The Dr. House Approach to Information Warfare

Stefan Soesanto

Defending against information warfare across the vastness of the social media space is difficult, if not impossible, or so the story goes. Many are trying, many are failing, and we have all heard of the many solutions that will turn the tide someday, somewhere, somehow: increased media literacy, expanded factchecking, banning bots, deleting accounts, redirecting users, curtailing free speech, boosting counter-messaging, etc. But what if there were one solution, better than all others, that no democratic nation dares to touch ... yet?

The approach this paper outlines draws deep inspiration from the TV character Dr. Gregory House, played by Hugh Laurie, in the widely acclaimed US hospital drama *House*. Over the course of eight seasons, the "fascinatingly unsympathetic,"[1] "self-pitying, deeply sarcastic and sometimes smug"[2] medical genius of Dr. House captured audiences across the globe with his "straight, no-chaser approach to patient care."[3] House's thinking is perfectly summarized in the show's pilot, when his colleague Dr. Foreman asks: "Isn't treating patients why we became doctors?" to which House retorts, "No, treating illnesses is why we became doctors. Treating patients is what makes most doctors miserable."[4]

This article takes the Dr. House approach, with all its dark, provocative, and unconventional wisdom, and applies it to information warfare. Thus, in the same vein as House's cases hit eerily close to home and showcased the fallibility of the medical system, this article calls out the failures and misconceptions of current defensive strategies in the information warfare space to craft a better path forward. First, let us recap the problem we are trying to solve.

Stefan Soesanto is a Senior Researcher on the Cyber Defense Team at the Center for Security Studies (CSS) at ETH Zurich. Before joining CSS, he was the Cybersecurity & Defense Fellow at the European Council on Foreign Relations (ECFR) and a non-resident James A. Kelly Fellow at Pacific Forum CSIS. At ECFR, he designed and held cyber wargame exercises in cooperation with Microsoft, and organized a closed Cybersecurity and Defense conference in Odense together with the Center for War Studies at the University of Southern Denmark and the Office of the Danish Tech Ambassador. He also served as a Research Assistant at RAND's Brussels office, co-authoring reports for the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE), the European Network Information Security Agency (ENISA), and the Dutch Ministry of Security and Justice.

Information warfare operations encompass a wide range of strategies, tactics, tools, goals, and motivations. In the broadest terms, info ops can be divided into two categories: Morale operations, which the U.S. Office of Strategic Services (OSS) defined in 1943 as, "all measures of subversion–other than physical–used to create confusion and division, and to undermine the moral and the political unity of the enemy through any means,"[5] and political warfare operations, which, according to Angelo Codevilla, is the "marshaling of human support, or opposition, in order to achieve victory in war or in unbloody conflicts as serious as war."[6] In other words, while the former seeks to sow chaos and division, the latter aims to generate trust and unity amid likeminded groups. Naturally, there are numerous spillover effects between the two categories, particularly on social media platforms specifically designed to facilitate relationships and build trust through continuous content engagement.

At its most elemental level, every information warfare operation is an input-output communication cycle. Operators post a message, image, or video, which intermediaries carry, through algorithms, relationships, hashtags, etc., to a target audience to elicit a response. Given the operator's visibility as to how his product moves (retweets, likes, reverse image searches, etc.), the operation can leverage real-time social network analysis and initiate a feedback loop to tailor his messaging and fine-tune the trust-building process to gain credibility, authority, and importance within the target network. Operations will sometimes run on top of pre-existing beliefs and emotions to radicalize or strengthen opposition within a target group. Or they will create new emotions and new beliefs that run counter to existing ones. Static defenders cannot react timely or compete in this fast-paced dynamic environment.

But many elemental questions surrounding information warfare remain unresolved. Veteran information security researcher The Grugq summarized it aptly in three sentences: "What [are] the adversary's most effective strategies, tactics, and tools? Where should [the defender] invest resources to mitigate [adversarial] strengths? [And] where should [the defender] invest resources to address [his own] weaknesses?"[7] From the defender perspective, it is extremely difficult to find credible metrics that reliably ascertain the effectiveness or impact of an adversarial information warfare operation. Daily, weekly, or monthly polling of the same target group may be an acceptable starting point to map changes in attitude and identify potential causal linkages. But doing so at scale outside of an election cycle would be expensive, tedious, and most likely result in diminishing returns over time as answers become repetitive and habitual. Similarly, identifying operations in their preparatory stages, such as a meme being tested "in-house," provides little to no value if the target group cannot take reasonable defensive actions, or is overwhelmed by the sheer volume of incoming threat intelligence.

Absent reliable information warfare metrics, defenders have veered in their fight against what RAND calls "truth decay" toward user trust generating solutions and an increase in platform responsibilities.[8] On the trust side, the aim is to change how information is consumed. Solutions range from increasing media literacy,[9] spreading user awareness on propaganda,[10] to providing easy access to open-source tools that fact-check items or rate entire news outlets on their trustworthiness.[11] On the platform end, the goal is to change how information moves. YouTube, for instance, demonetized and deleted accounts that feed into certain political narratives,[12] WhatsApp limited the number of users to which a single message can be forwarded,[13] and Facebook increased the visibility of political ads by disclosing their sources of funding.[14]

The limits of the current information-centered approach become apparent in a simple thought experiment. Let us assume that platforms are continuously "politically-cleansed" and the average user is "resilient." Instead of seeing beliefs and opinions move toward the political center, the overall political discourse outside the platform environment will most likely veer into the opposite direction and become more radical, divisive, and siloed. If we take the US, for example, the reasons for this negative trend are straightforward. First, audience mapping is showing repeatedly that the majority of "reliable" US news outlets are not seen to be situated in the political center. [15] Second, increased media literacy and higher education do not translate into apolitical and non-radical views. In fact, proponents of media literacy have long championed the notion that they actually encourage political engagement,[16] and a 2018 World Bank study based on leaked Islamic State records found that "higher education seems to be associated with high intrinsic motivation to join the terror group."[17] Third, political content moderation always creates winners and losers, particularly if it is leveraged against truthful content that has been reframed (i.e., is the glass half-full or half-empty?), or when it is purposefully exploited to push a political agenda. This can range from suspended Twitter accounts of Chinese political dissidents ahead of the 30th anniversary of the Tiananmen massacre[18] to activists feeding the social media outrage machine in an effort to push a platform to act beyond its community platform standards.[19] Lastly, while fake news and outright lies naturally struggle with limited shelf life and constrained reach, memes, rumors, and half-truths will never stop resonating with political beliefs, emotions, and prejudices held offline.

If the current defense posture does not push hard enough against the underlying information warfare dynamics, or worse, allows counter-productive results in the real world, can we think up a better way to fight back? Enter the Dr. House approach to information warfare.

Instead of focusing on information as the primary subject, Dr. House would take a social network analysis (SNA) point of view. This means, what matters most is not the message, image, or video posted, but the social network structure that moves the product. SNA has most notably been employed for counterterrorism and deradicalization purposes online, such as identifying ISIL users on Twitter and clustering related communities based on shared interactions.[20] SNA primarily uses open source information to display a network's structure as nodes (accounts) and edges (relationships) in line with graph theory to understand "how humans relate, communicate, and spread information."[21] While many different algorithms allow for visually ordering a network structure, two elements are considered standard measurement features: The number of edges of a node, which measures a node's network centrality, and how close a node is to other nodes measures a node's importance within the network.[22]

Once mapped, we can start thinking about network intervention strategies. Bargar, et al., identified four overarching techniques: (1) Identification techniques try to "engage actors in key positions in a network for training or messaging, with the expectation that their actions will impact the overall network." (2) Segmentation techniques are used to "intervene with an echo chamber as a collective set so all actors receive content simultaneously." (3) Induction techniques aim to "reframe a narrative by actively encouraging people to communicate with each other." And (4) alteration techniques seek to "modify a network structure by adding or deleting [edges] and/or nodes."[23]

All four techniques have one aspect in common: they seek to make the network healthier and less radical while respecting the user/patient rights. The Dr. House approach does the opposite. It wants to make the network sicker and sicker to the point of inducing cardiac arrest. In this context, user/patient rights do not matter, and finding a cure is merely the cherry on top. As Dr. House would put it, "Don't do what a patient wants. Do what a patient needs."

A second mental hurdle Dr. House throws out the window is the notion that to fight lies one must tell the truth. Facts against fiction, or a push for transparency and openness, are not the ingredients for a winning strategy in the information warfare space. Study after study has proven that lies travel faster than truths,[24] that fact-checking websites confront the same onslaught of disaffection and distrust that plagues "reliable" news outlets,[25] and that bursting echo chambers will most likely entrench partisan views rather than reduce biases and prejudices.[26] At its heart, the evidence points in only one direction: Facts do not create reality, and the information warfare space is an offense-dominant domain. Staunchly defending the truth perimeter is simply not going to cut it, because in the world of Dr. House "everybody lies. The only variable is about what."[27]

The third mental hurdle that needs to vanish is the idea of asymmetry. Contrary to popular belief, the information warfare space is not an asymmetric space. Anyone can hit any target anywhere. The only limiting factors are language skills, cultural familiarity, and social media penetration within the target network. Strategically, everyone, apart from the platform owner, plays on the same level battlefield. The story is a bit different when we talk about operations and tactics. Those who know their offline audience best essentially dominate the network online, which is why Alex Stamos, former Chief Security Officer at Facebook, noted that "if you look globally at disinformation campaigns, the median victim of a professional disinformation campaign is a victim of a campaign being run by their own government."[28] In the English-speaking online world, the reality is reversed primarily because democratic governments seldom can gain political and legal approval to run disinformation campaigns against their own populations. Consequently, non-state actors reign supreme in this space. 4Chan's /pol/ is probably the best example of an English-speaking online community that is both resilient on the defensive end, and able to mobilize the most sophisticated offensive information warfare teams out there. Nudging /pol/ in a certain direction is extremely difficult, as members are inherently suspicious that the CIA, Mossad, the FBI, or any number of activist groups from across the political spectrum tries to run rumors, propaganda, and lies on its platform. The tin-foiled hat is certainly not undeserved as /pol/ has been the birthplace of many conspiracy theories and executed numerous successful information warfare campaigns over its eight years of existence.[29] However, given that the community worships Christchurch shooter Brandon Tarrant as a martyr and saint,[30] turned milk and the "ok" sign into white supremacy symbols,[31] and considers itself to be the home of "the most diverse group of people from all over the world to fight against diversity and globalism,"[32] it should hardly come as a surprise that /pol/ is widely seen as the dark underbelly of the Internet.[33] But no matter your political views on the content posted on /pol/, when it comes to information warfare, learning from /pol/ probably means learning from the best. As a teenage patient explains to a third-year medical student on House's team, "At the top of the game, you play by different rules."[34]

The fourth point Dr. House would seek to exploit is the notion that information warfare operations are difficult to execute. A sophisticated campaign takes a lot of preparation, which is why simply firing off a single tweet and hoping it will stick and go viral within a target community is not the professional way to go. As The Grugq explains, "You need to do a lot of research, you need to have a lot of material. You need to prepare all the stuff. Get your narratives ready and then build up your channels. Get your credibility and so on."[35] State and non-state actors essentially go through the same tedious planning process whether their campaigns are malicious or not. The only major difference is how and when they leverage certain instruments and tools within their individual campaigns. Russia's Internet Research Agency, for instance, relied heavily on agitprop,[36] sock puppets, useful idiots, and hacked documents to run its campaign against the 2016 US Presidential Election.[37] /pol/ instead prefers to subvert existing beliefs and then let motivated individuals carry their products across the information space.[38] In late 2019, /pol/ ran a campaign that consisted of numerous A4 print-outs with the simple sentence "Islam is right about women" plastered around the sleepy town of Winchester, Massachusetts. Numerous local and regional news outlets naturally reported on the "incident," but clearly shied away from tackling the implied logic of the statement. Instead, Boston 25 News went on to report comically that "in Winchester, signs that read 'Islam was RIGHT about women' have residents scratching their heads to figure out exactly what the poster meant by those words. [...] 'I assume it's negative,' said Dorothy Kruger, a resident. 'That's not cool, that's not a cool thing to do."[39]

The only major exception to the planning rule encompasses spammers and scammers, who try to monetize disinformation campaigns based on sheer volume. That Nigerian prince trying to share his fortune with you if you just transfer a bit of money makes for a very effective campaign at scale, but is plain amateur hour when compared to a professionally run in-depth campaign. In House's words: "Welcome to the world. Everyone's different, everyone gets treated different. You try fighting that, you end up dying of TB."[40]

Turning now to the practical side of things, the Dr. House approach envisions a government agency, department, or state-affiliated actor to pro-actively defend society against information warfare campaigns in two ways.

The first option starts with mapping out networks and identifying possible adversarial campaigns. Importantly, the defender need not waste time and resources to conduct attribution or assigning political motivation as to why outrage is building around a specific issue or topic. The only relevant metric is whether the activity could potentially undermine national cohesion, break the civil political discourse, or threaten the overall functioning of society over time. If any of the three are met, the defender is mostly likely dealing with either a foreign state adversary or a motivated non-state actor. In both cases, the solution is to run an information warfare campaign on top of the adversarial one. Synchronize our nodes and edges with theirs, and gain centrality and importance within the existing network by being more extreme, but also qualitatively better, and quantitatively richer than anyone else in the network. By opening up the internal fight on network position, user mobilization, and content, we essentially take away the adversary's luxury of capturing the network unchallenged through mere radicalization tactics.

Once the combined network has reached a critical mass, the plan is for operators to burn down the barn with counter-messaging from the center out. The mathematical NP-hard problem that still needs to be solved to make this end game strategy successful is figuring out how many nodes and edges we would have to turn and burn to break a complex network into small, disconnected parts. Network science calls this the optimal network demolition problem,[41] which also closely relates to the yet unresolved optimal influence problem that tries to localize a specific set of structural nodes, that if activated, spreads the same information to every node in the entire network.[42] According to Patron et al., research has so far concentrated on three types of network demolition attacks: random attacks, targeted attacks, and localized attacks.[43] In a random attack, "the attacker has no information about the network, its topology, or characteristics" and thus choses a fraction of nodes to be randomly destroyed. Social media companies and political activists are currently practicing this approach in pretty much all of their cleansing campaigns. In a targeted attack, "the attacker has some information about the topology and the nodes of the network," and thus "determines which nodes to attack and in which order." Meanwhile, in a localized attack, "the attack begins against one node" and then continues against its neighbors, and the neighbors of its neighbors, and so forth, until a certain fraction of the network is destroyed.[44] For our purposes, it is important to note that the Dr. House approach does not attack at random and does not need to concern itself with the order of node destruction. A 2015 Nature article by Kovacs and Barabasi is probably the better approach for network destruction, as it speculates that "it is not certain whether targeting and removing network hubs – defined as the nodes with the largest number of [edges] – can inflict maximum disruption on a network. It may be more effective to eliminate a combination of hubs and central, but less-well-connected, nodes."[45] These are the exact target positions Dr. House would seek to occupy.

What might complicate matters for the defender is that the same adversary will probably move on different platforms simultaneously forcing the defender to create cascading demolition effects that concurrently attack specific networks across multiple platforms. However, what does play in the defender's favor is that he is not only searching for the optimal damage calculus, but also injects fear, uncertainty, and doubt into the network by his very action. If members cannot trust and believe in the messaging coming out of the most central and important nodes in one network, then whom else can they trust and believe in on other platforms? Thus, rather than spreading the truth and trying to convince the network to take on a certain belief, Dr. House would want all nodes to put on their tin foil hats. Question everything, doubt everything, double-check everything – taking media literacy to the extreme. Notably, destroying networks and belief systems in such a way is not tantamount to erasing an individual's ability to make sense of reality nor his desire to create new trust relations over time. Just because you question, doubt, and double-check everything does not mean that you do not believe or trust in anything.

The second option employs an even more aggressive tactic. Instead of mapping and identifying adversarial networks, a defender will proactively search for exploitable political, social, and economic cracks in his society. Thus, rather than letting a contentious issue grow organically over time, the defender runs an information warfare campaign preemptively into those cracks to create networks artificially, thereby fighting from a position of centrality and importance and forcing the adversary to latch onto and synchronize with this artificial network. If executed well, the defender might even enjoy the luxury of total visibility on the specific crack-issue, thus making mapping, nudging, and controlling the network much easier. On top of the network position advantage, this option also inserts doubts and uncertainty, forcing adversaries to continuously make cost-benefit calculations, and think twice before kicking off a tedious planning process and investing more scarce resources into radicalizing a network that might not be organically grown and is potentially controlled by a defender. The goal is to make an adversary so paranoid that he will doubt every action he takes in every network in which he operates.

One issue we have yet to tackle is where a government agency or non-state actor would get all the talent needed to run these vile and radical operations. The politically correct answer would be simply to hire people and train them in-house, but then again, how do you practically train someone to shitpost and express more radical thoughts than ISIL, the alt-right, and Antifa combined. The unconventional answer is to hire those who already wage information warfare for free in their spare time on platforms like 4Chan, Reddit, and Discord. Agencies would merely have to restrain and pull operators who lose themselves in the mission back into reality. There are even some ethical parallels that one could draw from how the cybersecurity community has embraced the hacker culture over the past decade. A similar transformation might be necessary in the information warfare space to fill the lack of talent, skills, and evil ingenuity.

In sum, today's thinking on information warfare self-curtails itself based on the misguided belief that "it's hard to fight fire with fire, especially when you can't use the same evil techniques, manipulations, and lies as the opposition employing propaganda against you."[46] The Dr. House approach is different. It is politically incorrect, violates numerous ethical standards, and is probably illegal in most states around the world. Maybe ... just maybe, though, it is time to give Dr. House a chance, because, as he argues in his own words, "I take risks, sometimes patients die. But not taking risks causes more patients to die, so I guess my biggest problem is I've been cursed with the ability to do the math."[47]

NOTES

1. Rob Owen, "TV Review: Hugh Laurie makes 'House' worth a visit," *Pittsburgh Post-Gazette,* November 14, 2004, https://web.archive.org/web/20081208154155/http://www.post-gazette.com/pg/04319/410715-237.stm.
2. Tom Shales, "House: Watching Is the Best Medicine," *The Washington Post*, November 16, 2004, http://www.washingtonpost.com/wp-dyn/articles/A53025-2004Nov15.html.
3. Paul Brownfield, "Obnoxious doctor in the 'House'," *The Los Angeles Times*, November 16, 2004, https://www.latimes.com/archives/la-xpm-2004-nov-16-et-house16-story.html.
4. House, Season 1, Episode 1: Pilot.
5. Office of Strategic Services, "Morale Operations Field Manual - Strategic Services," January 25, 1943, https://www.cia.gov/library/readingroom/docs/CIA-RDP89-01258R000100010002-4.pdf, 1.
6. Angelo M. Codevilla, "Political Warfare," in *Political Warfare and Psychological Operations–Rethinking the US Approach,* National Defense University Press–National Strategy Information Center, 1989, https://www.files.ethz.ch/isn/139664/1989-01_Political_Warfare_8-Chap.pdf, 77.
7. The Grugq, "After Action Reviews and Lessons Learned," *Medium.com,* December 3, 2018, https://medium.com/@thegrugq/after-action-reviews-and-lessons-learned-ec13218973c6.
8. Jennifer Kavanagh and Michael D. Rich, "Truth Decay – An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life," RAND Corporation, 2018, https://www.rand.org/pubs/research_reports/RR2314.html.
9. Marin Lessenski, "Common Sense Wanted – Resilience to 'post-Truth' and Its Predictors in the New Media Literacy Index 2018," Open Society Institute – Sofia, March 2018, http://osi.bg/downloads/File/2018/MediaLiteracyIndex2018_publishENG.pdf.
10. Jed Willard, "What Europe can teach America about Russian Disinformation," *The Atlantic*, June 9, 2018, https://www.theatlantic.com/international/archive/2018/06/what-europe-can-teach-america-about-russian-disinformation/562121/.
11. Issie Lapowsky, "Newsguard wants to fight fake news with humans, not algorithms," *Wired*, August 23, 2018, https://www.wired.com/story/newsguard-extension-fake-news-trust-score/.
12. Kelly Weill, "YouTube Crackdown on Extremism Also Deleted Videos Combating Extremism," The Daily Beast, June 6, 2019, https://www.thedailybeast.com/youtube-crackdown-on-extremism-also-deleted-videos-combating-extremism.
13. Jacob Kastrenakes, "WhatsApp Limits Message Forwarding in Fight against Misinformation," The Verge, January 21, 2019, https://www.theverge.com/2019/1/21/18191455/whatsapp-forwarding-limit-five-messages-misinformation-battle.
14. Rory Cellan-Jones, "Facebook Tool Makes UK Political Ads 'Transparent,'" *BBC News*, October 16, 2018, https://www.bbc.com/news/technology-45866129.
15. Nic Newman and Richard Fletcher, "Bias, Bullshit and Lies – Audience Perspectives on Low Trust in the Media," Reuters Institute for the Study of Journalism, 2017, https://agency.reuters.com/content/dam/openweb/documents/pdf/news-agency/report/nic-newman-and-richard-fletcher-bias-bullshit-and-lies-report.pdf, 19.
16. Paul Mihailidis and Benjamin Thevenin, "Media Literacy as a Core Competency for Engaged Citizenship in Participatory Democracy," *American Behavioral Scientist* 57, no. 11 (2013): 1611–22, https://pdfs.semanticscholar.org/8f26/be24b8669fe1a15832a5b9a4f96aa9db2790.pdf.
17. Mohammed Abdel Jelil et al., "Unemployment and Violent Extremism – Evidence from Daesh Foreign Recruits," World Bank Group, March 2018, http://documents.worldbank.org/curated/en/967561522155860057/pdf/WPS8381.pdf, 2.
18. Paul Mozur, "Twitter Takes Down Accounts of China Dissidents Ahead of Tiananmen Anniversary," *The New York Times*, June 1, 2019, https://www.nytimes.com/2019/06/01/business/twitter-china-tiananmen.html.
19. Jason Koebler and Mack Lamoureux, "YouTube Miserably Fails to Explain Why It Didn't Ban Steven Crowder," *Vice Motherboard*, June 5, 2019, https://www.vice.com/en_us/article/3k37yk/youtube-miserably-fails-to-explain-why-it-didnt-ban-steven-crowder-for-antagonizing-carlos-maza.
20. Elizabeth Bodine-Baron et al., "Examining ISIS Support and Opposition Networks on Twitter," RAND Corporation, 2016, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1328/RAND_RR1328.pdf.
21. Alicia Bargar et al., "Challenges and Opportunities to Counter Information Operations through Social Network Analysis and Theory," in *11th International Conference on Cyber Conflict: Silent Battle*, 231-48. NATO CCD COE Publications, n.d., https://ccdcoe.org/uploads/2019/06/CyCon_2019_BOOK.pdf, 232.

NOTES

22. Andrew Disney, “KeyLines FAQs: Social Network Analysis,” *Cambridge Intelligence,* December 3, 2014, https://cambridge-intelligence.com/keylines-faqs-social-network-analysis/.
23. Alicia Bargar et al., “Challenges and Opportunities to Counter Information Operations through Social Network Analysis and Theory,” In *11th International Conference on Cyber Conflict: Silent Battle*, 231– 48. NATO CCD COE Publications, n.d., https://ccdcoe.org/uploads/2019/06/CyCon_2019_BOOK.pdf, 245.
24. Soroush Vosoughi et al., “The Spread of True and False News Online.” S*cience* 359, no. 6380 (March 9, 2018): 1146–51, https://science.sciencemag.org/content/359/6380/1146.
25. Glenn Kessler, “Rapidly Expanding Fact-Checking Movement Faces Growing Pains,” *The Washington Post*, June 25, 2018, https://www.washingtonpost.com/news/fact-checker/wp/2018/06/25/rapidly-expanding-fact-checking-movement-faces-growing-pains/?utm_term=.cadbd8fa4317.
26. Carolyn Y. Johnson, “Bursting People’s Political Bubbles Could Make Them Even More Partisan,” *The Washington Post*, September 7, 2018, https://www.washingtonpost.com/science/2018/09/07/bursting-peoples-political-bubbles-could-make-them-even-more-partisan/?utm_term=.cd44d9170bb4.
27. House, Season 1, Episode 21: Three Stories.
28. Victoria Kwan, “Facebook’s Ex-Security Chief on Disinformation Campaigns: ‘The Sexiest Explanation Is Usually Not True,’” *First Draft News*, July 9, 2019, https://firstdraftnews.org/alex-stamos-interview-disinformation-campaigns/.
29. Ben Schreckinger, “World War Meme.” *Politico*, April 2017, https://www.politico.com/magazine/story/2017/03/memes-4chan-trump-supporters-trolls-internet-214856.
30. 4Chan /pol/, “Saint Tarrant,” *Archive.4plebs.org*, March 19, 2019, https://archive.4plebs.org/pol/thread/206981854/Tarant.
31. Joseph Bernstein, “The Trump Internet Keeps Making Fake Hate Symbols, And People Keep Falling For It,” *Buzzfeed News*, April 30, 2017, https://www.buzzfeednews.com/article/josephbernstein/the-trump-internet-keeps-making-fake-hate-symbols-and.
32. /pol/ Memeball, “When you bring together the most diverse group of people from all over the world to fight against diversity and globalism,” *KownYourMeme*, https://knowyourmeme.com/photos/1387762-picardia.
33. Gabriel Emile Hine et al., “Kek, Cucks, and God Emperor Trump: A Measurement Study of 4chan's Politically Incorrect Forum and Its Effects on the Web.” *ArXiv,* 2017. https://arxiv.org/abs/1610.03452, 1.
34. House, Season 7, Episode 19: Last Temptation.
35. Zack Pokorny, “The Grugq Illuminates Influence Operations,” *Recorded Future*, March 25, 2019, https://www.recordedfuture.com/podcast-episode-100/.
36. The Grugq, “Russian Propaganda Isn’t Even That Good,” *Medium.com*, November 8, 2018, https://medium.com/@thegrugq/russian-propaganda-isnt-even-good-c438f7d49902.
37. U.S. House of Representatives, “Exposing Russia’s Effort to Sow Discord Online: The Internet Research Agency and Advertisements,” Permanent Select Committee on Intelligence, n.d., https://intelligence.house.gov/social-media-content/.
38. 4Chan /pol/, “Operation Rainbow,” *Archive.4plebs.org*, April 24, 2017, https://archive.4plebs.org/pol/thread/122568047/.
39. Boston 25 News, “'Islam is right about women': Odd signs spark confusion in local town,” Boston 25 News, September 18, 2019, https://www.boston25news.com/news/-islam-is-right-about-women-odd-signs-spark-confusion-in-local-town/987837653.
40. House, Season 2, Episode 4: TB or Not TB.
41. Istvan A. Kovacs and Albert-Laszlo Barabasi, “Destruction Perfected.” *Nature*, August 6, 2015, 524 edition, https://www.nature.com/articles/524038a?proof=true&draft=journal.
42. Flaviano Morone and Hernan A. Makse, “Influence Maximization in Complex Networks through Optimal Percolation,” *Nature*, August 6, 2015, 524 edition, https://www.nature.com/articles/nature14604.pdf, 65.
43. Amikam Patron et al., “Optimal Cost for Strengthening or Destroying a given Network,” *Physical Review W* 95, no. 5 (May 2017). https://arxiv.org/pdf/1705.09930.pdf, 1.
44. Amikam Patron et al., “Optimal Cost for Strengthening or Destroying a given Network,” *Physical Review W* 95, no. 5 (May 2017), https://arxiv.org/pdf/1705.09930.pdf, 1.

NOTES

45. Istvan A, Kovacs and Albert-Laszlo Barabasi, “Destruction Perfected.” *Nature,* August 6, 2015, 524 edition, https://www.nature.com/articles/524038a.pdf?proof=true&draft=journal, 38.
46. Guy Bergstrom, “How to Defend Against Rumors, Lies, and Propaganda,” *The Balance Small Business*, February 18, 2019, https://www.thebalancesmb.com/defending-against-rumors-lies-and-propaganda-2295244.
47. House, Season 1, Episode 11: Detox.