The United States Disciplinary Barracks at Fort Leavenworth, Kansas, serves as the military's sole maximum-security facility for male service members.

(U.S. Army courtesy photo)

Entanglement: Using Social Network Analysis for Military Justice Applications

Maj. Dan Maurer, U.S. Army

This article takes part of its title from the quantum property of *entanglement*, a strange and perplexing feature of subatomic physics. After two particles have interacted, entanglement describes how the properties of one particle directly and simultaneously influence the behavior or properties of the other particle, even *after they stop directly interacting* and *even when separated by great distances of space*. They behave as if they remain tethered by an invisible web.[1] Einstein famously called this phenomenon "spooky action at a distance."[2]

Likewise, common life experience demonstrates that our interpersonal connections often influence our social behavior and conduct—in both positive

and negative ways. Social network analysis (SNA) is a method for discovering and describing webs of relationships among social actors.[3] By describing soldiers as entangled nodes within a web-like social network in which they are connected by numerous (perhaps unseen) affiliations or shared characteristics, this essay proposes that commanders can make use of SNA in two ways. First, the approach can serve in a reactive sense, by enabling commanders to develop and execute wide-impact and *strategic* disciplinary choices in the wake of criminal misconduct. Second, but no less important, SNA can serve as part of a philosophy of proactive leader engagement and risk management. This article will focus on the first mode, and it will introduce potentially innovative applications of SNA within military justice practice.

Introduction

SNA takes as its fundamental premise the common sense notion that we are products of our social environments. Where we live, what jobs we take, our race, our gender, our personal hobbies, the sports we play, our children, our children's friends, our addictions, and our institutional affiliations are just some of the factors that give color to our personas and drive our interpersonal actions. Inasmuch as we orient our lives around what others close to us are doing, thinking, saying, and believing, each of the factors we share with other people can be modeled as a link between them and us.

In an early (1991), influential merger of the fields of SNA and police work, Malcolm Sparrow's critical contribution to SNA was to characterize its attributes as relevant to strategic decision making for very practical, socially-significant ends—such as fighting crime. In arguing that SNA's tools could and should be applied by civilian law enforcement investigators, Sparrow argued that fiscal constraints and ambiguities in evidence made conventional police investigations outmoded and inefficient. He then illustrated how SNA's techniques could better allocate public resources for the more effective and efficient targeting of criminal enterprises.[4]

Building on that premise, SNA has potential utility for military leaders attempting to disarm informal or formal networks of soldiers tied together by their misconduct. Similarly, it has potential in the manner in which military leaders might disable networks tied

together by collective disenfranchisement or low morale. In other words, network analysis can help to upset a cart full of bad apples.[5]

First, I will sketch some of the basic conceptual elements of SNA. Then, I will propose some ways in which commanders could adopt this perspective to more accurately understand just how entangled their soldiers are with one another, including some ways in which commanders could use their increased situational awareness to make more strategic, warranted, and appropriate disciplinary choices.

While certainly not a panacea for widespread indiscipline, SNA could improve command visibility over these common problems in a way deserving more robust attention and critical review. To facilitate such a review, I will conclude by laying a foundation of common-sense variables: case-by-case factors that bear on whether a commander should rely on heuristics (experienced-based techniques for problem solving and learning) or, instead, augment a heuristic approach with SNA in the wake of misconduct.

Basics of Social Network Analysis

SNA is simply a way of looking at sets of relationships among people to discern the attributes and patterns of those relationships. Knowing these attributes and patterns provides a foundation for making qualitative judgments, meting out punitive consequences, or predicting future behavior based on those models.[6] This network-centric approach has been defined as a "perspective [that] emphasizes structural relations as its key orienting principle, where social structure consists of the body of patterns between and among a people, groups, organizations, and other entities with respect to their beliefs, decisions, and actions."[7] Due to its emphasis on patterns of relationships between individuals over some period of time, SNA has been a well-known and much-employed methodology for studying clique formation, the evolution of fads, and the spread of rumors or knowledge. As one researcher has phrased it, SNA is the "science of the real world," which relates to an "interlocking pattern of friendship, business, family, and community ties through which paths could be traced between any random person and any other … the length of these paths might have something to do with the way that influences—whether they be diseases, rumors,

ideas, or social unrest—propagate through a human population."[8]

These interlocking patterns of relationships are ubiquitous throughout nature and human-driven activities.[9] Many have observed that the key concepts of the network perspective were "almost simultaneously discovered" by independent researchers in distinct fields.[10] As a result, SNA has become an interdisciplinary approach to research and problem solving across many fields and has been applied in diverse areas. These include cultural anthropology, genetics, studying the structure of the World Wide Web, neurology, corporate sociology, research collaboration among scientists in numerous disciplines, decision making by community elites, group problem solving, and the formation of coalitions.[11] SNA also has found a home in investigations of organized crime, terrorism, and militant insurgencies.[12]

SNA researchers study network patterns: the presence and absence of ties between various individuals, the strength of those ties, and the extent to which those ties remain static or evolve over time and under what circumstances.[13] These patterns can illuminate specific actors' social opportunities and constraints. This, in turn, creates potential insight into who in any particular network has a capacity to "extract better bargains in exchanges, have greater influence, and [be a] focus for deference and attention from those in less favored positions."[14]

This observation of the real world shifts the focus away from behavior of discrete actors and their purely intrinsic motivations. Instead, researchers adopt a view that may better depict the social context and other mechanisms that influence the behavior of individuals or, alternately, how a one person's behavior could influence others.[15]

Effectively applying a network perspective may appear to be a paradigm shift for traditional military culture as this perspective tasks us to look not just at isolated offenses committed by individual parties but also at poor discipline brewing among soldiers in their off-duty affiliations—the connections that hold units together beneath the surface lines of authority, command, and control.[16] Thinking of "good order and discipline" problems as related to the *structure* of relationships is an adaptation of problem solving in other domains, such as health, where harms are spread from person to person.

Strategic Analysis for Targeting Widespread Misconduct
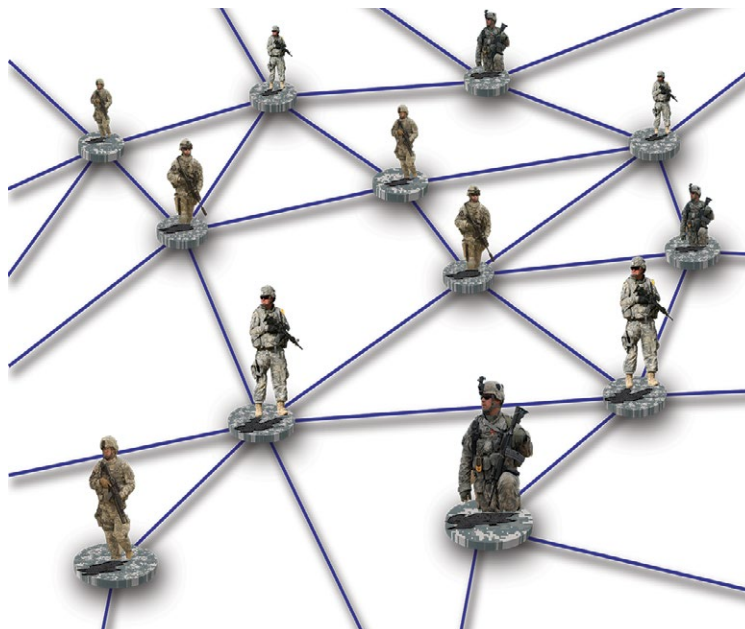
To prevent a disease outbreak from exploding into an epidemic, public health officials target not just the infected individuals with healing medications but also engage the social network by which the infection spreads. They may use preventive vaccines, quarantine to close lanes that would otherwise facilitate the spread, and public education (such as safe-sex campaigns or the exchange of needles contaminated with HIV).[17]

This approach is both proactive and scalable—its strategy is network-centric, and its tactics can be tailored to suit a given type and size of community.[18] In other words, when undesirable contagions propagate along the social links between and among individuals, efforts are aimed at disrupting the *network* itself to abort, stem, contain, or otherwise influence those negative consequences.[19]

Similarly, the military—as an institution, organization, and social community—is susceptible to the spread of misconduct and mission-defeating behaviors

within its organizations and units in somewhat the same way as contagions are spread among susceptible populations.[20] Unlike disease epidemiologists, however, military justice practitioners and unit commanders responsible for enforcing standards of conduct and the military criminal law tend to be reactive and individual-centric in practice.[21] While military commanders are afforded great power and discretion, they cannot predict undesirable or illegal behaviors in order to circumvent them, including whether a particular soldier will commit a crime. Thus, commanders' responses to misconduct are just that: responses after the fact. Moreover, it is largely axiomatic that a service member is legally accountable only for his or her own criminal acts (exceptions, of course, for conspiracies, accessories, and aiding and abetting), and that due process demands that authorities treat each case on its own merits.[22]

Due to normal resource constraints and operational tempos, little empirical attention generally is paid by the commanders to the larger community in which misconduct occurs, except to the extent that a particular crime might have several victims or disturb the good order of the organization as a whole.[23]

Thinking of the offender as part of a *community of other offenders* is like asking commanders to view the world in more than the three physical dimensions in which we are accustomed to living.

As a result, military commanders tend to employ their judicial power in a vacuum, largely ignoring the pervasive social background in which the incident, behavior, or offense often occurs.[24] Lying beneath the surface hierarchy and command structure of a military organization is an often-recognized but rarely described or exploited subarchitecture. Like the ruins of ancient European cities buried beneath centuries of urban development, this hidden architecture helps shape the landscape of the unit; its personality, its network of interpersonal relationships, its command climate, its distribution of information, and its ability to adapt to external environmental changes or challenges.[25]

What leaders often encounter when dealing with systemic discipline problems are the consequences of this complicated, shifting web of personal relationships that may cross gender, rank, and duty-position divides. The complexity of this network often hampers the chain of command's ability to recognize and address problems that are, potentially, deeper or wider than just one soldier's discrete misconduct. Yet, the law does not demand that pre-prosecutorial decisions search for situational explanations beyond an individual's intrinsic pathology or consider much more beyond the type of crime and the scale of the harm inflicted.

In other words, conventional military criminal justice does not examine how large-scale patterns of misconduct may be related to, or caused by, small-scale interpersonal interactions.[26] The community, however, is a salient feature that can and should be a consideration as the commander "disposes" of an offense.[27]

The *Manual for Courts-Martial* is, in a sense, complicit because it also ignores any network-centric perspective. Rule for Courts-Martial (RCM) 306, for example (contained in the manual), tasks the commander to consider and subjectively weight various normative factors to ensure that the disposition choice—whether it takes the form of charges for court-martial, reprimand, administrative reduction, or nonjudicial punishment—is "warranted, appropriate, and fair" under all circumstances.[28]

However, the catalog of factors over which a commander must mull in deciding how to fairly address misconduct by subordinate soldiers does not *expressly* account for the interpersonal relationships underpinning some misconduct's context. As a result, the rule induces a missed opportunity—a failure to direct the commander's attention to visualizing and comprehending network-centric causes and influences.

Nevertheless, the conventional use of RCM 306 is not an actual barricade to creative military justice problem solving and decision making. Nothing in the *Manual for Courts-Martial*'s rules or in military law precludes a commander from looking beyond the four corners of RCM 306 or from taking innovative steps to help make a disciplinary choice. Therefore, the disposition of offenses, or even the administrative personnel transfers over which unit commanders have control, need not remain blind to the role that a soldier's social network plays in fostering, sustaining, or aggravating individual misconduct.

SNA offers military commanders and their supporting legal advisors a lexicon of new descriptive terms and concepts: *nodes, hubs, centrality, brokers, geodesic distances, cut points,* and *bridges,* to name a few. For example, a *node* is simply a discrete entity or

actor that may be connected along relational lines to other nodes based on a shared characteristic.[29] *Hubs* are especially well-connected nodes when compared to the average number of connections of the other nodes in a particular network.[30] Such powerful nodes demonstrate (or at least have potential to demonstrate) a disproportionate influence over other nodes.[31]

In another example, a *broker* is a node that serves as the single "go-between" or intermediary for other nodes.[32] The *geodesic distance* between two nodes is the shortest path length—in other words, length is measured by how many other nodes separate the two. The shortest path may depict the most efficient routes for sending or receiving information between nodes. Generally, the greater the proportion of geodesic (short, direct) distances in a network, the more clustered and cohesive it is. The more cohesive, the more resilient it can be to attempts to disrupt communication or resource sharing among the nodes.[33]

A *cut point* is a node that, if removed from a network, would sever all connectivity between two or more nodes, like a keystone in an archway.[34] Likewise, a *bridge* describes a relationship or tie that, if removed from a network, would sever the flow between two or more nodes or sections of the network.[35]

When applied to the social network existing in any particular military unit, these concepts (and their mathematical calculations, if more precision is needed) may provide leaders a lens through which to observe interactions among their personnel.

When circumstances warrant, these concepts may provide solid footing on which to act preemptively with administrative mechanisms or to consider the RCM 306 factors more realistically. In other words, SNA would provide commanders with a means to "perform strategic analysis of organized [misconduct]."[36]

Additionally, seeing where, and to what extent, social networks exist among soldier-to-soldier relationships may create opportunities to advantageously "invest" and "disable."[37] For instance, if one measures the *prestige* and *in-degree* values over time, for a particular subject of interest, one can get a sense of a person's stickiness or attractive power, or the attractive power of the person's web.[38] A person's *centrality* in a network reflects the scope of his or her involvement with the other actors and can be regarded as an "important ingredient" in locating criminal "network vulnerabilities."[39]

The concept of centrality can be parsed into three types: the extent to which the node connects to all other nodes, the proximity of that node to other nodes, or the extent to which a given node mediates the relations between various other groups of nodes.[40] These quantitative values, in turn, are suggestive of a capacity to restrain other nodes—other soldiers—from separating away into *isolates* or leaving the orbit of that particular hub.[41]

Moreover, if the network is a group of soldiers affiliated by some common interest, activity, or other bond, and members of that network appear to engage in various levels of misconduct (together or individually), knowing the network's *density* and identifying potential brokers, cut points, or bridges may facilitate developing novel (but targeted) disciplinary strategies tailored to each node's unique place, strength, and influence in the network.[42]

Scenario: Drug Distribution Ring Investigation

An example emphasizing the reactive utility of SNA, based on a real-world proof of concept, illustrates this strategic potential. Imagine a scenario in which your legal advisor comes into your office and presents you with evidence that a dozen soldiers in your unit are involved—to some degree—in a series of criminal acts involving illicit methamphetamine use and distribution within the barracks. While discussing the current law enforcement investigation with your trial counsel, your mind reels with the second and third order effects across the command: the distracting impact of the lengthy investigation on the unit's ability to conduct required live-fire exercises in advance of an upcoming deployment; the individual cost to the command of losing (by court-martialing) the mid-level sergeants who helped to cover-up and participate in the drug use; the low likelihood that the distribution ring was confined to soldiers in just one platoon—but instead had spread across the battalion; the long-term health and physical cost to each drug user; and, of course, the need to deter future distribution and use.

Suddenly, something your lawyer casually mentioned pulls you back into the conversation, and you begin to focus on the seemingly mundane, trivial

| 2nd Platoon | 1st Platoon | 3rd Platoon |

Directed ties indicating sellers and buyers of methamphetamines

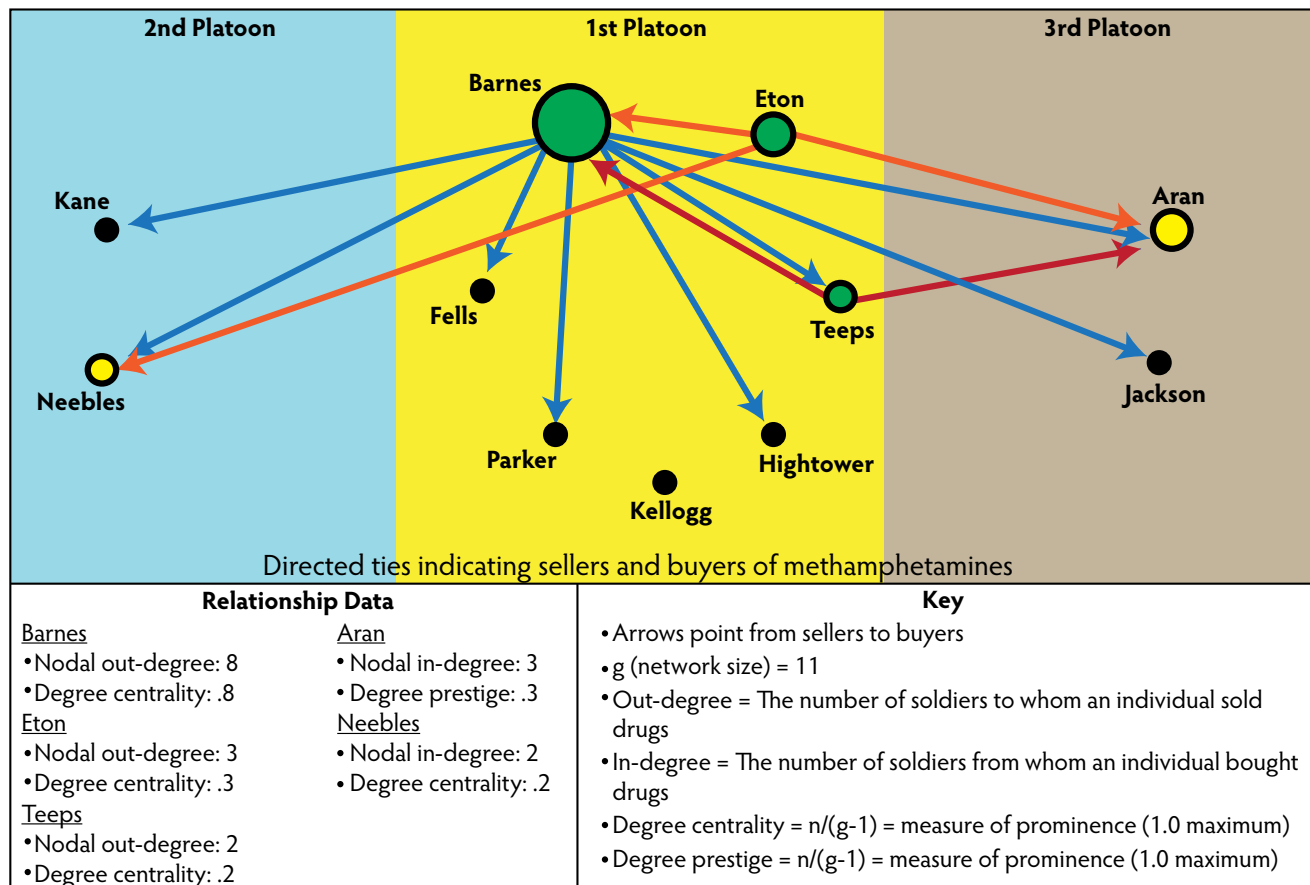| Relationship Data		Key
Barnes •Nodal out-degree: 8 •Degree centrality: .8 **Eton** •Nodal out-degree: 3 •Degree centrality: .3 **Teeps** •Nodal out-degree: 2 •Degree centrality: .2	**Aran** •Nodal in-degree: 3 •Degree prestige: .3 **Neebles** •Nodal in-degree: 2 •Degree centrality: .2	•Arrows point from sellers to buyers •g (network size) = 11 •Out-degree = The number of soldiers to whom an individual sold drugs •In-degree = The number of soldiers from whom an individual bought drugs •Degree centrality = n/(g-1) = measure of prominence (1.0 maximum) •Degree prestige = n/(g-1) = measure of prominence (1.0 maximum)

Figure 1. Affiliation Network (Drug Selling)

information he describes as context and background: where the soldiers live in relation to each other, where the drugs and paraphernalia were found, and what were the various overlapping details provided in some sworn statements. Your sergeant major pipes in with detailed recall of the squads, sections, and platoons to which the suspects are assigned and ably summarizes previous overlapping criminal histories of some of the suspects.
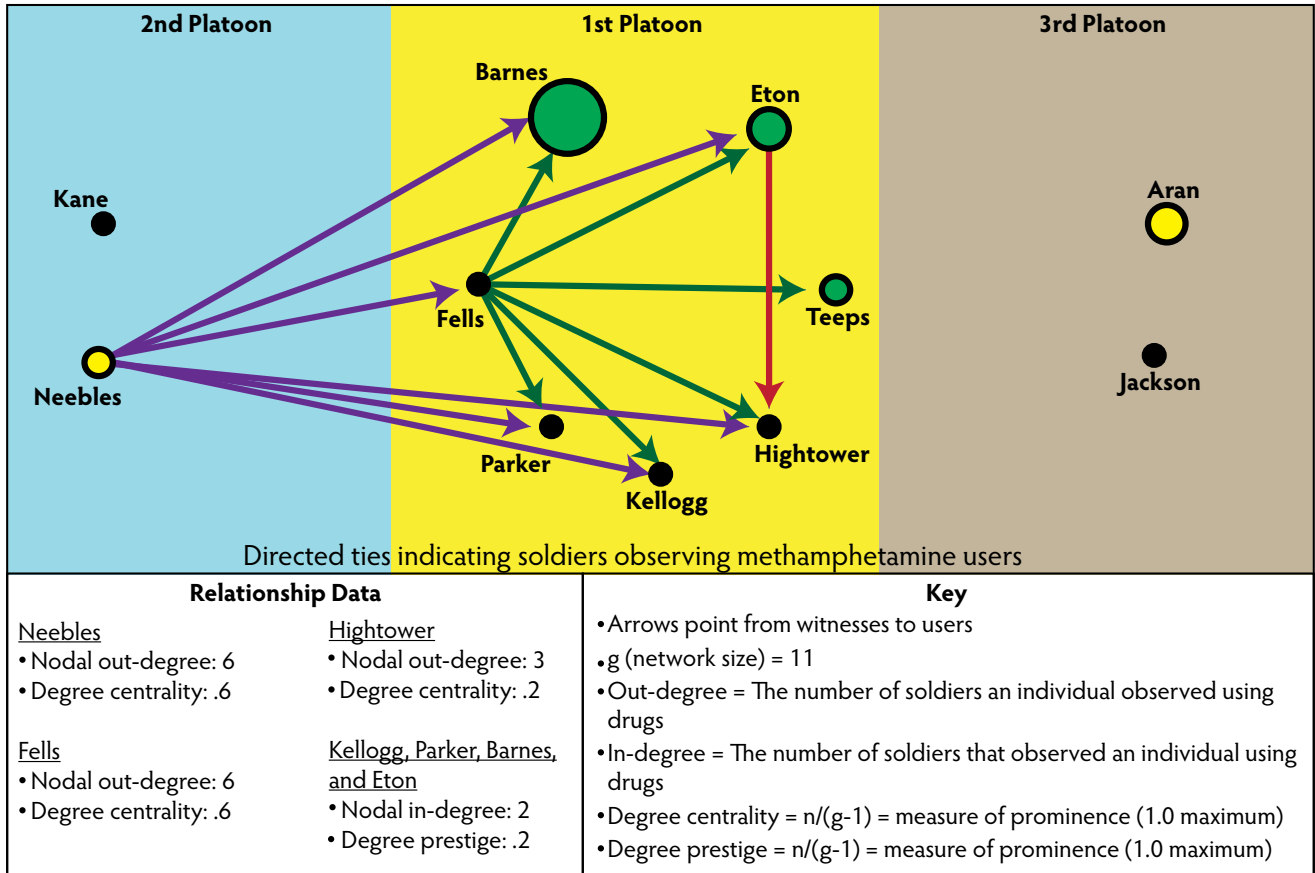
On scrap paper from your desk, you begin sketching out the lines of relationships between the suspects, and you juxtapose that interconnected web against their background characteristics. Unexpectedly, you begin to see visual patterns of influence and power emerge on the page—patterns that do not reflect traditional presumptions of who is leading whom astray. You wonder if this exercise would help you make the *right* disciplinary decision in each case in a way that more holistically accounts for the second and third order consequences you were just imagining. For instance, one course of action—such as a court-martial with a cap on confinement, to spur a swift offer to plead

guilty—would be better than another (say, indiscriminate nonjudicial punishment under Article 15 of the Uniform Code of Military Justice for all soldiers in the ring) if that course of action would have a domino-like deterrent effect in this social network of drug use and distribution.

Such an effect could either stem the repeated offenses or allow the subordinate commanders to use a targeted disciplinary choice on a particularly influential hub in order to nudge or shepherd the more easily led (or misled) individuals in the right direction. Choosing one course of action over another, therefore, has implications for the substantive equity of the disciplinary action, as well as for the command's allocation of investigative resources and attention.[43]

Such a scenario is not only hypothetical, but it was employed by a brigade and battalion commander to more efficiently, fairly, and robustly address a drug distribution ring infesting a particular company deployed to Iraq during combat operations.[44]

Figures 1 and 2 represent two layers of data drawn from the law enforcement investigation into that

2nd Platoon	1st Platoon	3rd Platoon

Barnes
Eton
Kane
Aran
Fells
Teeps
Neebles
Jackson
Parker
Hightower
Kellogg

Directed ties indicating soldiers observing methamphetamine users

Relationship Data		Key
Neebles • Nodal out-degree: 6 • Degree centrality: .6	Hightower • Nodal out-degree: 3 • Degree centrality: .2	• Arrows point from witnesses to users • g (network size) = 11 • Out-degree = The number of soldiers an individual observed using drugs • In-degree = The number of soldiers that observed an individual using drugs • Degree centrality = n/(g-1) = measure of prominence (1.0 maximum) • Degree prestige = n/(g-1) = measure of prominence (1.0 maximum)
Fells • Nodal out-degree: 6 • Degree centrality: .6	Kellogg, Parker, Barnes, and Eton • Nodal in-degree: 2 • Degree prestige: .2	

Affiliation Network (Observed Drug Use)

company-wide misconduct, taken from the sworn statements given by some of the suspects. The brigade's legal section used this data to create two separate sociograms—visual depictions of a social network. Figure 1 represents an *affiliation network*—the involvement of a set of actors in a particular social event—depicting which soldiers sold the drug to whom. The relational lines, with arrows pointing at the buyers, are overlaid against the division of the unit into its three platoons. The size of the circle representing each soldier-node is a function of the number of outward-directed links he has. Barnes, for example, is the largest circle because he sold to the greatest number of other soldiers (eight). Manipulating the size of the circle, while not critical, helps visualize the relative weight of the hubs and other nodes.

In this sociogram, a soldier's *nodal out-degree* represents the number of other soldiers in the network to whom he sold the drugs; conversely, in-degree represents the number of soldiers from whom a particular soldier-node purchased drugs. The degree centrality value indicates how prominent an individual node is within the network by calculating the proportion of

the whole network to which he directs a tie (here, sells drugs to another node).

Figure 2 depicts this affiliation network from a slightly different perspective: who has been observed using the drugs, and by whom. In this sociogram, a soldier's nodal out-degree is the number of soldiers that a particular node observed using the drugs, whereas his in-degree represents the number of other soldiers who observed this node using drugs. His centrality, as one measure of his prominence, is calculated as a proportion of the network this node witnessed using drugs.

These affiliation network sociograms were built only from the information gleaned from multiple law enforcement interviews and the resulting sworn statements provided by the suspected soldiers. Additional layers of data that could be depicted, if evidence was available, include the amount of methamphetamines sold to each individual in the network; the number of transactions per individual buyer; the same sociogram over multiple points in time or by location, which shows whether the network animates or changes over

time or space; the labeling of nodes that have previous drug use or distribution histories; and adding nodes for all network members' noncommissioned officers (NCOs), depicting each suspect's geodesic distance from formal NCO supervision. The amount of information that one can collect and illustrate using SNA techniques becomes a function of the time, patience, and—ultimately—the goals of the commander.

In this real-world illustration, some of the observations the command teams gleaned from the SNA exercise included data that could not be easily deduced or inferred from the sworn statements alone. For instance, the commanders were able to note that—

• Aran was buying from three different sources, which suggested significant dependency, and that cutting his ties to any one of the sellers would not significantly disrupt his use.

• Seven soldiers from one platoon were implicated as buyers or sellers of the drug, suggesting that NCO and officer leadership were either negligent or derelict in enforcement of good order and discipline, or possibly that they knew of the misconduct already but chose to ignore it.

• There was no single *cutpoint* in this network of sellers (i.e., removing only one seller would not substantially diminish the availability of the drug from other sources within the company).

• Available evidence showed that five soldiers had an in-degree value of at least 2. This suggests methamphetamine use was a social activity engaged in by multiple personnel within this network.

• Aran, despite buying from three sources, was never observed using the drugs, suggesting he was a more isolated node.

• Neebles had a high in-degree (by purchase) and the highest out-degree (by observation of others).

• Fells and Neebles each witnessed sixty percent of the network using methamphetamines.

With this rich portrait of the social relationships among the suspected users and sellers, the battalion and brigade commanders were able to make disciplinary choices that more aptly and more precisely accounted for considerations of rehabilitative need and the various scales of criminal culpability for each individual in the network. Some were obviously more central to the use and distribution of the drugs than others, and the type of discipline imposed accounted for relative passivity

of occasional users or the critical role of brokers of this resource between other soldiers across the unit.

Employment Considerations

Case-by-case circumstances compel how, when, and if certain military justice options should be used. That calculus is equally appropriate for the choice to employ SNA as a methodology, and it should remain within the judicious discretion of the commander. Admittedly, the drug distribution ring from figures 1 and 2 could have been investigated and prosecuted without the use of SNA. Indeed, most networks of misconduct typically are. SNA, however, can give more analytical justification to the way in which investigators, prosecutors, and commanders label and attack certain elements of those networks. It can also help military justice practitioners visualize the scope and scale of the unseen entanglements that inspire or influence the misconduct. This essay offers several situational variables—extensions from the traditional RCM 306 considerations—that commanders should reflect on before turning to SNA:

• The number of potential offenders

• The span of disciplinary command and control over the potential offenders

• The variation of culpability among the potential offenders

• Disparate positions and rank of the potential offenders

With these additional employment considerations in mind, it is not a large leap to imagine how SNA might be extended beyond military justice. Applications run the range from better (or at least earlier) identification of hubs of misconduct to the more careful observation of those service member nodes that may be susceptible to the negative influences of their more assertive or aggressive comrades. Such observations may trigger opportunities beyond traditional disciplinary measures.

Four opportunities come to mind. The first is conducting more precise and targeted leader engagement to affect those more susceptible nodes. The second, and less direct, opportunity is leveraging the *gate-keeping, liaising, consulting,* or *coordinating broker* nodes as a way to subtly influence the conduct of those nodes.[45] The third is deliberately rearranging personnel to break up or disable disreputable networks. The fourth opportunity is selectively embedding or "investing" constructively influential and

trusted service members (of virtually any rank), like firewalls, to block connections to or from undesirably influential nodes and to positively influence the conduct of their weaker-willed compatriots.[46] Both the value and the cost of using SNA in that proactive, risk-management approach is a subject that deserves further exploration and review.

Conclusion

At a fundamental level, SNA is another tool to measure, understand, and react to problems influenced by the social connectivity we all naturally share to various degrees. SNA is a powerful tool for uncloaking the critical context that remains obscured or unmeasured by traditional military investigations into widespread misconduct. SNA is neither new nor groundbreaking in its most basic applications.

However, its relatively long history of use since its inception is a result of its demonstrated utility across a broad range of disciplines and of its usefulness in answering a wide variety of questions. SNA's adaptation as a visual or quantitative aid to commanders in making strategic military justice decisions would be an innovative departure from current conventional practice. Given SNA's ample potential and current applications, it is worth further exploration by military justice practitioners.[47]

The author wishes to thank his colleagues in the U.S. Army Government Appellate Division for their insights and Dr. Luke Gerdes, Minerva Fellow in the Department of Behavioral Sciences and Leadership, United States Military Academy, for his technical review and astute suggestions. The opinions in this article are the author's alone and do not represent official policy of the Department of the Army or the Judge Advocate General's Corps. ◾

Maj. Dan Maurer, U.S. Army, is an LL.M. candidate at The Judge Advocate General's Legal Center and School. He was a 2013-2014 Fellow in the Chief of Staff of the Army's Strategic Studies Group. As a judge advocate, he has served as appellate counsel, brigade judge advocate, and trial prosecutor. Before law school, Maurer served as a combat engineer officer. He has deployed to Iraq twice. He is a distinguished military graduate from James Madison University's ROTC program, and he earned his J.D. from The Ohio State University.

Notes

1. Brian Greene, *The Fabric of the Cosmos: Space, Time, and the Texture of Reality* (New York: Vintage Books, 2004), 80-84, 115-123.

2. Walter Isaacson, *Einstein: His Life and Universe* (New York: Simon and Schuster, 2008), 450.

3. Stanley Wasserman and Katherine Faust, *Social Network Analysis: Methods and Applications*, (Cambridge University Press, 1994).

4. Malcolm K. Sparrow, "The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects," *Social Networks* 13 (1991): 251-74.

5. Extending Sparrow's observations further, SNA may also allow military leaders to proactively "invest" in these informal networks as a consequence of a more nuanced awareness of the social structures underlying their organizations. As a result, leaders might uncover opportunities to reinforce the cohesive bonds in such networks and thereby increase their resistance to harmful internal "insurgencies" (such as peer-induced misconduct) and to widely felt external traumas (such as combat losses). In other words, network analysis can help plant healthy trees in an orchard where few bad apples can grow.

6. Wasserman and Faust, 3.

7. David Knoke and Song Yang, *Social Network Analysis* (Los Angeles: Sage Publications, 2008), 4.

8. Duncan J. Watts, *Six Degrees: the Science of a Connected Age* (London: Vintage, 2003), 13 and 37.

9. Albert-Laszlo Barabasi, *Linked* (New York: Plume, 2003), 16.

10. Wasserman and Faust, 10; Linton C. Freeman, *The Development of Social Network Analysis* (Vancouver: Empirical Press, 2004): 10-30.

11. Barabasi, 30-34; Watts, 98; Wasserman and Faust, 6.

12. Field Manual (FM) 3-24, *Insurgencies and Countering Insurgencies* (Washington, DC: U.S. Government Printing Office [GPO], May 2014), Appendix B.

13. Robert A. Hanneman and Mark Riddle, *Introduction to Social Network Methods*, online textbook, chapter 1, "Social Network Data," http://www.faculty.ucr.edu/~hanneman/nettext/; Mark S. Granovetter, "The Strength of Weak Ties," *American Journal of Sociology*, 7(6)(May 1973): 1366 and 1378; Knoke, 8.

14. Hanneman and Riddle, chapter 10.

15. Knoke, 5.

16. Brian Reed, "A Social Network Approach to Understanding an Insurgency," *Parameters* (Carlisle, PA: U.S. Army War College, Summer 2007),:19.

17. Stephen F. Morin, Margaret A. Chesney, and Thomas J. Coates, "Discovering Global Success: Future Directions for HIV Prevention in the Developing World," AIDS Research Institute Policy Monograph #1 (April 2000), http://ari.ucsf.edu/science/reports/dgs.pdf; "The Public Health Impact of Needle Exchange Programs in the

United States and Abroad: Summary, Conclusions, and Recommendations," report from the School of Public Health, University of California, Berkeley, and the Institute for Health Policy Studies, University of California, San Francisco (1993), http://caps.ucsf.edu/uploads/pubs/reports/pdf/NEPReportSummary1993.pdf.

18. Watts, 166-181.

19. Thomas W. Valente, *Social Networks and Health: Models, Methods, and Applications* (New York: Oxford University Press, 2010).

20. Watts, 207-12 and 223-24.

21. *Manual for Courts-Martial* (MCM) (Washington, DC: U.S. GPO, 2012), V1.d., http://www.apd.army.mil/pdffiles/mcm.pdf; Army Regulation (AR) 27-10, *Military Justice* (Washington, DC: U.S. GPO, 3 October 2011), para. 3-2a.; AR 600-20., *Army Command Policy* (Washington, DC: U.S. GPO, RAR 20 September 2012), para. 4-7c. This reactionary and narrow approach need not be the *only* method. Indeed, some military regulations hint at a more proactive and preventive strategy. *See* AR 600-20, para. 1-5c.(4)(b) and para. 4-1 through 4-7; and, FM 1-04, *Legal Support to the Operational Army*, (Washington, DC: U.S. GPO: March 2013), para. 4-6 and 4-21.

22. MCM, see RCM 306.

23. Phillip Zimbardo, *The Lucifer Effect*, (New York: Random House, 2007) 7-8, 195.

24. Donald W. Hansen, *Judicial Functions for the Commander?*, 41 Mil. L. Rev. 1 (1968), http://heinonline.org/HOL/LandingPage?handle=hein.journals/milrv41&div=4&id=&page=. Like many investigators or prosecutors, commanders display a "commitment to particularized judgments—to judging the individual's likely guilt or innocence based primarily upon his own actions, beliefs, and character." *See* Andrew E. Taslitz, *Police Are People Too: Cognitive Obstacles to, and Opportunities for, Police Getting the Individualized Suspicion Judgment Right*, 8 Ohio St. J. Crim. Law 7 (2010) at 17 (discussing the cognitive flaws in police investigators' application of "reasonable suspicion" and "probable cause").

25. Peter Sheridan Dodds, Duncan J. Watts, and Charles F. Sabel., "Information Exchange and the Robustness of Organizational Networks," *Proceedings of the National Academy of Sciences*, 100(21)(14 October 2003): 12,516.

26. Granovetter, 1360-80.

27. Reed, 21.

28. MCM, V-lc; RCM 306, RCM 307, and RCM 401.

29. An individual or discrete entity that may be connected along relational ties to other individuals or entities based on a shared characteristic, relationship, or action.

30. I use the term *hub* subjectively, based on the particular features and characteristics of the network being studied.

31. Watts, 52.

32. Hanneman and Riddle, chapter 8.

33. Knoke, 60-61.

34. Ibid., 49.

35. Ibid. These bridging relationships serve as essential conduits of information, resources, or access between various nodes, and thus affect the ability of such commodities or actions to diffuse across the network; Granovetter, 1364.

36. Sparrow, 260.

37. Reed, 20.

38. In any given social network, one could characterize actors as senders or receivers of directed ties. Such labeling signals an actor's access to, or control over, information, resources, and influence (authority or deference to authority). *Prestige* measures the extent to which a social actor receives or serves as the object of relations sent by other actors. Actors with higher values can be thought of as more prestigious within that particular network study, in that they receive many ties and need only initiate a few. This value, however, has limitations: by mathematically equating all senders, one could oversimplify the nature of the prestigious relationship because it does not account for variation in the prestige value of the senders themselves. In other words, an actor's prestige in a group may be qualitatively enhanced if he or she receives ties from another prestigious actor. Knoke, 69; The total number of relations a particular node or actor has is that node's nodal degree in a *nondirected* graph (that is, where studying whether the tie exists or it does not without regard to who is initiating or receiving some relation). Conversely, in a *directed* graph (where we can distinguish who initiates or sends a relation to another node), we can further distinguish between that node's in-degree (the number of relations *received* by one actor from other actors) and out-degree (the number of relations *sent* by one actor to all others). Like the limitations of the prestige value noted above, the in-degree and out-degree value for any focal, actor is limited because it does not distinguish the intrinsic quality of those other actors sending relations to, or receiving relations from, the focal actor.

39. Sparrow, 264.

40. *Degree* centrality measures the extent to which a node connects to all other nodes in a given social network. *Closeness* centrality measures the proximity of a given node to other nodes, serving as a proxy characteristic for how long it may take that node to interact with others. *Betweenness* centrality measures the extent to which a given actor mediates the relations between various other dyads that are not directly connected themselves. This value articulates and helps visualize the actor's potential for influence or control over information exchange or resources within a network. Knoke, 63-69.

41. An isolate is an actor unconnected to any other actor in a particular network of some specified relation. *Knoke,* 48.

42. Knoke, 53-56; Watts, 72; Sparrow, 260-61. Generically, in a given network, density equals the proportion of *potential* ties that exist between nodes. If this value is assessed over time, one could develop a measure of the network's resiliency, or ability to withstand destabilizing internal or external events.

43 Ibid.

44. Personal notes and records for the investigation and adverse actions resulting from a drug use and distribution ring in this particular unit are on file with the author. All names used in this essay are fictional.

45. Hanneman, chapter 8. Over time, and in relation to other actors in a network, a specific individual could play one or several roles as this *broker*. For example, if the actor sits between two other nodes and all three share the same affiliation (*e.g.*, membership in an organization), that actor could be characterized as a coordinator. If that actor, however, does not share an affiliation with those two connected nodes, he or she could be thought of as consultant. When the actor controls access by non-network members to his or her nodes, that actor is a gatekeeper. Additionally, the degree of the actor's affiliation with some of his connected nodes may characterize him or her as representative (of one group, in contact with non-group actors), or as a liaison (affiliated with no group, but mediating contact between groups in the network).

46. Watts, 230. The firewall analogy is mentioned by Watts in the context of discussing how SNA might identify triggers for domino-like cascades (as in power grid failures) and, conversely, locations in which to place stop-gaps to prevent, if needed, the cascade; Knoke, 5. "Direct contacts and more intensive interactions dispose entities to better information, greater awareness and higher susceptibility to influencing or being influenced by others."

47. In the author's opinion, the most useful SNA reference guide for commanders and their legal advisors is Wasserman and Faust's *Methods and Applications* (specifically, chapters 2, 3, and 4).