

PSYOP, CYBER, and Internet Influence: Firing Digital Bullets

CL Cook

*Headquarters
Department of the Army
Washington, D.C., United States*

E-mail: Chaveso.l.cook.mil@mail.mil

Abstract: *With the ubiquitous nature of the Internet, social media, and their continued exponential growth across society, it is necessary to comprehensively understand these platforms to engage threat networks at home and abroad. Undergirding all web-based actions, however, is human behaviour. Therefore, understanding human behaviour and the dynamic range of characteristics, actions, and attributes that are influenced by culture and context, for web-based offensive and defensive actions, is an ever-evolving niche skill. As such, non-kinetic activities and change efforts, especially in the cyber domain, require cross-cultural competence and experience in addition to any cyber capability.*

Keywords: *Information Warfare, Cyber, Irregular Warfare, Psychological Operations*

Introduction

The 21st century's revolution of military affairs made countries like the United States have limited near-peer competitors in conventional military power. In turn, many adversaries are progressively turning to irregular and asymmetric methods for engaging in conflict (Lin & Kerr 2021). Cyber is a domain that offers many of these adversaries an opportunity to counter conventional military advantages, especially within the realm of information warfare. The cyber domain has become a key means to distribute propaganda and extremist ideologies to conduct information warfare. As such, radical ideology and its associated acts of both domestic and foreign terrorism remain a threat to the global community.

Ideology is the manifestation of deep beliefs based upon intensely held but rarely understood underlying assumptions. A bullet may kill an extremist, but it will not kill his or her ideology; that is, “bullets do not kill ideas; a ‘hot’ war against an idea is destined to be a losing prospect” (Staton 2015). Perhaps a 9/11-type event is not as likely to happen again in the form of planes, trains, or suicide bombs—it is more likely to happen through mass media exploitation, political chess, electoral manipulation, and cyber intrusion via social influence mediums. Arguably most dangerously, the event will likely be just beneath the surface, more IED than WMD.

The ubiquity of the Internet and social networking involves exponential growth of, today, a globally connected culture. Cilluffo and Clark (2014) adroitly state that “the ability to use cyberspace

to create advantages and influence events in all other operational environments and across instruments of power will ensure significant advantage” (p.112). Information is the newest joint function (Paul 2020). Information warfare is now decidedly a part of modern conflict (Ventre 2016). Consequently, a comprehensive understanding of the web is critical for the defence of any nation, as the Internet has deemed our borders borderless. As a manifestation of Moore’s (1965) Law, technology has advanced at an exponential pace and the associated technological platforms have evolved at an even higher rate (Bondyopadhyay 1998). These platforms need to be understood, as recognised in the creation of organisations like the U.S. Cyber Command (USCYBERCOM) in 2009 in support of America’s Department of Defense (DoD). Today, US CYBERCOM’s mission is to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners (United States Cyber Command 2021).

However, if the social network is the IED of choice for tomorrow’s battlefield, then it may be the case that large, sprawling establishments like USCYBERCOM will not be best positioned to fight without parallel efforts that align with specially trained elements that focus on the human terrain. Winning in multi-domain operations of space, cyberspace, air, land, and sea will not occur without a critical understanding of the behaviour and political wills of the enemy, particularly in the case of China and Russia (Czege 2020). The goal here is to examine what smaller, more agile Psychological Operations (PSYOP) forces bring to the fight as distinct advantages regarding targeted online influence efforts, as well as show their connection to the efforts of the cyber community. This paper will use the history, tactics/techniques, and doctrine of the U. S. DoD to illustrate.

Critical Background and Context

Both state and non-state actors are heavily investing in the “informational sphere, placing their actions of communication, influence, propaganda, [and] psychological operations, at the heart of their strategies” (Ventre 2016, p. xiii). From individual hackers to nation states, cyber warfare activities can do everything from crippling economies to causing political unrest (Atreus 2020). Senior political and military leaders across the globe have repeatedly expounded on the importance of the information environment for military operations and declared it a priority (Paul 2020). Arguably, success against propaganda in the cyber domain hinges less on deftly maneuvering within the hypertext transfer protocol and more in the psychological battlespace, for example, the ‘gray matter’, or decision-making apparatus, of both the adversary and its population. Therefore, the Internet must be seen as the means, not the ends. Perspective with precedent matters here. If it is still believed that Clausewitz’s (1984) idea that war is an extension of politics, while also believing Naim’s (2014) claims in his book *The End of Power*, that power no longer resides exclusively (if at all) in states, institutions, or large corporations, then centers of gravity will remain located in the networks that structure society.

The information revolution has created new economic entities, ones predicated on streams of data and social networks and possessing at least as much power as other forms of organisation. However, these endeavours remain human endeavours animated by psychological functioning. As such, the fight of today and tomorrow is one of understanding minds, beliefs, and behaviours (Cowan & Cook 2018). To this end, as stated in a podcast from the United States Military Academy’s *Modern Warfare Institute*, “exquisite understanding is more important than exquisite technology” (Amble & Stephenson 2020).

Before the advent of both USCYBERCOM and the U.S. Special Forces, the PSYOP practitioner (PSYOPer) shouldered the ability to understand, operate within, and influence populations (Cook 2014). Nations across the globe will continue to encounter foes who seek to conduct non-standard, unconventional, irregular warfare. However, regardless of the methods that may be used by these adversaries, the ultimate objective is to change perception and opinion. After decommissioning the U.S. Information Agency, influencers have had no choice but to leverage the Internet as a critical piece of infrastructure. The Internet, especially social media, has become an integral part of the kill chain (Shallcross 2017). Nevertheless, to use this infrastructure effectively, an online information warfare practitioner must also be well-versed and well-practiced in changing the behaviours of the Internet's human users (Cukier 2005).

Doctrinal Underpinnings and Challenges

The multiplicative efforts by organisations like USCYBERCOM and PSYOP elements create two challenges. From an American DoD perspective, the first is tied to doctrine. At the inception of USCYBERCOM, the Joint Publication 3-13 (2014) had an Information Operations Roadmap, consisting of interrelated pillars: computer network operations (like computer network attacks, computer network defence, and computer network exploitation); PSYOP; electronic warfare; operations security; and military deception. Cyberspace is defined as “the global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers” (DoD JP3-13 2014). However, this definition lacks the cognitive, human element that the Internet represents; this omission has adversely affected how the military organises, trains, and utilises its forces (DoD JP1-02 2014).

The second challenge involves the velocity and volume of disinformation, propaganda, and threats to cyber security in the contemporary information space. The erosion of global borders is perhaps inversely proportional to the growth in Internet usage. Contemporary life, therefore, has a ubiquitous digital component; increasingly, people around the globe log on to a thriving online society that mirrors their physical communities. Therefore, cyberspace and its influence have undoubtedly shaped all interactions, up to and including warfare, and technology has increased options for the antagonist as much as it has for protagonist (Rid & Hecker 2009). Those that “seize the key terrain of social media exploitation will have a strategic military advantage” (Duggan 2014, p. 68).

As such, cyber-based influence has become a continually iterative and time-sensitive process. Who can message *first* (be “quick on the draw”), but also *most often* (keep a sustained rate of fire)? Shirky (2011) noted that “as the communication landscape gets denser, more complex, and more participatory, the networked population is gaining greater access to information, more opportunities to engage in public [sentiment] and an enhanced ability to undertake collective action” (p. 29). As much as this situation has been positive for global growth, in the modern operating environment “the nearly limitless potential for strategic communication on the Internet has [also] not gone unnoticed by terrorist organisations” (Gendon, Blass-Irizarry & Boggs 2009, p. 9).

Increasingly, there has been a belief that if “used preemptively, [online activities] could keep a conflict from evolving in a more lethal direction” (Gjelten 2013, p. 34). As today's battlefield is dominated by electronic media, the reality is that ALL future conflict will contain cyber elements

at all levels of warfare; regardless of asymmetries in capabilities, usage of cyber components is “now a part of the strategic environment writ large” (Cilluffo & Clark 2014, p. 112). Whereas every command needs to focus on its priorities, USCYBERCOM undoubtedly should not own the majority of offensive or defensive cyber operations. In turn, there are natural voids that PSYOP should fill. In particular, leveraging social networks and the human terrain for targeted influence should be a paired responsibility of entities with similar efforts and goals like USCYBERCOM and the PSYOP community, but with PSYOP in the lead.

Leveraging Social Network Analysis (SNA) for Targeted Psychological Actions in Cyberspace

Practitioners, PSYOP and otherwise, practicing information operations have long leveraged the social network. At its core, a social network—whether face-to-face or web-based—is a map of relevant ties among participants in the network through nodes and links (Gendon, Blass-Irizarry & Boggs 2009). Analysis of the information passing through the network empowers the strategic influencer with thematic guidelines to craft products that ensure messages appear indigenous in nature. SNA identifies primary information sources within the social network, thereby allowing friendly forces to target ‘influence brokers’ and key communicators. Holistically, studying this information can provide influence experts with behavioural data required to execute effective, focused, timely, and decisive influence operations. In addition to baseline data, SNA can also be another tool with which to measure operational success or battlefield effectiveness.

Often, it is only through accessing primary network nodes (or key communicators) and, exploiting them as secondary dissemination platforms, that influence operations can effectively alter the behavior of a given target audience (TA) that receives most, if not all information, from the primary node. Understanding the utility of influence brokers within a social network relies relatively little on how a computer network’s hardware is wired or how its software is implemented. The greatest reliance should be placed on attaining an intricate understanding of the node’s individual networks and what information they craft and pass on to their networked consumers. Therefore, whereas cyber elements may provide access to a node or a TA, PSYOP elements working in concert should be the ones conducting actions that influence the network. It is through iterative analyses of these specific actions and their respective influence brokers, as well as the data transiting within the network, that provide what the influence expert needs to leverage for targeted influence.

Targeting is the act of selecting and prioritizing targets via operational requirements and capabilities and matching appropriate responses to them (Bourne 2019). Whereas the targeting cycle of F3EAD (*find, fix, finish, exploit, analyze, disseminate*) is consistent with the *decide, detect, deliver, and assess* (D3A) methodology (see **Figure 1**), F3EAD has grown in prominence as it provides maneuver commanders an additional tool to address certain targeting challenges, particularly those found in the cyber domain (DoD FM 3-60 2015). Using the approach of the U.S. Army’s seven-step PSYOP planning process overlaid onto a targeting cycle can help influence experts provide advice for information warfare efforts (see **Figure 2**, below). During the steps of the seven-step process (Planning [PLAN], Target Audience Analysis [TAA], Series Development [SDEV], Product Development and Design [PDEV], Approval [APP], Production, Distribution and Dissemination [PD&D], Evaluation [EVAL]), PSYOPers are essentially in a targeting cycle (DoD FM 3-05.301

2015). Starting with the intent and the end state desired, as given by the commander, through to establishing baselines, initial assessments of measures of performance/effect, and moving through the rest of the process, the use of SNA inherently augments the targeting process (Brown 2012). Using this adapted targeting cycle, the inclusion of SNA into offensive and defensive operations can appropriately shift and direct how influence experts fire digital bullets, but it also can translate to decision makers the effects they desire to achieve.

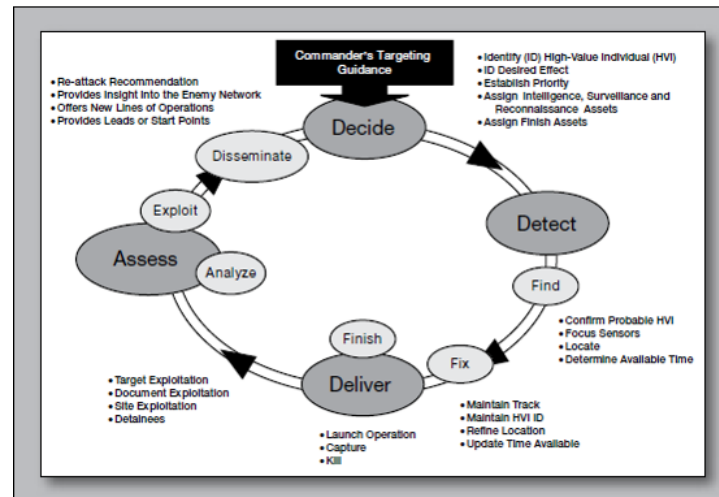


Figure 1: D3A and F3EAD (DoD FM 3-60 2015).

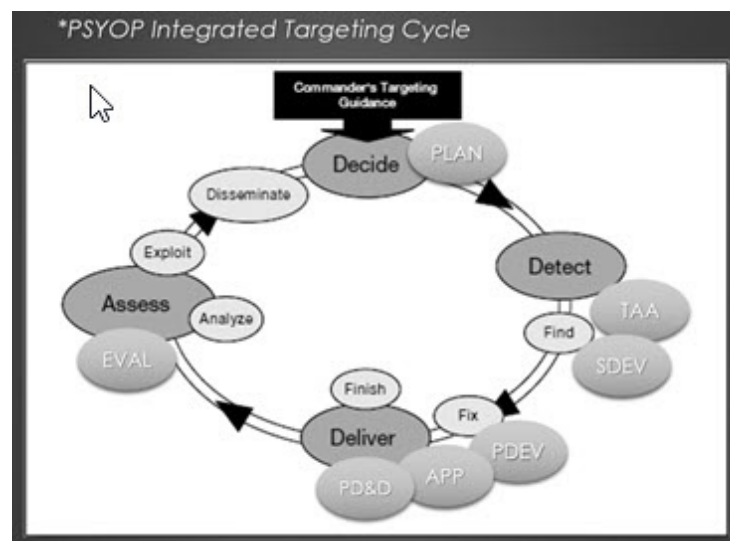


Figure 2: PSYOP process overlaid on the targeting cycle

The most profound ability SNA provides is that it gives leaders the ability to glean real-time atmospherics and sentiment of TAs for targeting efforts—a critical component of the execution of successful and decisive operations with or without the traditional ‘boots on the ground’ presence. SNA sheds “unprecedented light onto what people think and, more importantly, why they think it, as well as unparalleled access to those who see value in understanding [a population’s] perspectives” (Bostick 2011, p. 17). Lin (2020) states that USCYBERCOM is on the information *delivery* side of any psychological effects. Through extensive experience in executing information operations,

USCYBERCOM experts should be in sync with PSYOPers who have developed deep and broad psychological, anthropological, and cultural expertise on the information *content* side of creating psychological effects (Lin 2020). These operations run parallel and are supplemental to existing processes within cyberspace and are not meant to replace existing functional capabilities.

Furthermore, cyber skills are seen as ‘hard skills’, such as understanding, crafting, and infiltrating network structure or managing malware and architectural vulnerabilities, whereas PSYOP skills are ‘soft skills’, and include human psychology, cultural linguistics, deception/ruse, influence tactics, and marketing techniques, for example (Lin 2020). SNA can be enhanced by technology, but undoubtedly, understanding human networks began long before the advent of the Internet. There are certainly limits to computer programming; programs can be flawed from inception when interpreting human behaviors and may give errors (for example, ‘sentiment’ is a concept that is hard to capture in the English language, let alone in a foreign language or slang). SNA, and an appropriate understanding of the human element, allows the Internet influencer to be present in an area of conflict without the use of physical or possibly even technological actions, unlike a cyber element which ostensibly cannot operate *without* technology. Therefore, PSYOPers, with little to no technology, can provide the opportunity to operate in an irregular warfare capacity that can be just as successful as having technological resources.

On the Subject of Irregular Warfare

Inevitably, the DoD’s engagement in online influence activities, whether offensive or defensive, will move into the realm of irregular warfare. In turn, social media networks can best be understood as unconventional weapons. As such, cyber-based irregular warfare efforts must engage the threat discriminately and apply capabilities indirectly as “technology abhors homogeneity”: difference is the standard rather than the exception (Cukier 2005, p. 13).

The conduct of irregular warfare requires studying the confluence of the land, cyber, and human domains. Although the methods of social network and link analysis are not new to the analytical community, the challenge of collecting the right data at the right time in the right context makes these methods difficult to apply to the irregular warfare fight. If SNA (and influence efforts in general, for that matter) solely focus on the relationships between people, groups, and/or organisations without a thorough understanding of the human psychological terrain, any irregular warfare practitioner will be inadequately informed about key aspects of the operating environment (Serrat 2017). Irregular warfare operations require, therefore, an understanding of the political, social, military, economic, terrestrial, and informational architecture of the environment from broad and deep psychological, social relationship, and cultural perspectives.

To be an effective strategic communicator in the irregular warfare context requires a broad and deep integration of cultural/regional acumen in concert with technical knowledge, skills, abilities, and attributes (KSAs) (Krawchuck 2006). PSYOP forces are collectively trained and equipped with cultural expertise and KSAs *before* they utilise any cyber-based equipment. SNA, and other activities, require certain technical skills, like coding, which CYBERCOM has and PSYOP does not necessarily have. They can work in cross functional teams with PSYOP in the lead, as the hallmark of the special operations community that PSYOP is a part of is a “penchant for creatively incorporating unique and unconventional tools into its arsenal” (Bostick 2011, p. 46). The fourth

industrial revolution, where there is a hybrid of cyber and physical systems operated by people, is well underway (Dawson 2020). When using these systems and implementing strategic communication in the irregular warfare environment, “systematic surveys, opinion polls, focus group interviews, and cultural attitudinal databases are just a few examples of tools used to establish baselines of perceptions, monitor social movements, and measure impacts”—all activities that PSYOPers currently do with particular expertise (Krawchuck 2006, p. 38).

Finally, to conduct irregular warfare, an influencer must understand the art and science of influence regarding human behavior and its structure and development. The art and science of influence has two key aspects. First, it is rooted in a consistent drive to understand the global information environment from the perspective of all sources of influence, including human psychological and social functioning, media, technological or others (Cook 2014). Second, it is rooted in focusing one’s experience, training, and education on leveraging this understanding to initiate actions that change people’s attitudes, values, and beliefs, which ultimately underscore and drive behavior (Cook 2014). As essential precursors to any influence campaign, within or outside of the cyber domain, non-kinetic activities and change efforts require an understanding of human behaviour in the context of the environment and cross-cultural competence. Arguably the PSYOPers have their own influence platform. They are a highly effective human weapons delivery system, when appropriately equipped. If influence is the projectile and the PSYOPER is the delivery system, then psychology and human understanding are the gunpowder behind the bullet, be it digital or not.

Final Thoughts

A key argument to be made here is not myopically focusing on USCYBERCOM versus PSYOP. That will categorically miss the point of where technical expertise and psychological know-how are both needed, as they are finite skills. Scholars and practitioners in the field of influence should not forget the many commands and units (both in the U.S. and abroad) with assigned PSYOP, information operations, human intelligence collectors, and other professionals who are also in the influence battle. Of utmost importance is the understanding that actions and activities by the PSYOP community are not meant to replace any component of USCYBERCOM or any other element for that matter. These activities and their specialised training do not give the PSYOPER some ‘silver bullet’ on the battlefield. A concrete understanding of human behavior and an expert competency in foreign cultures clearly differentiates the cyber practitioner from the PSYOPER, but defensive and offensive cyber and a robust understanding of computer systems and their technology are what cyber specialists also bring to the fight.

Moreover, the use of SNA as dictated by the operational environment (and the information gleaned) should be both shared and deconflicted across *all* available assets. The critical roles that information gathering, analysis, and operations play in the cyber realm to facilitate the timely sharing of cyber threat information can only enhance situational awareness (Grant *et al.* 2021). The SNA process, targeting cycle, and influence within the cyber domain should supplement all ground level practitioners with specific tools to capitalise on the exponential increase of the use of the Internet as a means of irregular warfare. Disrupting connections within social networks requires more than stopping or infiltrating technology; we must strive to stop digital enemies by changing their desire to weaponise the Internet, and not just react to the “boom” (for example, a viral post). Also, as new artificial intelligence systems become more widespread, information warfare will also be waged by non-humans, and this fact must be acknowledged.

This work asks that tomorrow's practitioners continue to raise the question of who potentially has the most institutional expertise when conducting information warfare as the nature of the battlefield changes. In the future, many problems will not be solved through force alone and the advent of cyber warfare exacerbates the risk of inadvertent escalation of conflict (Acton 2020). It has been argued that, since USCYBERCOM's creation, "it has specialised in the conduct of cyber operations and thus has concentrated on acquiring the technical expertise that such operations require" (Lin 2020). Whereas those technical talents are no doubt important, expertise in influence, be it on the Internet or otherwise, requires adept psychological understanding of human behavior, how it develops, and how it may be changed. Cyber-enabled information warfare should take advantage of fundamental characteristics of both modern information technology *and* irregular warfare. Certainly, no one could argue against the fact that "cyber operations are intended to hack silicon-based processors and technology, [whereas] psychological operations are intended to hack carbon-based processors (that is, human brains)" (Lin 2020). Tomorrow's fight will not be easy; it will require an all-hands-on-deck approach, whether those hands are on a rifle or a keyboard. Technology only magnifies the effects of force employment; however, technology is never a substitute for good force employment, regardless of whether the bullet is real or digital (Biddle 2004).

References

- Acton, J 2020, 'Cyber warfare and inadvertent escalation', *Daedulus*, vol. 149, no. 2, pp. 133-49.
- Amble, J & Stephenson, D 2020, 'Competition, conflict, and the future of irregular warfare', viewed 22 July 2020, <<https://mwi.usma.edu/mwi-podcast-competition-conflict-and-the-future-of-irregular-warfare>>.
- Atrews, R 2020, 'Cyberwarfare: Threats, security, attacks, and impact', *Journal of Information Warfare* vol. 19, no. 4, pp. 15-27.
- Biddle, S 2004, *Military Power: Explaining Victory and Defeat in Modern Battle*, Princeton University Press, Princeton, NJ, US.
- Bondyopadhyay, P 1998, 'Moore's law governs the silicon revolution', *Proceedings of the IEEE*, no. 86, pp. 78-81.
- Bostick, R 2011, 'Initiating the cognitive revolution: An examination of special operations military information support operations', *U.S. Army War College*, pp. 1-29.
- Bourne, K 2019, 'Targeting in multi-domain operations', *Military Review*, vol. 99, no. 3, pp. 60-7.
- Brown, J 2012, 'Improving nonlethal targeting: A social network analysis for military planners', *Naval Postgraduate School*, pp. 1-27.
- Cilluffo, F & Clark, J 2014, 'Repurposing cyber command', *Parameters*, vol. 43, no.4, pp. 111-18.
- Cook, C 2014, 'Continuing education: The brains behind the brawn of the operator', *IO Sphere*, Winter, pp. 22-25.

Cowan, D & Cook, C 2018, 'What's in a name? Psychological operations versus military information support operations and an analysis of organizational change', *Military Review*, March, pp. 1-7.

Cukier, K 2005, 'Who will control the internet', *Foreign Affairs*, November/December, pp. 7-13.

Czege, H 2020, 'Commentary on the US Army in multi-domain operations 2028', *Strategic Studies Institute and US Army War College Press*, pp. 1-66.

Dawson, M 2020, 'Cyber warfare threats and opportunities', *Universidade Fernando Pessoa*, pp. 1-63.

Duggan, P 2014, 'UW in cyberspace: The cyber UW pilot team concept', *Special Warfare*, vol. 27, no. 1, pp. 68-70.

Gendon, G, Blass-Irizarry, H & Boggs, J 2009, 'Next generation strategic communication: Building influence through online social networking', *Joint Forces Staff College*, pp. 1-18.

Gjelten, T 2013, 'First strike: US cyber warriors seize the offensive', *World Affairs*, vol. 175, no. 5, pp. 33-43.

Grant A, Billman, A, Cell, T, Meador, B, Halter, T, Hartley-McBride, S & Kaspar, B 2021, 'Critical roles of information, analysis, research, and operations in the cyber realm', *Journal of Information Warfare*, vol. 20, no. 2, pp. 67-80.

Krawchuck, F 2006, 'Strategic communication: An integral component of counterinsurgency operations', *Connections – The Quarterly Journal*, no. 46, pp. 35-50.

Lin, H 2020, 'On the integration of psychological operations with cyber operations', *Lawfare*, viewed 9 October 2020, <<https://www.lawfareblog.com/integration-psychological-operations-cyber-operations>>.

—& Kerr, J 2021, 'On cyber-enabled information warfare and information operations', *Oxford Handbook of Cybersecurity*, Oxford University Press, Oxford, UK.

Moore, G 1965, 'Cramming more component onto integrated circuits', *Electronics*, no. 8, pp. 114-17.

Naim, M 2014, *The End of Power*, Basic Books, New York, NY, US.

Paul, C 2020, 'Understanding and pursuing information advantage', *The Cyber Defense Review*, Summer, pp. 109-23.

Rid, T & Hecker, M 2009, *War 2.0: Irregular Warfare in the Information Age*, Praeger, Westport, CT, US.

Serrat, O 2017, 'Social network analysis', *Knowledge Solutions*, ed. O Serrat, Springer, Singapore, pp. 39-43.

Shallcross, N 2017, 'Social media and information operations in the 21st century', *Journal of Information Warfare*, vol. 16, no. 1, pp. 1-12.

Shirky, C 2011, 'The political power of social media', *Foreign Affairs*, vol. 90, no. 1, pp. 28-41.

Staton, W 2015, 'A millennial's perspective on the legacy of Vietnam', viewed 21 October 2020, <<https://medium.com/@WStaton85/a-millennial-s-perspective-on-the-legacy-of-vietnam-21e247dde019>>.

United States Cyber Command 2021, *Our History*, viewed 23 August 2021, <<https://www.cybercom.mil/About/History/>>.

United States Department of Defense (DoD) 2014, *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, viewed 22 October 2020, <http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf>.

—2014, *Joint publication 3-13: Information Operations*, viewed 22 October 2020, <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf>.

—2015, *Field Manual 3-05.301: Psychological Operations, Tactics, Techniques, and Procedures*, viewed 23 August 2021, <<https://fas.org/irp/doddir/army/fm3-05-301.pdf>>.

—2015, *Field Manual 3-60: The targeting process*, viewed 23 August 2021, <https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/atp3_60.pdf>.

Ventre, D 2016, *Information Warfare*, Wiley, Hoboken, NJ, US.

von Clausewitz, C, Howard, M, Paret, P, & Brodie, B 1984, *On War*, Princeton University Press, Princeton, NJ, US.

Reproduced with permission of copyright owner. Further reproduction prohibited without permission.