2016 8th International Conference on Cyber Conflict
Cyber Power
N.Pissanidis, H.Rõigas, M.Veenendaal (Eds.)
2016 © NATO CCD COE Publications, Tallinn

The Social Side of 'Cyber Power'? Social Media and Cyber Operations

Drew Herrick
Department of Political Science
George Washington University
Washington D.C., USA

Abstract: Evaluating an actor's 'cyber power' is an inherently complex problem involving a laundry list of military, normative, and technical variations. However, one important but under-theorised factor is the relationship between *military* social media operations and cyber operations. Policymakers, journalists, and even some academics often treat social media activity as a proxy variable for an actor's latent technical proficiency and even cyber capability, in other words, its cyber power. Actors that are extremely successful at engaging in social media activities are assumed to be technically proficient and even capable of engaging in cyber operations. This paper argues that an actor's social media use is a poor proxy for its technical and cyber security competency. In fact, under certain conditions social media activity may actually magnify the vulnerability of that actor. This paper synthesises cross-disciplinary research from strategic studies, political science, and technologists to develop a theoretical framework for better understanding the role of social media in cyber operations. It outlines the similarities and differences between social media and cyber security, and categorises different military social media operations into three types: information-gathering (IGMO), defensive social media operations (DeSMO), and offensive social media operations (OSMO).

Keywords: *future threats, situational awareness, data/information as power, international norms and governance, information operations*

1. INTRODUCTION

Correctly measuring an actor's offensive and defensive cyber capabilities or its aggregate 'cyber power' is an important goal for both policymakers and academics.[1] Knowing an actor's *true* capabilities affects not only expectations of success or failure on the battlefield, but also peacetime bargaining situations, escalation dynamics, balancing, deterrence, and even the durability of international norms.[2]

Unfortunately, evaluating an actor's cyber capabilities ex ante is extremely difficult for at least four reasons. First, technology in cyberspace is inherently dual use.[3] Even under ideal conditions, an accurate assessment of an actor's technological capabilities does not sufficiently reveal whether those capabilities are offensive or defensive in nature, assuming such distinctions even make sense.[4] Second, traditional assessment tools such as counting troops and materiel do not work well in a cyber context. Physical instantiations of cyber capabilities are rare.[5] Even attempts to examine an actor's ratio of successful to unsuccessful cyber operations are riddled with severe data limitations and selection bias issues.[6]

Third, in some cases there may be public financial or personnel disclosures that reveal how much money is being allocated to distinct operational areas, or how many people are working

1 This paper uses 'cyber capabilities' and 'cyber power' interchangeably. Other non-military elements that may or may not be part of an actor's aggregate cyber power such as commercial sector variables and Internet governance are bracketed. For a good overview on conceptualizing cyber power see Joseph S. Nye Jr., 'Cyber Power' (Cambridge: Belfer Center for Science and International Affairs, May 2010), http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf; Joseph S. Nye Jr, *The Future of Power* (New York: PublicAffairs, 2011); 'Cyber Power Index. Findings and Methodology' (Economist Intelligence Unit, 2011), http://www.boozallen.com/content/dam/boozallen/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf; Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: PublicAffairs, 2016).

2 For kinetic examples see, James D. Fearon, 'Rationalist Explanations for War,' *International Organization* 49, no. 3 (1995): 379–414; Robert Powell, 'Bargaining Theory and International Conflict,' *Annual Review of Political Science* 5, no. 1 (2002): 1–30, doi:10.1146/annurev.polisci.5.092601.141138; Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton, N.J.; Oxford: Princeton University Press, 2006); Keir A. Lieber, *War and the Engineers: The Primacy of Politics over Technology* (Ithaca; London: Cornell University Press, 2008); Charles L. Glaser, *Rational Theory of International Politics: The Logic of Competition and Cooperation* (Princeton University Press, 2010).

3 Trey Herr and Paul Rosenzweig, 'Cyber Weapons & Export Control: Incorporating Dual Use with the PrEP Model,' *Journal of National Security Law & Policy* 8 (2015), http://jnslp.com/2015/10/23/cyber-weapons-export-control-incorporating-dual-use-with-the-prep-model/.

4 Keir A. Lieber, 'Mission Impossible: Measuring the Offense-Defense Balance with Military Net Assessment,' *Security Studies* 20, no. 3 (2011): 451–59; Stephen Biddle, 'Rebuilding the Foundations of Offense-Defense Theory,' *Journal of Politics* 63, no. 3 (August 1, 2001): 741–74, doi:10.1111/0022-3816.00086.

5 Jon R. Lindsay, 'Stuxnet and the Limits of Cyber Warfare,' *Security Studies* 22, no. 3 (July 1, 2013): 365–404, doi:10.1080/09636412.2013.816122; Erik Gartzke and Jon R. Lindsay, 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace,' *Security Studies* 24, no. 2 (April 3, 2015): 316–48, doi:10.1080/09636412.2015.1038188; Brandon Valeriano and Ryan C. Maness, 'The Fog of Cyberwar,' *Foreign Affairs*, December 21, 2015, https://www.foreignaffairs.com/articles/2012-11-21/fog-cyberwar; Drew Herrick and Trey Herr, 'Combating Complexity: Offensive Cyber Capabilities and Integrated Warfighting' (International Studies Association, Atlanta, GA, 2016).

6 Attribution problems and the covert nature of cyber operations make data collection extremely difficult. Both sides of a conflict may have incentives to strategically not report or misreport an incident. In the most advanced cases, successful cyber operations may not even be known let alone publically reported.

in a specific area.[7] Unfortunately, even this is an unreliable metric since cyber power is better framed as a function of actor skill and time, not of allocated raw resources.[8] Throwing large amounts of money or people at a problem may or may not be sufficient to close a large skill gap or neutralise first mover advantages. More importantly, states have strong incentives to misrepresent their capabilities or even take credit (or not take credit) for past successful operations regardless of their actual participation or true capability.

Finally, power is relational and therefore even having a static measure of one actor's cyber capabilities is not particularly helpful. Instead, observers need to have a more dynamic and relational measure of multiple actors' capabilities over time. The core problem is that even under ideal conditions there is still a large degree of uncertainty that afflicts operational planning and peacetime bargaining situations. In many situations, having a poor assessment of an actor's cyber power may be just as damaging or even more so than having no prior knowledge.[9] For example, assessments of another actor's power that are too low may incentivise various states to engage in risky or escalatory behaviour that they otherwise should avoid. Similarly, assessments that are on the high side may incentivise states to select out of conflicts that in reality they are well placed to win.

One possible solution to the uncertainty problem is for states to leverage their well-established intelligence apparatus to gather information and narrow the gap. However, even for advanced states it is unlikely that espionage can completely close the uncertainty gap. Regardless, the key issue is that the public and the cyber security research community face a large data collection problem and are forced to rely on declassified documents, interviews, and open source alternatives.[10] Therefore, finding a reliable set of public and directly observable proxy variables to measure an actor's latent cyber capabilities is critical. One potential variable that is repeatedly referenced by policymakers, journalists and even some academics is 'advanced social media use' by so-called 'keyboard warriors' or 'cyber-jihadis'[11] Unfortunately as will be

7 Aliya Sternstein, 'The Military's Cybersecurity Budget in 4 Charts,' *Defense One*, March 16, 2015, http://www.defenseone.com/management/2015/03/militarys-cybersecurity-budget-4-charts/107679/; 'China Creates 3 New Army Units to Modernize Military,' *The Washington Post*, January 1, 2016, https://www.washingtonpost.com/world/asia_pacific/china-creates-3-new-army-units-to-modernize-military/2016/01/01/33648432-b10a-11e5-b281-43c0b56f61fa_story.html.

8 Drew Herrick and Trey Herr, 'Combating Complexity.'

9 See for example, Randall L. Schweller, *Unanswered Threats: Political Constraints on the Balance of Power* (Princeton University Press, 2006); Aaron L. Friedberg, *The Weary Titan: Britain and the Experience of Relative Decline, 1895-1905* (Princeton University Press, 1988).

10 For example, see Kim Zetter, 'Security Manual Reveals the OPSEC Advice ISIS Gives Recruits,' *WIRED*, November 19, 2015, http://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/.

11 For helpful examples, see James P. Farwell, 'The Media Strategy of ISIS,' *Survival* 56, no. 6 (November 2, 2014): 49–55, doi:10.1080/00396338.2014.985436; Doina Chiacu, 'U.S. NSA Chief Says Monitoring Tech-Savvy Islamic State,' *Reuters*, September 16, 2014, http://www.reuters.com/article/us-cybersecurity-usa-islamic-state-idUSKBN0HB22A20140916; Brian Nussbaum, 'Thinking About ISIS And Its Cyber Capabilities: Somewhere Between Blue Skies and Falling Ones,' November 29, 2015, http://cyberlaw.stanford.edu/blog/2015/11/thinking-about-isis-and-its-cyber-capabilities-somewhere-between-blue-skies-and-falling; Benjamin Runkle, 'Is the Islamic State a Cyber Threat?,' *War on the Rocks*, September 9, 2015, http://warontherocks.com/2015/09/is-the-islamic-state-a-cyber-threat/; Michael Sheetz, 'How ISIS Is Using High-Tech Tools for Planning and Propaganda,' *The Fiscal Times*, December 4, 2015, http://www.thefiscaltimes.com/2015/12/04/How-ISIS-Using-High-Tech-Tools-Planning-and-Propaganda; Ashish Sen, 'How Do You Disrupt ISIS' Social Media Strategy and Safeguard Freedoms?,' *Atlantic Council*, January 21, 2016, http://www.atlanticcouncil.org/blogs/new-atlanticist/how-do-you-disrupt-isis-social-media-strategy-and-safeguard-freedoms; Manuel R. Torres-Soriano, 'The Caliphate Is Not a Tweet Away: The Social Media Experience of Al Qaeda in the Islamic Maghreb,' *Studies in Conflict & Terrorism* 0, no. ja (March 1, 2016): 1–35, doi:10.1080/1057610X.2016.1159430.

demonstrated in this paper, social media use, at least in the way that it is traditionally viewed, is a poor proxy for an actor's technical proficiency or cyber capabilities, and under certain conditions may actually highlight actor insecurity rather than competence.

Despite sharing some basic characteristics, social media activity does not translate frictionlessly into cyber capability. Each environment faces distinct problems and requires different tools and skills. A non-state or even a state actor's social media prowess is not a strong indicator of its technical proficiency or cyber capabilities. In fact, in many cases, social media use and its bidirectional nature can actually make a target *more* vulnerable. What is overlooked is that social media does play a role in cyber operations, just not the one that is often acknowledged. Social media's military utility extends far beyond broadcasting and counter-messaging operations. Social media operations can have value at the operational and tactical levels, and directly contribute to the effectiveness of Cyber Intelligence, Surveillance, and Reconnaissance (Cyber ISR) and Cyber Operational Preparation of the Environment (Cyber OPE).[12] For example, gathering direct content and metadata can reveal a target's specific software and hardware configuration or even its physical location. Social media can also provide a useful attack platform for the targeted delivery of a capability and an alternative command and control (C2) mechanism.[13] Thinking strategically about the use of social media in terms of active information-gathering, phishing, spamming, offensive cyber delivery methods, and targeted network degradation may provide a key advantage during conflict.

The structure of this paper is as follows. Section two outlines similarities and differences between social media and cyber security. Section three categorises different military social media operations into three types: information-gathering (IGMO), defensive operations (DeSMO), and offensive social media operations (OSMO). Section three also outlines key variables for social media platforms (e.g. type of content, filtering tools) and target actors (e.g group cohesion, size) to show that there is an important interaction between the type of social media operation, the type of platform, and the target actor's characteristics. Simply put, certain types of groups and social media platforms are more or less vulnerable to certain types of military social media operations. Finally, the paper ends by offering specific conclusions and recommendations for policymakers and academics.

2. SOCIAL MEDIA AND CYBER

Social media use is an increasingly important political and social science research area.[14] Domestically and internationally, social media and networked systems are being deployed to organise anti-government dissent, spread disaster information, enhance political campaigning,

12 'JP 3-12(R), Cyberspace Operations' (Department of Defense, February 5, 2013).

13 James C. Foster, 'The Rise Of Social Media Botnets,' *Dark Reading*, July 7, 2015, http://www.darkreading.com/attacks-breaches/the-rise-of-social-media-botnets/a/d-id/1321177; Spencer Ackerman, 'Pentagon Admits It Is 'Looking to Accelerate' Cyber-Attacks against Isis,' *The Guardian*, February 29, 2016, sec. World news, http://www.theguardian.com/world/2016/feb/29/pentagon-admits-cyber-attacks-against-isis; David E. Sanger and Nicole Perlroth, 'Iranian Hackers Attack State Dept. via Social Media Accounts,' *The New York Times*, November 24, 2015, http://www.nytimes.com/2015/11/25/world/middleeast/iran-hackers-cyberespionage-state-department-social-media.html.

14 Nils B. Weidmann, 'Communication, Technology, and Political Conflict Introduction to the Special Issue,' *Journal of Peace Research* 52, no. 3 (May 1, 2015): 263–68, doi:10.1177/0022343314559081.

and magnify the effects of terror recruitment campaigns.[15] While existing studies have closely examined social media use during periods of civil unrest and, more recently, in post-conflict reconstruction, its use for operational planning and specifically during conflicts is still under-theorised.[16] As demonstrated in Table 1, there are several recent examples of intrastate and interstate conflict where actors have deployed social media operations.[17] The selected cases are meant only to highlight useful examples and are not a representative sample of all potential cases. Two examples are worth discussing in greater detail.

TABLE 1: SOCIAL MEDIA USE

Interstate Conflict	Intrastate Conflict	Non-Conflict Operation Areas
Russia-Ukraine	ISIS Syria Libya Egypt Anonymous	Bin Laden raid

A. Existing social media use

1) Russia-Ukraine

Social media use in the Ukraine conflict demonstrates the increasing importance of states supplementing conventional capabilities with social media operations.[18] Social media platforms have been used by Russian military forces, intelligence agencies, and proxies to conduct information operations and for targeting and operational planning purposes.[19] Ukrainian military forces, proxies, and civilians have similarly deployed social media to spread information or gain an advantage.

15 See a good overview in Pablo Barberá and Thomas Zeitzoff, 'The New Public Address System: Why Do World Leaders Adopt Social Media?,' 2016, http://pablobarbera.com/static/world_leaders_paper.pdf; David C. Benson, 'Why the Internet Is Not Increasing Terrorism,' *Security Studies* 23, no. 2 (April 3, 2014): 293–328, doi:10.1080/09636412.2014.905353.

16 Thomas Zeitzoff, 'Using Social Media to Measure Conflict Dynamics: An Application to the 2008-2009 Gaza Conflict,' *Journal of Conflict Resolution*, June 20, 2011, 0022002711408014, doi:10.1177/0022002711408014; Jacob N. Shapiro and David A. Siegel, 'Coordination and Security How Mobile Communications Affect Insurgency,' *Journal of Peace Research* 52, no. 3 (May 1, 2015): 312–22, doi:10.1177/0022343314559624; Thomas Elkjer Nissen, *#TheWeaponizationOfSocialMedia: @ Characteristics_of_ Contemporary_Conflicts* (Royal Danish Defence College, 2015).

17 Doug Gross, 'Twitter User Unknowingly Reported Bin Laden Attack,' CNN, May 2, 2011, http://www.cnn.com/2011/TECH/social.media/05/02/osama.twitter.reports/index.html; 'Mapping the Syrian Conflict with Social Media,' Crisis.Net, 2014, http://crisis.net/projects/syria-tracker/; Masudul Biswas and Carrie Sipes, 'Social Media in Syria's Uprising and Post-Revolution Libya: An Analysis of Activists' and Blogger's Online Engagement,' Fall 2014, http://www.arabmediasociety.com/articles/downloads/20140925085334_BiswasSipes_SocialMedia_Final.pdf; Paul Roderick Gregory, 'Inside Putin's Campaign Of Social Media Trolling And Faked Ukrainian Crimes,' *Forbes*, May 11, 2014, http://www.forbes.com/sites/paulroderickgregory/2014/05/11/inside-putins-campaign-of-social-media-trolling-and-faked-ukrainian-crimes/; Dmitry Volchek and Claire Bigg, 'Ukrainian Bloggers Use Social Media to Track Russian Soldiers Fighting in East,' *The Guardian*, June 3, 2015, sec. World news, http://www.theguardian.com/world/2015/jun/03/bloggers-social-media-russian-soldiers-fighting-in-ukraine.

18 See above. Also see Kenneth Geers, *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn: NATO CCD COE Publications, 2015); 'Twitter's Role in Modern Warfare,' *BBC News*, March 21, 2016, http://www.bbc.com/news/technology-35842265.

19 There are actor attribution issues but for the purposes of this paper it is sufficient to lump military forces together with intelligence forces, state-sponsored proxies, and activists. The key point is to highlight how social media is now a fundamental element of modern conflict zones.

A key part of Russia's strategy is to use social media platforms for military disinformation and propaganda campaigns.[20] The Russian government employs citizens as a 'troll army', consisting of social media users that inundate websites with pro-Putin rhetoric.[21] These trolls have been increasingly active in the lead up to major Russian foreign policy initiatives, including those in Crimea. Russian trolls can be savvy and technically sophisticated, and are capable of orchestrating advanced information campaigns while working from Russian territory.[22]

Russian military units have also been active in Ukraine, as evidenced by numerous incidents where Russian soldiers posted geotagged content (e.g., photos of weaponry) and commentary (referring to active fighting in Ukraine) to Instagram.[23] Through social media, reporters and academics have been able to document Russian military equipment deployed in places like Crimea and Ukraine.[24] Ukrainian civilians have also used social media to effectively communicate events as they are transpiring. For example, civilians have used social media to track Russian soldiers and to signal for help when caught between Ukrainian soldiers and pro-Russian separatists.[25]

2) ISIS

Social media provides ISIS with a flexible and streamlined set of tools for creating and distributing videos, images, and other content. ISIS routinely uses multiple social media platforms to broadcast anti-United States propaganda.[26] Inherent network effects then magnify the reach and effect of this propaganda. Social media also provides ISIS with a valuable means of engaging in targeted recruitment campaigns and attempts to radicalise target populations.[27]

20 Roman Skaskiw, 'Nine Lessons of Russian Propaganda | Small Wars Journal,' *Small Wars Journal*, March 27, 2016, http://smallwarsjournal.com/jrnl/art/nine-lessons-of-russian-propaganda.

21 Daisy Sindelar, 'The Kremlin's Troll Army,' *The Atlantic*, August 12, 2014, http://www.theatlantic.com/international/archive/2014/08/the-kremlins-troll-army/375932/.

22 Adrian Chen, 'The Agency,' *The New York Times*, June 2, 2015, http://www.nytimes.com/2015/06/07/magazine/the-agency.html.

23 Oscar Jonsson and Robert Seely, 'Russian Full-Spectrum Conflict: An Appraisal After Ukraine,' *The Journal of Slavic Military Studies* 28, no. 1 (January 2, 2015): 1–22, doi:10.1080/13518046.2015.998118 ; Max Seddon, 'Does This Soldier's Instagram Account Prove Russia Is Covertly Operating In Ukraine?,' *BuzzFeed*, July 30, 2014, http://www.buzzfeed.com/maxseddon/does-this-soldiers-instagram-account-prove-russia-is-covertl.

24 Jenny Hauser, 'Speed in Context: Real-Time News Reporting and Social Media,' 2014, http://arrow.dit.ie/aaschmedcon/36/; Maksymilian Czuperski et al., *Hiding in plain sight: Putin's war in Ukraine*, 2015, https://www.dropbox.com/s/7uzlm8aspdls5wh/Hiding-in-Plain_Sight_0527.pdf?raw=1.

25 Jenny Hauser, 'Speed in Context: Real-Time News Reporting and Social Media,' 2014, http://arrow.dit.ie/aaschmedcon/36/; Maksymilian Czuperski et al., *Hiding in plain sight: Putin's war in Ukraine*, 2015, https://www.dropbox.com/s/7uzlm8aspdls5wh/Hiding-in-Plain_Sight_0527.pdf?raw=1.

26 P.W. Singer and Emerson Brooking, 'Terror on Twitter,' *Popular Science*, December 11, 2015, http://www.popsci.com/terror-on-twitter-how-isis-is-taking-war-to-social-media; Brendan I. Koerner, 'Why ISIS Is Winning the Social Media War—And How to Fight Back,' WIRED, March 29, 2016, http://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/; J.M. Berger, 'How Terrorists Recruit Online (and How to Stop It),' *The Brookings Institution*, November 9, 2015, http://www.brookings.edu/blogs/markaz/posts/2015/11/09-countering-violent-extremism-online-berger; Daveed Gartenstein-Ross, 'The Social Science of Online Radicalization,' *War on the Rocks*, October 29, 2015, http://warontherocks.com/2015/10/the-social-science-of-online-radicalization/.; Klint Finley, 'It'd Be Great to Kick ISIS Offline—If It Were Possible,' *WIRED*, March 30, 2016, http://www.wired.com/2016/03/how-is-isis-online/.

27 Jytte Klausen, 'Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq,' *Studies in Conflict & Terrorism* 38, no. 1 (January 2, 2015): 1–22, doi:10.1080/1057610X.2014.974948.; Haroro J. Ingram, 'Three Traits of the Islamic State's Information Warfare,' *The RUSI Journal* 159, no. 6 (November 2, 2014): 4–11, doi:10.1080/03071847.2014.990810.; Sabrine Saad Stéphane Bazan, 'Infowar on the Web: When the Caliphate Goes Online,' 2015, doi:10.13140/RG.2.1.1851.5043.

However, it is important to note that, like the social media activity in Ukraine, ISIS's social media activity is bidirectional. All parties can use social media for information-gathering and targeting purposes. For example, the United States Air Force used social media data posted by an ISIS supporter to target an ISIS military compound.[28] More recently, the United States Department of Defense has been engaged in ongoing social media and cyber operations against online ISIS targets.[29] Open source investigators have also successfully mapped the Twitter network of known ISIS supporters by analysing commonly used location and content data.[30] Even other non-state actors have similarly used social media to target and report ISIS social media accounts and websites.[31]

B. Social media meets cyber operations

The high profile nature and rise of social media activity by states and especially non-state actors has recently drawn the attention of those interested in cyber security. Specifically, commentators and researchers appear to view social media's relationship to cyber operations primarily in one of two ways. First, some observers have stretched the concept of cyber operations or cyber power to explicitly include social media activity.[32] Under this view, social media prowess becomes a primary example of an actor engaging in cyber operations.[33] Cyber technology and cyber operations then include a variety of different operations such as viral messaging on social media platforms, building internal messaging apps, intragroup operational security, deploying Distributed Denial of Service (DDoS) capabilities or even the deployment and use of advanced offensive cyber capabilities to achieve physical effects.

The second view maintains a narrower concept of cyber operations but still views social media activity or prowess as having a positive relationship with cyber capabilities.[34] Under this second view, social media operations are not synonymous with cyber operations but are instead an indicator of an actor's cyber capabilities. Actors that are successful at engaging in social

28 Walbert Castillo, 'U.S. Bombs ISIS Using Social Media Intel,' *CNN*, June 5, 2015, http://www.cnn.com/2015/06/05/politics/air-force-isis-moron-twitter/index.html.

29 Ackerman, 'Pentagon Admits It Is 'Looking to Accelerate' Cyber-Attacks against Isis'; Koerner, 'Why ISIS Is Winning the Social Media War—And How to Fight Back'; Christina Nemr, 'Strategies to Counter Terrorist Narratives Are More Confused than Ever,' *War on the Rocks*, March 15, 2016, http://warontherocks.com/2016/03/strategies-to-counter-terrorist-narratives-are-more-confused-than-ever/; Jared Cohen, 'Digital Counterinsurgency,' *Foreign Affairs*, December 2015, https://www.foreignaffairs.com/articles/middle-east/digital-counterinsurgency; Kimberly Dozier, 'Anti-ISIS-Propaganda Czar's Ninja War Plan: We Were Never Here.,' *The Daily Beast*, March 15, 2016, http://www.thedailybeast.com/articles/2016/03/15/obama-s-new-anti-isis-czar-wants-to-use-algorithms-to-target-jihadis.html.

30 JM Berger and Jonathan Morgan, 'The ISIS Twitter Census Defining and Describing the Population of ISIS Supporters on Twitter' (Washington, D.C: Brookings, March 2015), http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf.

31 David Auerbach, 'The Hacktivist War on ISIS?,' *Slate*, December 10, 2015, http://www.slate.com/articles/technology/bitwise/2015/12/ghostsecgroup_is_taking_on_isis_it_s_not_clear_they_re_helping.html.

32 See footnote 12; Doina Chiacu, 'U.S. NSA Chief Says Monitoring Tech-Savvy Islamic State'; Brian Nussbaum, 'Thinking About ISIS And Its Cyber Capabilities'; Michael Sheetz, 'How ISIS Is Using High-Tech Tools for Planning and Propaganda'; Sen, 'How Do You Disrupt ISIS' Social Media Strategy and Safeguard Freedoms?'; Torres-Soriano, 'The Caliphate Is Not a Tweet Away'; Warwick Ashford, 'Social Media the Main Cyber Terror Threat Facing the UK, Says Former MI6 Officer,' *Computer Weekly*, October 16, 2015, http://www.computerweekly.com/news/4500255638/Social-media-the-main-cyber-terror-threat-facing-the-UK-says-former-MI6-officer.

33 Here social media 'use' and 'prowess' are largely used interchangeably. It is not always clear whether the people who make this first type of link between social media and cyber capabilities are addressing *any* use of social media or just instances of highly effective use.

34 Michael Sheetz, 'How ISIS Is Using High-Tech Tools for Planning and Propaganda'; Sen, 'How Do You Disrupt ISIS' Social Media Strategy and Safeguard Freedoms?'

media operations are also viewed to be broadly technically competent even to the degree of engaging in cyber operations. This argument has recently been used in debates surrounding the capabilities of ISIS, Anonymous, and Iranian forces.[35]

Both avenues of argument must logically rely on at least an implicit assumption that the same skills that allow actors to be successful at social media operations also enable them to be successful at other technical skills or even offensive and defensive cyber operations. In the first argument, social media skills and cyber security skills match one-to-one. Broadening the concept of cyber capabilities to include social media operations means that, by definition, the actor that just engaged in successful social media operations is now 'cyber capable.' Unfortunately, this conceptual stretching is not only tautological but is also not particularly helpful. At best, it indicates that the actor is capable of deploying only one minor type of cyber operations, social media operations. The argument is agnostic on the real question of whether that actor is able to successfully engage in defensive and offensive military cyber missions. At worst, this first type of argument stretches the concept of cyber capability to the point of incoherence.

The second avenue of argument initially appears more promising. Perhaps there are shared traits or skillsets between successful social media operations and cyber capabilities. If so, then successful social media operations may be a useful proxy variable for an actor's latent cyber capability. Even a weak positive relationship may demonstrate that an actor that engages in successful social media operations is more likely than other actors to have functioning cyber capabilities. Unfortunately, the link between social media and cyber in terms of shared traits and skills remains to be demonstrated.[36]

At the most basic level, both social media operations and cyber operations share common elements. First, they both rely heavily on building up skilled human capital. Second, they both involve some degree of technical or computer knowledge. Third, they both involve some knowledge of network effects. Fourth, they both involve elements of working in real time. Fifth, they both involve working within limitations set by a system. In the case of social media operations, these limitations are set by the specific platform being used. In the case of cyber operations, the limitations are primarily dictated by the target's systems and the nature of the specific vulnerability that is being exploited. However, even at this most basic level the differences in terms of scale and degree of skill, technical knowledge, network effects, and system limitations are extremely large.

The technical knowledge involved in social media operations is primarily focused on deploying an already publically or commercially developed tool. The actor only needs to understand how

35 See footnote 12; Ibid.; Doina Chiacu, 'U.S. NSA Chief Says Monitoring Tech-Savvy Islamic State'; Brian Nussbaum, 'Thinking About ISIS And Its Cyber Capabilities'; Michael Sheetz, 'How ISIS Is Using High-Tech Tools for Planning and Propaganda'; Sen, 'How Do You Disrupt ISIS' Social Media Strategy and Safeguard Freedoms?'; Torres-Soriano, 'The Caliphate Is Not a Tweet Away'; Warwick Ashford, 'Social Media the Main Cyber Terror Threat Facing the UK, Says Former MI6 Officer'; Meg King and Grayson Clary, 'Opinion: The Shocking Mediocrity of Islamic State 'Hacker' Junaid Hussain,' *Christian Science Monitor*, October 26, 2015, http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/1026/Opinion-The-shocking-mediocrity-of-Islamic-State-hacker-Junaid-Hussain; 'Twitter's Role in Modern Warfare'; Elias Groll, 'Welcome to the Future of War: ISIS Has a Smartphone App,' *Foreign Policy*, December 8, 2015, https://foreignpolicy.com/2015/12/08/welcome-to-the-future-of-war-isis-has-a-smartphone-app/; 'Who's at the Controls of Iran's Bot Army?,' *BBC News*, March 16, 2016, http://www.bbc.com/news/blogs-trending-35778645.

36 For space reasons, this paper will only briefly cover a few key similarities and differences between social media operations and cyber operations.

to deploy the tool, but does not need to have working knowledge of how that tool was built or how it functions. The same argument applies to the degree of skill that is needed and knowledge of systems and networks effects. Moreover, unlike social media, cyber operations involve a strategic interaction between attackers and defenders.[37] Defenders are able to react and respond in a way that requires a high degree of skill and time to successfully overcome.

Even bracketing skill comparisons, the two types of operations involve antithetical problems. In almost all cases, social media platforms ensure access by default. An actor has direct access to a target or a specific network because it is a built-in property of the platform. For example, social media platforms such as Twitter or Facebook are public by default. In the case of cyber operations, the key problem is to overcome restricted access. The target in a cyber operation is restricting access by default whereas with social media the target welcomes the actor. Similarly, in the social media case the actor wants to magnify and broadcast a message or type of content using network properties. In the offensive cyber case, the actor often wants to conceal and narrow the scope of the operation.

There is a relationship between social media and cyber operations, just not the one that is traditionally acknowledged. Social media operations directly contribute to Cyber Intelligence, Surveillance, and Reconnaissance (Cyber ISR) and Cyber Operational Preparation of the Environment (Cyber OPE). As will be demonstrated below, social media operations can be valuable at the operational and tactical levels. Operations can reveal useful information for weaponeering a specific cyber capability against a specific target.[38] Social media operations may also reveal both a means of capability deployment against a target's systems and alternative mechanisms for command and control. Actors that are highly active on social media may actually be increasing their vulnerability to offensive cyber capabilities by revealing target-specific information and widening the attack surface.

3. A FRAMEWORK FOR SOCIAL MEDIA OPERATIONS

The previous section demonstrated a number of ways that social media has been used in existing conflict zones and hinted at social media's usefulness as a complement to an actor's existing cyber capabilities. This section further unpacks social media operations (SMO) into its component types and directly links each to cyber operations. Social media operations consist of three distinct types: information-gathering, defence, and offense.

A. Information-gathering media operations

Information-gathering media operations (IGMO) focus on passive information-gathering. As demonstrated in the Ukraine, ISIS, and Bin Laden Raid cases, passive information-gathering

37 Drew Herrick and Trey Herr, 'Combating Complexity.'
38 See also, Ibid.

can be used for monitoring adversary activities and for targeting.[39] Through IGMO, military and intelligence forces are not interacting with known social media actors but instead are passively monitoring and documenting social media activity. IGMO focuses on two types of data: (1) direct data collection (the content displayed on social media); and (2) metadata collection (technical details related to the characteristics of social media users and the mechanics of their social media use). Direct data collection allows access to the actual content displayed on social media services.

Metadata collection is not as qualitatively rich as direct data collection, but can reveal important details regarding a population or target's location, the time of day that the target is active, the target's social graph (network connections), specific applications that the target is using to access services, whether the target is using a mobile device, and in some cases even the specific hardware and software configuration of the device that the target is using.[40]

This information can then be refined for non-kinetic purposes such as cyber ISR or OPE, or for kinetic targeting (e.g., physical destruction). Whether used for direct data or metadata collection, IGMO can be a useful complement to other information collection activities. The primary risk to using IGMO for these purposes is that strategic and competent adversaries may intentionally cleanse or manipulate social media information in order to mislead those trying to monitor various sources. For example, strategic actors that realise they are being observed may take steps to mask their location, use automation to schedule activity, or intentionally communicate false information to influence the observer forces to act in a certain way.[41] Similarly, maintaining the ability to engage in IGMO requires that an adversary's social network accounts be left up and running.[42] Legal attempts to cut off an adversary from using social media platforms directly trades off with the ability to gather key information.

39 Jamie Bartlett and Louis Reynolds, *The State of the Art 2015: A Literature Review of Social Media Intelligence Capabilities for Counter-Terrorism* (London: Demos, 2015), http://www.demos.co.uk/wp-content/uploads/2015/09/State_of_the_Arts_2015.pdf; Aliya Sternstein, 'Pentagon Mapmakers Are Using Social Media to Chart Syrians' Exodus,' *Defense One*, March 20, 2016, http://www.defenseone.com/technology/2016/03/pentagons-cartographers-are-mapping-syrias-exodus-thanks-social-media/126808/; Patrick M. Gillen, 'Real-Time Detection of Operational Military Information in Social Media' (Thesis, Monterey, California: Naval Postgraduate School, 2015), null/handle/10945/47261; Swati Agarwal, Ashish Sureka, and Vikram Goyal, 'Open Source Social Media Analytics for Intelligence and Security Informatics Applications,' in *Big Data Analytic*s, ed. Naveen Kumar and Vasudha Bhatnagar, Lecture Notes in Computer Science 9498 (Springer International Publishing, 2015), 21–37, http://link.springer.com/chapter/10.1007/978-3-319-27057-9_2; Robert Chesney, 'Anonymous vs ISIS Online: Pondering the Intelligence Impact of Social Media Takedowns,' *Lawfare*, November 18, 2015, https://www.lawfareblog.com/anonymous-vs-isis-online-pondering-intelligence-impact-social-media-takedowns; Alastair Paterson, 'Using an Attacker's 'Shadow' to Your Advantage | SecurityWeek.Com,' *Security Week*, November 5, 2015, http://www.securityweek.com/using-attackers-shadow-your-advantage.

40 Bo Zhao and Daniel Sui, 'True Lies in Big Data: Detecting Location Spoofing in Social Media,' *Journal of Spatial Information Science*, 2016, http://www.josis.org/index.php/josis/article/viewArticle/273.

41 Michela Del Vicario et al., 'The Spreading of Misinformation Online,' *Proceedings of the National Academy of Sciences* 113, no. 3 (January 19, 2016): 554–59, doi:10.1073/pnas.1517441113.

42 Patrick Tucker, 'Twitter Steps Up Efforts To Combat ISIS,' *Defense One*, February 5, 2016, http://www.defenseone.com/technology/2016/02/twitter-steps-efforts-combat-isis/125739/; J.M. Berger and Heather Perez, 'The Islamic State's Diminishing Returns on Twitter: How Suspensions Are Limiting the Social Networks of English-Speaking ISIS Supporters' (Washington, D.C: George Washington University, February 2016), https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Berger_Occasional%20Paper.pdf.

B. Defensive social media operations

Defensive social media operations (DeSMO) involve using social media in a more active way than IGMO, but not as active as OSMO. Actors can use social media as a broadcasting platform to conduct counter-messaging or counter-propaganda activities.[43] As demonstrated in the Russian troll and ISIS cases, social media can be used effectively to widely broadcast information to otherwise difficult-to-reach audiences. In fact, US government agencies are already using social media services to counteract known propaganda and radicalisation campaigns.[44] However, existing operations are extremely limited and, at best, produce minor effects.[45]

Despite its value, DeSMO has the potential downside of providing an adversary with direct data collection opportunities and metadata that would otherwise not be revealed. Put differently, engaging in DeSMO activities allows the adversary to engage in IGMO or even OSMO. While this information can be shielded, its emission is nonetheless a risk that must be acknowledged. By engaging in counter-messaging, the actors involved are revealing information about, for example, their own capabilities, location, or system configurations. DeSMO does not play a direct role in terms of cyber operations, but has been acknowledged as a key component of de-radicalisation campaigns.

C. Offensive social media operations

Social media operations are commonly viewed as a broadcasting or counter-narrative tool; DeSMO under this paper's new framework. More recently, social media operations as a passive information-gathering (or IGMO) tool have received some attention as the conversation surrounding ISIS and online radicalisation has subtly shifted from 'shut it down' towards a monitoring mentality.[46] Instead of actively shuttering known ISIS accounts and websites, intelligence agencies and even non-governmental actors can passively observe and analyse their content.

43 David P. Fidler, 'Countering Islamic State Exploitation of the Internet' (Washington, D.C: Council on Foreign Relations, June 2015), http://www.cfr.org/cybersecurity/countering-islamic-state-exploitation-internet/p36644; Dann Albright, 'How Social Media Is The Newest Military Battleground,' *MakeUseOf*, February 19, 2015, http://www.makeuseof.com/tag/social-media-newest-military-battleground/; P.W. Singer and Emerson Brooking, 'Terror on Twitter'; David Ensor, 'How Washington Can Win the Information War,' *Foreign Policy*, December 14, 2015, https://foreignpolicy.com/2015/12/14/how-washington-can-win-the-information-war/.

44 Greg Miller and Karen DeYoung, 'Obama Administration Plans Shake-up in Propaganda War against ISIS,' *The Washington Post*, January 8, 2016, https://www.washingtonpost.com/world/national-security/obama-administration-plans-shake-up-in-propaganda-war-against-the-islamic-state/2016/01/08/d482255c-b585-11e5-a842-0feb51d1d124_story.html.

45 Koerner, 'Why ISIS Is Winning the Social Media War—And How to Fight Back'; Charlie Winter and Jordan Bach-Lombardo, 'Why ISIS Propaganda Works,' *The Atlantic*, February 13, 2016, http://www.theatlantic.com/international/archive/2016/02/isis-propaganda-war/462702/; Patrick Tucker, 'Pentagon: State Doesn't Have Enough People Tweeting At ISIS,' *Defense One*, October 22, 2015, http://www.defenseone.com/technology/2015/10/pentagon-state-doesnt-have-enough-people-tweeting-isis/123063/; Christina Nemr, 'Strategies to Counter Terrorist Narratives Are More Confused than Ever'; Jared Cohen, 'Digital Counterinsurgency.'

46 Julia Greenberg, 'Facebook And Twitter Face Tough Choices As ISIS Exploits Social Media to Spread Its Message,' *WIRED*, November 21, 2015, http://www.wired.com/2015/11/facebook-and-twitter-face-tough-choices-as-isis-exploits-social-media/; Albanesius, 'Obama: Intelligence Officials 'Constantly' Monitor Social Media Posts,' *PCMAG*, December 18, 2015, http://www.pcmag.com/article2/0,2817,2496846,00.asp.

Offensive social media operations (OSMO) are still largely ignored in existing research and in the cases discussed above.[47] OSMO includes activities conducted on social media platforms to actively gather information, conduct information campaigns, deliver precision cyber effects, and counter, degrade, deny, or destroy an adversary's social media capability. In these respects, social media's bidirectional nature can be used as a vector to target and attack adversaries by and through their own social media activity.

For example, OSMO can enable military forces or intelligence agencies to spam known actors or networks to increase the overall signal-to-noise ratio within a given social media environment. Depending on the specific filtering tools of the social media services being employed, strategic spamming may allow friendly forces to disrupt an adversary's social media use while still leaving the broader service and supporting networks up and running. Using OSMO in this manner would allow IGMO and DeSMO efforts to continue uninterrupted while still allowing for the disruption of an adversary's social media use. In cases where an adversary is using several social media platforms simultaneously, military forces can also selectively disrupt one platform to shift activity to another where they may have a larger comparative advantage.

Militaries can also use 'trolling' techniques to target normally unresponsive or inactive accounts. This more active form of engagement with an account may incentivise the target actor to lash out in response, thereby revealing more direct and indirect information. Similarly, social media can be used for phishing purposes. These specific techniques may especially benefit from deploying proxies or 'cyber mercenaries.'

Finally, social media platforms can be used as both an attack avenue for offensive cyber capabilities and as an alternative means for command and control (C2).[48] Since access is often built in by default, using social media as a delivery platform may reduce the cost and time associated with traditional ways of deploying offensive cyber capabilities.

D. Limitations and opportunities

Despite IGMO, DeSMO and OSMO yielding potentially valuable advantages, these benefits are not universal. First, social media operations only yield a benefit in conflict areas that already have a high degree of connectedness and social media activity. Trying to use social media techniques in non-networked environments will not be particularly fruitful. Second, social media operations are bidirectional; actively using social media might provide unintended benefits to an adversary. Third, social media operations are likely to involve very large networks, requiring a high degree of competency and sophistication to effectively monitor and influence. Finally, many social media operations will have to be conducted in real-time or near real-time, and effective operations will require continuous monitoring and response.

There are also non-network considerations that may limit the utility of social media operations. First, there is an intrinsic authenticity problem. Depending on whether the target is aware that they are under surveillance and the sophistication of their understanding of the social media environment, there may be significant uncertainty concerning the veracity of information

47 For a few examples, see Adam Weinstein, 'Here's How the US Should Fight ISIS With Social Media,' *WIRED*, March 12, 2015, http://www.wired.com/2015/03/heres-us-fight-isis-social-media/; Nissen, *#TheWeaponizationOfSocialMedia*; Heather M. Roff et al., 'Fight ISIS by Thinking Inside the Bot,' Slate, October 21, 2015, http://www.slate.com/articles/technology/future_tense/2015/10/using_chatbots_to_distract_isis_recruiters_on_social_media.html.

48 James C. Foster, 'The Rise Of Social Media Botnets.'

gathered. One other interesting point is the effect of group size. There may be good reasons to anticipate that faking information will be more difficult as social media groups grow over time.

Second, the effectiveness of social media operations is contingent on the characteristics of the specific social media service and the target group. There is a key interaction effect between the type of action chosen (IGMO, DeSMO, or OSMO), the specific attributes of the social media platform in use, and the specific dynamics of the target. This interaction effect then directly impacts the effectiveness (high, medium, or low) of a given option. For example, social media services with high entry costs and very good filtering tools will be highly resistant to network or even individual node spamming. Likewise, groups that have a high degree of familiarity with technology and have been using a specific social media service for a long time will be more resistant to certain types of operations. However, targets with low group cohesion, high turnover, and low familiarity with a given platform may be especially vulnerable to targeted social media operations. Low cohesion and high turnover mean that it is less likely that every actor within the group knows every other actor. Impersonation tactics may be particularly effective. Finally, there are significant regulatory, doctrinal, and structural issues that must be resolved if social media operations are going to be conducted by military forces or even intelligence agencies. Overall, these limitations restrict the use social media operations but do not eliminate their utility.

4. CONCLUSION

Social media use, as it is traditionally viewed, is a poor indicator of an actor's *true* technical ability, cyber capabilities, or 'cyber power.' Viewing social media operations as either a direct example of an actor's cyber operations in action or as a reliable proxy for latent cyber capabilities is misguided. Both options hinge on false assumptions about the relationship between social media and cyber operations. This paper has made two arguments. First, that if social media operations are to be directly connected to cyber operations then it is better to view those operations as complementary to an already existing cyber capability. Second, it has outlined a preliminary framework for social media operations that can be unpacked into three distinct types: information-gathering, defence, and offence. In short, social media operations provide potentially useful information for targeting purposes and defensive threat intelligence, and expand the attack surface.

Policymakers and academics should focus on the broader utility of social media operations for military effectiveness. How can social media operations be successfully integrated with existing cyber and information operations? Should states push for international norms or treaties that apply to the use of social media during peace and conflict? Can offensive strategies be developed to successfully counter social media use by an adversary?

Overall, successful social media operations may act as a powerful force multiplier for both conventional and cyber capabilities. Thinking seriously about the nature of social media operations may help inform the future direction of military force structure and policies surrounding how to counter violent state and non-state actors.