The Troller Report: A Discursive Observational Study into Troll Groups

(2019) Cody Webb & Nicole Martin
Contact: The_Troller_Report@protonmail.com

Abstract

This literature examines the structure and strategy of an extremist alt right online troll farm covering recruitment, radicalization, indoctrination, sociology and behavior and the similarity these type groups share with cyber terrorist.

The primary strategies employed by the in-group that will be examined are the Social Identity model of Deindividuation Effects (SIDE) and the Deindividuation Theory (DT).

This paper seeks to demonstrate how the operations are effective and what can be done to combat them, by defining a framework to understand the intergroup biases between the online extremist ideologies and how they can be leveraged to provide an exit path.

We will also discuss possible paths of solution to monitor abusive users and to combat coordinated harassment campaigns by different methods of self-moderation and platform changes.

Participants and Procedures

Twitter was the platform observed in the study. 326 million people use the platform each month and Twitter processes over 500 million tweets per day. Twitter is the number one platform of government leaders and organizations as it has the ability to reach the widest audience in the information space.

The in- group consisted of approximately 20 primary, radicalized, internet trolls. Due to the anonymous nature of the platform and its users, there is no real method for qualifying their makeup, however, given personas, linguistics and certain other characteristics, suppositions were made regarding their makeup.

The in-group appeared to be made up of ages ranging from 20's to 50's, comprised of both males and females, residing in the following countries: The United States, England, Australia and Germany. Personas were adopted by the test group throughout identifying as: Jewish, to push an anti-Zionist narrative, African American, to support hate speech by the group, Incel (Involuntary Celibate), to glorify mass shooting violence, rape culture and misogyny, Progressive Satirists, to mask neo-Nazi dog whistles, neo Confederates, to mask racism with patriotism.

Within the test subject group, there were clearly delineated roles and tasks that became readily apparent fairly early on in observations.

- Social engineers
- Planted targets
- De-anonymizers
- Disinformation
- Infiltrators
- Archivists
- Memetic propaganda
- Provocateurs
- Identity personas to appear "deradicalized" eg. Jewish, Lesbian, Black, etc.

The control group consisted of 2 teams of roughly 25 trolls each. While they were primarily partitioned there was cross-pollination using key members of the team. The Tuckman forming–storming–norming–performing model of group development was used in developing two primary counter trolling hubs. Training and educating the counter subject group in the alt

right lexicon, forms of extremism, memetic warfare, identity politics and how to control the narrative when engaging was ongoing.

As abilities and aptitudes became more apparent, some members took on other more defined roles

- Data collection
- Social engineers
- Publicists
- Planted targets
- Infiltrators
- Researchers
- Archivists
- Agit prop
- Provocateurs

One thing became very apparent in this closed model, the narcissistic, outspoken personality type that is strongly associated with individual trolls becomes synergized in a closed group setting. Subversion quickly led to various trolls in the closed group to entrench and subvert others plans from collected intel if they had minor disagreements with the other participants.

We identified this effect would likely happen with the use of analytics and incorporated it into part of our study to identify how information propagated into and out of the closed group and quickly identified sympathizers and infiltrators working for the far-right trolling/harassment campaigns. We also implemented this strategy to determine the opposite as well and used the attrition of the group to identify the provocateurs.

Deindividuation Of The In-Group

We will discuss The Social Identity Model of deindividuation effects and deindividuation theory and how anonymity within the in-group is leveraged with manipulative psychology in-group to indoctrinate into the in-group and also how they use this tactic to discourage dissent and leverage personal attacks against their perceived out-group enemies.

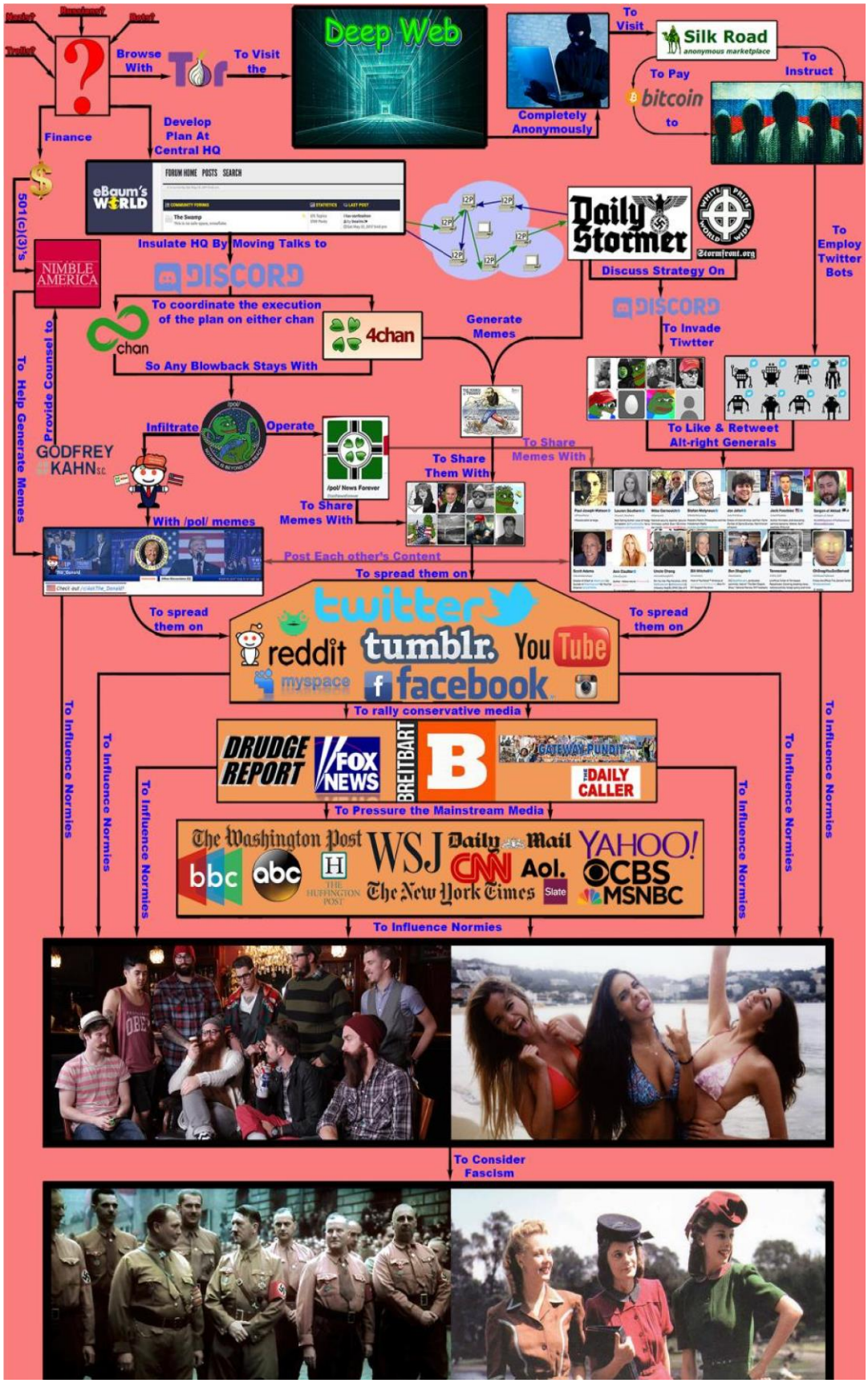
Deindividuation as defined by Festinger, Pepitone, and Newcomb (1952) describes the effect of a group on the behavior of an individual; as a result of that, the individual sheds normally accepted behavior for behaviors socially accepted in the group. The individual loses their sense of self identity and in the process, they act more aggressively in the group setting. This is especially persistent in an anonymous online group structure. The larger the group, coupled with the higher degree of anonymity, individuals exhibit higher antisocial behaviors that go

against societal norms (Kugihara (2001)). These behaviors are socially accepted in the group and the group protects the individual from the social disproval of their actions. Mann, Newton, Innes (1982). This very action causes conformity to the group's norms of anti-social behavior (Kugihara,2001).
When online communication was used and individual's identities were concealed, Douglas and McGarty (2001) identified that those individuals with concealed identities had exchanged in "flaming behavior" more frequently. This included sending threatening messages to other participants in chat rooms or through instant messaging. Once an individual has been accepted into the in-group, manipulative psychological techniques are used to elicit emotion in the subconscious. Conscious feelings have traditionally been viewed as a central and necessary ingredient of emotion. Positive and negative reactions can be provoked subliminally and remain inaccessible to introspection. Subliminally induced affective reactions still influence people's preference judgments and even the amount they "voluntarily" drink. (Unconscious Emotion, Piotr Winkielman and Kent C. Berridge Current Directions in Psychological Science, Vol 13, Issue 3, pp. 120–123, First Published June 1, 2004, First Published June 1, 2004) At a larger scale, this fact can be manipulated to keep a person or group in a negative mood. If used properly, intrusive thoughts have the power to negatively amplify mood more substantially in people with obsessive-compulsive tendencies, anxiety, and depression. (Comparison of positive and negative intrusive thoughts and experimental investigation of the differential effects of mood, Martina Reynolds Paul M. Salkovskis , Behaviour Research and Therapy, Volume 30, Issue 3, May 1992, Pages 273–281) (AKrolla47 POLICING THE INTERNET – How Social media is not only destroying Democracy but Common Morality and what can we do about it to better navigate the tightrope between safety and privacy?, 2018)

Identifying The Information Spaces

Currently, deft users are able to extract and analyze data at a micro and macro level and make determinations that can affect entire countries. Polarization and social manipulation at a personal level can be achieved with manipulation of big data, through divisive topics specifically designed to elicit a certain emotional response and can drive wedges between even the closest of friends. These capabilities can also be leveraged to identify the information spaces used to recruit potential in-group members. (Akrolla47, POLICING THE INTERNET – How Social media is not only destroying Democracy but Common Morality and what can we do about it to better navigate the tightrope between safety and privacy? , 2018)

Identifying the information spaces the in-group participants operated in was instrumental to the progression of this study. This allowed us to take the "hacker" approach, and identify the endpoints of the information diffusion, and also the group mechanics of the in-group. The process of the diffusion of information, monitoring from initiation to completion of some of their memetic campaigns, allowed us to identify participants in their groups, also interactions between members allowed us to define a hierarchy within the in-group structure.


Browse With
To Visit the
Deep Web
Completely Anonymously
To Visit
Silk Road
anonymous marketplace
To Pay
bitcoin
to
To Instruct
Finance
Develop Plan At Central HQ
501(c)(3)'s
NIMBLE AMERICA
eBaum's WORLD
FORUM HOME POSTS SEARCH
Insulate HQ By Moving Talks to
DISCORD
Daily Stormer
Discuss Strategy On
To Employ Twitter Bots
To coordinate the execution of the plan on either chan
4chan
chan
Generate Memes
So Any Blowback Stays With
To Invade Tiwtter
To Like & Retweet Alt-right Generals
Provide Counsel to
To Help Generate Memes
GODFREY & KAHN S.C.
Infiltrate
Operate
/pol/ News Forever
To Share Them With
To Share Memes With
With /pol/ memes
Post Each other's Content
To spread them on
twitter
reddit
tumblr.
YouTube
myspace
facebook
To rally conservative media
DRUDGE REPORT
FOX NEWS
BREITBART
GATEWAY PUNDIT
THE DAILY CALLER
To Pressure the Mainstream Media
The Washington Post
WSJ
Daily Mail
YAHOO!
bbc
abc
THE HUFFINGTON POST
CNN
Aol.
CBS
MSNBC
The New York Times
Slate
To Influence Normies
To Consider Fascism

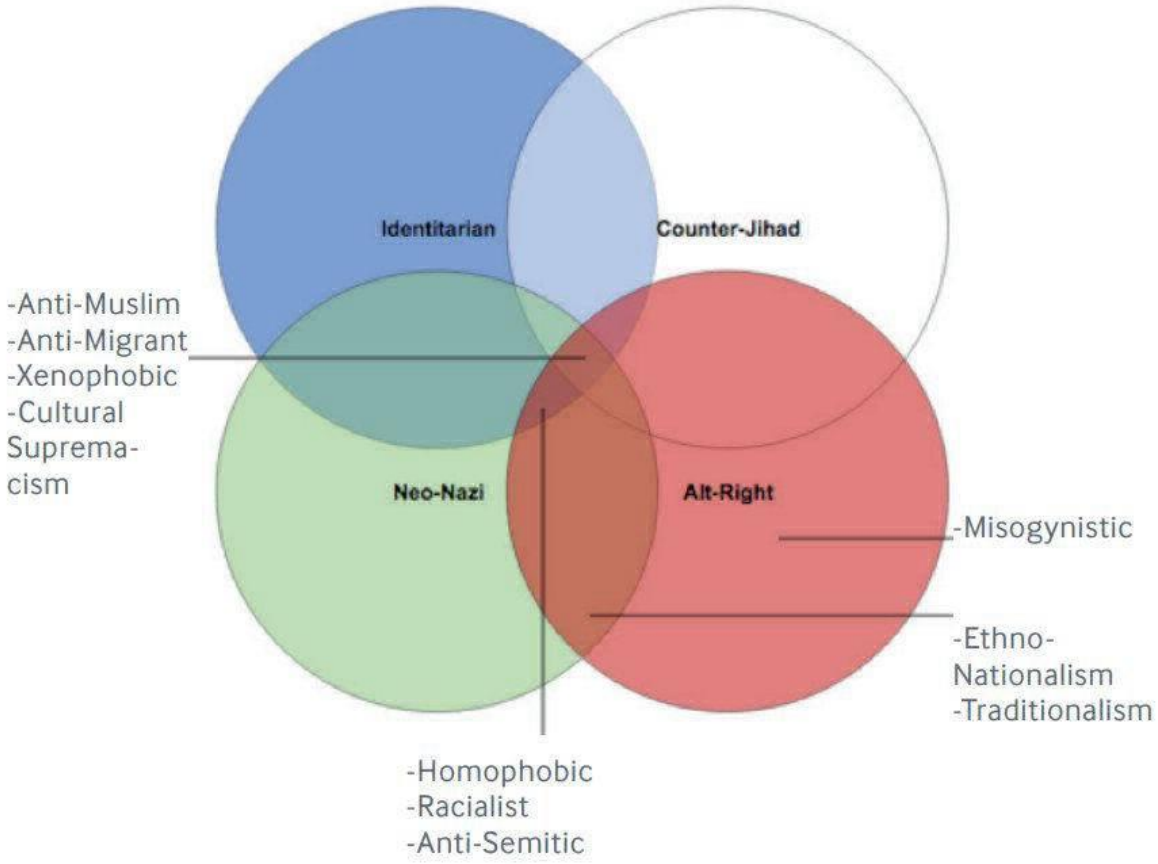


Figure 15: Ideological Convergence Points of the Extreme Right

(The Fringe Insurgency – Connectivity, Convergence and Mainstreaming of the Extreme Right, JACOB DAVEY AND JULIA EBNER, OCTOBER 2017)

Ideological Convergence Points

The chosen in-group was of particular interest because of the blurring of the different extremist ideologies and also how the participants seemed to come from all walks of life. These were the determining factors we looked for because of the appeal of these anonymous troll groups. The shedding of the cultural differences and ideologies in favor of group think extremism is of particular importance for effectiveness and cohesiveness of the group. It is their identity and also an attempt to normalize those extremist views as fast as possible. While the in-group generally reject mainstream conservatism and liberalism, they share Ideological viewpoints in the overlap between the different radical ideological views. The in-group commonly employ co-opting trending topics to create a blurring of issues and ideologies in what is used in an accelerated nature to lead to an increasingly radical ideology

as quickly as possible. The in-group attempt to control the narrative on both sides by implementing controlled opposition; the process of gaining control and attempted distortion of the narrative from both sides of the aisle. They achieved this by making hundreds of parody accounts of their opposition using them in tandem with far-right accounts to deliver devastatingly effective harassment campaigns and narrative distortion. Because the in-group has an international footprint; and multiple accounts, they are able to sustain large harassment campaigns for extended periods of time. Emphasizing broad issues such as “globalism", "identity politics", "free speech". This allows the group to quickly blur the lines between radical and mainstream in such a way that they are able to incorporate a number of extremist ideologies into their radicalization efforts in a short period of time.
The in-group converged around different relevant online social movements. From occupy Wall Street, Gamersgate, Anonymous Anti Jihadist groups, Anonymous Opferguson . The in-group trolls converged and grew in size during these events they were known to participate in based on public and private conversations. Some of these events were also around the time Russian influence campaigns started taking place and one of the in-group leaders interacted with a Russian based Internet Research Agency account frequently on an old account dating back to 2013.

Leveraging the ideological differences of the group could be useful in breaking up larger groups, also the differences between the different ideological movements within the larger ecosystem. This could also be used to provide an opening for exit paths to leave the different movements. If these exit paths are placed at different points in the path of informational flow this effect could cascade.

Radicalization Process

Table 1. Six conceptual models of the radicalization process.[5]

Model	Factors or stages
Sageman (2008a)	(1) Sense of moral outrage (2) Frame used to interpret the world (3) Resonance with personal experience (4) Mobilization through networks
Precht (2007)	(1) Pre-radicalization (2) Conversion and identification (3) Conviction and indoctrination (4) Acts of terrorism
Silber and Bhatt (2007)	(1) Pre-radicalization (2) Self-identification (3) Indoctrination (4) Jihadization
Moghaddam (2005)	(1) Psychological interpretation of material conditions (2) Perceived options to fight unfair treatment (3) Displacement of aggression (4) Moral engagement (5) Solidification of thinking and perceived legitimacy (6) The terrorist act
Wiktorowicz (2004b)	(1) Cognitive opening (2) Religious seeking (3) Frame alignment (4) Socialization
Borum (2003)	(1) Context: Deprivation/Grievance (2) Comparison: Inequality and resentment/Injustice (3) Attribution: Blame (4) Reaction: Demonizing the enemy/Distancing

(War Studies Department, King's College London How does the Internet facilitate radicalization? Homegrown Radicalisation and Counter-Radicalisation Dr. Sarah Beadle March 19, 2017)

The in-group in the study demonstrated and deployed regularly, the precepts of radicalization specifically for the purposes of terrorism. It is generally agreed upon in the literature that there is no standard set of factors for radicalization or an archetypal trajectory toward violent extremism. Reviewing relevant literature, one can identify at least six conceptual models presenting radicalization as a series of stages (see Table 1). Drawing from Borum (2003), Wiktorowicz (2004b), Moghaddam (2005), Silber and Bhatt (2007), Precht (2007), and Sageman (2008b), this paper classifies RVE into three main affairs: (1) Background factors and 'activators,' (2) Issues of identity, and (3) Social network mechanisms.

Multiple models were observed by the ingroup, particularly the Moghaddam model representing Incels and gender-based attacks, Sageman for White Nationalists, Borum observed with respect to defectors to opposition, and Precht represented in the attacks on journalists and researchers. All of which were highly effective as they were typically deployed in tandem in coordinated attacks.

In-Group Tactics From A Discursive Perspective

Tactic	Purpose
Deindividuation Manipulation	Dividing a perceived out-group enemy and also recruitment
De-anonymization	Induces fear in the perceived enemy
Coordinated harassment	Induces fear in the perceived enemy
Threats & Intimidation	Induces fear in the perceived enemy
Driving 'wedges' in their perceived opponents online relationships	To recruit and groom potential in-group members , intimidation,
Narrative creation & control	impression control
Forging documentation to support Narrative	Impression control
Manipulative psychological techniques	To develop rapport and build relationships as indoctrination into in-group occurs
Memetics - heavier use of E-memes vs. I-memes (see Dr. Robert Finkelstein's presentation on Military Memetics)	To change group behavior and perceptions of narrative.
Hostage taking using de-anonymization	To maintain loyalty and/or dependence upon the group through fear .
Indoctrination Through Deindividuation	Taking in outcasts and providing "protection" and "acceptance".
Identity politics immunity	Allows for impression control of the in-group's outward perception.

Using multiple coordinated racist satire accounts the in-group has the ability to manipulate public perception of how Oppositional political parties see each other and to generate outrage within and outside their respective online communities.

Andrew Anglin acknowledges in his blog post that the alt-right's use of ironic hyperbole "can be confusing to the mainstream, given the level of irony involved.

The amount of humor and vulgarity confuses people." But he's also very clear that the point of using irony is to mask something utterly straightforward: "The true nature of the movement, however, is serious and idealistic." In a postmodern, post-ironic culture, he argues, "absolute idealism must be couched in irony in order to be taken seriously."]

https://www.vox.com/ 2016/11/23/13659634/alt-right-trolling

The in-group also coordinates harassment campaigns against journalist and anyone else who threatens the public impression of the in-groups Social Identity. In these campaigns they typically de-anonymize their target and coordinate in private chat rooms with the information gained to leverage a sustained harassment campaign, with some participants international these campaigns can last for weeks to months or even years at a time.
https://www.theguardian.com/world/ 2018/jun/14/doxxing-assault-death-threats-the-new-dangers-facing-usjournalists-covering-extremism

Conversely the use of de-anonymization against the in-group by a ideologically opposite out-group has had a profound effect on the in-group members, this is in part because it works to reintroduce societal expectations and norms back into the individual and constrains the individual to the social contract once again. We also deployed the inverse of Stockholm Syndrome, Lima Syndrome, whereby we were able to elicit empathy for their victims from those wielding the power to deanonymize, harass, etc.

Methods and Countering of In-group to Out-group Aggression

Understanding the tactics of the in-group , the flow of the information they consume, and the differences in their ideologies , how they converge and how it leads them to radicalization are of importance to developing a long term strategy to combat this type of terrorism, this need not apply only to politically and socially aligned groups, but by any subject whom participates in online harassment can follow the same paths to radicalization. These observations enable us to identify the “endpoints” of the group identity and can work to “defang” the group of their power to harass. At the personal level it helps to understand the psychological profile of the particular participant to develop a method to individually “defang” them of their power to harass as well. We can then use these observations to divide the group at the ideological seams and work towards re-humanization from within the group and also provide exit paths to leave the group.

Out-group to In-group Tactics
Reintroduction of humanization after indoctrination- This helps to rebind the participants back to the social contract.
Identifying psychological profiles of the participants identifying hierarchy Identifying skillsets

Out-group Tactics
Public Awareness of the group’s ideological activities- provides a focal point for group aggression as this challenge the groups social identity and impression management.

Rebinding To The Social Contract

Whilst de-anonymization has been extremely effective in rebinding of the ingroup participant to the social contract, it is unsustainable way to move forward. Although public awareness is important but de-anonymization can lead participants further down the path of radicalization. This will increase the likelihood of violent isolated outburst from participants dealing with the effects that come with de-anonymization. This requires a better approach from the community aimed at de-radicalizing these people and solving the root causes of the problem. De-anonymization is not sustainable and can result in in-group and out groups both proceeding further down the path of radicalization by participating in the process.

Self-Moderation

Self-moderation falls short of solving the problem of coordinated troll harassment campaigns, for multiple reasons; It can act to further alienate the participants in the in-group furthering their descent down the path of radicalization. It also further alienates the participant to increasingly make more violent postings and lash out more frequently. The methods to self-moderate also do not go far enough. To ensure a comfortable and safe online environment for all the members of the service, Platform moderation tools have to be applied more on the personal level than platform level. Political bias at the platform level happens because the users on the service might be majority a certain political ideology, and if moderation features are only at platform level, it could appear that the smaller ideology is being censored because the only moderation is done by reporting abusive posts, so if the majority ideology is reporting, it stifles the exchange of political discourse for the minority ideology . If users have the ability to moderate their own spaces more effectively, it would return the platform to objectivity. This would also allow for control of the harassment campaigns that leverage different tactics to control impression.

Tracking Habitual Abusive Users

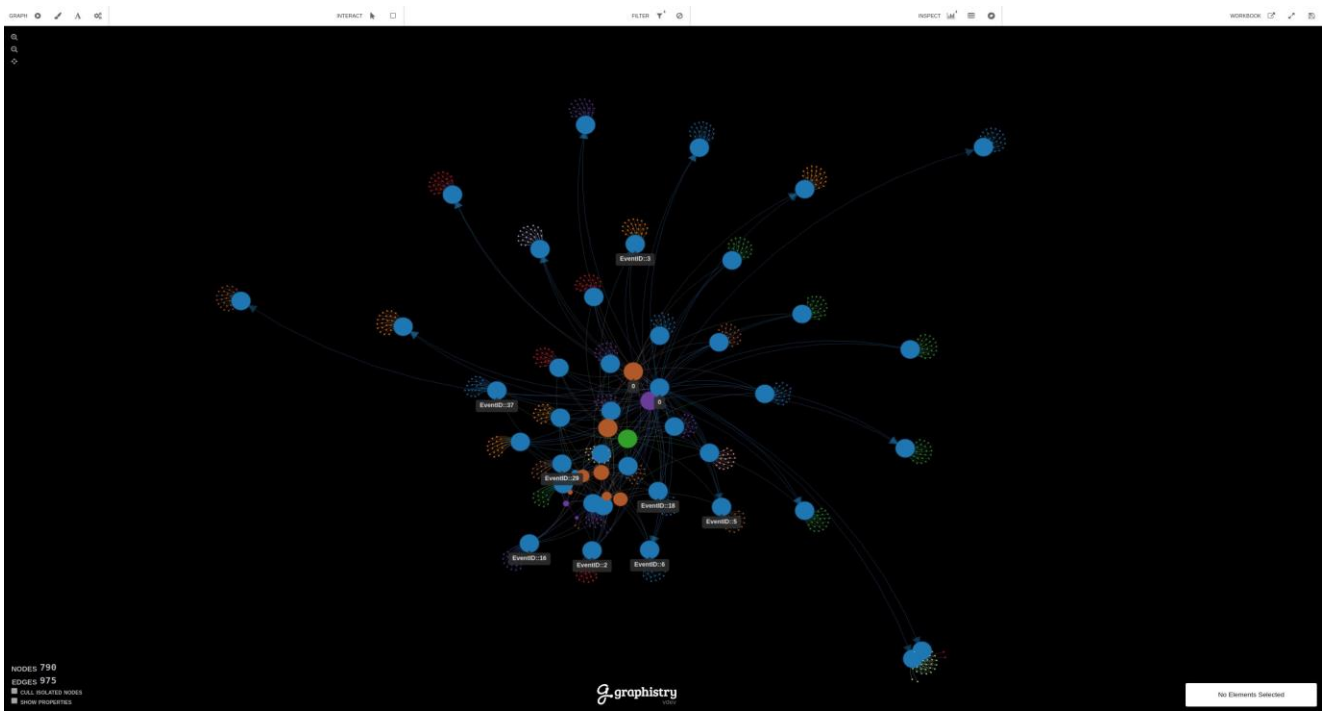
There has been much research into tracking habitual users on social media platforms without de-anonymization. It is important for platforms moderation to track habitually abusive users. It is important to the overall health of the platform to track the abusive users as it allows for healthier social discourse and exchange of ideas.

One study that took place by Cheng, Danescu-Niculescu-Mizil, Leskovec in 2015 characterized different forms of antisocial behavior and then used retrospective longitudinal analyses to quantify a user's behavior throughout his tenure in the community. This allowed the group to accurately predict undesired users early on in their community life.

Attribution of authorship with Stylometric Analysis is another area that can be used to track habitual users. Authorship Attribution of messages from an anonymous account can help to determine a lexical fingerprint of abusive users with a small sample of their messaging. A model was developed to collect and extract certain characteristics from online post using Natural Language Processing and gathering the corpus of posts from a user's accounts, removing any repost and post not written by the account being analyzed. This was then rendered into a network analysis to identify individual characteristics of a single user in the entire dataset.

LexicalDiversity	MeanWordLen	MeanSentenceLen	StdevSentenceLen	MeanParagraphLen	DocumentLen	Commas	Semicolons	Quotes	Exclamations	Colons	Dashes	Mdashes	Ands	Buts	Howevers	Ifs	Thats	Mores	Musts	Mights	This	Verys
24.4527	6.53914	14.1203	11.0445	8328	49864	37.3024	4.71189	0	22.5778	7.46049	2.84677	0	18.9457	1.86512	0	0.588986	6.96967	2.45411	1.3743	0	2.45411	2.84677
11.6104	7.85016	13.3917	12.8992	125.556	268157	5.35452	6.40256	0	9.68006	14.844	0.0571657	0	4.19215	0.76221	0	0.819375	4.02066	0.743154	0.171497	0.0952762	1.02898	0.171497
47.5524	6.07983	36.8571	32.0317	110.571	5303	13.986	0.999001	0	1.998	23.976	0	0	11.988	2.997	0.999001	0	7.99201	0	0	0.999001	0	0
20.2217	7.74227	24.5202	21.9817	536.615	101790	12.2938	0.682988	0	1.15583	16.9696	0	0	12.3463	1.6812	0.0525376	1.62866	6.77735	1.05075	0.315225	0.420301	4.25554	0.577913
38.5593	5.2381	19.8333	18.0921	133.875	7145	14.8305	0	0	4.9435	8.47458	0	0	9.88701	3.53107	0	0.706215	4.9435	0.706215	0	0	2.11864	0
28.4312	6.38286	11.7614	8.57044	84.3654	26697	4.90798	0.701139	0	1.22699	17.5285	0.35057	0	11.9194	4.03155	0	1.75285	8.58896	1.05171	0	0	6.31025	0.525855
23.3596	6.18569	48.1895	49.8894	14.4873	32239	2.05047	0	0	5.20505	12.1451	2.83912	0	5.36278	2.99685	0	1.1041	6.15142	0.315457	0	0.157729	4.73186	0
9.00132	8.36153	12.1981	8.01515	31.68	512182	30.471	2.29583	0	0.475964	8.28737	1.73587	0	11.6658	2.39848	0.0373305	1.89452	9.33262	1.7732	0.242648	0.195985	2.74379	0.597288
17.3899	8.07909	14.472	15.2304	123.777	147125	27.207	0.599421	0	0.333011	29.0719	0.333011	0.0666023	15.8846	3.09701	0.0333011	1.63176	8.8914	2.19788	0.233108	0.499517	5.8943	1.43195
13.4487	7.7841	21.7436	21.3947	353.486	324450	33.1924	2.68425	0	1.41428	15.4417	1.94825	0	13.0172	4.34387	0.0288629	2.15029	9.74124	0.88032	0.0432944	0.274198	6.39314	0.187609
28.0397	7.31755	13.0065	12.4339	1004.75	28508	8.0434	1.6835	0	37.5982	18.1444	0	0	13.6551	1.12233	0	1.87056	2.80584	2.43172	0.187056	0	4.11523	0
55.9671	4.83824	10.2353	4.47909	174	1144	53.4979	0	0	0	0	0	0	8.23045	4.11523	4.11523	0	8.23045	0	0	0	0	0
18.1627	10.3521	29.1772	28.6968	475.208	596453	20.0347	12.5285	0	3.15953	66.5327	1.10492	10.2822	8.74806	0.986211	0.0365263	0.529632	3.82613	1.19624	0.237421	0.0547895	1.55237	0.200895
32.3253	6.69848	23.4091	23.0777	327.727	24914	9.6036	2.04332	0	0.817327	48.2223	2.86065	0	8.17327	2.04332	0	1.02166	5.1083	0.817327	0.612996	1.02166	2.86065	0.408664
40.6758	6.03077	19.8833	26.3541	198.833	8531	6.8836	0	0	3.75469	17.5219	0	0	14.393	1.25156	0	0.625782	5.63204	0.625782	0.625782	0	1.25156	0.625782
17.7954	8.1063	9.56772	8.17749	729.938	256599	22.7723	1.77526	0	4.61159	8.83547	0.346889	0.0408105	10.5291	1.24472	0	0.775399	3.40768	0.85702	0.775399	0.0204052	1.9589	0.285673
36.2839	5.93846	10.4409	9.11511	971	6214	39.8724	0	0	0	2.39234	0	2.39234	19.9362	0	0.797448	1.5949	7.97448	0	0	0.797448	7.17703	1.5949
26.3431	7.79703	15.9048	14.2513	2409.43	120613	26.5005	10.3365	0	22.1192	24.3736	2.25446	0.297758	6.63576	1.57387	0.0425369	1.27611	3.44549	0.765664	0.467906	0.0425369	2.93505	0.425369
21.722	9.26312	134.833	172.325	1011	41891	3.36208	0	0	1.90031	7.30887	0	0	15.0563	0.292355	0	0.438532	1.75413	0	0	0.146177	0.292355	0
59.2437	4.71631	12.7143	7.12569	44.5	1042	25.2101	0	0	0	21.0084	0	0	8.40336	0	0	4.20168	8.40336	0	0	0	16.8067	0
26.1548	8.70939	42.2585	45.7492	334.963	215496	19.5779	2.15307	0	10.54	46.3661	0.700999	0.951356	9.11299	1.00143	0	1.30186	4.40628	0.575821	0.300428	0.200285	3.07939	0.250357
29.4716	6.71053	14.883	12.0101	254.364	21710	11.3912	0	0	4.12021	20.8434	0	0	4.12021	0.969462	0	0.484731	6.3015	0.727096	0.242365	0	2.42365	0
13.8087	7.84075	10.9561	8.87696	77.62	256732	7.71845	2.216	0	1.03288	16.1318	1.07044	0.0938985	7.41798	0.769968	0	1.12678	6.62923	0.60095	0.169017	0.150238	5.46489	0.431933
22.5269	7.19526	54.1053	62.6414	9251	56832	22.8831	5.96563	0	13.4449	15.938	0	0	12.4655	2.67118	0	2.40406	5.34236	1.06847	0.267118	0.0890393	3.82869	0.801353
13.051	8.52259	33.2857	44.3035	10485	112610	1.29807	0.703121	0	6.81486	23.2571	0	0	0.973552	0.486776	0	0.216345	1.67667	0.324517	0.162259	0	1.83893	0.270431
17.1485	8.14913	30.55	35.4315	2427.18	313197	11.2253	0.910162	0	1.17786	27.3584	0.107078	0	9.60131	1.57048	0.0356926	1.30278	6.5139	0.981547	0.374772	0.321234	3.42649	0.392619
17.2889	7.74818	18.7918	17.5412	376.652	138093	11.3453	0.196286	0	12.6016	24.7713	0	0	8.12625	2.55172	0	1.84509	5.65304	0.667373	0.196286	0.314058	3.65092	0.157029
51.4286	6.4537	9.27273	8.31673	153	2241	30.9524	0	0	19.0476	59.5238	0	0	14.2857	7.14286	0	0	9.52381	2.38095	4.7619	0	4.7619	0
37.4414	5.96014	10.293	7.20957	53.8	11121	25.1599	0.426439	0	28.145	23.4542	0	0	5.54371	0.852878	0	0.426439	3.41151	0	0.426439	0	6.82303	0
56.8571	6.22111	52.4	72.8577	262	2030	0	0	0	0	57.1429	0	0	5.71429	0	0	2.85714	2.85714	5.71429	0	0	0	0
17.4345	7.07947	15.4564	13.1163	85.947	83246	4.04883	6.99344	0	14.2936	14.539	0.0613459	0	6.31863	1.41096	0.0613459	0.674805	4.66229	0.552113	0.122692	0.184038	0.429422	0.0613459
17.3899	8.07909	14.472	15.2304	123.777	147125	27.207	0.599421	0	0.333011	29.0719	0.333011	0.0666023	15.8846	3.09701	0.0333011	1.63176	8.8914	2.19788	0.233108	0.499517	5.8943	1.43195
33.0124	5.9375	10.8944	10.0413	110.5	10710	4.12655	3.66804	0	13.2967	6.41907	0	0	3.66804	3.66804	0	0.917011	7.33608	0.458505	0	0	3.20954	0.458505
68.7861	5.23529	69	31	27.6	903	17.341	5.78035	0	0	28.9017	0	0	5.78035	0	0	0	5.78035	0	0	0	17.341	0
12.7029	10.8213	19.4541	32.4473	112.052	274188	10.5677	0.195296	0	11.3488	48.238	0.043399	0	3.58042	1.73596	0	1.04158	1.56236	0.108498	0.130197	0.130197	0.45569	0.0650985
55.9671	4.83824	10.2353	4.47909	174	1144	53.4979	0	0	0	0	0	0	8.23045	4.11523	4.11523	0	8.23045	0	0	0	0	0
65.0558	4.96	114.5	40.5	229	1390	3.71747	0	0	3.71747	14.8699	0	0	0	0	0	0	0	0	0	0	3.71747	0
41.5357	6.73259	18.625	16.8131	22.9231	14684	13.2143	7.14286	0	10.7143	30.3571	0.714286	0	9.28571	0.714286	0	0	6.07143	0.357143	0.357143	0	6.42857	0.357143
36.361	6.97038	24.0973	14.8371	2723	18195	31.7322	1.74672	0	0.291121	31.441	0.291121	0	18.3406	2.91121	0.291121	0.582242	11.0626	2.03785	0.582242	0	2.91121	1.16448

(Table 1 : A sample of the Lexical data derived from the written posts on anonymous accounts)



(Figure 1: Network analysis of the Lexical data derived from the written posts on an anonymous account)

Redefining Cyber Terrorism

In the ever-evolving digital landscape, it is imperative to look at the framework that defines what we know as terrorism, specifically, cyber terrorism. The term "terrorism" comes from French terrorisme, from Latin: terror, "great fear", "dread", related to the Latin verb terrere, "to frighten". The current definiton of cyber terrorism at the federal level is limited to crimes resulting in financial loss to businesses, governments or individuals. The reality of what was documented during this study, were acts not committed against governments or institutions, but civilians.

The observations in this study can be directly compared to The Terror of the French Revolution. In today’s climate, one can replace pitchforks and torches with troll troops and coordinated networks, and the targets character replaces the victims' head at the guillotine. And every terror needs a Robespierre, the ideological leader directing the group. The most frequently used methodology observed for this paper involves character assassination and smear campaigns of targets in opposition. These campaigns resulted in long lasting collateral damage to its victims ranging from professional, educational, legal, familial, emotional and physical impacts. Coordinated optics, deanonymization, memetics, social engineering and information distortion being heavily utilized tools in information and psychological warfare.

Deindividuation is the modern equivalent of stripping the populace of title, religion, status, and creating citizens during The Great Terror. The stripping of all identifiers in that society, be they indicators of race, financial status, political status, marital status, it was an historical form of deindividuation and anonymization. Deindividuation and anonymization of the ingroup allowed the attackers to behave in such a way that their targets became dehumanized and facilitated the most inhuman acts of aggression. Information warfare need not be restricted to group contexts, a fact that is little acknowledged in much of the relevant literature. Ordinary citizens are vulnerable to various kinds of overt and covert attack by cyber-terrorists acting alone or in concert, whether the motivation is ostensibly ludic or demonstrably criminal (Kirsner,1998; Foote,1999). Underlying many of these attacks is terrorism: an attempt to extract political concessions by instilling fear in the civilian population. In this way, cyber terrorism is no different from conventional terrorism. (2016) The psychological effects of cyber terrorism, Michael L. Gross, Daphna Canetti, and Dana R. Vashdi.

The ingroup in the study demonstrated and deployed regularly, the precepts of radicalization specifically for the purposes of cyber terrorism. It is generally agreed upon in the literature that there is no standard set of factors for radicalization or an archetypal trajectory toward violent extremism. Reviewing relevant literature, one can identify at least six conceptual models presenting radicalization as a series of stages (see Table 1). Drawing from Borum (2003), Wiktorowicz (2004b), Moghaddam (2005), Silber and Bhatt (2007), Precht (2007), and Sageman (2008b), this paper classifies RVE into three main affairs: (1) Background factors and ‘activators,’ (2) Issues of identity, and (3) Social network mechanisms.

THE 'THREE CIRCLES MODEL' OF IF-RVE

Acknowledging the breadth of existing research on radicalization and the Internet, there is still no prominent graphical model illustrating the links and influences of the online environment on RVE dynamics. Therefore, this paper introduces an explanatory 'three-circles model' for Internet-facilitated radicalization into violent extremism (IF-RVE) resulting from a structured literature analysis of current research in extremism and terrorism studies, identity theory, and Internet studies.

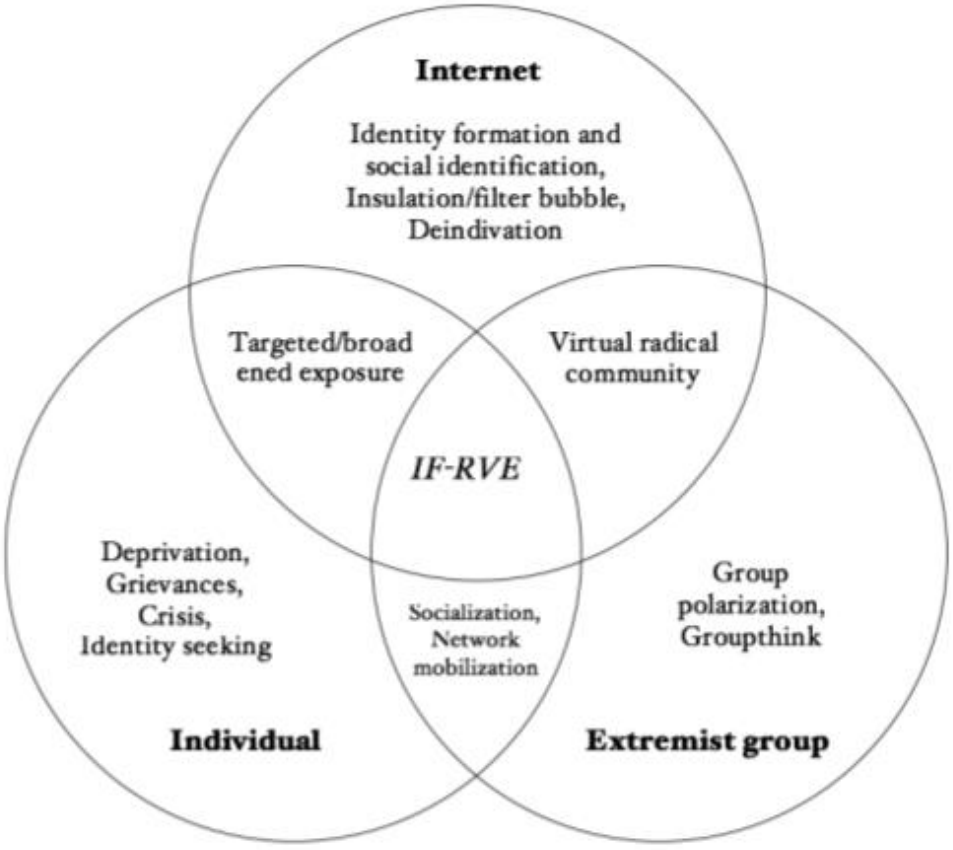


Figure 1. The 'three-circles model' for Internet-facilitated radicalization into violent extremism.

Table 1. Six conceptual models of the radicalization process.[5]

Model	Factors or stages
Sageman (2008a)	(1) Sense of moral outrage (2) Frame used to interpret the world (3) Resonance with personal experience (4) Mobilization through networks
Precht (2007)	(1) Pre-radicalization (2) Conversion and identification (3) Conviction and indoctrination (4) Acts of terrorism
Silber and Bhatt (2007)	(1) Pre-radicalization (2) Self-identification (3) Indoctrination (4) Jihadization
Moghaddam (2005)	(1) Psychological interpretation of material conditions (2) Perceived options to fight unfair treatment (3) Displacement of aggression (4) Moral engagement (5) Solidification of thinking and perceived legitimacy (6) The terrorist act
Wiktorowicz (2004b)	(1) Cognitive opening (2) Religious seeking (3) Frame alignment (4) Socialization
Borum (2003)	(1) Context: Deprivation/Grievance (2) Comparison: Inequality and resentment/Injustice (3) Attribution: Blame (4) Reaction: Demonizing the enemy/Distancing

War Studies Department, King's College London How does the Internet facilitate radicalization? Homegrown Radicalisation and Counter-Radicalisation Dr. Sarah Beadle March 19, 2017

Multiple models were observed of the ingroup, particularly the Moghaddam model supporting radical Incels and gender-based attacks, Sageman for White Nationalists, Borum with respect to defectors to opposition, and Precht in the attacks on journalists and researchers. All of which were highly effective as they were typically deployed in tandem in coordinated attacks. It was observed that anyone in both the ingroup and outgroups were capable of being radicalized, particularly vulnerable individuals. Ideologues were not necessarily aligned. While being radical in ideals and advocation, they ranged from a variety of belief systems. Protection from opposition and a sense of belonging was far more powerful than a set of mutually supported beliefs. Further blurring the lines is the concept of eliminating territorially defined physical locus. One's country, nation or sovereignty are no longer relevant. It is simply an ideology that knows no specific citizenship.

Digital media afford one's enemies a much richer and more powerful set of tools with which to engage in psychological warfare, whether at the local or global level. With estimates of e-mail traffic for the year 2000 put at 7 trillion (McHugh, 1998), cyber-smearing or digital defamation campaigns have the potential to reach unprecedentedly large audiences with great speed, in the process creating considerable frustration and collateral damage for the

victim (Table 4). The reconstitution of trust and salvaging of reputations in the wake of virtual vilification campaigns will likely pose major challenges for targeted individuals and collectivities.

TABLE 4
Digital defamation and virtual vilification

- Ease, swiftness, and stealth of attack
- Overt and covert options
- Target placed on defensive footing
- Extended psychological warfare
- Vulnerability and suggestibility of target
- Cyber-stalking and cyber-smearing
- Ontological warfare possibilities
- Jurisdictional confusion

Ingroup tactics of deanonymization, then protracted coordinated defamation and vilification, both online and offline were by far the most successful in instilling enough fear in the outgroups to both stifle political discourse and push groups towards the edges of radicalization as a defense mechanism. By limiting social discourse through fear practices, they were able to silence critics of radical political attacks against governments, journalists and personages of note. Targeting civilians in coordinated attacks to terrorize, defame and demoralize the outgroup as a whole being the goal of the ingroup. Once a target was deanonymized, their families, children, jobs, social groups, finances, any personal data found, was abundantly shared in such a way as to instill threat to personal security. Heavy use of memetics involving the photos of the target, their family and/or children being the most effective in eliciting a response from a psychological warfare concept.

Not surprisingly, exposure to cyber terrorism is stressful. Figure 1 uses the State-Trait Anxiety Inventory (STAI) to show how stress and anxiety grow as attacks become more deadly. With a score of 4.00, conventional mass-casualty terrorism (e.g., suicide bombings) evokes a level of anxiety at the top of the scale. The stress scores for lethal and non-lethal cyber terrorism are not far behind, and all the scores significantly surpass the control group. But the interesting point is this: Individuals were equally disturbed by lethal and non-lethal cyber terrorism, meaning there is no significant difference between the two when it comes to stress. Both cause significant panic and anxiety and both, it seems, are equally capable of cracking the foundations of personal wellbeing and human security.

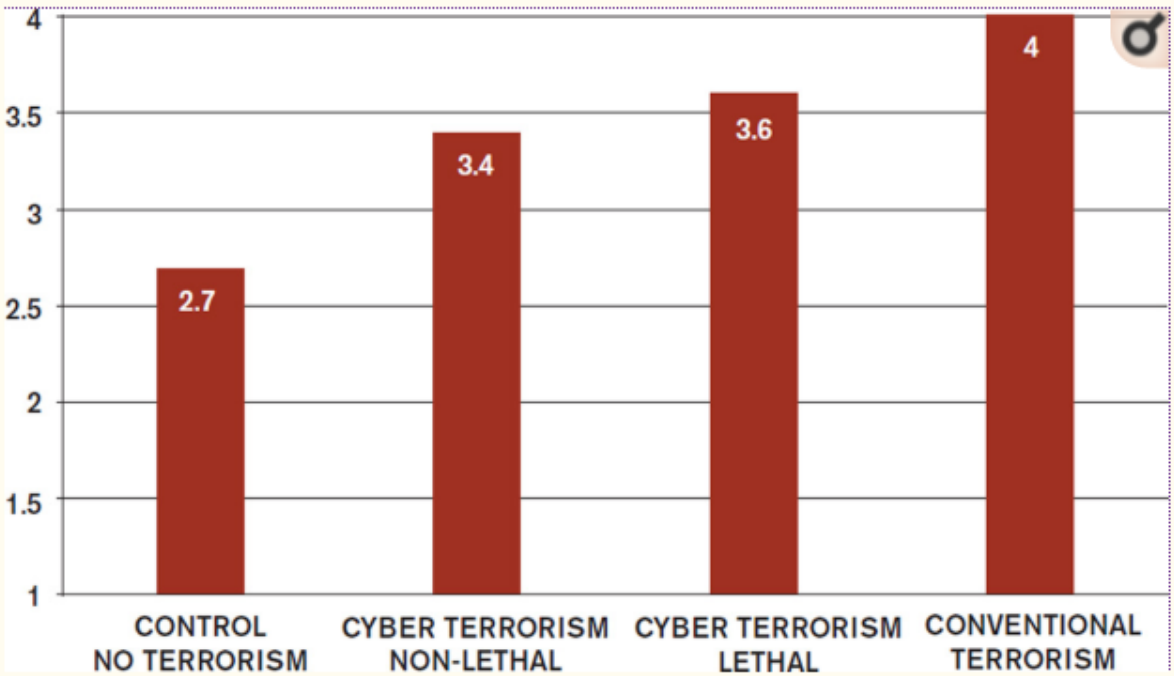


Figure 1

Anxiety in the Wake of Terrorism

CONTROL: No terrorism

CYBER TERRORISM, NON-LETHAL: Disclosure of account information, loss of funds

CYBER TERRORISM, LETHAL: Deaths and injuries

CONVENTIONAL TERRORISM, LETHAL: Deaths and injuries

(2016) The psychological effects of cyber terrorism, Michael L. Gross, Daphna Canetti, and Dana R. Vashdi

With the increasing awareness of just how devastating deanonymization, victimization, cyber troop bullying and defamation campaigns it is vital to look at the way we classify the behavior. As most defamation campaigns generally last anywhere from 2-4 years, the reality is that the consequences for the victim are very real and long lasting. Many change their addresses and phone numbers, their names, their jobs in an effort to regain a sense of personal security.

“Cyber threats” can simply mean threatening communications that are conveyed via the Internet, cellphone, or other digital means. The communication in interstate commerce of threats to harm a person or property, to kidnap a person, or to damage a person’s reputation, is a violation of federal law pursuant to 18 U.S.C. § 875. Because the Internet is a means of interstate commerce, threats sent online may be federally prosecuted. See 18 U.S.C. § 875(c)

(2015). It is axiomatic that “cyberthreats” are “threatening” to the victim, as the perpetrator generally intends the victim to feel threatened. For instance, the victim in a recent Supreme Court case addressing section 875 stated, “I felt like I was being stalked. I felt extremely afraid for mine and my children’s and my families’ lives.” Elonis v. United States, 135 S. Ct. 2001, 2007 (2015).

The suffering visited upon the victims of such conduct has led district judges pronouncing sentence to call these defendants “cyber terrorists.” Referring to a defendant who hacked into his ex-girlfriend’s online account and used that access to overdraw her bank account, max out her credit card, and send graphic sex photos of the victim to her family, friends, and coworkers, one sentencing judge remarked that he had never seen a person so dedicated to utterly destroying the victim in all aspects of her life. United States v. Ledgard, 583 F. App'x 654 (9th Cir. 2014). Furthermore, the harm is long-lasting. (2016) Joey L. Blanch, Wesley L. Hsu, Cyber Misbehavior, United States Department of Justice, Volume 64, Number 3.

A common ingroup tactic involves damage to an opposition targets reputation. Manufacturing "sextortion" materials was common, ranging from pornographic images, memes and accounts, to pedophile blogs, in the targets name using their face as an avitar with the intention to incite group harassment of the target both online and offline. Incitement of harassment campaigns have been known to have deadly consequences. "Cyber extortion" was also commonly used, whereby the personal identity of an individual would be used as a threat for others personal identities in exchange for protection from the ingroup. Section 875 of 18 U.S.C. "prohibits the interstate and foreign communication of a threat to physically harm, kidnap, or injure the reputation of another." Most certainly reputations are gravely harmed in the practices by the ingroup, but by publishing a targets address, work, family, full name, age, it is now publicly available and a prelude to physical harm by others in the form of vigilantism as well as other ancillary crime, such as identity theft.

The United Nations has developed a working definition of terrorism as "Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them." 1994 United Nations Declaration on Measures to Eliminate International Terrorism annex to UN General Assembly resolution 49/60 ,"Measures to Eliminate International Terrorism", of December 9, 1994, UN Doc. A/Res/60/49.

Given that the ingroup tactics definitively mimic radicalization schema and the results of their behavior performed explicitly with the intent to provoke terror and instill a sense of threat to personal safety, it is essential to look at how this is handled by authorities who respond to the victims. The ingroup engaged in long, protracted campaigns using defamation,

deanonymization, and other methods to instill fear, intimidation and terror in oppositional targets. The protracted campaigns deployed with the intent to undermine a sense of security as to when the next attack or personal information disseminations will occur. In essence, placing the victim in a perpetual state of hyper vigilance. To provoke a state of terror. A long, protracted state of terror, coordinated across a defined cyber troop operating on an international level, resulting in terrorizing without cease. Currently, there are 50 states with laws against cyber stalking and cyber harassment though they vary from state to state although none cover the social aspect of civilians at the hands of cyber terrorists. There currently are no laws addressing those engaging in such acts against United States citizens perpetrated in another country.

Technology is continuously improving, which in turn influences the way that people interact by promoting global communication and allowing individuals to connect with others more readily. However, the Internet and related technology have also become new mediums for misconduct, in that communications via the Internet can be used to threaten, harass, intimidate, and cause harm to others (2008) Recupero, P. R. Forensic evaluation of problematic internet use. Journal of the American Academy of Psychiatry Law, 36, 505-514.).

Anonymity And Cyberterrorism

Anonymity of the perpetrators is problematic in legal recourse. 45% of the states (n =22) make reference to Anonymity in their cyber harassment/cyberstalking statutes. Many of these states acknowledge that it constitutes harassment of the victim if a perpetrator "Anonymously or otherwise…" engages in the prohibited behaviors. Another method of hiding one's identity is to enlist the help of a Third Party person to deliver a message to the victim on behalf of the harasser or stalker … 27% of the states (n = 13) make reference to Third Party acts…in which a Third Party may be a knowing participant in the harassment, and in these cases the Third Party may be held criminally responsible along with the primary perpetrator. (2013) Steven D. Hazelwood, Sarah Koon-Magnin, Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis, International Journal of Cyber Criminology, July-December 2012, Vol 7 (2): 155-168. Jurisdiction is also problematic. Interstate laws establish jurisdictional applicability; however, it is largely unclear, on behalf of law enforcement, how to enforce protective orders across state lines and from a judicial aspect, how to process such cases.

Group Effort

Despite the broad definitions, which can vary across organizations, as currently understood, cyber terrorism has multidimensional overlap with cyber warfare, cybercrime and traditional terrorism. Currently, the Federal Bureau of Investigations defines cyber terrorism as "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by subnational groups or clandestine agents". (2008) Centre of Excellence Defense Against Terrorism, ed. Responses to Cyber Terrorism. This definition is woefully lacking in addressing the other aspects of terrorism that affect civilian populations. It is clear that law enforcement, the judicial system and advocates are struggling to keep pace with the agile, adaptive environment in which of cyber terrorism proliferates and thrives.

Given the right circumstances and radical ideology, such socially engineered cyber terrorism could in fact be, and likely is, deployed against governments and military with far reaching consequences. Given the radicalization methodology, modality of cyber troop behavior, engaged against political opposition, with the intended result of the behavior being to instill terror, we propose that given that set of defined parameters, such activities should be classified and approached as cyber terrorism.

Literature Citations

Information Warfare: Its Application in Military and Civilian Contexts, Blaise Cronin and Holly Crawford School of Library and Information Science, Indiana University, Bloomington, Indiana, USA

(2008) Responses to Cyber Terrorism: Centre of Excellence Defence Against Terrorism, NATOP Science for Peace and Security Series E: Human and Societal Dynamics - Vol. 34

(2016) The psychological effects of cyber terrorism, Michael L. Gross, Daphna Canetti, and Dana R. Vashdi (Kirsner,1998; Foote,1999)

(2017) War Studies Department, King's College London How does the Internet facilitate radicalization? Homegrown Radicalisation and Counter-Radicalisation Dr. Sarah Beadle March 19, 2017 (McHugh, 1998)

(2016) Joey L. Blanch, Wesley L. Hsu, Cyber Misbehavior, United States Department of Justice, Volume 64, Number 3

(2008) Recupero, P. R. Forensic evaluation of problematic internet use. Journal of the American Academy of Psychiatry Law, 36, 505-514.

(2013) Steven D. Hazelwood, Sarah Koon-Magnin, Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis, International Journal of Cyber Criminology, July-December 2012, Vol 7 (2): 155-168

(2008) Centre of Excellence Defense Against Terrorism, ed. Responses to Cyber Terrorism

AKRolla47 (2018). POLICING THE INTERNET – How Social media is not only destroying Democracy but Common Morality and what can we do about it to better navigate the tightrope between safety and privacy? Medium https://extranewsfeed.com/https-medium-com-akrolla47-how-social-media-is-not-only-destroying-democracy-but-common-morality-c69b51f6f1fc

Wilson, Jason, (2018). Doxxing, assault, death threats: the new dangers facing US journalists covering extremism. The Guardian

Coles, B. A., & West, M., (2016). Trolling the trolls: Online Forum Users Constructions of the Nature and Properties of Trolling, Computers in Human Behavior, 60, 233-244. doi:

Festinger, L., Pepitone, A., & Newcomb, T. (1952). Some consequences of deindividuation in a group. Journal of Social Psychology, 47, 382-389

Kugihara, N. (2001). Effects of aggressive behaviour and group size on collective escape in an emergency: A test between a social identity model and deindividuation theory. British Journal of Social Psychology, 40, 575-598.

Mann, L., Newton, J. W., & Innes, J. M. (1982). A test between deindividuation and emergent norm theories of crowd aggression. Journal of Personality and Social Psychology, 42, 260-272.

Zimbardo, P. G. (1969). The human choice: Individuation, reason, and order versus deindividuation, impulse, and chaos. In W. D. Arnold & D. Levine (Eds.), Nebraska Symposium on Motivation, (pp. 237-307). Lincoln: University of Nebraska.

Douglas, K. M., & McGarty, C. (2001). Indentifiablity and selfpresentation: Computer-mediated communication and intergroup interaction. British Journal of Social Psychology, 40, 399-416.

(2010) A Sociological Perspective on Internet Trolling, Sean Li, Internet Society

(2007) Ideologies of moral exclusion: a critical discursive reframing of depersonalization, delegitimization and dehumanization. British Journal of Social Psychology, 46 (4), pp. 717-737

Chang, Jenna. The Role of Anonymity in Deindividuated Behavior: A Comparison of Deindividuation Theory and the Social Identity Model of Deindividuation Effects (SIDE). The Pulse: Undergraduate Journal of Baylor University

(2013) Frances Shaw, University of Sydney, FCJ-157 Still 'Searching for Safety Online': collective strategies and discursive resistance to trolling and harassment in a feminist network, The Fibreculture Journal, // Issue 22 2013: Trolls and The Negative Space of the Internet

(2015) Antisocial Behavior in Online Discussion Communities, Justin Cheng, Cristian Danescu-Niculescu-Mizil, Jure Leskovec

(2017) Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation, Samantha Bradshaw, University of Oxford, Philip N. Howard, University of Oxford

(2018) Internet trolling and everyday sadism: Parallel effects on pain perception and moral judgment, Erin E. Buckels, Paul D. Trapnell, Tamara Andjelovic, Delroy L. Paulhus, Journal of Personality. 2018;1–13

Comparison of positive and negative intrusive thoughts and experimental investigation of the differential effects of mood, Martina Reynolds Paul M. Salkovskis, Behaviour Research and Therapy, Volume 30, Issue 3, May 1992, Pages 273–281

Unconscious Emotion, Piotr Winkielman and Kent C. Berridge Current Directions in Psychological Science, Vol 13, Issue 3, pp. 120–123, First Published June 1, 2004, First Published June 1, 2004

(2011) TUTORIAL: MILITARY MEMETICS, Robert Finkelstein, Social Media for Defense Summit, Alexandria, Virginia

TILEAGA, C., 2007. Ideologies of moral exclusion: a critical discursive reframing of depersonalization, delegitimization and dehumanization. British Journal of Social Psychology, 46 (4), pp. 717-737

The Fringe Insurgency – Connectivity, Convergence and Mainstreaming of the Extreme Right,JACOB DAVEY AND JULIA EBNER, OCTOBER 2017

Stylometric Analysis for Authorship Attribution on Twitter - Mudit Bhargava, Pulkit Mehndiratta, and Krishna Asawa

Hardaker, C. 2013. Uh.... not to be nitpicky, but... the past tense of drag is dragged, not drug. JLAC.