Kellen Myers[1,2] / Ashley DeNegre[3] / Lazaros Gallos[4] / Natalie Lemanski[1,3] / Alexander Mayberry[3] / Agnesa Redere[3] / Samantha Schwab[3] / Oliver Stringham[3] / Nina H. Fefferman[1,2,5]

Dynamic *Ad Hoc* Social Networks in Improvised Intelligence/Counter-Intelligence Exercises: A Department of Homeland Security Red-Team Blue-Team Live-Action Roleplay

[1] University of Tennessee, Department of Ecology and Evolutionary Biology, Knoxville, TN, USA, E-mail: nina.h.fefferman@gmail.com. https://orcid.org/0000-0003-0233-1404.
[2] University of Tennessee, Department of Mathematics, Knoxville, TN, USA, E-mail: nina.h.fefferman@gmail.com. https://orcid.org/0000-0003-0233-1404.
[3] Rutgers The State University of New Jersey, Department of Ecology, Evolution, and Natural Resources, New Brunswick, NJ, USA
[4] Rutgers The State University of New Jersey, Center for Discrete Mathematics and Computer Science (DIMACS), New Brunswick, NJ, USA
[5] Rutgers The State University of New Jersey, Center for Command Interoperability Control and Data Analysis (CCICADA), New Brunswick, NJ, USA, E-mail: nina.h.fefferman@gmail.com. https://orcid.org/0000-0003-0233-1404.

Abstract:
We discuss a Red Team-Blue Team (RT-BT) study conducted to examine the formation and efficacy of social networks in self-organizing, *ad hoc*, or crowd-sourced intelligence and counter-intelligence operations in grassroots, improvised communities. Student volunteers were sorted into two teams: one team (Blue) was asked to find puzzle pieces using clues provided by the organizers, with the goal of reconstructing a message contained therein, while the opposing team (Red) was tasked with disrupting this process. While the Blue Team quickly organized into an efficient, centrally-governed structure, the Red Team instead adopted a decentralized, distributed operational network to hinder puzzle completion, using creative and diverse infiltration and disruption methods to interfere in the more centralized, hierarchical organization of their opponents. This exercise shows how untrained, unaffiliated individuals may self-organize into different types of social organizations to accomplish common tasks when aware of potential adversarial organizations, and how these choices may affect their efficacy in accomplishing collaborative clandestine goals.

Keywords: clandestine networks, communication networks, counterintelligence, counterterrorism, emerging organization, emerging social network
DOI: 10.1515/jhsem-2018-0027

1 Introduction

Industrial organizational theory dictates, and evidence bears out, that particular community structures lend themselves to efficiency and efficacy for various types of operations. While many businesses and agencies have the luxury of purposefully structuring their operational and social networks in aid of their organizational goals (Argyris 1960; Hersey and Blanchard 1993; Mishra 1996; Organ 1988), grassroots organizations, by definition, do not. It is therefore of great importance to understand the networks that arise from *ad hoc*, self-organized communities, (Brabham 2008) particularly in security and intelligence scenarios (Monahan and Mokos 2013; Tewksbury 2012). How these individuals self-organize is likely to have a major impact on the operation of the group, not only in the trivial sense that the functions of the group occur within some ambient group structure, but ideological and decision-making matters may be determined by the group structure. Strengths and weaknesses of the operation may be evident in the structure of the social network. Understanding the structure of such emergent cooperative networks is of particular importance in efforts to disrupt the activities of militia and terrorist groups.

Nina H. Fefferman is the corresponding author.

In addition to the abstract notion of social networks, technologically enabled social media forums, like Twitter and Facebook, act as communications systems, networking platforms, and data repositories. A number of significant events like the Arab Spring have proven that such media can be used effectively, and in novel fashion, to self-organize not just small activities and operations, but major political and social movements.

In defense and security applications, decentralized social networks may be sensitive to disruptions and may allow for detection and response to anomalies and events in real-time. (File et al. 2012) It is possible to leverage untrained assets for intelligence-gathering activities effectively, due to the diffuse and distributed structure of the social network and communication avenues provided by online social media platforms (Tang et al. 2011; File et al. 2012).

We present here the results of a study of a Live-Action Role-Playing game (LARP) in which participants were asked to engage in an intelligence/counter-intelligence exercise. To study how untrained teams of civilians might self-organize into clandestine groups, we designed an experiment following the paradigm of Maker-Breaker gameplay, (Erdős and Selfridge 1973; Hefetz et al. 2014) in which one team (designated "Makers") is tasked with solving a puzzle of some kind, while the other team (designated "Breakers") is tasked with preventing the first team from achieving its goal. To avoid exploitation of meta-knowledge about game structure, teams were designated only as the "Blue Team" (Makers) and the "Red Team" (Breakers). In our experimental LARP design, we asked the Blue Team to collect puzzle pieces from hidden locations using clues provided by the study administrators. Communication between participants was collected to examine how each team's strategy was affected by their communication and organizational decisions and the resulting emergent team structure. In particular, we studied whether this organizational structure or the communication methods impacted each team's efficiency and effectiveness. In this way, we build on the diverse literature that has separately considered elements of related questions, including self-organization (Fuchs 2003; Heylighen 2013; Linsker 1988; Van Dyke Parunak and Brueckner 2001), particularly in social movements (Fuchs 2006; Ulrich and Probst 2012); social network analysis (Borgatti et al. 2009; Carrington, Scott, and Wasserman 2005; Sabater and Sierra 2002; Wang et al. 2007; Wasserman and Faust 1994), including specific studies of organizational (Tichy, Tushman, and Fombrun 1979) and criminal/intelligence-related networks (Chen et al. 2005; Coffman, Greenblatt, and Marcus 2004; Koschade 2006; Sparrow 1991); organizational behavior (Argyris 1960; Hersey and Blanchard 1993; Organ 1988), particularly with respect to decentralization (King 1983; Mishra 1996); operational and communication efficiency (Garicano and Posner 2005; Marschak and Reichelstein 1998); and technology-enabled organization (Huber 1990; Nilles 1975; Zammuto et al. 2007), specifically in social movements (Agarwal et al. 2014; Gulledge and Haszko 1996).

These studies have helped us understand how self-organization accounts for internal and external effects, as well as structural and active aspects of social movements (Fuchs 2006), particularly in a technology-aware population using decentralized social media platforms (Agarwal et al. 2014; Gulledge and Haszko 1996), and the ways in which a theoretical framework of this type can account for the coalescence of a collective communication, decision-making, and intelligence (Heylighen 2013). We have seen analyses of criminal (Sparrow 1991) and terrorist (Koschade 2006) networks, indicating that centrality within communications network is a key to understanding these groups' organization.

However, there are still unanswered questions about how untrained actors might participate in activities like intelligence gathering or other security operations would form their own *ad hoc* communications networks, and in particular how the structure of those networks impacts the groups' effectiveness at accomplishing tasks and how the choice of social media influences or is influenced by this network structure.

The insights from these fields and studies have allowed us to assemble an understanding of the importance of self-organization and network organizational strategy, but to the best of our knowledge, no study has yet considered how motivated-but-untrained individuals might self-organize to accomplish complicated, time-sensitive, collaborative tasks. Where would such groups fall in the scope of the academic predictions for emergent structures and operational efficiency?

To accomplish this, the study presented was designed specifically to provide data on how *untrained and initially unstructured groups* are likely to self-organize. It is not our goal to replicate or recreate the organization of preexisting intelligence agencies or any subset thereof, nor to understand self-organization among agents and assets of such agencies with specific grounding in agency doctrine or intelligence training. To the contrary, we hope to understand better precisely how those without such training or doctrine will self-organize, specifically with an eye towards the completion of a complex set of tasks and with an awareness of their use of digital platforms and social media.

In order to understand how different types of social media/communication platforms affect the organization of these teams, we considered several particular questions. Do these platforms support grassroots/crowdsourced networks of actors? Are there gaps in the capabilities of these new technologies that can be filled (or exploited)? How do *ad hoc* networks organize themselves over a social media platform? Do groups assemble

and communicate differently depending on their goals? Do social networks evolve differently over time or depending on progress towards goal completion?

We found, generally, that the Blue Team, using a Facebook group page, formed a centralized network, while the Red Team, using the group-texting app GroupMe, operated as a decentralized set of agents, enabling dynamic and creative responses to operational challenges, successful infiltration of the Blue Team, and victory in the LARP exercise.

2 Methods

The LARP exercise was conducted over a one-week period, April 20–25, 2015. Participants were recruited from the student body at Rutgers University through on-campus advertising and word-of-mouth. Volunteers were asked to apply to participate either as individuals or as groups of friends, so that friends could be assigned to the same team. Applicants were asked to self-report how they heard about the experiment and if they were aware of the identity of any other volunteers. An effort was made to construct the groups so that, even among those who did not volunteer as a group, acquaintances were not on opposing teams, to avoid giving such individuals additional knowledge – if a friend is known to be participating, and that friend is not assigned to one's team, one may conclude that the friend is a known opponent.

The Blue Team was instructed that its goal was to collect puzzle pieces based on clues from the "Ideological Leader" – the in-game persona of the study administrators. The Red Team was instructed to disrupt the Blue Team's attempt to solve the puzzle.

The puzzle itself was an oversized jigsaw puzzle, where the image was a still-frame from the movie *Spaceballs* (Brooks 1987), constructed such that each piece bore a letter and assembling the puzzle reconstructed a "secret message." The Blue Team was given the following winning condition: They win the LARP by delivering this secret message to a particular location at the end of the week of game-play. The secret message was a short quotation from the film *Jumpin' Jack Flash* (Marshall 1986). We will refer to this end-of-exercise meeting as the "Jigsaw Assembly."

Study administrators were identified collectively in-game as the "Ideological Leader," providing information directly to participants. Clues about the location of puzzle pieces were provided by email to a subset of the participants (including some from each team). This subset was selected on a rotating basis, changing daily. Some clues were hiding in public areas, e.g. behind books on a shelf in a University library, while others were held by helpful non-player individuals, e.g. a (Name of Large, Public Institution) staff member in his/her office, requiring a password that was included in or suggested by the clue.

The Blue Team was constructed to be slightly larger than the Red Team, with 25 Blue vs. 19 Red, meant to approximate the asymmetry of real-life scenarios where there are unlikely to be even numbers of individuals acting on behalf or intelligence agencies or organizations as there are being recruited to act with grassroots or cellular movements. At the commencement of the LARP exercise, participants were informed of their team affiliation, as well as the name of two teammates and one opponent. However, this did not expose the entirety of each team to its opponents – half of the Blue Team and one fifth of the Red Team were chosen to be exposed, and one of those names was randomly selected (with repetition) to be revealed to a player on the opposing team.

Participants' in-game communication was restricted either to technologically-enabled social media and similar platforms, or else to in-person communication. These included social media/networking websites (e.g. Facebook Events/Groups, Twitter, Instagram, Reddit), feed-based websites (e.g. Tumblr, Instagram), and direct person-to-person messaging (e.g. text message, GroupMe, Snapchat, email, face-to-face conversation). All conversations either included the study administrators or else were logged and reported to the Ideological Leader's email at the end of each day. Players, individually or as teams, were free to use any medium or platform (or combination thereof) freely, and they were free to either choose platforms to reflect their organization or to organize according to their preferred platform.

Although players were not required to meet daily, to encourage consistent and regular engagement, for each day three different dinner locations were selected: one for each team at 7PM ("team dinner") and one for both teams together at 9PM ("late dinner"). Dinner was provided at all three locations by study administrators. Each morning, two members of each team were given the location of their own team's individual dinner that evening, and teams were required to coordinate the distribution of this location in order to meet. All individuals were provided the location of the "late dinner." The availability of "late dinner" was not only for participants who might have missed their team's dinner to eat, but also to allow for strategic attendance by players who might be identified by the opposing team, or to allow any number of other strategies related to interaction with the opposing team. Players were not required to attend these meetings, and it was possible for a player to

move between these meetings. There was no restriction on which dinner a player could attend, including the opposing team's dinner.

Participants were restricted by a number of (voluntary) behavioral ground-rules, in order to maintain the integrity of the study and ensure the safety of participants. Players could not use money to accomplish the teams' objectives – neither buying any items that may be useful, nor paying any individuals within or outside the participant group for information or assistance. Participants' interactions were restricted to fair play only: no adversarial physical contact, threats of such contact, or emotional intimidation were allowed. In-game communication was limited to exercise-related information to allow clear and firm separation from other aspects of students' day-to-day lives apart from the exercise. No cases of violation of these policies were noted.

Additional criteria for judging the performance of the two self-organizing groups were as follows: the number of pieces collected by each team and delivered to the Jigsaw Assembly; the number of each team who attended the Jigsaw Assembly; the Blue Team's successful delivery of some or all of the secret message; and, how many Red players were identified by the Blue Team throughout the week.

Other end-of-exercise information that would not necessarily indicate the success of the Blue Team directly, but of particular interest, includes the number of Blue players identified by the Red Team and the number of players on each team that successfully infiltrated the opposing team, either for the entirety of the study or even just for a short time.

After the conclusion of the LARP, we analyzed communication and social media usage information to answer the following questions: What types of communication are used? How are they used? (Does usage vary by team, by medium, by message?) Did players identify any limitations of a medium? Did we observe any such limitations? Did players use technology in unanticipated ways? How did these social media and communication platforms affect the outcome of the LARP?

To analyze the emergent organizational networks, we first identified the primary mode of communication for each team: The Blue Team organized through a private Facebook group page, while the Red Team relied on group texting through the mobile app GroupMe. Note that this was not a single long group text for the entire Red Team, but rather, a series of texts between different subsets of the Red Team throughout the LARP exercise. In addition, each team had a small number of in-person meetings (in addition to the daily dinner meetings) and a few messages through a different electronic medium, mainly direct email. Most of these in-person and email interactions were between members of the Red Team; none of the Blue Team's electronic communication occurred outside the Facebook page.

Communication records for teams' conversations on Facebook and GroupMe were collated to reconstruct a social media/communication network in a way that allows direct comparison of the datasets for the two teams. The network structure was extracted as follows: players' messages occur one-by-one in both Facebook and GroupMe. Assuming that most messages are meant to respond most directly to the previous message, we create a link between these two players. (One person posting more than once in a row is considered to be just one longer message.) The links between each player are weighted such that the connection between players who respond frequently to each other have greater weight.

Reports from players of in-person conversation and other media were added manually – increasing the weight of each link for each such message.

Note that talking about an individual does not result in any link being formed with that individual. Only the two players exchanging messages in response to one another are linked.

We measure the organization of each network by examining the frequency of communication from each individual (total, and per teammate). We also measure the betweenness centrality of each node. Betweenness centrality is defined in a somewhat straightforward way. It measures the centrality of a vertex – how much this vertex is at the center of this graph – with respect to betweenness. For a particular vertex v, in the following way: we consider all possible pairs of other vertices, say u and w, and look at the shortest path from u to w. We credit v with one unit of betweenness centrality if v is on this path for each (u, w) pair. If there are multiple shortest paths for some (u, w), we give v partial credit depending on the portion of shortest u – w paths that contain v. This is then normalized to reflect the total number of individuals in the network.

It is also possible to examine the structure of the network over time, considering the potential for dynamic network structuring and restructuring.

In addition to the structure of the social network, the dynamics of player interactions on those networks, and the nature of the two networks, require careful consideration. There are major differences between the use of Facebook and GroupMe, in the organization of the network in measures of centrality or frequency of communication. The attendance at team dinner meetings, as well as the content of those meetings, also varied.

3 Results and Discussion

Communications records for the Blue Team spanned the entire 6-day exercise, while the Red Team did not begin collaborative efforts in earnest until the third day, preferring instead to work individually after making initial contact with each other. Hence, our first significant study-wide observation is that the Red Team did not immediately organize itself in a consistent, structured way on any particular platform. The first 2 days consisted of sporadic in-person meetings and one-to-one contacts, and in fact, the Red Team was not entirely sure of its objectives for the first 2–3 days – several Red players misunderstood the objectives and believed they were charged with completing the puzzle before the Blue Team did so, rather than disrupting the Blue Team's efforts.

Another aspect of in-person meetings, particularly outside the scheduled dinners, was the designation and use of a "safe house" by the Blue Team. This safe house was a reflection of the centralized organization of the Blue Team – holding meetings, storing puzzle pieces, and centralizing the team's operations. This proved to be a significant vulnerability when the Red Team infiltrated their operation and used this safe house as a target for intelligence gathering.

Additionally, infiltration played a major role in this exercise. Having a mole with access to communication, team meetings, or the puzzle pieces themselves provides a team with a major advantage. In this study, a member of the Red Team successfully infiltrated the Blue Team from almost the very beginning of the LARP exercise, and this player was never outed as a mole. In addition to the mole, the Red Team also wound up using its knowledge of the Blue Team's activities to coordinate undetected subterfuge as a part of their successful strategy.

On the other hand, the Blue Team attempted and failed to infiltrate the Red Team. The hopeful infiltrator was asked to confirm her identity by presenting group-only emails and could not do so. Her attempt to persuade the Red Team players at that particular team meeting with spoofed versions of the communication in question (using screenshots but insisting she could not access the email itself due to a forgotten password) were unsuccessful.

The presence of an undetected mole allowed the Red Team to execute a highly-effective strategy, obtain puzzle pieces, and gain the strategic upper hand. Indeed, they used this advantage to deliver what would be the final blow to the Blue Team. In order to make the best use of their puzzle pieces, the Red Team manipulated the textual content on one of the puzzle pieces. Using the mole, the piece was delivered to the Blue Team as if it were stolen from the Red Team, a fiction they took at face value (and, indeed, celebrated). Unfortunately, this alteration was accomplished before either team determined that the text of the puzzle pieces would together form a plain-text sentence.

The Red Team's success in spite of this oversight came from its ability to adapt to novel challenges in real-time. When the Blue Team discovered they needed to reconstruct a message contained in the puzzle, the Red Team found out too, via the mole. Having unknowingly altered part of that message, they realized the Blue Team would discover the alteration as soon as the final message was found to be incoherent due to this alteration. In response to this new information, they designed a substitution cipher that would translate the (altered) text on the puzzle pieces (known to them through the mole) into a message other than the correct solution. Using a fake email address that closely resembled the actual email address of the Ideological Leader (i.e. they spoofed the email address of the study administrators), the Red Team transmitted a series of messages including instructions to decode their cipher.

This spoofed email and altered puzzle piece lead to the Red Team's victory in the exercise. The Blue Team used the altered puzzle piece to construct the incorrect secret message, precisely as reverse-engineered by the Red Team. Both teams attended the Jigsaw Assembly. The Blue Team appeared to be confident that they had successfully determined the secret message, but they instead presented the spoofed message. The Red Team then announced their successful subterfuge, and the study administrators declared them the unambiguous winners of the exercise.

The Red Team's victory came from a number of strategic choices, and the success of these choices depended on a few factors related to group structure and function. The Blue Team's choice of Facebook provided an avenue for deception: the mole who infiltrated the Blue Team unfriended all the Red players on his Facebook profile – easily providing cover in case any of those friends had been identified as members of the Red Team, and insulating the team should the mole be exposed. The Red Team also spoke openly about the mole with no fear of being overheard or themselves infiltrated – the mole was codenamed "Felicity," which convinced the Blue Team that the mole was female. (He was male.) He was never discovered and was considered credible by the Blue Team.

This was not the only identity-based deception. When members of the Blue Team first identified a Red Team member, he was identified (correctly) by only his first name, not appearance. His name is one that is not common and did not indicate clearly to anyone on the Blue Team whether he was male or female. The Red Team circulated a new strategy based on this encounter, and individual members of the Blue Team accepted

this name as the name of any Red player they encountered, male or female, and made no effort to verify the individual's identity or collect additional information. They were not aware that they had discovered a number of previously unknown opponents – each Blue player believing in the moment that it was the individual their team had already identified.

In addition to the apparent structural advantages of decentralized organization, the Red Team required some creativity to properly capitalize on the advantages of a more dynamic, *ad hoc* operation. In addition to successful infiltration, the Read Team engaged in significant, coordinated acts of deception. *They may have been decentralized, but that does not mean they were disorganized.* While this observation is not new, we have demonstrated in this exercise that it can play out even among *ad hoc*, self-organized groups of untrained individuals.

In discussing electronic communication platforms, first and foremost, the choice of social network and communication platform itself is very significant. A Facebook group page provides a convenient centralized location for organizing events, communicating with a group, and logging group activities and communication. The use of text messaging (through GroupMe or any other similar service) allows for communication that is decentralized, selective, secretive, compartmental, and dynamic. It allows communication with the entire group or with only a particular subgroup.

This is very strongly reflected in the network structure of the two teams. The Blue Team is extremely centralized. A leader node clearly emerges in the network, and the activity of the team focuses almost exclusively around the Facebook page and the *de facto* group leader. The central individual acts as a sort of unilateral organizer of the Facebook page, and thus of the team itself. The Red Team was much the opposite, displaying significant decentralization. The network structure of both teams is visualized in Figure 1. Note the central node (13), as well as the mole (6), in the Blue Team's network.

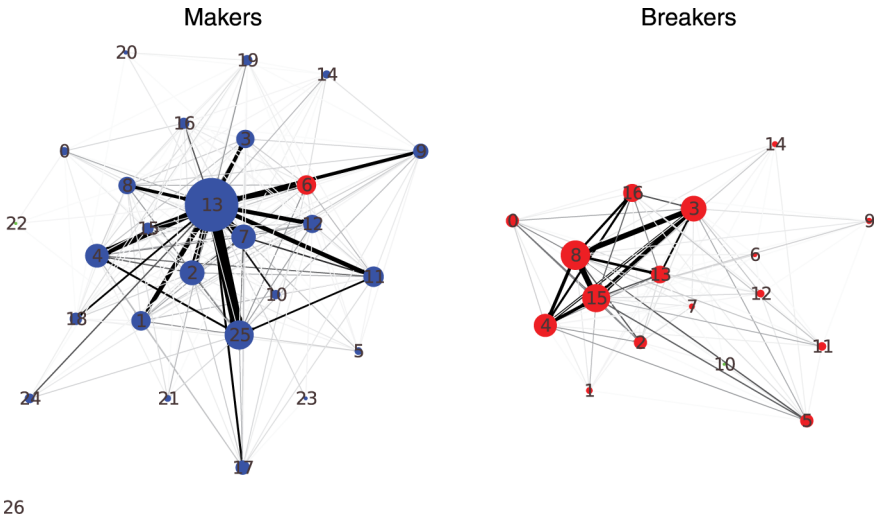

Figure 1: Network Structure of Blue (Left) and Red (Right) Teams for the Entire Study Period, using Data from Facebook (Left) and GroupMe (Right) Platforms.
Node size is proportional to frequency of communication. Note that node 6 on the left is colored red because it is the mole from the Red team that infiltrated the Blue team. (This node is not included in the figure on the right because the mole used only the Blue team's Facebook page and not the Red team's GroupMe chats).

The time evolution of these networks was relatively uninteresting. The data show that both teams' network are relatively static, changing very little over the course of the LARP exercise. The only major observation of time-dependent phenomena was the increase in overall frequency of communication among the Red team on the day before the Jigsaw Assembly. The network structure for each day is shown in Figure 2.

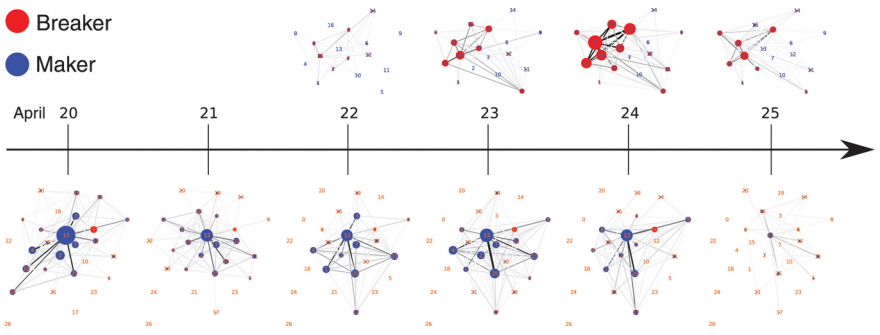

Figure 2: Network Structure of Each Team Over Time, using Data from Facebook (Left) and GroupMe (Right) Platforms. Node size is proportional to frequency of communication.

The organization of these two networks reflects our previous understanding of how a Facebook group page would function, compared to a communication network comprised of text-messaging.

Frequency-of-communication data indicates that node 13 is extremely central in the Blue Team's network, and that the Red Team's network is decentralized. This is confirmed by the computation of the betweenness centrality for the nodes of each network. These values are given in Figure 3.

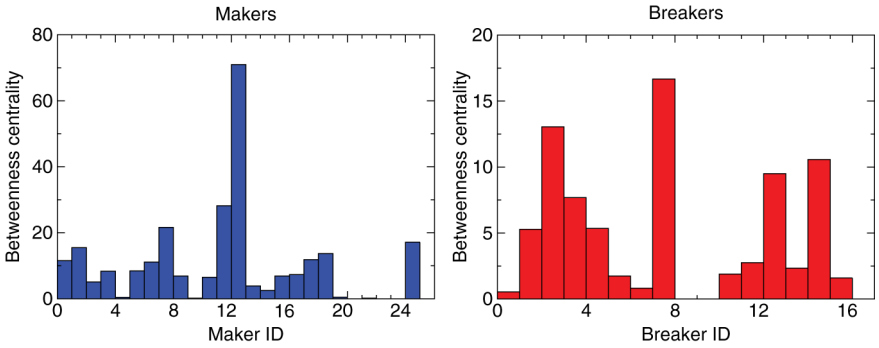

Figure 3: Betweenness Centrality for Blue (Left) and Red (Right) Teams. Note that the axes are not the same scale.

Node 13 is again confirmed as the most central node for the Blue Team, with a few more active nodes making up an inner circle and other nodes a sort of outer circle. The Red Team included a more active inner clique and outer clique, but besides this distinction, nodes seemed to be relatively similar in their communication frequency and position in the network. This demonstrates a major difference in the groups' structures. The Blue Team relies on a centralized structure, while the Red Team is decentralized.

We conclude that a decentralized group is more effective in this intelligence/counter-intelligence exercise. Although it is less efficient and lacks certain structures that may enable efficient or effective collaboration and organization, a decentralized model for organization makes up for this inefficiency with adaptability. The dynamic, flexible, creative potential of the Red Team appears to have been central to several key in-game events like the successful infiltration by a mole, the planting of an altered puzzle piece, and the spoofing of the Ideological Leader. This reflects the text-book intuition of decentralized networks as dynamic and adaptable (Fraher 2010; Jansen, Simsek, and Cao 2012).

We also believe that the choice of social network and communication platform played a key role in shaping the structure of each team, contributing to the immediate emergence of differing networks which may have been critical to the outcome of the exercise. The creativity and dynamic, adaptive strategy employed by the Red Team, which reflects its organization, was not only a major component of their winning strategy, but reflected the more judicious use of different technological platforms.

Players on the Blue Team found significant opportunity to collaborate effectively and centrally on Facebook, mirroring their real-life safe house. This proved to facilitate efficient and effective gathering of puzzle pieces and collaboration in assembling the puzzle. However, even as this more efficient struture allowed them to move towards their objectives, as the operation evolved, the Red Team's decentralized structure allowed the group to effectively respond to more dynamic situations, to adapt to new information, and to make use of technology more effectively – including GroupMe chat and email spoofing.

GroupMe provided the minimal amount of structure needed to effectively communicate as a group or within subgroups of the team. In this case, the adage "Less is more" seems to apply. A Facebook group page may have provided significantly more structure and functionality than self-organized text-messaging, but it fostered a centralized – and therefore vulnerable and inflexible – group structure and exercise strategy. The creative and insightful use of technology also enabled the Red Team to spoof a study administrator, leading to the successful engineering of a false message based on the planted, altered puzzle piece.

A key to understanding how groups such as these might organize in contemporary settings is the use of electronic communications and social media platforms. The use of peer-to-peer chat systems and/or centralized group pages in a number of different media will provide significantly different functionality and security. Whether the medium conforms to the group's intended structure, in addition to whether that structure is more effective in the operational environment, may play a significant role in the outcome.

4 Conclusion

This LARP exercise suggests effective organizing principles for grassroots, crowdsourced, and *ad hoc* intelligence/counter-intelligence style operations. It suggests that the strengths and weaknesses of social media and communication platforms may correlate with how each platform functions to foster or discourage centralized organization. Less structured and more flexible modes of communication and networking may provide greater dynamic and creative potential, far outweighing the inefficiencies of unstructured and decentralized organization.

It is also important to observe that, based on this case study, the self-organization of these teams motivated their choice of platform (and not the opposite). The Blue Team chose to concentrate its organization centrally, and they arrived at the choice of a Facebook group page because it easily allows such organization. Likewise, the Red Team used GroupMe chat because it would allow dynamic, decentralized communication between small subsets of the team. Further study may show that teams select their platforms according to their intended organizational structure, or this may depend on the team. Although it is not what we observe here, it is conceivable that a group would instead choose a platform for reasons besides their intended organizational structure and adapt that structure to best fit their communications platform.

We conclude that, in this case, the success of self-organizing, untrained groups engaged in covert, strategic operations is strongly influenced by each group's emergent organizational structure. Self-organizing groups with concrete goals may choose to organize in an efficient hierarchy, consolidating resources, communication, and/or other assets important to goal attainment. While such structure does provide efficiency, it is also a potential vulnerability, whether it stems from an inability to adapt and reorganize in a dynamic situation or from a weakness to certain types of adversarial action, as evident in our Blue Team's outcome.

Alternatively, we observed a decentralized group structure adapt effectively to changing circumstances and new information. The narrative of this exercise shows just how effective self-organizing distributed networks can be, even in spite of the inherent weaknesses, including limited communication, difficulty articulating goals (recall: the Red Team was not entirely aware of its goal for at least the first 36–48 hours of the exercise), and other drawbacks that mirror the strengths of a centralized hierarchy: inefficient or poor use of resources, slow and inefficient communication, and an inability to effect any complex organization or action for which a top-down structure is necessary. However, we have seen that in an operational environment, with clear and concrete short-term goal(s), the more dynamic team was able to leverage its advantages in ways that more than offset its inefficiency and incoherence and ultimately succeeded.

While there exists a large body of work characterizing how best to design organizations to achieve particular goals, our experiment highlights a gap in understanding: how are naïve, civilian participants trying to form a grassroots organization likely to self-organize, and how are those emerging organizations likely to function? Do these self-organized actors achieve goals more or less effectively according to the structure of their self-organization? How does the function of such untrained, self-organized agents compare to those trained and/or centrally organized? How would this impact strategies for intelligence agencies acting either in collaboration with or in opposition to such groups?

We suggest that substantial and broad study is necessary in the future to better understand how apparently naïve civilians form decentralized *ad hoc* groups, especially such cases as militias and terrorist networks that may form in opposition to hierarchically structured governmental agencies.

Funding

The original LARP exercise was funded by the Department of Homeland Security (DHS) Next Generation Communications and Interoperability (NGCI) 2014 grant through the Command, Control and Interoperability Center for Advanced Data Analysis (CCICADA). Additional analysis of the study data and writing of this manuscript was funded in part by the DHS National Consortium for the Study of Terrorism and Responses to Terrorism (START) grant for "Modeling the Emergence of Leaders in Self-Organizing Social Networks."

References

Agarwal, Sheeta D., W. Lance Bennett, Courtney N. Johnson, and Shawn Walker. 2014. "A Model of Crowd Enabled Organization: Theory and Methods for Understanding the Role of Twitter in the Occupy Protests." *International Journal of Communication* 8: 646–672.

Argyris, Chris. 1960. *Understanding Organizational Behavior, Understanding Organizational Behavior.* Oxford, England: Dorsey.

Borgatti, Stephen P., Ajay Mehra, Daniel J. Brass, and Giuseppe Labianca. 2009. "Network Analysis in the Social Sciences." *Science* 323 (5916): 892–895.
Brabham, Daren C. 2008. "Crowdsourcing as a Model for Problem Solving: An Introduction and Cases." *Convergence* 14 (1): 75–90.
Brooks, Mel. 1987. *Spaceballs.* Beverly Hills, CA: Metro-Goldwyn-Mayer Studios. August 7, 2012. DVD.
Carrington, Peter J., John Scott, and Stanley Wasserman, eds. 2005. *Models and Methods in Social Network Analysis, Structural Analysis in the Social Sciences*. Cambridge: Cambridge University Press.
Chen, Hsinchun, Homa Atabakhsh, Jennifer Jie Xu, Alan Gang Wang, Byron Marshall, Siddharth Kaza, Lu Chunju Tseng, Shauna Eggers, Hemanth Gowda, Tim Petersen, and Chuck Violette. 2005. "Coplink Center: Social Network Analysis and Identity Deception Detection for Law Enforcement and Homeland Security Intelligence and Security Informatics: A Crime Data Mining Approach to Developing Border Safe Research." Proceedings of the 2005 National Conference on Digital Government Research, Atlanta, Georgia, USA.
Coffman, Thayne, Seth Greenblatt, and Sherry Marcus. 2004. "Graph-Based Technologies for Intelligence Analysis." *Communications of the ACM* 47 (3): 45–47.
Erdős, P., and J. L. Selfridge. 1973. "On a Combinatorial Game." *Journal of Combinatorial Theory, Series A* 14 (3): 298–301.
File, Charles, Rannie Teodoro, Mor Naaman, and Paul B. Kantor. 2012. "Alerts and Warnings in Social Media: A Simulation Experiment." *LAIR/TR-03/2012*, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.457.6860&rep=rep1&type=pdf.
Fraher, Amy 2010. "The Pros and Cons of Decentralized Leadership." *The Washington Post*, http://views.washingtonpost.com/leadership/panelists/2010/09/the-pros-and-cons-of-decentralized-leadership.html
Fuchs, Christian. 2003. "Structuration Theory and Self-Organization." *Systemic Practice and Action Research* 16 (2): 133–167.
Fuchs, Christian. 2006. "The Self-Organization of Social Movements." *Systemic Practice and Action Research* 19 (1): 101–137.
Garicano, Luis, and Richard A. Posner. 2005. "Intelligence Failures: An Organizational Economics Perspective." *Journal of Economic Perspectives* 19 (4): 151–170.
Gulledge, Thomas R., and Ruth A. Haszko. 1996. The Information Technology Enabled Organization: A Major Social Transformation in the USA, edited by MOST: Management of Social Transformations: UNESCO.
Hefetz, Dan, Michael Krivelevich, Miloš Stojaković, and Tibor Szabó. 2014. *Positional Games.* Basel: Springer.
Hersey, Paul, and Kenneth H. Blanchard. 1993. *Management of Organizational Behavior: Utilizing Human Resources*. Englewood Cliffs, NJ: Prentice Hall.
Heylighen, Francis. 2013. "Self-Organization in Communicating Groups: The Emergence of Coordination, Shared References and Collective Intelligence." In *Complexity Perspectives on Language, Communication and Society*, edited by Àngels Massip-Bonet and Albert Bastardas-Boada, 117–149. Berlin, Heidelberg: Springer Berlin Heidelberg.
Huber, George P. 1990. "A Theory of the Effects of Advanced Information Technologies on Organizational Design, Intelligence, and Decision Making." *Academy of Management Review* 15 (1): 47–71.
Jansen, Justin J. P., Zeki Simsek, and Qing Cao. 2012. "Ambidexterity and Performance in Multiunit Contexts: Cross-Level Moderating Effects of Structural and Resource Attributes." *Strategic Management Journal* 33 (11): 1286–1303.
King, John Leslie. 1983. "Centralized versus Decentralized Computing: Organizational Considerations and Management Options." *ACM Computing Surveys* 15 (4): 319–349.
Koschade, Stuart. 2006. "A Social Network Analysis of Jemaah Islamiyah: The Applications to Counterterrorism and Intelligence AU – Koschade, Stuart." *Studies in Conflict & Terrorism* 29 (6): 559–575.
Linsker, R. 1988. "Self-Organization in a Perceptual Network." *Computer* 21 (3): 105–117.
Marschak, Thomas, and Stefan Reichelstein. 1998. "Network Mechanisms, Informational Efficiency, and Hierarchies." *Journal of Economic Theory* 79 (1): 106–141.
Marshall, Penny. 1986. *Jumpin' Jack Flash*. Century City, CA: Twentieth Century Fox. May 28, 2013. DVD.
Mishra, Aneil K. 1996. "Organizational Responses to Crisis: The Centrality of Trust." In *Trust in Organizations: Frontiers of Theory and Research*, edited by Roderick M. Kramer and Tom R. Tyler. Thousand Oaks, CA, USA: Sage Publications, Inc.
Monahan, Torin, and Jennifer T. Mokos. 2013. "Crowdsourcing Urban Surveillance: The Development of Homeland Security Markets for Environmental Sensor Networks." *Geoforum* 49: 279–288.
Nilles, J. 1975. "Telecommunications and Organizational Decentralization." *IEEE Transactions on Communications* 23 (10): 1142–1147.
Organ, Dennis W. 1988. *Organizational Citizenship Behavior: The Good Soldier Syndrome, Organizational Citizenship Behavior: The Good Soldier Syndrome.* Lexington, MA, England: Lexington Books/D. C. Heath and Com.
Sabater, Jordi, and Carles Sierra. 2002. "Reputation and Social Network Analysis in Multi-Agent Systems." Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems: Part 1, Bologna, Italy: Association for Computing Machinery.
Sparrow, Malcolm K. 1991. "The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects." *Social Networks* 13 (3): 251–274.
Tang, John C., Manuel Cebrian, Nicklaus A. Giacobe, Hyun-Woo Kim, Taemie Kim, and Douglas "Beaker" Wickert. 2011. "Reflecting on the DARPA Red Balloon Challenge." *Communications of the ACM* 54 (4): 78–85.
Tewksbury, Doug. 2012. "Crowdsourcing Homeland Security: The Texas Virtual BorderWatch and Participatory Citizenship." *Surveillance & Society* 10 (3): 249–262.
Tichy, Noel M., Michael L. Tushman, and Charles Fombrun. 1979. "Social Network Analysis For Organizations." *Academy of Management Review* 4 (4): 507–519.
Ulrich, H., and G. J. B. Probst, eds. 2012. *Self-Organization and Management of Social Systems: Insights, Promises, Doubts, and Questions, Springer Series in Synergetics*. Berlin Heidelberg: Springer.
Van Dyke Parunak, H., and Sven Brueckner. 2001. "Entropy and Self-Organization in Multi-Agent Systems." Proceedings of the Fifth International Conference on Autonomous Agents, Montreal, Quebec, Canada: Association for Computing Machinery.
Wang, F., K. M. Carley, D. Zeng, and W. Mao. 2007. "Social Computing: From Social Informatics to Social Intelligence." *IEEE Intelligent Systems* 22 (2): 79–83.

Wasserman, Stanley, and Katherine Faust. 1994. *Social Network Analysis: Methods and Applications*, *Structural Analysis in the Social Sciences*. Cambridge: Cambridge University Press.

Zammuto, Raymond F., Terri L. Griffith, Ann Majchrzak, Deborah J. Dougherty, and Samer Faraj. 2007. "Information Technology and the Changing Fabric of Organization." *Organization Science* 18 (5): 749–762.