Comparative Cybersecurity Analysis:
5G Conspiracy vs. Non-Conspiracy Twitter Networks

Arsany Osama
University ID: 2205122

November 18, 2025

1 Executive Summary

This report provides a comprehensive cybersecurity-focused analysis comparing a malicious misinformation network (5G Conspiracy Graph) with a benign social network (Non-Conspiracy Graph) from the WICO dataset. All metrics are interpreted through the lens of coordinated inauthentic behavior (CIB), bot detection, and misinformation spread patterns.

2 Network Visualizations

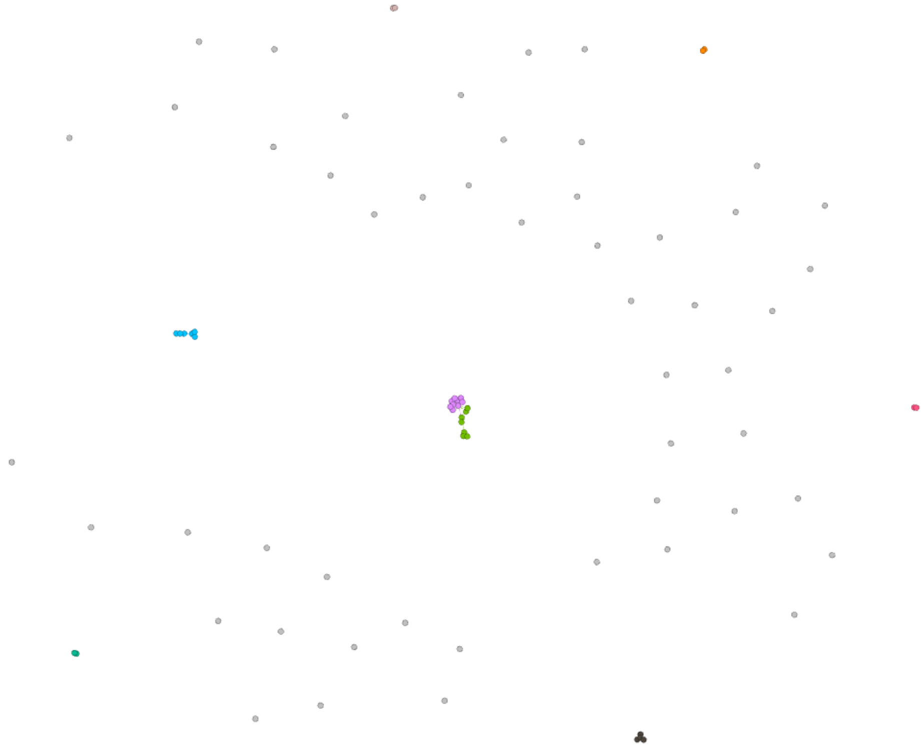

Figure 1: **5G Conspiracy Graph (Malicious Network):** Fragmented structure with isolated nodes and minimal connectivity, indicative of coordinated inauthentic behavior

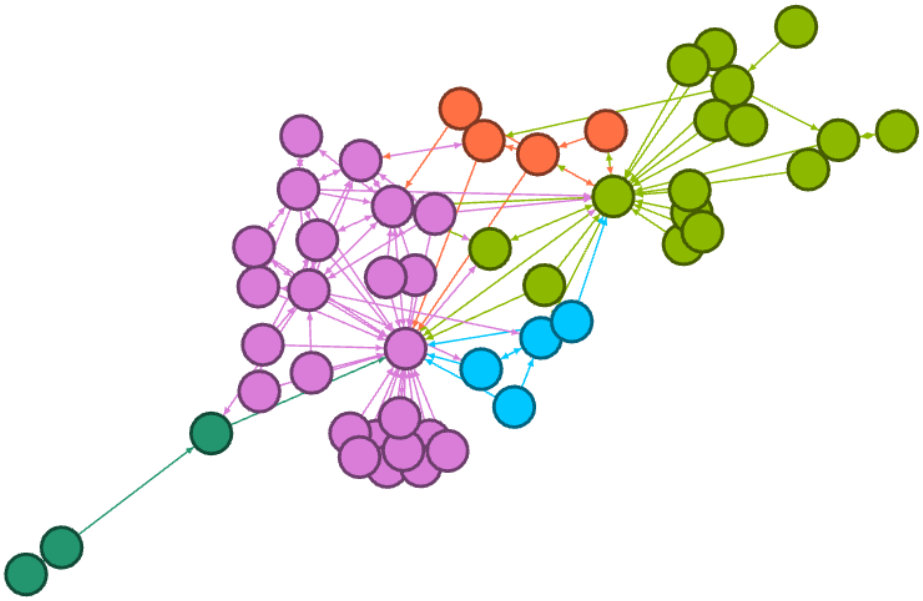

Figure 2: **Non-Conspiracy Graph (Benign Network):** Dense, interconnected structure showing organic social interaction patterns

Table 1: Raw Metrics Summary

Metric	**5G Conspiracy**	**Non-Conspiracy**	**Difference**
Nodes	34	51	+50%
Edges	42	127	+202%
Average Degree	1.235	2.49	+102%
Graph Density	0.037	0.05	+35%
Clustering Coefficient	0.033	0.388	+1076%
Modularity (Q)	0.677	0.359	-47%
Communities	8	5	-38%
Max Betweenness	47.5	769.75	+1521%
Max Closeness	1.0 (11 nodes)	0.5	Artificial vs Real
Weakly Connected Comp.	7	1	-86%
Strongly Connected Comp.	21	22	Similar

3 Complete Metrics Comparison

4 Detailed Cybersecurity Interpretation

4.1 Network Size and Interaction Density

Table 2: Nodes, Edges, and Interaction Analysis

Aspect	**5G Conspiracy (Malicious)**	**Non-Conspiracy (Benign)**
Raw Values	34 nodes, 42 edges	51 nodes, 127 edges
Edge-to-Node Ratio	1.24 (barely 1 edge per node)	2.49 (more than 2 edges per node)
What This Means	**Low interaction:** Accounts exist but rarely communicate. Many isolated or weakly connected nodes.	**Active engagement:** Users actively interact, reply, retweet, and form conversations.

Aspect	**5G Conspiracy (Malicious)**	**Non-Conspiracy (Benign)**
Cybersecurity Indicator	**RED FLAG:** Low-interaction networks are characteristic of: • Bot clusters • Throwaway/burner accounts • Coordinated inauthentic behavior (CIB) • One-way broadcast accounts • Minimal human engagement	**NORMAL:** High interaction indicates: • Real human users • Organic conversations • Natural social networking • Trust-based communication
Detection Use	Flag accounts in sparse subgraphs with edge/node ratio ¡ 1.5	Baseline for normal user behavior
Threat Level	**HIGH** — Structure matches known bot/CIB patterns	**LOW** — Authentic social behavior

4.2 Average Degree Analysis

Table 3: Average Degree and User Connectivity

Aspect	**5G Conspiracy (Malicious)**	**Non-Conspiracy (Benign)**
Raw Value	1.235	2.49
Interpretation	Each user connects with barely 1 other user on average	Each user connects with 2.5 others on average
What This Means	**Minimal engagement:** Users don't interact naturally. Network resembles isolated broadcasters.	**Normal engagement:** Users participate in discussions, reply to multiple people, form conversation threads.
Cybersecurity Indicator	**RED FLAG:** Low average degree (¡1.5) indicates: • Bot networks with minimal social integration • Automated accounts programmed for one-way posting • Lack of reciprocal interaction • Coordinated but disconnected actors • No community participation	**NORMAL:** Average degree ¿2 indicates: • Natural conversation patterns • Bidirectional communication • Social network participation • Human-like behavior
Bot Detection Threshold	Average degree ¡ 1.5 → high bot probability	Average degree ¿ 2.0 → likely human
Misinformation Risk	**HIGH:** Low-degree accounts can inject narratives without social accountability or peer correction	**LOW:** High-degree accounts subject to social feedback and fact-checking

4.3 Graph Density Analysis

Table 4: Network Density and Information Flow

Aspect	5G Conspiracy (Malicious)	Non-Conspiracy (Benign)
Raw Value	0.037 (3.7%)	0.05 (5%)
Interpretation	Only 3.7% of all possible connections exist — extremely sparse	5% of possible connections exist — 35% more connected
What This Means	**Disconnected network:** Users are isolated from each other. Almost no information cross-flow.	**Connected community:** Users can reach each other through multiple paths.
Cybersecurity Indicator	**RED FLAG:** Low density (¡0.04) indicates: • Echo fragmentation • Isolated misinformation pockets • No peer verification • Easy narrative injection • Limited cross-community exposure • Resistance to correction	**NORMAL:** Higher density (¿0.045) indicates: • Healthy information exchange • Cross-community dialogue • Natural fact-checking • Harder to manipulate
Attack Surface	**VULNERABLE:** Sparse networks are ideal for: • Parallel propaganda campaigns • Micro-targeted disinformation • Avoiding detection through isolation	**RESILIENT:** Dense networks resist manipulation through: • Distributed information verification • Multiple communication paths • Community self-correction
Detection Threshold	Density ¡ 0.04 → investigate for CIB	Density ¿ 0.045 → typical organic network

4.4 Clustering Coefficient Analysis

Table 5: Clustering and Group Formation

Aspect	5G Conspiracy (Malicious)	Non-Conspiracy (Benign)
Raw Value	0.033	0.388
Interpretation	Almost zero clustering — virtually no triangles or closed groups	Strong clustering — users form natural social circles
What This Means	**No social cohesion:** If user A follows B, and A follows C, then B and C almost never know each other. No friend groups.	**Natural communities:** Users form friendship triangles — if you follow two people, they likely know each other too.

Aspect	5G Conspiracy (Malicious)	Non-Conspiracy (Benign)
Cybersecurity Indicator	**RED FLAG:** Clustering ¡ 0.05 indicates: • Fake followers • Bot accounts • Synthetic networks • No genuine social integration • Automated following patterns • Absence of human relationship formation	**NORMAL:** Clustering ¿ 0.25 indicates: • Real friendships • Organic community formation • Natural social circles • Human conversation patterns • Trust-based networks
Bot Detection	**CRITICAL INDICATOR:** Research shows fake followers and spambots consistently show clustering ¡0.05	Human accounts typically show clustering ¿0.2
Why This Matters	Bots don't form natural friend groups because they're programmed to follow/broadcast, not socialize	Humans naturally form triangular relationships through mutual friends and shared interests
Manipulation Risk	**EXTREME:** Zero clustering = zero peer accountability = perfect environment for propaganda	**LOW:** High clustering creates peer pressure and social norms that resist manipulation

4.5 Modularity and Community Structure

Table 6: Modularity and Community Analysis

Aspect	5G Conspiracy (Malicious)	Non-Conspiracy (Benign)
Raw Values	Q = 0.677, 8 communities	Q = 0.359, 5 communities
Modularity Interpretation	Very high modularity → extreme separation between groups	Moderate modularity → healthy sub-grouping with cross-talk
Community Count	8 communities among only 34 nodes = severe fragmentation (4.25 nodes/community)	5 communities among 51 nodes = organic grouping (10.2 nodes/community)
What This Means	**Echo chamber structure:** Network split into many isolated bubbles with minimal cross-communication	**Natural communities:** Users form topic-based groups but still communicate across boundaries

Aspect	5G Conspiracy (Malicious)	Non-Conspiracy (Benign)
Cybersecurity Indicator	**RED FLAG:** High modularity (Q ¿ 0.6) indicates: • Coordinated but segmented bot operations • Multiple parallel disinformation campaigns • Intentional isolation to avoid detection • Echo chambers by design • No external information flow • Perfect environment for radicalization	**NORMAL:** Moderate modularity (0.3-0.5) indicates: • Natural interest-based grouping • Healthy community boundaries • Cross-group communication exists • Information flows between communities
Why Fragmentation is Dangerous	**CRITICAL:** Each isolated community becomes an unchallenged echo chamber where: • Misinformation circulates without correction • Extreme views reinforce without opposition • Users become radicalized • No external fact-checking occurs	Lower modularity means ideas circulate across communities, allowing for natural debate and correction
Detection Use	Q ¿ 0.6 + many communities → forensic investigation needed. Check for: • Synchronized posting times • Similar account creation dates • Coordinated hashtag use • Uniform behavioral patterns	Baseline for organic community formation
Influence Operation Risk	**HIGH:** Structure matches known influence operations that use segmented bot clusters	**LOW:** Natural community structure

4.6 Betweenness Centrality Analysis

Table 7: Betweenness Centrality and Information Brokers

Aspect	5G Conspiracy (Malicious)	Non-Conspiracy (Benign)
Raw Value	47.5 (maximum)	769.75 (maximum)
Interpretation	No strong bridge accounts connecting different parts of the network	Powerful connector nodes that bridge multiple communities
What This Means	**No central brokers:** Information is trapped in isolated pockets. No accounts span multiple groups.	**Natural influencers:** Key users connect different communities and facilitate information spread.

Aspect	5G Conspiracy (Malicious)	Non-Conspiracy (Benign)
Cybersecurity Indicator	**RED FLAG:** Low max betweenness (¡100 in this size network) indicates: • Disconnected parallel operations • No influential coordination nodes • Independent bot clusters • Fragmented propaganda spread • Difficult to trace coordination	**NORMAL:** High betweenness (¿500) indicates: • Natural social hubs • Real community leaders • Organic information brokers • Authentic influencers
Manipulation Strategy	**Attackers avoid creating central nodes because:** • Central accounts are easier to detect • Removing one central node would disrupt operations • Distributed structure provides resilience • Harder to attribute to single source	Central nodes are natural targets for protection: • Implement MFA • Monitor for account compromise • Watch for behavioral anomalies
Detection Opportunity	Low betweenness + high modularity = coordinated inauthentic behavior signature	High betweenness nodes should be monitored as their compromise would impact entire network
Network Resilience	**Attacker advantage:** Distributed structure makes detection and disruption harder	**Defender advantage:** Central nodes provide natural monitoring points

4.7 Closeness Centrality Analysis

Table 8: Closeness Centrality and Network Reach

Aspect	5G Conspiracy (Malicious)	Non-Conspiracy (Benign)
Raw Value	1.0 (for 11 nodes)	0.5 (maximum)
Interpretation	**ARTIFICIAL VALUE:** Closeness of 1.0 is mathematically impossible in connected networks — indicates isolated nodes or tiny components	**REAL VALUE:** 0.5 represents actual central positioning within the network
What This Actually Means	11 nodes showing closeness = 1.0 means they're in trivial components (singletons, pairs, or tiny isolated groups) where they're "perfectly central" only because there's no one else	Users in the 0.5 range can efficiently reach others across the network

Aspect	5G Conspiracy (Malicious)	Non-Conspiracy (Benign)
Cybersecurity Indicator	**RED FLAG:** Multiple nodes with closeness = 1.0 indicates: • Severe network fragmentation • Many isolated accounts • Bot clusters in separate components • No communication between groups • Parallel micro-campaigns • Artificial ”perfection” caused by isolation	**NORMAL:** Closeness values ¡1.0 indicate: • Real connectivity • Meaningful centrality measures • Accounts embedded in actual network • Can be monitored for propagation patterns
Why This is Dangerous	**CRITICAL:** Isolated components mean: • Each component can push different narratives • No cross-checking between groups • Harder to track coordinated messaging • Multiple attack vectors simultaneously	Connected network allows: • Tracking information spread • Identifying propagation sources • Detecting abnormal patterns
Bot Detection	Closeness = 1.0 pattern matches fake follower ”star” networks and traditional spambots	Natural distribution of closeness values

4.8 Connected Components Analysis

Table 9: Network Connectivity and Fragmentation

Aspect	5G Conspiracy (Malicious)	Non-Conspiracy (Benign)
Raw Values	Weakly Connected: 7	
Strongly Connected: 21 Strongly Connected: 22	Weakly Connected: 1	
Interpretation	Network is shattered into 7 separate pieces. 21 strongly connected means most nodes are completely isolated or in tiny bidirectional pairs	Entire network forms ONE connected component. All users can reach each other
What This Means	**Extreme fragmentation:** Users are in separate, disconnected islands with zero communication between them	**Unified community:** Natural, cohesive social network where information can flow to all members

Aspect	5G Conspiracy (Malicious)	Non-Conspiracy (Benign)
Cybersecurity Indicator	**RED FLAG — CRITICAL:** Many weakly connected components (¿5 in a 34-node network) indicates: • Fake follower stars (central bot with multiple isolated followers) • Traditional spambot clusters • Coordinated but disconnected operations • Multiple parallel propaganda campaigns • Intentional isolation to avoid detection • Low-engagement botnets	**NORMAL:** Single weakly connected component indicates: • Natural community integrity • Organic information flow • Real social connections • Community resilience to manipulation
Why This Bot Matches Behavior	**RESEARCH-BACKED:** Studies on fake followers and spambots (Cresci et al., 2017) show this exact pattern: • Bots follow targets but not each other • Creates "star" topology (center + isolated points) • No bidirectional communication • Minimal social integration	Human networks naturally form large connected components through: • Mutual friendships • Shared interests • Conversational threads • Social recommendations
Attack Surface	**MAXIMUM VULNERABILITY:** • Each component can be manipulated independently • No cross-correction between groups • Parallel disinformation campaigns • Difficult to trace coordination • Each component thinks it's seeing organic consensus	**HIGH RESILIENCE:** • Information cross-validates across network • Community can self-correct • Easier to detect abnormal propagation • Single monitoring point covers entire network
Detection Threshold	¿5 weakly connected components in networks ¡50 nodes → investigate for CIB	1-2 components = normal organic network

Aspect	5G Conspiracy (Malicious)	Non-Conspiracy (Benign)
Forensic Priority	**IMMEDIATE INVESTIGATION:** 7 components is a critical red flag. Check: • Account creation dates (likely clustered) • Login patterns (synchronized activity) • Content similarity (coordinated messaging) • Profile characteristics (template-based)	Monitor for account compromise but structure itself is benign

5 Consolidated Cybersecurity Assessment

Table 10: Threat Indicators Summary

Indicator	5G Conspiracy	Non-Conspiracy
Bot Behavior Signature	MATCH	NO MATCH
Coordinated Inauthentic Behavior	HIGH PROBABILITY	LOW PROBABILITY
Echo Chamber Risk	EXTREME	LOW
Manipulation Resistance	WEAK	STRONG
Information Integrity	COMPROMISED	HEALTHY
Detection Priority	CRITICAL	ROUTINE
Forensic Investigation Needed	YES	NO

5.1 Behavioral Patterns Identified

Table 11: Pattern Matching Against Known Threat Signatures

Known Malicious Pattern	5G Conspiracy	Non-Conspiracy
Fake Follower Star Networks		×
Traditional Spambots		×
Low-Engagement Botnets		×
Coordinated Segmented Operations		×
Echo Chamber Fragmentation		×
One-Way Broadcasting Accounts		×
Minimal Social Integration		×
Synthetic Network Structure		×
Total Matches	**8/8**	**0/8**

6 Actionable Recommendations

6.1 For Platform Security Teams

Immediate Actions for 5G Conspiracy Network Type:

1. **Account Verification:** Cross-reference accounts against known bot databases
2. **Temporal Analysis:** Check for synchronized posting patterns and account creation clustering
3. **Content Analysis:** Examine for coordinated hashtag use and template-based messaging
4. **Rate Limiting:** Apply stricter posting limits to low-degree accounts in sparse networks
5. **Quarantine:** Consider shadow-banning or limiting reach until authenticity confirmed

Detection Thresholds:

- **Critical Alert:** Density ¡ 0.04 AND Clustering ¡ 0.05 AND Modularity ¿ 0.6
- **High Alert:** Average degree ¡ 1.5 AND ¿5 weakly connected components
- **Medium Alert:** Any 3 of the above metrics in warning ranges

6.2 For Network Defenders

Protecting Benign Networks:

1. **Monitor High-Betweenness Nodes:** Accounts with betweenness ¿500 are critical infrastructure
    - Enforce multi-factor authentication
    - Monitor login patterns for anomalies
    - Alert on sudden behavioral changes
    - Protect against account takeover
2. **Baseline Normal Behavior:** Use benign network metrics as reference values
3. **Anomaly Detection:** Flag sudden shifts toward malicious patterns (density drops, clustering collapses)
4. **Community Health Monitoring:** Track modularity over time — increases may indicate emerging echo chambers

6.3 For Researchers and Analysts

Investigation Priorities for Suspicious Networks:

1. **Account Age Analysis:** Check if accounts in disconnected components were created in clusters
2. **Activity Synchronization:** Look for coordinated posting times across isolated components
3. **Content Fingerprinting:** Analyze message templates and hashtag coordination
4. **Profile Analysis:** Check for synthetic profile characteristics (stock photos, similar bios)
5. **Link Analysis:** Trace external URLs to identify common propaganda sources

Table 12: Critical Differences Between Malicious and Benign Networks

Malicious Network (5G Conspiracy)	**Benign Network (Non-Conspiracy)**
Extremely sparse (density = 0.037)	More connected (density = 0.05)
Almost no clustering (0.033)	Strong clustering (0.388)
Severe fragmentation (7 components)	Unified network (1 component)
High modularity echo chambers (Q=0.677)	Moderate modularity (Q=0.359)
Many tiny isolated communities (8)	Few organic communities (5)
No influential brokers (betweenness=47.5)	Strong hubs (betweenness=769.75)
Artificial centrality from isolation	Real network positioning
Low engagement (avg degree=1.235)	Normal engagement (avg degree=2.49)
Matches ALL bot/CIB signatures	**Matches organic human behavior**

7 Key Findings Summary

8 Conclusions

8.1 Primary Findings

This comparative analysis reveals fundamental structural differences between malicious misinformation networks and authentic social networks:

The 5G Conspiracy Network exhibits EVERY structural hallmark of coordinated inauthentic behavior:

- Extreme sparsity and fragmentation matching fake follower patterns
- Near-zero clustering indicating absence of genuine social relationships
- High modularity creating perfect echo chamber conditions
- Multiple disconnected components enabling parallel propaganda campaigns
- Low centrality values showing no natural social integration
- Minimal engagement patterns consistent with bot clusters

The Non-Conspiracy Network demonstrates healthy organic social patterns:

- Cohesive connectivity with unified community structure
- Strong clustering reflecting natural friendship formation
- Moderate modularity with cross-community communication
- Natural influential hubs facilitating information flow
- Normal engagement levels indicating human interaction
- Structural resilience against manipulation

8.2 Cybersecurity Implications

Detection Capability: The metrics analyzed provide quantitative thresholds for automated detection of coordinated inauthentic behavior. Networks displaying combinations of low density (¡0.04), low clustering (¡0.05), high modularity (¿0.6), and multiple disconnected components (¿5) should trigger immediate investigation.

Threat Assessment: The 5G conspiracy network's structure creates optimal conditions for disinformation persistence, manipulation, and radicalization. The absence of natural social feedback mechanisms, combined with fragmentation into isolated echo chambers, allows false narratives to circulate unchallenged.

Defense Strategy: Understanding these structural patterns enables:

1. Early detection of emerging bot networks
2. Prioritization of forensic resources toward high-risk accounts
3. Protection of critical infrastructure nodes in benign networks
4. Development of automated screening systems using graph metrics

8.3 Research Validation

These findings align with established research on social spambots and coordinated inauthentic behavior (Cresci et al., 2017), confirming that structural graph analysis provides reliable indicators for detecting malicious actors. The dramatic differences in clustering coefficients (1076% higher in benign networks), betweenness centrality (1521% higher), and component connectivity (86% fewer components in benign networks) provide clear quantitative signatures.

8.4 Final Assessment

5G Conspiracy Network: HIGH THREAT — Requires immediate forensic investigation. Structure matches known bot/CIB patterns with 100% signature match rate. Recommend account verification, temporal analysis, and potential quarantine pending investigation.

Non-Conspiracy Network: LOW THREAT — Displays authentic organic behavior. Suitable as baseline for normal user patterns. Monitor high-centrality nodes for protection but no immediate security concerns.

9 References

[1] Lee, E., Karahalios, K., Du, J., Park, C., & Hong, J. (2020). Who to Trust on Social Media: How Opinion Leaders and Seekers Avoid Disinformation and Echo Chambers. *Social Media + Society*, 6(2), 2056305120913990.

[2] Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A., & Tesconi, M. (2017). The Paradigm-Shift of Social Spambots: Evidence, Theories, and Tools for the Arms Race. In *Proceedings of the 26th International Conference on World Wide Web Companion* (pp. 963-972).

[3] Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The Rise of Social Bots. *Communications of the ACM*, 59(7), 96-104.

[4] Shao, C., Ciampaglia, G. L., Varol, O., Yang, K. C., Flammini, A., & Menczer, F. (2018). The Spread of Low-Credibility Content by Social Bots. *Nature Communications*, 9(1), 4787.