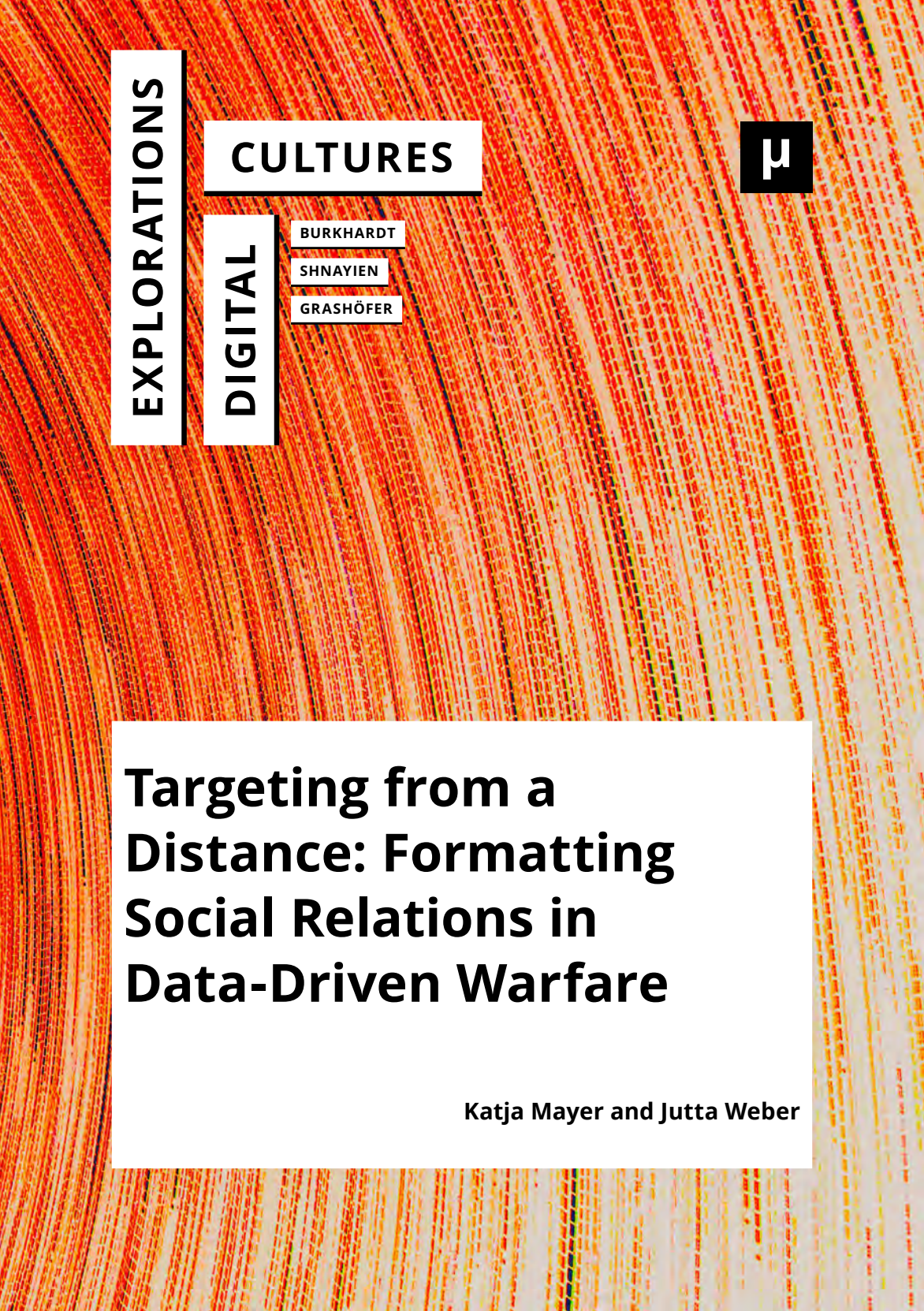
EXPLORATIONS
CULTURES
DIGITAL
BURKHARDT
SHNAYIEN
GRASHÖFER
μ
Targeting from a Distance: Formatting Social Relations in Data-Driven Warfare
Katja Mayer and Jutta Weber

Bibliographic information:

Mayer, Katja and Jutta Weber. 2021. "Targeting from a Distance: Formatting Social Relations in Data-Driven Warfare." In *Explorations in Digital Cultures*, edited by Marcus Burkhardt, Mary Shnayien, and Katja Grashöfer. Lüneburg: meson press. DOI: 10.14619/1716 <Online first version>.

NETWORK CENTRIC WARFARE

SOCIAL NETWORK ANALYSIS

NETWORK SCIENCE

COUNTERINSURGENCY

SOCIAL TECHNOLOGY

Targeting from a Distance: Formatting Social Relations in Data-Driven Warfare

Katja Mayer and Jutta Weber

In this paper we analyze enactments of a social scientific methodology, namely social network analysis (SNA) as described and depicted in contemporary US military discourses. We follow the progressive digital grounding of military organization and knowledge through the lens of SNA. Framing SNA in this context, as a social technology that is co-constituting the worlds it studies, we see that it is embedded deeply in the logics of data-driven warfare, as well as the massive industrial and governmental efforts to map the social graph. By navigating through military applications and realizations of the network metaphor, we find SNA at the core of a rhetoric of precision that underlines the potential to deliver "high value" targets, and is outlined as computational counterterrorism and counterinsurgency from a distance.

Introduction

Social network analysis (SNA) has rapidly gained momentum in the 21st century, especially as a component of military discourses and practices. SNA makes use of sociometrics, statistics and graph theory, along with qualitative approaches, to study social structures. It is well documented how military human (HUMINT) and signals (SIGINT) intelligence increasingly uses data mining and analysis tools based on this relational perspective to wade through telecommunications, social networks, and video feeds (Joint Warfighting Center 2011; Ressler 2006; Sageman 2004).

This paper discusses enactments of social network analysis around the turn of the millennium, at the heart of network science in US military discourses with regard to their impact on concepts and practices such as targeting, computational counterterrorism and counterinsurgency[1] (COIN). We first take a look at the description of SNA as a powerful tool for threat evaluation in the context of the (now famous) counterinsurgency field manual 3-24, which established the doctrine of network centric warfare in 2006. Secondly, we will elaborate on the recent misappropriation of the so-called "cultural turn" in military evidence practices and the revived high hopes of a computational counterinsurgency from a distance. By framing SNA as a social technology that is both de- and inscribing the world it studies (Akrich and Latour 1992), we analyze its role and transformation in the network centric approach to warfare: from face-to-face to remote access to the social graph, rendering the world "actionable and amenable to intervention" (de Goede 2012, 216).

Social Network Analysis: A Social Technology Shaping Warfare

Network concepts come with a powerful methodology. Rooted in the social psychology, anthropology, sociometry, and sociography of the early 20th century, social network analysis enables researchers to study groups of actors (human and non-human) and their relationships (e.g. in terms of kinship, trust, transfer, and infrastructures) as networks (Freeman 2004). Actors are described as "nodes" and their relationships as "ties" in a

1 Computational counterinsurgency dates back to Vietnam and the US Phoenix program, when IBM mainframe computers were used to order, categorize and classify populations and groups to generate statistics and models for the prediction of insurgent activity in "real time" (Belcher 2014, 183) and to create "kill lists" (González 2015, 14).

network or in a component of a network. From its beginnings, sociometry was connected to a political goal: the "sociometrical revolution" (Moreno 1934) of social change. Whereas Moreno, in line with many other early contributors to sociometics, aimed at designing scientific instruments for the self-empowerment of individuals and small groups (Mayer 2012), today's social network science comprises a fast-growing set of methodologies, including methods based on graph theory and statistics as well as qualitative methods that provide powerful tools for investigating, describing, intervening and predicting complex social relationships. By measuring elements such as node centrality or clusters, researchers gain answers to questions such as "[W]ho are the connectors, … leaders, bridges, isolates, where are the clusters and who is in them, who is in the core of the network?" (Krebs 2002). SNA focuses on the relational dimensions rather than on the individual characteristics of actors. It assumes that the network structure will affect the network's capacity to build trust, gain power, access information, and so forth. Data collection based on SNA principles produces social graphs, depicting social relations from groups of people to whole populations, like whistleblowers from the NSA claiming that they created a "big-ass graph" (Binney quoted in Moser, 2015) of communications metadata from 2.2 billion individual users at the turn of the new millennium. Social network analysis – the social scientific basis of the social graph – has long been appropriated by security services and the military. It is a tool for social engineering, a social technology that not only describes but also constitutes the social and as such, is predisposed to support social surveillance and control (Derksen and Beaulieu 2011).

Revolution in Military Affairs: Network-Centric Warfare

Today, we are witnessing an increasing shift from nation-state wars towards asymmetric and unconventional warfare, and the privatization of (at least some) military tasks, as well as an increasing entanglement of domestic security and surveillance architectures with (post-colonial) counterinsurgency (Gregory 2011). A "revolution in military affairs" (RMA) has transformed the US military and US foreign policy since 1989 (Dillon 2002). This has been accompanied by a gradual crumbling of the Cold War balance of power and the policy of nuclear deterrence. RMA is based on the paradigm of technological superiority, information sovereignty (Arquilla and Ronfeldt 2001), and the close networking of information technologies, including the concept of "network-centric warfare" (Cebrowski and Garstka 1998). The information network becomes the key military unit. At the core of the ideal of network-centric warfare are smart, small, flexible and

geographically-dispersed troops, constantly linked to a high-performance information grid. This grid consists of all appropriate information sources and allows for high-speed command and control processes, such as automated assignment of resources to need, or integrated sensor networks for augmented context awareness of soldiers.

According to the doctrine, network-centric warfare is applicable to all levels of warfare and contributes to the coalescence of strategy, operations, and tactics. It is conceptualized as being fully transparent to mission, force size and composition, as well as geography, striving for "total battlespace awareness" (Harris 2006, 103). This revolution in military affairs turns war into "a capital-intensive process of high-tech killing at a distance" (Graham 2011, 29), while the rhetoric of precision and surgical strikes aims at making war more humane. The war in Iraq that started in 2003 is regarded by many as the first operational test of network-centric military strategies, and the realization of Bush's "American exceptionalism", building on aggressive, proactive high-tech warfare and Network Science.

Connecting the Dots: Network Science for Targeting

When, after 9/11, the US intelligence services and armed forces were blamed for not having been able "to connect the dots" (US Senate Select Committee in Intelligence and US House Permanent Select Committee on Intelligence 2004) to predict and prevent the attacks, retrospective reading was turned into proactive and pre-emptive action: in hindsight, the plots and the actors seemed obvious, but anticipating future risks and identifying potential terrorists poses new challenges that SNA can supposedly help to resolve. In 2002, for example, Valdis Krebs argued in his paper "Uncloaking Terrorist Networks" for the usefulness of SNA for mapping terrorist networks in a rigorous scientific manner from publicly available sources (Krebs 2002). By 2006 the Counterinsurgency Field Manual 3-24 included SNA in its recommendations (US Army / US Navy 2006), along with accounts of the capture of Saddam Hussein attributed to the mapping of his social relations (Reed 2006). This new prominence of SNA was further underlined by the discovery and killing of Osama bin Laden based on insights about his courier network in 2011 (Knoke 2013). The possibility of revealing hidden patterns (e.g. the behavior of members of terror cells) in publicly available data was just one of many attributions. Finally, there seemed to be a sound scientific method at hand to fight terrorism and many other threats with precision. In that regard, the network terminology

became an epistemic device that not only measures the world, but also prepares it for intervention and action (de Goede 2012).

The network doctrine is regarded as a "secularized cosmological vision" (Belcher 2014, 169), which "is novel in its pursuit to explain the entirety of the human and non-human chain of being as one wholly comprised of networks and dynamic relational systems – agents, clusters, lattices, and randomness abound" (ibid.). The network has since penetrated many academic as well as non-academic discourses – including those of the military. One of those military discourses already mentioned revolves around counterinsurgence – the label used to describe the totality of actions aimed at defeating irregular forces. The concept dates back to the Vietnam war and its many challenges, such as unpredictability and scaling, and it was taken up again and adapted by US and NATO partners to tackle the multitude of problems and failures of the military apparatus in Iraq and Afghanistan. In 2006 US generals David H. Petraeus and James F. Amos developed the their highly influential counterinsurgency doctrine with a special focus on continuous strategic learning (US Army / US Navy 2006). According to the field manual, military action and reconstruction assistance should be coordinated as optimally as possible. These military leaders called for more awareness when intervening in foreign polities, and for this new understanding of the situation to be supported by social science instruments (Ucko 2012). At the time of its publication and for many years afterwards, the counterinsurgency approach was considered by many decision-makers to be an adequate way of combating terrorism and a guarantee of stability. But later evaluations concluded that the success of the COINS strategy was overestimated, and by 2020 transitions from counterinsurgency operations to multi-domain and large-scale combat operations had already become apparent in US military tactics (Egel et al. 2016; SIGAR 2018; US Army 2018, 2020).

A Networked Cultural Turn in Military Strategy

Back in the early 2000s, the notion of a scientifically grounded and actionable understanding of the socio-cultural context of populations was clearly dominating Western military operations, and the concept of social networks was core to this approach.

In the aforementioned field manual, SNA is presented as tool for tracing covert actors from diverse geopolitical backgrounds. The authors consider the idea of "networking among military services to defeat enemy networks" (Knoke 2013, 7) as being among the most radical innovations of network

centric warfare: SNA helps units formalize the informality of insurgent networks by portraying the structure of something not readily observed: a form of latent knowledge. Network concepts deduce roles, organizational positions, prominence and the influence of actors from preexisting socio-technical relationships. Therefore, commanders can grasp how organizations are structured and how groups function, how members are influenced, and power is exerted, and how resources are exchanged (US Army / US Navy 2006, B17). In this context, insurgent organizations are described, above all, as flexible and mutable networks.

The field manual's authors' fascination with networked organizations mirrors their wish to shed the disadvantages of over-organization and bureaucratization of a traditional institution such as the US military, and to become as mutable as the highly successful Afghan insurgent networks, but with information-technological superiority. The goal of militarized network analysis, in line with the concept or revolution in military affairs, is

> [a]n Army-led effort to realize a network science to enable Network Centric Warfare through the incorporation of interdependency and networked human and organizational behavior leading to effective employment of the full spectrum of C4ISR [Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance] technologies (Arney 2010, 10).

Network science is now considered capable of extracting and analyzing meaningful common patterns, principles and behaviors typical of quite diverse kinds of networks, and thereby, hoping to predict their activities (Arney 2010). From 2006 onwards, military research communities have implemented and institutionalized network science. Efforts to include network science in military education and research gave rise to new army research laboratories, including a Network Science Center at West Point Academy and many other initiatives funded by the Minerva program – a Department of Defense-sponsored research program initiated in 2008. Its goal was to "improve DoD's basic understanding of the social, cultural, behavioral, and political forces that shape regions of the world of strategic importance to the US" (Anon 2020). Many of those initiatives are rooted in the broad popularity of the COIN manual. Its authors write:

> "[F]or an insurgency, a social network is not just a description of who is in the insurgent organization; it is a picture of the population, how it is put together and how members interact with one another. … The ways in which insurgents exploit a tribal network does not represent an

evolved form of insurgency but the expression of inherent cultural and social customs (US Army / US Navy 2006, B15).

Messy Data: Maneuvering through Networked Human Terrain

In many papers co-authored by military scientists, SNA is highlighted as a precise methodology for dealing with "messy" social data (Dekker 2002; Tsvetovat and Latek 2008). The idea of using SNA to formalize informalities appears consistently throughout our document corpus (Reed and Segal 2006). Rarely is this taken-for-grantedness shaken or questioned. Only a few critical voices – mostly from academic research institutions funded partly by the military - called for military network science to be developed further methodologically, e.g. by incorporating more elements of dynamic and multiplex social network analysis. It was pointed out that it will become more and more difficult to "remove the noise" (Bohannon 2009, 410) in big (meta) data contexts where "network analysis tools … handle millions or tens of millions of nodes" (ibid. 411). Others question whether military applications of SNA can effectively distinguish between the ability to network in terms of communication and connectivity and "the ability to mobilize, control and coordinate members for specific planned acts" (Stohl and Stohl 2007, 110). Furthermore, they doubt whether there is a profound understanding of different network forms and modes and their effects. Connections are often rashly misinterpreted as contacts and shared opinions are wrongly equated with organization. However, as set out in the field manual, local knowledge gathered by "patrols" (US Army / US Navy 2006, 3.26) is the most important ingredient in conducting SNA on networked insurgent organizations. This quest for local knowledge by armed forces was termed the "cultural turn" and included the establishment of the infamous and now discontinued Human Terrain System (HTS, 2007-2014) (González 2015; Weinberger 2008).

Network science was also central in the HTS program run by the United States Army Training and Doctrine Command. HTS teams were to provide military services and field commanders with knowledge about the local population in war zones. It is not a simple task to differentiate "friendly and enemy social structures" (Crane 2010, 67). Therefore, the authors of the US counterinsurgency doctrine focus on strong ties, such as kinship, and strong bonds formed over time as key information to be collected by patrols engaged in analyzing documents, interviewing individuals, and studying photos and books. In order to "formalize the informality of insurgent networks" (US Army / US Navy 2006, B17.55), links are established

between network nodes by identifying similarities, such as co-participation in the same activities, roles or organizational positions. Furthermore, the *HTS Handbook* (Finney 2008) paints a picture of a three-sided conflict that consists of a local population struggling between friendly or coalition forces and the enemies or insurgents. Gaining the trust of the local population is considered imperative for the forces and another core objective of the HTS.

Hence, the cultural turn in military affairs and network-centric warfare brought about the embedding of social scientists in battlefield operations to collect ground truth and to monitor the human landscape. Human Terrain information is a conglomeration of socio-cultural attributes extracted from interview data, and secondary sources in public repositories such as libraries, internet resources, geospatial facts, and many other shared intelligence resources used to conduct battlefield operations – all of which could be data relevant to SNA. In military strategy, this is regarded as an enriched information network for decision making in command and control contexts. The *HTS Handbook* lists core software components for advanced data analysis, such as *Analyst Notebook*, *ArcGis*, *Anthropac*, and *UCInet* with *Netdraw*; the latter two are SNA specific programs which were very popular at that time (Finney 2008, 47). Originally, these were supposed to be used for handling information gathered about local group leaders, "tribes"[2] or social groups, political controversies, economic issues and social challenges, turning them into maps of the spatial distribution of groups or producing link charts and timelines. However, human terrain specialists supposedly used those toolsets to bring together ground truth with information from remote databases shared by military and other government agencies. It is likely that social networks and socio-cultural patterns could be visualized, modeled and evaluated nearly in real-time. "Our research is performed in the same manner in which academic social scientists conduct their research and is similarly rooted in theory and complete with ethical review boards" (Finney 2008, 56): the *HTS Handbook* reads as an attempt to give the impression of an ethically immaculate social scientific research project, complete with notions of social engineering and social control of environments. The industrial-military complex supplied HTS with human resources and data analytics.

2 Belcher (2013), Gregory (2011), Mamdani (2012) and others have pointed out that categories such as tribe or clan are often the product of (neo-)colonial politics and counterinsurgency strategies, which construct group identities in order to better manage the population and to provide orientation in a complex and fluid (battle) environment in which the enemy is hard to pinpoint.

Optimizing Networked Insights: Computational Counterinsurgency

Although the importance of gaining a more rigorous, objective understanding of "tribes", "clans", and various ethnic groups in war-torn countries and their relationships to ongoing insurgencies had been acknowledged long before, military contractors began stressing once more the significance of socio-cultural knowledge management for military forces and armed peacekeepers who were taking part in the wars in Iraq and Afghanistan, keen to reap the profits to be made from such activities (Weinberger 2008). Reports state that the US Army quietly terminated the HTS program in September 2014 (González 2015). Indeed, as far back as 2008 it had been criticized for not being able to recruit and retain qualified social scientists (Weinberger 2008). Moreover, despite the rhetoric of scientific precision and targeting power, it was shown that the socio-cultural knowledge they referred to tended to produce only reifications, clichés and stereotypes (Price 2011). Furthermore, sifting through the publicly available documentation and critique of the HTS, we find rather divergent accounts of its efficiency and of the scope of its assignments. Besides having rather untrained personnel patrolling villages and interviewing the local "populace" without systematic methods, so called "reachback centers" and intelligence analysts worked with the data collected and rashly combined it with data from other unverified sources, such as Wikipedia and social media (Arnold, 2010; González, 2017; Price, 2008).

However, in 2015, companies such as Cyberspace Solutions, Silverback7, and Streamline Defense still advertised dozens of positions with job titles such as "Human Terrain Analyst", "Cultural Subject Matter Expert", and "Human Terrain Specialist" (Gonzáles and Price 2015), with requirements such as: "having advanced targeting skills and a comprehensive understanding of the operational cycle as well as the data, tools, and techniques used for each phase of the … targeting cycle" (Engility 2015). The company Silverback7 looked for HTAs as well: "Human Terrain Analysts shall have firsthand experience targeting networks or individuals within networks and identifying vulnerabilities for exploitation" (Gonzáles and Price 2015). From such job adverts it can be inferred that "analyst-warfighters" produce target data and play their part in the imagined precision of targeted killing or "manhunting" warfare (Chamayou 2011; Gregory 2011).

The job adverts demonstrate a shift in the concept of sociocultural understanding: what was once regarded as micro level human interaction on site is transformed into a navigation of sociocultural landscapes from a

distance. Besides the fact that the actual deployment and proclaimed efficiency of the HTS have been overrated, programs like these were a perfect stepping stone for new, improved and de-humanized remote methods of assessing the social graph. The rapid rise of military network science or "computational counterinsurgency" is by far more powerful and "scandalous" (Belcher 2013; Duffield 2015, 89). In 2016, Palantir Technologies Inc. won a US$222 million sole source contract to support the Department of Defense's Special Operations Command. The aim was to provide a technology and logistics software and support project called All-Source Information Fusion that "meant to bring together intelligence and other information gathered by SOCOM, which oversees the special operations units of all branches of the U.S. military" (Fazzini and Macias 2019). At that time, Palantir Defense's website boasted how it did not need social scientists on the ground anymore: instead it allows warfighters to interact with all data,

> unstructured message traffic, identity data, link charts, spreadsheets, telephony, documents, network data, sensor data—even full motion video can be searched simultaneously and intuitively, without the need for a specialized query language. With SIGINT, [...] fused into a single, coherent model, users can discover previously unseen links across their entire universe of data. Palantir Defense enables warfighters to rapidly turn mountains of data into plans of action by asking the questions they need answered in a language they understand (Palantir 2017).

This deal is dwarfed by Palantir's most recent (2019) success: winning a contract potentially worth more than US$800 million to deploy a complex battlefield intelligence system for US Army soldiers, a Distributed Common Ground System, "which lets users gather and analyze information about enemy movements, terrain and weather to create detailed maps and reports in real-time. The system is designed to be used by soldiers fighting in remote, harsh environments" (Harris 2019). The Department of Defense's decision for a Silicon Valley "data science" company that had been steadily evolving from its origins in national security circles – first into business and government domains, and now, to a major defense contractor – was based on bad experiences with previously installed intelligence systems.

Formatting Social Reality from a Distance

Hence, the trend is moving further away from embedding social scientists as "ground truth" collectors, mediators and analyst-warfighters directly in

the battlefield. Big data has long promised to accompany a turn in network science away from social scientific involvement and towards engineering expertise in computational modeling of the social – a "full data ecosystem" (Brayne 2020), which looks like a good alternative to the messy entanglements in human terrain.

Warfighters should not "drown in data" before they can make their decisions (Weinberger 2011, 566). Instead, they should be able to drill down and gain situational awareness. Therefore, automated filter systems are needed, systems capable of converging data and models that can predict behavior and evaluate induced behavior change. Several years later, we already find SNA at the heart of platforms such as DARPA's Nexus7, which combine "reality mining" with behavioral modeling, predictive analytics, and the simulation of networks from multiple converging data sources. Reality mining is used to measure and predict, for example, whether groups are falling apart or stabilizing, or if insurgent support is increasing or not. It involves the analytic assemblage of all kinds of environmental and social behavioral data, often gathered via sensors and algorithms to identify patterns. Data sources include biometric databases, village surveys, checkpoint intelligence, social media analysis, and indicators of local issues, such as commodity prices and wage rates (Belcher 2013, 181–92; Duffield 2015, 89). Other "rapid ethnographic retrieval" (Diesner 2012, 328) systems include opinion records, lists of ethnic attitudes, and thesauri on subject matters relevant to groups or societies, which are assembled by domain experts. Modeling networks from the data collected and factoring in such cultural variables can help, it is claimed, to automatically identify potential targets or "selectors", such as information brokers, gatekeepers to critical resources, and influencers. Such platforms are intended to help with formalizing "local knowledge" by quantifying, modeling and predicting all of the available dimensions of conflict in nearly real-time. Today, network science is an integral part of data science. Military spending for such types of next generation data science is increasing steadily, as the Palantir defense contract discussed above shows. Since 2008 the US defense budget has been dedicating only a fraction of around $20 million to the social science research program Minerva every year (National Academies of Sciences, Engineering, and Medicine 2020), whereas the funding of R&D efforts related to big data and artificial intelligence is rising across all military services. Market analysts report projected spending of a combined US$5.2 billion in fiscal year 2021 for 319 research and development programs with a focus on big data and "some AI/ML component" (Doubleday

2020) of which at least US$1 billion will be dedicated to data analytics for intelligence (Rossino 2020).

Conclusions

Studying the use of social network analysis in data-driven warfare inadvertently makes SNA's ubiquity in the operationalization of the network concept come to the fore. SNA is used as a tool and medium to promote the (trans)formation of networked military organization, to facilitate targeting, and to co-shape the very concept of counterinsurgency. SNA rendered the social graph actionable for militaries and security forces and supplied both guiding imaginaries of situational awareness and formal tools to measure the performance and impact of operations[3]. With its promise to make hidden structures accessible, SNA formats its objects of research as targetable nodes and ties based on a rhetoric of precision that is not appropriate given the rather unreliable data basis, and its lack of experience in extracting meaning and knowledge from big and often messy data.

The attractiveness of SNA rests on its hybrid character of being a social science, a computational method and a technology for social engineering and intervention all at once. However, critics from academic social sciences have argued that a well-grounded expertise of the 'social' is lacking in the methodology itself, best illustrated by the institutionalization of "Network Science" in the US military research system, without the preposition "social" (Knoke 2013). With its measurement and quantification of activities, military network science follows the general ontological shift in contemporary technosciences from describing the features of an entity towards mapping its behavior (Weber 2014). Models, quantitative metrics and indicators are supposed to be more precise than the reflection of complex cross-cultural practices, or anthropological assessment, as if it was just a matter of getting the programming right. The current focus of military funding, however, has shifted from the social sciences to data science. The emphasis lies on the automated gathering of cultural knowledge of behavior, and the latent communication contained in big data obtained from various sources. Drilling down the social graph, the data analytic techniques of combining social media data with geospatial intelligence from other sensor systems and chaining latent contacts have become central beyond the military and security complex (Brayne 2020; Gellman 2020).

3 This can be observed in many other sectors as well, which deal with big data, e.g., from social media, such as marketing, political campaigning, public health management or behavioral engineering.

Therefore, once again the social sciences are being called upon to "humanize" data-driven warfare. After two decades worth of multi-billion-dollar investments into artificial intelligence and cybersecurity "in everything from image recognition in surveillance, to brain computer interfaces for drone pilots" (Evans 2020), research on the social entanglements within those technologies have not kept pace. The rise of military data science based on automated (meta) data collection from vast sources and the application of network analysis as well as machine learning has prompted widespread critique: the killing of innocent "people based on meta-data" – as detailed in leaked documents about the NSA programme Skynet and its "scientifically unsound algorithms" (Grothoff and Porup 2016) – has been condemned and documented in various forms, the drone warfare, which is modeled on the basis of these methods, has also been critized (Weber 2016). Today, SNA is an integral part of this toolset and has thus turned into a central technology of sovereignty, surveillance and remote control, not only in the military realm. This movement towards the increased digital grounding of military organization and knowledge is realized further by the US military's (once) revolutionary objective of becoming a network itself – though resting on a dubious epistemology of precision and control of the social.

References

Akrich, Madeleine, and Bruno Latour. 1992. „A Summary of a Convenient Vocabulary for the Semiotics of Human and Nonhuman Assemblies". Pp. 259–64 in *Shaping Technology, Building Society. Studies in Socio-technical Change*, edited by W. Bijker and J. Law. Cambridge MA.

Anon. 2020. „Minerva Research Initiative". *Minerva Research Initiative*. Retrieved 29 December 2020 (https://minerva.defense.gov/).

Arney, Chris. 2010. „The Army's Network Science Needs and Opportunities: Realizing the Potential of Network Science through the NRC Recommendations". *Papers of the 5th Annual Network Science Workshop 26-28 October 2010*. West Point, New York: Network Science Center at Westpoint.

Arnold, Matthew. 2010. „Human Terrain Mapping in Kapisa Province: Improving the Coalition's Understanding of 'The People' in Afghanistan". *Small Wars Journal*. Retrieved 30 December 2020 (https://smallwarsjournal.com/jrnl/art/human-terrain-mapping-in-kapisa-province).

Arquilla, John, and David Ronfeldt. 2001. „The Advent of Netwar (Revisited)". *Networks and Netwars: The Future of Terror, Crime, and Militancy* 1–25.

Belcher, Oliver. 2013. „The Afterlives of Counterinsurgency: Postcolonialism, Military Social Science, and Afghanistan 2006-2012". diss., The University of British Columbia, Vancouver.

Belcher, Oliver. 2014. „Staging the Orient: Counterinsurgency Training Sites and the U.S. Military Imagination". *Annals of the Association of American Geographers* 104(5):1012–29. doi: 10.1080/00045608.2014.924736.

Bohannon, John. 2009. "Counterterrorism's New Tool: 'Metanetwork' Analysis". *Science* 325(July):409–11.

Brayne, Sarah. 2020. „Enter the Dragnet". *Logic Magazine* 12.

Cebrowski, Arthur K., and John J. Garstka. 1998. „Network-Centric Warfare: Its Origin and Future". *US Naval Institute Proceedings* (January):28-35.

Chamayou, Grégoire. 2011. „The Manhunt Doctrine". *Radical Philosophy* 169(3):15.

Crane, Conrad. 2010. "'Doctrine: United States'". Pp. 46–58 in *Understanding counter-insurgency: doctrine, operations and challenges*, edited by T. Rid and T. Keaney. London: Routledge.

Dekker, Anthony. 2002. „Applying Social Network Analysis Concepts to Military C4ISR Architectures 1". 24(3):93–103.

Derksen, Maarten, and Anne Beaulieu. 2011. „Social Technology". Pp. 703–20 in *The SAGE Handbook of the Philosophy of Social Science*, edited by I. C. Jarvie and J. Zamora-Bonilla. London: SAGE Publications.

Diesner, Jana. 2012. „Extracting Socio-Cultural Networks of the Sudan from Open-Source, Large-Scale Text Data". *Journal of Computational and Mathematical Organization Theory* 18(3):328–39. doi: 10.1007/s10588-012-9126-x.

Dillon, Michael. 2002. „Network Society, Network Centric Warfare, and the State of Emergency". *Theory, Culture & Society* 19(4):71–79.

Doubleday, Justin. 2020. „New Analysis Finds Pentagon Annual Spending on AI Contracts Has Grown to $1.4B". *InsideDefense.Com*. Retrieved 29 December 2020 (https://insidedefense.com/insider/new-analysis-finds-pentagon-annual-spending-ai-contracts-has-grown-14b).

Duffield, Mark. 2015. „The Digital Development-Security Nexus: Linking Cyber-Humanitarianism and Drone Warfare". Pp. 80–94 in *Handbook of International Security and Development*, edited by P. Jackson. Cheltenham: Edward Elgar Publishing.

Egel, Daniel, Charles P. Ries, Ben Connable, Todd C. Helmus, Eric Robinson, Isaac Baruffi, Melissa A. Bradley, Kurt Card, Kathleen Loa, Sean Mann, and others. 2016. *Investing in the Fight: Assessing the Use of the Commander's Emergency Response Program in Afghanistan*. RAND Corporation.

Engility. 2015. „Human Terrain Specialist". *Engility - Job Announcement*. Retrieved (http://www.engilitycorp.com/).

Evans, Nick. 2020. „Don't Shutter The Minerva Initiative: Social Science Helps DoD". *Breaking Defense*, March 16.

Fazzini, Kate, and Amanda Macias. 2019. „Peter Thiel's Company Palantir Just Won a Major Pentagon Contract, Beating out Traditional Military Vendors". *CNBC*. Retrieved (https://www.cnbc.com/2019/03/27/palantir-in-multi-million-dollar-pentagon-deal-ipo-on-horizon.html).

Finney, Nathan. 2008. *Human Terrain Team Handbook*. Fort Leavenworth, KS: Human Terrain Systems.

Freeman, Linton C. 2004. *The Development of Social Network Analysis: A Study in the Sociology of Science*. Vancouver: Empirical Press.

Gellman, Barton. 2020. „Inside the NSA's Secret Tool for Mapping Your Social Network". *Wired*, May 24.

de Goede, Marieke. 2012. „Fighting the Network: A Critique of the Network as a Security Technology". *Distinktion: Scandinavian Journal of Social Theory* 13(3):215–32.

Gonzáles, Roberto J., and David Price. 2015. „Remaking the Human Terrain: The US Military's Continuing Quest to Commandeer Culture". *Www.Counterpunch.Org*. Retrieved 16 September 2015 (http://www.counterpunch.org/2015/07/31/remaking-the-human-terrain-the-us-militarys-continuing-quest-to-commandeer-culture/).

González, Roberto J. 2015. „Seeing into Hearts and Minds: Part 1. The Pentagon's Quest for a "Social Radar" (Respond to This Article at Https://Www.Therai.Org.Uk/Publications/Anthropology-Today/Debate)". *Anthropology Today* 31(3):8–13. doi: 10.1111/1467-8322.12174.

González, Roberto J. 2017. „Ethnographic Intelligence: The Human Terrain System and Its Enduring Legacy". Pp. 51–73 in *Reconfiguring Intervention*. Springer.

Graham, Stephen. 2011. *Cities under Siege: The New Military Urbanism*. London: Verso.

Gregory, Derek. 2011. „The Everywhere War". *The Geographical Journal* 177(3):238–50. doi: 10.1111/j.1475-4959.2011.00426.x.

Grothoff, Christian, and J. M. Porup. 2016. „The NSA's SKYNET Program May Be Killing Thousands of Innocent People". *Ars Technica*. Retrieved 29 December 2020 (https://arstechnica.com/information-technology/2016/02/the-nsas-skynet-program-may-be-killing-thousands-of-innocent-people/).

Harris, Chad. 2006. "The Omniscient Eye: Satellite Imagery, 'Battlespace Awareness,' and the Structures of the Imperial Gaze". *Surveillance & Society* 4(1/2).

Harris, Shane. 2019. "Palantir Wins Competition to Build Army Intelligence System". *Washington Post*, March 26.

Joint Warfighting Center. 2011. *Commander's Handbook for Attack the Network*. Joint Chiefs of Staff.

Knoke, David. 2013. "'It Takes a Network': The Rise and Fall of Social Network Analysis in U.S. Army Counterinsurgency Doctrine". *Connections* 33(1):1–10.

Krebs, Valdis E. 2002. „Uncloaking Terrorist Networks". *First Monday* 7(4).

Mamdani, Mahmood. 2012. "What Is a Tribe". *Lond. Rev. Books* 34:20–22.

Mayer, Katja. 2012. „Objectifying Social Structures: Network Visualization as Means of Social Optimization". *Theory & Psychology* 22(2):162–78.

Moreno, Jacob Levi. 1934. *Who Shall Survive? A New Approach to the Problem of Human Interrelations*. New York, NY, USA: Beacon House.

Moser, Fritz. 2015. *A Good American*.

National Academies of Sciences, Engineering, and Medicine. 2020. *Evaluation of the Minerva Research Initiative*. *Consensus Report*. Washington, D.C.: National Academies Press.

Palantir. 2017. „Palantir Defense". *Palantir Technologies*. Retrieved (https://www.palantir.com/solutions/defense/,).

Price, David. 2008. „The Leaky Ship of Human Terrain Systems". *CounterPunch. Org*. Retrieved 30 December 2020 (https://www.counterpunch.org/2008/12/12/the-leaky-ship-of-human-terrain-systems/).

Price, David H. 2011. *Weaponizing Anthropology: Social Science in Service of the Militarized State*. Petrolia, Oakland, CA: Counter Punch & AK Press.

Reed, Brian. 2006. „Formalizing the Informal: A Network Analysis of an Insurgency". *Digital Repository at the University of Maryland*.

Reed, Brian J., and David R. Segal. 2006. „Social Network Analysis and Counterinsurgency Operations: The Capture of Saddam Hussein". *Sociological Focus* 39(4):251–64. doi: 10.1080/00380237.2006.10571288.

Ressler, Steve. 2006. „Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research". *Homeland Security Affairs* 2(2).

Rossino, Alex. 2020. „Big Data in DOD's FY 2021 Procurement and RDT&E Budget Programs | GovWin IQ". Retrieved 29 December 2020 (https://iq.govwin.com/neo/marketAnalysis/view/Big-Data-in-DODs-FY-2021-Procurement-and-RDTE-Budget-Programs/4504?researchTypeId=1&researchMarket=).

Sageman, Marc. 2004. *Understanding Terror Networks*. University of Pennsylvania Press.

SIGAR. 2018. *Stabilization: Lessons From The U.S. Experience in Afghanistan*. Special Inspector General for Afghanistan Reconstruction.

Stohl, Cynthia, and Michael Stohl. 2007. „Networks of Terror: Theoretical Assumptions and Pragmatic Consequences“. *Communication Theory* 17(2):93–124. doi: 10.1111/j.1468-2885.2007.00289.x.

Tsvetovat, Maksim, and Maciej Latek. 2008. „Dynamics of Agent Organizations: Application to Modeling Irregular Warfare“. Pp. 60–70 in *International Workshop on Multi-Agent Systems and Agent-Based Simulation*. Springer.

Ucko, David. 2012. „Whither Counterinsurgency: The Rise and Fall of a Divisive Concept“.

US Army. 2018. *The US Army in Multi-Domain Operations 2028*. 525-3–1. Fort Eustis, VA: United States Army Training and Doctrine Command.

US Army. 2020. „Army to Discontinue Asymmetric Warfare Group and Rapid Equipping Force“. Retrieved (https://www.army.mil/article/239622/army_to_discontinue_asymmetric_warfare_group_and_rapid_equipping_force).

US Army / US Navy. 2006. *Counterinsurgency Field Manual*. US Army and Marine Corps.

US Senate Select Committee in Intelligence, and US House Permanent Select Committee on Intelligence. 2004. *Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001: Hearings Before the Select Committee on Intelligence, US Senate and the Permanent Select Committee on Intelligence, House of Representatives*. Vol. 107. US Government Printing Office.

Weber, Jutta. 2014. „Wild Cards: Imagination Als Katastrophenprävention“. *Zeitschrift Für Kulturwissenschaften* 8(2):83–97.

Weber, Jutta. 2016. „Keep Addin: Kill Lists, Drone Warfare and the Politics of Databases“. *Environment and Planning D. Society and Space*.

Weinberger, S. 2011. „Web of War“. *Nature* 471:566–68.

Weinberger, Sharon. 2008. „Military Research: The Pentagon's Culture Wars“. *Nature News* 455(7213):583–85. doi: 10.1038/455583a.