P riproducono le situazioni di come combattiamo il razzismo e l'intolleranza nel mondo reale. Poiché le tecnologie P2P si affidano al potere delle reti come fanno le comunità umane fisiche, non possiamo semplicemente programmare regole rigide in questo genere di tecnologia. Questi approcci umani per affrontare i problemi tecnici sono molto più difficili, ma sono anche più sostenibili nel lungo periodo.

La domanda su come possiamo costruire strumenti che aiutino la tecnologia sociale esistente per massimizzare la cooperazione positiva senza scatenare conseguenze pericolose, come il terrorismo nazista in espansione, è una questione critica del nostro tempo. Rabble, di Planetary, si riferisce a questi problemi quando dice:

"La mia speranza è che possiamo costruire un livello sociale che ci permetta

di costruire un intero mondo dove non abbiamo bisogno di permessi per partecipare o organizzare e creare spazi che incoraggino un comportamento prosociale egualitario e umanitario. Il web fa un sacco in questo campo e anche i social media. Abbiamo ancora molta strada da fare. Se avremo successo [nell'usare la tecnologia P2P per questo] avremo nuovi problemi da affrontare".

Il futuro della tecnologia P2P è già alle porte e lo sviluppo è tale che continuerà ad espandersi e a raggiungere un'adozione più diffusa nei prossimi anni. Perciò affrontare queste domande seriamente, apertamente e precocemente è fondamentale per capire dove ci porterà la tecnologia.

Il corso del P2P nel suo complesso dipende in gran parte dal tipo di comunità che vi accorrono e investono tempo ed energia in questi primi giorni. Perciò, è essenziale che coloro che investono nel sevizio, nella prosperità multiculturale e nell'evoluzione della società guidino la carica in questo nuovo ambito. Lo spazio P2P spalanca questo nido intimo e spinoso di domande e ci chiede di crescere collettivamente per affrontare la prossima era di sfide. Se riusciamo a guidarla per il bene, ci aspetta un futuro più complesso, interconnesso e significativo.

A proposito dell'autrice:

Emmi Bevensee è una Mozilla Open Web Fellow, tra le altre cose ha fondato il Social Media Analysis Toolkit (SMAT)[91] e Rebellious Data LLC. è anche Doctoral Fellow[92] presso il Center for Analysis of the Radical Right. Ha ricevuto un M.A. in Conflict Transformation and Peace building con un'enfasi sulla decentralizzazione della governance nelle zone di conflitto e ha studiato Machine Learning nel programma di dottorato iSchool all'Università di Arizona.

Note

1 https://scuttlebutt.nz/

2 https://newdesigncongress.org/en/pub/this-is-fine

3 https://arxiv.org/abs/1908.08313

4 https://www.latimes.com/archives/la-xpm-2002-aug-25-op-arquilla25-story.html

5 https://www.adl.org/resources/reports/funding-hate-how-white-supremacists-raise-their-money#the-new-kid-on-the-block-crowdfunding

6 https://www.forbes.com/sites/juttasteiner/2018/10/26/what-the-heck-is-web-3-0-anyway/#41716356661 4

7 https://www.adl.org/resources/reports/funding-hate-how-white-supremacists-raise-their-money#bitcoin-and-cryptocurrencies

8 https://fieldnotes.resistant.tech/what-is-decentralization/

9 https://hacks.mozilla.org/2018/07/introducing-the-d-web/

10 https://techterms.com/definition/p2p

11 https://techterms.com/definition/server

12 https://hacks.mozilla.org/2018/07/introducing-the-d-web

13 https://www.dictionary.com/browse/open--source

14https://blog.mozilla.org/firefox/what-is-cryptocurrency/

15 https://twitter.com/jack/status/1204766078468911106

16https://fieldnotes.resistant.tech/what-is-decentralization/

17https://viewer.scuttlebot.i/%25Uh6Qk%2F9ncyKFJWJXDOeLSU1CLIagXc%2BANyT999Ol5dw%3D.sha256

18

https://www.bellingcat.com/news/uk-and-europe/2019/09/03/lega-nords-bedfellows-russians-offering-illicit-funding-to-italian-far-right-party-identified/

19

https://www.splcenter.org/hatewatch/2019/11/12/stephen-millers-affinity-white-nationalism-revealed-leaked-emails

20

https://www.buzzfeednews.com/article/josephbernstein/heres-how-breitbart-and-milo-smuggled-white-nationalism

21

https://www.adl.org/resources/reports/funding-hate-how-white-supremacists-raise-their-money#organizational-funding

22

https://networkcontagion.us/reports/cyber-swarming-memetic-warfare-and-viral-insurgency-how-domestic-militants-organize-on-memes-to-incite-violent-insurrection-and-terror-against-government-and-law-enforcement/

23 https://www.theatlantic.com/ideas/archive/2019/08/the-new-strategy-of-violent-white-supremacy/595648/

24 https://twitter.com/Jake_Hanrahan/status/1235618057202135040

25 https://www.adl.org/resources/backgrounders/atomwaffen-division-awd-national-socialist-order-nso

26

https://www.washingtonpost.com/news/the-intersect/wp/2017/08/14/a-twitter-campaign-is-outing-people-who-marched-with-white-nationalists-in-charlottesville/

27 https://twitter.com/slpng_giants - https://twitter.com/UR_Ninja

28 https://unicornriot.ninja/2019/neo-nazi-hipsters-identity-evropa-exposed-in-discord-chat-leak/

29 https://www.adl.org/resources/profiles/identity-evropaamerican-identity-movement

30 https://www.buzzfeednews.com/article/blakemontgomery/the-alt-right-has-a-payment-processor-problem

31 https://twitter.com/slpng_giants

32 https://rebelliousdata.com/

33 https://www.radicalrightanalysis.com/people/emmi-bevensee/?team_cpt=IMT_PAGE_TEMPLATE

34

https://www.smat-app.com/timeline?searchTerm=qanon&startDate=2020-11-28&endDate=2021-05-28&websites=reddit&aggRedditBy=author&numberOf=10&interval=day&limit=1000&changepoint=false

35 https://rebelliousdata.com/

36 https://ipfs.io/

37

https://www.bleepingcomputer.com/news/technology/archiveorg-has-created-a-decentralized-or-dweb-version-of-their-site/

38 https://www.splcenter.org/hatewatch/2019/01/11/problem-epik-proportions

39 https://www.govtech.com/security/why-the-next-terror-manifesto-could-be-even-harder-to-track.html

40 https://www.vice.com/en/article/43bnzd/neo-nazis-propaganda-decentralized-weev

41 https://www.dailydot.com/upstream/bitchute/

42 https://github.com/libremesh

43

https://www.bellingcat.com/news/americas/2019/08/04/the-el-paso-shooting-and-the-gamification-of-terror/

44 https://www.wsj.com/articles/notorious-8chan-forum-is-an-internet-nomad-11573909201

45 https://time.com/5645945/8chan-testify-congress-el-paso-shooting/

46 https://twitter.com/CodeMonkeyZ/status/1072513133598658560

47 https://twitter.com/LimTheNick

48 https://web.archive.org/web/20191103022706/isitwetyet.com/odin/

49 https://isitwetyet.com/8kun/

50 https://discordleaks.unicornriot.ninja/discord/search?q=riot.im&s=

51 https://element.io/

52 https://matrix.org/

53 https://archive.vn/mgBeL

54

https://www.theguardian.com/world/2020/jan/23/revealed-the-true-identity-of-the-leader-of-americas-neo-nazi-terror-group

55 https://www.huffpost.com/entry/atomwaffen-nazi-murder-bomb-plot_n_5a70825ae4b00d0de2240328

56 https://www.huffpost.com/entry/neo-nazis-virginia-gun-rally_n_5e221a24c5b63211761391ad

57 https://www.thedailybeast.com/why-arrest-of-richard-tobin-is-bad-news-for-neo-nazi-group-the-base

58 https://www.ironmarch.exposed/search?q=bitcoin

59 https://www.huffpost.com/entry/andrew-anglin-bitcoin-mysterious-donor_n_5d011cc6e4b0304a12087e0c

60 https://www.blockchain.com/btc/address/18gr2E6ubUdksNiaEGrNUD3e5FF8vxXaMf

51 https://www.wired.com/story/minds-anti-facebook/

62 https://twitter.com/NeonaziWallets

63 https://it.wikipedia.org/wiki/Legge_di_Conway

64 https://it.wikipedia.org/wiki/Dimostrazione_a_conoscenza_zero

65 https://www.dailydot.com/upstream/bitchute-decentralization-claims/

66 https://scuttlebutt.nz/

67 https://blog.datproject.org/2020/05/15/dat-protocol-renamed-hypercore-protocol/

68 https://holochain.org/

69 https://github.com/Happy0/ssb-chess

70 https://en.wikipedia.org/wiki/Walkaway_(Doctorow_novel)

71 https://staltz.com/

72 https://c4ss.org/content/52196

73 https://www.planetary.social/

74 https://arxiv.org/abs/1802.05287

75

https://www.theverge.com/2019/7/12/20691957/mastodon-decentralized-social-network-gab-migration-fediverse-app-blocking

76 https://ethereum.org/en/

77 https://blockchainhub.net/dao-decentralized-autonomous-organization/

78 https://twitter.com/leashless/status/937480981375746048

79 https://www.adl.org/blog/fascist-forge-a-new-forum-for-hate

80

https://cryptonewsmonitor.com/2017/11/15/uproar-as-ethereums-vinay-gupta-threatens-to-censor-twitter-clone-gab-calls-them-nazis-comes-out-as-communist/

81 https://cblgh.org/articles/trustnet.html

82 https://c4ss.org/content/23644

83 https://runyourown.social/

84 https://www.wired.com/2014/10/content-moderation/

85 https://news.ycombinator.com/item?id=19647692

86 https://github.com/opt-out-tools/opt-out]

87 https://torrentfreak.com/online-piracy-is-more-popular-than-ever-research-suggests-180321/

88 https://www.vox.com/2018/7/31/17634558/3d-printed-guns-trump-cody-wilson-defcad

89 https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

90 https://www.wired.com/story/russia-internet-disconnect-what-happens/

91

https://www.smat-app.com/timeline?searchTerm=qanon&startDate=2020-12-06&endDate=2021-06-06&websites=reddit&aggRedditBy=author&numberOf=10&interval=day&limit=1000&changepoint=false

92

https://www.radicalrightanalysis.com/people/emmi-bevensee/?team_cpt=IMT_PAGE_TEMPLATE

Tradotto e impaginato a Luglio 2021 da:
-Distrozione DIY Label
*-La_r*_go*
-Icchevoi
per info e contatti:
www.autistici.org/distrozione
distrozione@autoproduzioni.net