Rethinking Warfare Concepts in the Study of Cyberwar and Security

https://www.e-ir.info/2018/12/01/rethinking-warfare-concepts-in-the-study-of-cyberwar-and-security/

MEGAN ROGERS, DEC 1 2018

My objective here is to demonstrate that the extent to which the concepts of 'war', 'militarism' and 'militarization' are analytically useful for understanding what have come to be known as 'cyberwar' and 'cybersecurity', is limited. Firstly, I dismantle the concept of 'cyberwar' into its constituent parts, and in doing so demonstrate that the notion of 'war' in a digital context is problematic. Cyberwar, I infer, cannot satisfy the three central characteristics of war that are: political, instrumental, and violent. I will then demonstrate that the popularly framed *militarization of cyberspace* constitutes various analytic shortcomings. To conceive of cybersecurity through the lens of a strategic-militarist framework, I argue, requires subjecting it to the canons of hostile zero-sum logic of super- and sub-ordination, which is misguided due to the problem of attribution in cyberattacks. Furthermore, a genuine militarization of cyberspace rests on the premise that cyberspace harbours territory to defend and conquer which is logically impossible. Finally, I argue against the popular notion of *digital militarism*, and contend that the virality of military propaganda via new media does not adequately satisfy the central tenets of militarism that are: the social adoption of attitudes and/or beliefs that posit the military as the supreme protector and pursuer of national agendas, and thereby constituting a normal feature of everyday life. Characterising cyberspace through a language of warfare, I infer, has engendered the misnomer of new media forms of cyberactivism, cyberprotest, and cybersubversion as militarism.

Cyber

Once a feature limited to New Wave science fiction, the term 'cyber' is now one of the most frequented buzzwords in the international security lexicon – with sound reason.[1] The tech explosion of the past two decades has facilitated unprecedented global networking through the creation of new information sharing capabilities conducted in 'cyberspace', accessed via the Internet.[2] Egalitarian (theoretically) by nature, the proliferation of the 'open' Internet, however, has inevitably kindled national concerns surrounding the protection of state infrastructure and the potential for unauthorized access to mass amounts of sensitive online data through remote cyber 'attacks'.[3] Indeed, for the modern state operating critical infrastructure in cyberspace, the notion of a cyberattack is no longer dystopian fiction but an existential threat. Large-scale cyberattacks such as the coordinated 'hackings' against Estonia in 2007, in the 2008 Russo-Georgian territorial dispute over South Ossetia, and, most notably, the 2010 Stuxnet Worm, were watersheds in global perceptions of cyberspace as a 'new domain' of war, and cybertechnology a weapon.[4] Since so-called cyber vulnerabilities have been internationally exposed, rubric from US defence officials, and, indeed, states globally, have warned of the threat of 'foreign computer hackers' wielding the power to cause 'physical destruction and the loss of life' in a 'cyber-Pearl Harbour' attack.[5] However hyperbolic these premonitions are, the resulting increased support for cyberspace, a *civil* domain, to be characterized as under the jurisdiction of military defence authorities has engendered the permeation of warfare rhetoric into political, academic, and legal discussions addressing the apparent threat of what has popularly been coined, cyberwar.[6]

To accept the proposition of cyberwar, however, rests on the premise that cyberspace is a feasible (and likely) domain within which to conduct warfare, and that cyberattacks constitute acts of war. Analytically speaking, this thinking is highly problematic. There is a significant need within academe to intellectually reign-in the proliferation of 'cyber-hyped' warfare terminology and analyse cyberspace phenomena in logical, precise, and *unambiguous* terms.[7] Refreshingly, there is growing acknowledgement amongst scholars in this respect. Thomas Rid, for

instance, argues that so-called cyberattacks, past and present, constitute not acts of war but 'sophisticated versions of three activities… as old as warfare itself: subversion, espionage, and sabotage'.[8] In a similar vein, cyberespionage and cybercrime, James Lewis determines, are 'routine occurrences, but they are not acts of war and do not justify the use of military force in response'.[9] I infer, then, that a cyberattack, and thereby cyberwar, is unable to adequately satisfy the defining features that characterise a stand-alone act of war in the traditional sense, namely: its violent nature; its political purpose; its instrumentality.[10] Following Rid, in order for a defensive or offensive act to be framed as war, it 'must meet all three criteria', and herein lies the problem.[11]

War

On the essentiality of violence in war, Rid asserts that 'if an act is not potentially violent, it is not an act of war. A real act of war is always potentially or actually lethal, at least for some participants on at least one side'.[12] At present, however, there has not been a single malicious cyber offence with known direct, or indirect, lethal consequences.[13] The widely publicised 'hacktivist' attacks against Estonia, beginning in late April 2007, have often been appropriated as evidence foreboding kinetically destructive, large-scale cyberthreats.[14] But the damage potential of dedicated distribution of service (DDoS) attacks, website defacement, and email spam which characterised the incident is, essentially , non-existent beyond the short-term disruption of online services.[15] The cyberattacks against Estonia, moreover, were not regarded by the Estonian Government as anything more than individual cybercrimes, and certainly not an armed attack worthy of invoking Article 5 of the NATO Treaty.[16] As Yaroslav Radziwill determines, when considered in isolation, the actual damage produced by a cyberattack is 'not enough to characterize it more seriously than a nuisance'.[17] Analytically speaking, therefore, the inability of cyberattacks to produce kinetic outcomes renders it counterproductive to present notions of 'cyber-Armageddon' as a rational outcome of the trajectory of technological evolution. Following Sean Lawson, the proliferation of hypothetical 'cyber-doom' scenarios are ultimately reflective of a broader rhetoric of 'technology-out-of-control' within the West.[18] These scenarios, Lawson argues, are 'unrealistic' and merely 'encourage the adoption of counterproductive, even dangerous policies'.[19]

Notwithstanding, the hyperbole of 'potentially devastating' cyberdisasters has appeared to initiate a global race toward what has been termed the *militarization of cyberspace*.[20] With its origins in the concept of militarism, militarization has to do with 'the process by which a society organises itself for military conflict and violence'.[21] That is to say, as is commonly understood, 'militarization is military build-up'.[22] It is widely conceived that Russia, China, Iran, North Korea, and the US are positioned at the forefront of the development of offensive and defensive cyberspace capabilities.[23] In 2017, worldwide information-security spending hit a record-high $89.13 billion, and is expected to increase by eight percent by the close of 2018.[24] Large portions of security spending can be attributed to heightened perceptions of cyberthreat and market reactions to instances of cyberattack.[25] That this inclination toward strengthening cybersecurity feasibly constitutes *militarization*, however, is problematic.

To conceive of cyberspace through a strategic-militarist lens requires subjecting it to the canons of hostile zero-sum game logic where gains are made only through the other's loss.[26] The construction of the 'other' in this way subsumes a necessary power relationship of dominance and subordination where the preferences of the subordinate actor are in conflict to those of the dominant actor. As John Scott has noted, in this 'constant sum' or 'zero-sum' view, power relations are seen as asymmetrical, hierarchical relations of super- and sub- ordination in which one agent can gain only at the expense of another'.[27] As Myriam Dunn Cavelty points out, however, to view cybersecurity as a militaristic institutional structure 'invokes enemy images even though there is no identifiable enemy'.[28] That is to say, in the context of cyberspace there exists a powerful 'problem of attribution' which blurs the traditional power relationship in conflict. Following Nicholas Tsagourias, there are three particular features of cyberspace which make attribution difficult.[29] First, using relatively unsophisticated, technically speaking, VPN software cyber attackers are able to hide their identity.[30] Second, the potential infiltration of a large number of geographically scattered systems through 'multi-stage cyber attacks' increases the chain of infection making it difficult to trace the attack back to the original culprit.[31] Third, cyberattacks can be conducted at immense speed which, again, limits one's ability to discern who 'fired the first shot'.[32] This blurring of identity lines, therefore, amounts to serious issue for conceiving of cyberspace as a new plane upon which to construct war via militarization.

Linked to the problem of attribution, the concept of a militarized cyberspace is further problematized by the consideration that cyberspace harbours defendable and conquerable territory. The modern nation state exists within a highly interdependent, and increasingly globalized, economy where critical infrastructure providers often service several states, and multinational technology companies circumvent physical boundary lines.[33] It does not make sense, therefore, to conceive of networked cyberattacks as threats to territorial integrity inviting a military response.[34] As Jaap-Henk Hoepman succinctly observes, in the case of threats in cyberspace, 'whose territory is really being targeted?'.[35] In the infamous Stuxnet incident, for example, the 500-kilobyte computer worm targeted Windows systems and replicated itself through Windows-based Siemens Step7 software.[36] Siemens software is widely employed in industrial computing networks, including *but not limited to* nuclear enrichment facilities.[37] Although Iran was disproportionately infected by the Stuxnet Worm, other states, as similar employers of Siemens Software, including Indonesia, India, and Pakistan were also affected.[38] State actors, therefore, are only in control, or feasibly able to control, limited components of cyberspace, and critical (information) infrastructures lie outside the realm of military ownership and accessibility.[39] To speak of a militarized cyberspace 'hinge[s] upon determining the degree to which the military as an institution is the primary actor in responding to cybersecurity challenges'.[40] Taking widespread private ownership into account, the power and responsibility to enhance cybersecurity protections and respond to cyberthreats is located largely outside the realm of government institutions. Cyberspace is not a domain segregated nationally into defensible and conquerable territories – 'it is no space where troops and tanks can be deployed because the logic of national boundaries does not apply'.[41] The value of the concept of militarization for understanding cyberwar, therefore, is limited as any consideration of cyberspace as a conquerable, controllable territory is not simply illogical but illusionary.[42]

Whilst analytically distinct, the concept of militarism is similarly problematic for understanding cyberwar and security. On the concept of militarism, Julian Schofield asserts that, traditionally, militarism 'has to do with the glorification of the military and war as a value' as well as how this value is represented 'aesthetically and socially within that society'.[43] In a similar vein, Michael Mann conceives of militarism as 'a set of attitudes and social practices which regards war and the preparation for war as a normal and desirable social activity'.[44] M. V. Naidu, whilst also emphasising the attitudinal element of militarism, goes further to stress not just *desirability* but the *essentiality* of the military.[45] The core values or beliefs that constitute militarism, Naidu determines, are that 'military capability is the most meaningful and effective instrument for achieving any or all national goals, and that soldiers, weapons and wars are the most necessary and noble tools for national protections and advancement'.[46] Whilst the range of conceptual definitions on offer evidently show that militarism is a somewhat contested concept, there are certainly core features to be drawn out. I suggest, then, that 'militarism' occupies the ideological territory between the military and civil society. Within this space, there exists the attitude or belief that military presence and practices of war are conventional facets of everyday life; for a militarised society, military capability and war are considered essential to achieve the national agenda.

There has been salient discussion amongst academia that cyberspace harnesses the potential for a new mode of militarism – *digital militarism*. As a detailed report conducted in 2017 by the Stockholm International Peace Research Institute points out, much of the online mechanisms that shape new media messages are capable of being manipulated 'to sell national security as military security, and to promote the view that the presence of the military in everyday life is natural'.[47] For Adi Kunstman and Rebecca Stein, the extension of the Arab-Israeli conflict into social media in November 2014 by the Israeli military, appears to cement in cyber stone the advent of 'social media war' in an already established era of digital militarism.[48] Employing dedicated Twitter feeds, Facebook, YouTube, and Flickr to propagate military PR policy in real-time, the Israeli military's most viral material 'aimed to speak in the casual grammar that social media demanded and often adopted popular cultural and cinematic aesthetics as a means to reach global youth audiences'.[49] At first glance, the digital virality of military propaganda might appear to satisfy the causal element necessary to achieve militarised sentiment. At its core, however, militarism constitutes an effect – namely, the adoption of certain attitudes and beliefs. And herein lies the problem when applying the concept of militarism to cyberspace.

Whilst there is little doubt that the entry of the military into the cyberspace vernacular constitutes a new PR campaign, it is extremely difficult to measure the extent, if any, of the adoption of genuine militarist attitudes and beliefs by individuals represented by virtual "likes", "shares", and "views".[50] That is to say, it would be illogical to

suggest that the 'four thousand subscribers' to the Israeli Military's dedicated YouTube channel are representative of a militarised society governed by belief systems which posit military capability as the supreme national asset.[51] On the contrary, far removed from violent circumstances the digital linguistic of emojis, pixelated thumbs-ups, and hashtags serve to represent not digital militarism, but cyber *activism* and *subversion*.[52] The advent of social media has facilitated the organisation of non-violent protest and patriotic politics like never before.[53] It is, therefore, unsurprising that individuals seeking to undermine established power institutions have wielded new globalized networking capabilities as mechanisms for action. Contrary to journalistic cliché, however, 'subversion is not war, and cyber subversion is not cyberwar'.[54] To conceive of Facebook, Twitter, and the Blogosphere as 'targets, weapons, and battlefields in their own right' is not merely unproductive for understanding new modes of digital communication, but, more importantly, is problematic for properly conceptualising warfare.[55] . From an analytical perspective, the erroneous adoption of warfare terminology by scholars seeking to analyse new media only contributes to conceptual confusion over what constitutes genuine militarism within a legitimate context of warfare, which cyberspace is not.

Conclusion

To conclude, whilst there is little doubt that malicious cyberspace offenses are, and will not cease to be, a genuine and routine occurrence, the concepts of militarization, militarism and, indeed, war, are of limited value for understanding cyberwar and security. The notion of cyberwar is not merely unlikely but essentially metaphorical in that cyberattacks do not, analytically speaking, constitute acts of war. The militarization of cyberspace, therefore, is, by proxy, misleading. To speak of a militarized cyberspace rests on the false premise that cyberspace constitutes defendable and conquerable territory, and is ignorant to the existence of a globalized economy where private entities exercise transnational power and responsibility over critical infrastructure and online services. Furthermore, what has popularly been termed digital militarism is a misnomer for new forms of online protest, activism, and subversion. For those who suggest that Facebook, Twitter, and Instagram bear the echelons of a militarised society, there is a serious need to rethink these claims with the nature and function of the environment in mind. To analyse cyberspace phenomena through a language of warfare only serves to exacerbate already hyperbolic premonitions of a 'cyber-9/11'. A levelled, well-informed, and conceptually accurate analytical approach to cyberspace is necessary if we are to adequately assess the threat and risks associated with cybersecurity and modern warfare more broadly.

Bibliography

Ball, D. (2011), 'China's Cyber Warfare Capabilities', *Security Challenges*, Vol. 7, pp. 81-103.

Clausewitz, C V. (2008), *On War*, Oxford and New York, Oxford World's Classics.

Czosseck, C., Ottis, R., and Talihärm, A. (2011), 'Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security', Journal of Cyber Warfare and Terrorism. Vol. 1, pp. 24-34.

Deibert, R J. (2010), 'Black Code Redux: Censorship, Surveillance, and the Militarization of Cyberspace' in ed. Megan Boler, *Digital Media Democracy: Tactics in Hard Times*, Cambridge: Massachusetts, MIT Press.

Dunn Cavelty, M. (2008), *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* , Oxford and New York, Routledge.

Dunn Cavelty, M. (2012), 'The Militarisation of Cyber Space: Why Less May Be Better',*4th International Conference on Cyber Conflict*, Tallinn, NATO CCD COE, pp. 141-153.

Farwell, J. and Rohozinski, R. (2011), 'Stuxnet and the Future of Cyber War', *Survival*, Vol. 53, pp. 23-40.

Kuntsman, A and Stein, R L. (2015), *Digital Militarism*: *Israel's Occupation in the Social Media Age* , Stanford University Press.

Lawson, S. (2012), 'Beyond Cyber Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber Threats', *Journal of Information Technology & Politics*, Vol. 10, pp. 86-103.

Lawson, S. (2012), 'Is the United States Militarizing Cyber Space?', Forbes Online.

Lawson, S. (2012), 'Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States', *First Monday*, Vol. 17.

Lee, R M., and Rid, T. (2014), 'OMG Cyber!', *The Rusi Journal*, Vol. 159, pp. 4-12.

Lewis, J A. (2010), 'The Cyber War Has Not Begun', *Center for Strategic and International Studies*.

Mann, M. (1987), 'The Roots and Contradictions of Modern Militarism', *New Left Review*, Vol. 162, p. 35.

Naidu (1985), 'Military Power, Militarism and Militarization: An Attempt at Clarification and Classification', *Peace Research*, Vol. 17, pp. 2-10.

O'Connor, M., E. (2012), 'Cyber Security without Cyber War', *Journal of Conflict & Security Law*, Vol.17, pp. 187-209.

Ottis, R. (2010), 'The vulnerability of the information society', *futureGOV Asia Pacific*, Vol. 7, pp. 70–72.

Panetta, L E. (2012) quoted in 'Panetta Warns of Dire Threat of Cyber Attack on U.S', *The New York Times*, (2012).

Radziwill, Y. (2015), *Cyber-Attacks and the Exploitable Imperfections of International Law*, Leiden and Boston, BRILL.

Rid, T. (2012), 'Cyber War Will Not Take Place', *Journal of Strategic Studies*, Vol. 35, pp. 5-32.

Rid, T. (2013), 'End this phony cyber war', *New Scientist*, pp. 26-27.

Rinaldi, S M, Peerenboom, J P. and Kelly, T, K. (2001), 'Identifying, understanding, and analysing critical infrastructure interdependencies', *IEEE Control Systems*, Vol. 21, pp. 11-25.

Schofield, J. (2007), *Militarization and* War, New York, Palgrave Macmillan.

Scott, J. (2001), *Power*, Cambridge, Polity Press.

Tikk, E., Kaska, K., and Vihul, L. (2010), *International Cyber Incidents*, Cooperative Cyber Defence Centre of Excellence (CCD COE), p. 29.

Tsagourias, N. (2012), 'Cyber-attacks, self-defense and the problem of attribution', *Journal of Conflict and Security Law,* Vol. 17. p. 229-244.

[1] Mary Ellen O'Connell (2012), 'Cyber Security without Cyber War', *Journal of Conflict & Security Law*, Vol. .17, p. 188.

[2] O'Connell, 'Cyber Security', p. 188.

[3] O'Connell, 'Cyber Security', pp.188-189.

[4] Thomas Rid (2012), 'Cyber War Will Not Take Place', *Journal of Strategic Studies*, Vol. 35, pp. 5-32.

[5] Defense Secretary Leon E. Panetta quoted in 'Panetta Warns of Dire Threat of Cyber Attack on U.S',*The New York Times*, (2012), Accessed on 12/05/2018 at https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

[6] O'Connell, 'Cyber Security', p. 188.

[7] Robert M Lee and Thomas Rid (2014), 'OMG Cyber!', *The Rusi Journal*, Vol. 159, pp. 4-12.

[8] Rid, 'Cyber War', p. 6.

[9] James Andrew Lewis (2010), 'The Cyber War Has Not Begun', *Center for Strategic and International Studies*, p. 2.

[10] Carl Von Clausewitz (2008), *On War*, Oxford and New York, Oxford World's Classics.

[11] Rid, 'Cyber War', p. 7.

[12] Rid, 'Cyber War', p. 7.

[13] Myriam Dunn Cavelty (2008), *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* , Oxford and New York, Routledge.

[14] Eneken Tikk, Kadri Kaska and Liis Vihul (2010), *International Cyber Incidents*, Cooperative Cyber Defence Centre of Excellence (CCD COE), p. 29.

[15] Rid, 'Cyber War', p. 11-15.

[16] Christian Czosseck, Rain Ottis and Anna-Maria Talihärm (2011), 'Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security', Journal of Cyber Warfare and Terrorism. Vol. 1, pp. 24-34.

[17] Yaroslav Radziwill (2015), *Cyber-Attacks and the Exploitable Imperfections of International Law* , Leiden and Boston, Brill, p. 83.

[18] Sean Lawson (2012), 'Beyond Cyber Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber Threats', *Journal of Information Technology & Politics*, Vol. 10, p. 86.

[19] Lawson, 'Beyond Cyber Doom', p. 86.

[20] Ronald J Deibert (2010), 'Black Code Redux: Censorship, Surveillance, and the Militarization of Cyberspace' in ed. Megan Boler, *Digital Media Democracy: Tactics in Hard Times*, Massachusetts, MIT Press.

[21] M V Naidu (1985), 'Military Power, Militarism and Militarization: An Attempt at Clarification and Classification', *Peace Research*, Vol. 17, pp. 2-3.

[22] Naidu, 'Military Power', p. 3.

[23] Desmond Ball (2011), 'China's Cyber Warfare Capabilities', *Security Challenges*, Vol. 7, p. 81-83.

[24] 'Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017' (2017), Gartner Press Release, Accessed 16/05/2018 at https://www.gartner.com/newsroom/id/3836563.

[25] 'Gartner Forecasts Worldwide Security Spending'.

[26] (2012), 'The Militarisation of Cyber Space: Why Less May Be Better',*4th International Conference on Cyber Conflict*, Tallinn, NATO CCD COE, p. 1-2.

[27] John Scott (2001) *Power*, Cambridge, Polity Press, p.4.

[28] Myriam Dunn Cavelty, '(2012), 'The Militarisation of Cyber Space: Why Less May Be Better',*4th International Conference on Cyber Conflict*, Tallinn, NATO CCD COE, p. 1.

[29] Nicholas Tsagourias (2012), 'Cyber-attacks, self-defense and the problem of attribution',*Journal of Conflict and Security Law,* Vol. 17. p. 234.

[30] Tsagourias, 'Cyber-attacks', p. 234.

[31] Tsagourias, 'Cyber-attacks', p. 234.

[32] Tsagourias, ''Cyber-attacks' p. 234.

[33] S M Rinaldi, et al. (2001), 'Identifying, understanding, and analysing critical infrastructure interdependencies', *IEEE Control Systems*, Vol. 21, pp. 11-25.

[34] Jaap-Henk Hoepman (2017), 'How the military thinks about cyberspace', *Jaap-Henk Hoepman on Privacy, Security, And…*, Accessed on 14/05/2018 at https://blog.xot.nl/2017/11/03/how-the-military-thinks-about-cyberspace/.

[35] Hoepman, 'How the military thinks about cyberspace'.

[36] James Farwell and Rafal Rohozinski (2011), 'Stuxnet and the Future of Cyber War', *Survival*, Vol. 53, p. 23.

[37] Farwell and Rohozinski, 'Stuxnet', p. 24.

[38] Farwell and Rohozinski, 'Stuxnet', p. 24-25.

[39] Myriam Dunn Cavelty (2012), 'The Militarisation of Cyber Space: Why Less May Be Better',*4th International Conference on Cyber Conflict*, Tallinn, NATO CCD COE, p. 12.

[40] Sean Lawson (2012), 'Is the United States Militarizing Cyber Space?', Forbes, Accessed on 11/05/2018 at https://www.forbes.com/sites/seanlawson/2012/11/02/is-the-united-states-militarizing-cyberspace/#3fc1b957798d.

[41] Dunn Cavelty, 'The Militarisation of Cyber Space', p. 12.

[42] Dunn Cavelty, 'The Militarisation of Cyber Space', p. 12.

[43] Julian Schofield (2007), *Militarization and* War, New York, Palgrave Macmillan, p. 1.

[44] Michael Mann (1987), 'The Roots and Contradictions of Modern Militarism', *New Left Review*, Vol. 162, p. 35.

[45] Naidu, 'Military Power', p. 4.

[46] Naidu, 'Military Power', p. 4-5.

[47] Susan Jackson, Jutta Joachim, Nick Robinson and Andrea Schneiker (2017), 'Assessing Meaning Construction on Social Media: A Case of Normalizing Militarism', *Stockholm International Peace Research Institute*, Access on 10/05/2018 at https://www.sipri.org/sites/default/files/2017-10/mil_2_policy_brief.pdf.

[48] Adi Kuntsman and Rebecca Stein (2015), *Digital Militarism*: *Israel's Occupation in the Social Media Age*, Stanford University Press, p. 20.

[49] Kuntsman and Stein, *Digital Militarism*, p. 34.

[50] Kuntsman and Stein, *Digital Militarism*, p. 33.

[51] Kuntsman and Stein, *Digital Militarism*, p. 27.

[52] Thomas Rid (2013), 'End this phony cyber war', *New Scientist*, p. 26.

[53] Rid, 'End this phony cyber war', p. 26.

[54] Rid, 'End this phony cyber war', p. 26.

[55] Kuntsman and Stein, *Digital Militarism*, p. 25.

Written by: Megan Rogers
Written at: University of Sheffield
Written for: Dr. Nuray Aridici
Date written: May 2018