Child Soldiers in the Cyber Domain

Dustin Johnson
The Roméo Dallaire Child Soldiers Initiative
Dalhousie University, Halifax, Nova Scotia
CANADA

dustin@childsoldiers.org

Ben O'Bright
Dalhousie University
Halifax, NS
CANADA

benobright@gmail.com

ABSTRACT

Considerable attention has been devoted to understanding the dynamics and characteristics of cyber conflict, but little attention has been paid to the involvement of children and youth. Yet, incidents of children being recruited and used in cyber conflict are on the rise. In 2012, a twelve-year old Canadian was charged with participating in a series of cyberattacks on provincial websites and information technology systems. The so-called Islamic State has been using social media to recruit disenfranchised children in Western countries. The United Kingdom has started a cybersecurity recruitment programme known as Cyber Discovery, offering extracurricular training to children between ten and thirteen years old. While the role of children in physical, kinetic conflict as child soldiers has been widely studied and recognized, it has created a narrative and set of definitional parameters that are ill-suited for war, conflict and terrorism in the cyber domain. The authors present the results of an initial scoping study on child soldiers in the cyber domain, discuss the methods most suited for its investigation by the operations research & analysis community and the challenges involved. We also suggest an initial set of questions for further exploration by the OR&A community. This new area of focus will help NATO members and partners understand and mitigate threats and protect children from harm as modern conflict and technologies evolve and shift.

1.0 DEFINITIONS AND METHODOLOGY

The current accepted definition of a child soldier (which was developed based on their roles in traditional armed conflict and designed to afford maximum protection to affected children) appears in the Paris Principles and serves as the starting point for discussions of child soldiers in the cyber domain:

> *"A child associated with an armed force or armed group" refers to any person below 18 years of age who is or who has been recruited or used by an armed force or armed group in any capacity, including but not limited to children, boys and girls, used as fighters, cooks, porters, messengers, spies or for sexual purposes. It does not only refer to a child who is taking or has taken a direct part in hostilities.* [1]

While not a legally binding document, the Paris Principles make clear that being a child soldier consists of more than bearing arms and engaging in hostilities. International human rights law (IHRL) and international humanitarian law (IHL) both proscribe the use of child soldiers through various treaties, including the Convention on the Rights of the Child, Additional Protocols I and II to the 1949 Geneva Conventions, and the Optional Protocol on the involvement of children in armed conflict (OPAC), which draw the line at 15 years old for participation in hostilities, and at 18 years old for non-state armed groups in the case of OPAC.

As will be seen, extending these principles and definitions into the cyber domain leads to a significant grey area.

1.1 Scoping study methodology

This paper presents the findings of an initial scoping study [2] on the presence of child soldiers in the cyber domain. Its aim was to assess the current legal and policy framework applicable to this area, and what evidence currently exists on the involvement of children in cyberattacks, whether or not those attacks could be considered use of force. Based on this assessment, we propose an initial definition of child soldiers in the cyber domain and pose further questions that need to be addressed, enabling governments and international organizations to respond, and better protect children.

Consequently, the scoping study conducted a literature review of relevant available materials, focusing on 1) applicable national and international laws, and accompanying legal guidance, on armed conflict, children, and cyber conflict; 2) academic literature that addresses cyber conflict and child soldiers; 3) grey (non-academic) literature that addresses these subjects; and, 4) relevant accounts in the press of cyberattacks and children involved in it. The collected sources were analysed to assess the current legal structure applying to cyber conflict, how it addressed or impacted children, to what extent children may currently be involved in cyber conflict, and what some of the reasons for using children in cyber conflict might be.

2.0 RESULTS OF SCOPING STUDY

To understand the boundaries of what might constitute a child soldier in the cyber domain, policymakers and researchers must come to terms with a comprehensive definition of what constitutes an act of war in cyberspace. Speaking generally, the Tallinn Manual argues that a cyberattack is a "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects," which can be considered as a narrow interpretation of the application of *jus ad bellum* to cyber affairs [3]. This position was ultimately amended by noting that physicality should not formally preclude the application of this terminology to actions that cause something or someone to be harmed, damaged, or broken; calling this position the 'functionality test' [4]. The Joint Chiefs of Staff of the United States have termed cyber conflict as an armed conflict wholly conducted online or through cyber means [5]. In contrast, Rid [6] argues that cyberattacks cannot and should not be classified as acts of war for they lack a direct, meaningful connection to lethality, while Finlay suggests that cyber-operations can indeed be imbued with the features of what he called violent agency [7]. Other efforts to define cyber conflict have been made by Alford [8], who believed it was directly tied to advancing national will, while Carr [9] argues that cyber conflict does not ultimately impact the physical wellbeing of citizens of a country, group, or community [10]. Robinson et al. settle on use an Actor and Intent Definition Model: a cyberattack is assessed as such when one considered who has committed an act in cyberspace, whether it is reasonably expected to or has caused harm, the latter loosely defined [11].

D'Urso agrees that the application of the Geneva Conventions for cyber-combatants leaves too many gaps which can be exploited by enterprising countries and groups. It is unlikely, he suggests, that a civilian hacker unaffiliated with any external governing structure would wear a distinctive emblem, making their distinction from a larger population all the more difficult [12]. Indeed, under the Geneva Conventions, participation by a civilian in conflict enables the forfeiture of their protections from reprisal by other combat actors; thus, a non-military cyber combatant may well be considered an unlawful and unprivileged combatant under existing law [13]. The issue is compounded when considering the boundaries of participation by numerous members of a virtual community, collectively but without formal affiliation, participating in cyber action [14]. Ayalew notes that if an individual is associated with a group that is not a Party to a conflict but participates nonetheless, they are not afforded combatant status under existing international law and would not be afforded civilian immunity, nor prisoner of war treatment [15]. As such, D'Urso proposes that cyber-combatants should be considered those who engage in a 'continuous combat function,' which mandates that there be long-term

integration with an organised armed group, and that all other civilian participants may only be classified as such if their actions surpass thresholds of harm, direct causation of "damage," and that damage must be done in support of an identified party over another [16]. This then invites further discussion of what constitute "arms" or "combat" in the cyber domain.

The much broader definition of a child soldier from the Paris Principles provides more flexibility, and hence is easier to apply to the cyber domain, as it is based on children associated with armed forces and armed groups, not on the stricter definition based on continuous combat function under IHL. This however leaves open the question of what counts as an armed force or armed group in the cyber domain. While traditional armed forces and armed groups that conduct cyber operations would clearly apply in this case, there is a grey area when it comes to groups that are purely involved in cyber operations, especially ones which may not meet the traditional definitions of an armed group in terms of level of organization and command and control, while conducting cyber operations that would clearly count as use of force. For purposes of IHL, where definition of a combatant affects who can be lawfully targeted, it is in the best interests of children to maintain a restrictive definition, but analytically and for protection of children, it is better to cast a wider net. Consequently, we propose the following definition of a child soldier in the cyber domain, designed to be more inclusive and therefore to better protect children: *any person under the age of 18 who is, by their own volition or by compulsion, a participant in kinetic or non-kinetic cyber conflict activities under the formal or informal guidance, directive, or order of a group or entity with political objectives.*

While scholarly research has yet to touch specifically on child soldiers in the cyber domain, a wide range of media reporting and prosecutions of underage hackers provides a glimpse into the current state of affairs. For example, there is the 2014 case of a 14-year old British teen who was arrested for conducting cyberattacks on government agencies in Iraq, Thailand, and China, as well as three hackers who accessed the personal email account of former CIA Director John Brennan in 2015 [17]. There is the more recent case of Kane Gamble, who accessed intelligence operations plans for the CIA's work in Afghanistan and Iran, arguing that "it all started by me getting more and more annoyed about how corrupt and cold blooded the US Government are [sic] so I decided to do something about it" [18]. The large-scale cyberattack on Estonian internet infrastructure in 2007 is thought to have been carried out by a Russian-affiliated youth group which may have included children (those under 18-years of age) [19]. Child soldiers have been widely featured in propaganda distributed online by the so-called Islamic State, and they have been recruited over the internet [20]. As such, it is not unreasonable to assume that some of those conducting recruitment, or those carrying out cyberattacks on behalf of the so-called Islamic State, are children as well, although evidence of such is difficult to determine.

While the use of child soldiers in the cyber domain may not expose children to as severe a risk of injury, death, and psychological trauma as their use kinetically does, there is presently insufficient data to know how children may be affected by participation in cyber conflict. With the large proportion of children online and growing up technologically literate, especially in the global North, we do know that they provide a large pool of potential recruits. Research suggests that some 90% of young people in the United States aged 13-17 have a social media account, with more than 50% using those associated platforms at least once a day [21]. The United Kingdom's Office of Communications equally argues that, in the case of that country in particular, more than half of British children aged 10-12 have a social media account of some type, a salient conclusion when minimum age of use for most prominent platforms is 13 [22]. As is true with the use of social media by children or terrorist talent spotters, there is no barrier to entry, these platforms are free to use, conversations and interactions can be largely anonymized, and there are very few editorial gatekeepers [23]. As well, many of the same reasons children are recruited for kinetic armed conflict likely apply to the cyber domain as well, including their large portion of the population in some countries, lesser attention to the long-term ramifications of their actions, and vulnerability to coercion [24].

Consequently, it appears that children are presently actively engaged in cyber conflict, if broadly defined, and that they form a large pool of potential, digitally literate recruits. Beyond that, current grey areas in the overall

scope, definitions, international law, and how to respond to the issue make the case for further investigation of child soldiers in the cyber domain.

3.0 IMPLICATIONS FOR OR&A

The use of child soldiers in the cyber domain should, at present, be viewed as a "mess" or wicked problem [25]. As our study found, there is little information presently available on the involvement of children in cyber conflict making the problem poorly defined and understood, there are a variety of potential courses of action available which have various benefits and drawbacks, and a number of stakeholders (military, law enforcement, child protection organizations, industry) will be involved with different points of view and priorities. Currently, most data about the issue is anecdotal and qualitative, and further analysis will likely involve a combination of qualitative and quantitative data from a range of fields, from cyber security to children's rights to psychology. Addressing the issue will require a combined approach likely involving law enforcement, military, industry, international organizations, and other stakeholders. Consequently, a mixed-methods soft OA approach is likely to be most effective [26]. A particular challenge is the ease of masking one's identity when operating in the cyber domain, making it difficult to determine if children are involved in any given attack.

Some questions that we believe need to be explored further include: how common is the involvement of children in cyberattacks? What types of organizations are using child soldiers in the cyber domain? What ages are these children? How are they recruited? Does using children in this way confer specific advantages compared to the use of adults, such as ease of recruitment, lower cost, etc.? What measures can be taken to prevent the use of children in cyberattacks? How are children, and those facing them, harmed due to participation in cyber conflict?

We believe that our initial scoping study has demonstrated that there is an issue of child soldiers in the cyber domain, and that it is a problem that needs to be addressed, both to protect children and to counteract adversaries, whether state or non-state, in cyber conflict. As an emerging and little-studied area, the OR&A community is well placed to address the issue in the future and we hope this paper and the subsequent scoping study will provide a starting point from which others can begin exploring.

4.0 REFERENCES

[1] UNICEF, “The Paris Principles - Principles and Guidelines on Children Associated with Armed Forces or Armed Groups”, 2007, ¶2.1

[2] O’Bright, B., and Johnson, D., “Child Soldiery in 1s and 0s - A Thematic Scoping Report on the Advent of Digital Child Soldiers: Definitions, Approaches and Responses”, Halifax, NS: the Roméo Dallaire Child Soldiers Initiative, forthcoming.

[3] Schmitt, M. (ed.), “Tallinn Manual on the International Law Applicable to Cyber Warfare”, Cambridge: Cambridge University Press, 2013. Kilovaty, I, “Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare”, American University National Security Law Brief, 5(1), 2014, p. 92.

[4] Schmitt, M.N., “Rewired Warfare: Rethinking the Law of Cyber Attack”, International Review of the Red Cross 96(893), 2014, 189–206, DOI: 10.1017/S1816383114000381, p. 199.

[5] Kilovaty, “Cyber Warfare”, p. 99.

[6] Rid, quoted in Finlay, C.J., “Just War, Cyber War, and the Concept of Violence”, Philosophy & Technology, January 2018, 357-377, DOI: 10.1007/s13347-017-0299-6, p. 359.

[7] Finlay, “Just War”.

[8] Alford, quoted in Robinson, M., Jones, K., and Janicke, H., “Cyber Warfare: Issues and Challenges”, Computers & Security, 49, March 2015, 70–94, DOI: 10.1016/j.cose.2014.11.007, p. 72-73.

[9] Carr, quoted in Robinson, Jones, and Janicke, “Cyber Warfare”, p. 72-73.

[10] Robinson, Jones, and Janicke, “Cyber Warfare”, p. 72-73.

[11] Ibid., p. 74.

[12] D’Urso, M., 2015. “The Cyber Combatant: A New Status for a New Warrior”, Philosophy & Technology, 28(3), 2015, 475–78, DOI: 10.1007/s13347-015-0196-9, p. 476.

[13] Ibid.

[14] Ibid.

[15] Ayalew, Y.E., “Cyber Warfare: A New Hullaballoo under International Humanitarian Law”, Beijing Law Review, 6(4), 2015, 209–23, DOI: 10.4236/blr.2015.64021, p. 217.

[16] D’Urso, “The Cyber Combatant”, p. 477-8.

[17] O’Bright, B., “Child Soldiery in the Information Age”, Allons-y, 2, 2017, 53–70, p. 64)

[18] Dixon, H., “British 15-Year-Old Gained Access to Intelligence Operations in Afghanistan and Iran by Pretending to Be Head of CIA, Court Hears”, The Telegraph, 19 January 2018, https://www.telegraph.co.uk/news/2018/01/19/british-15-year-old-gained-access-intelligence-operations-afghanistan/, accessed on 28 September 2018.

[19] Lowe, C., "Kremlin Loyalist Says Launched Estonia Cyber-Attack", Reuters, 13 March 2009, http://www.reuters.com/article/us-russia-estonia-cyberspace-idUSTRE52B4D820090313, accessed on 28 September 2018.

[20] Awan, I., "Cyber-Extremism: Isis and the Power of Social Media", Society, 54(2), 2017, 138–49, DOI: 10.1007/s12115-017-0114-0.

[21] American Academy of Child & Adolescent Psychiatry, "Social Networking and Children", Social Media and Teens, March 2018, https://www.aacap.org/AACAP/Families_and_Youth/Facts_for_Families/FFF-Guide/Children-and-Social-Networking-100.aspx, accessed on 28 September 2018.

[22] BBC, "Under-Age Social Media Use 'on the Rise'", BBC News, 29 November 2017, https://www.bbc.com/news/technology-42153694, accessed on 28 September 2018.

[23] Misztal, B., Danforth, N., Hurley, M., and Michek, J., "Digital Counterterrorism: Fighting Jihadists Online", Washington, DC: Bipartisan Policy Center, 2018, p. 4-5.

[24] Johnson, D., Whitman, S., and Sparwasser Soroka, H., "Prevent to Protect: Early Warning, Child Soldiers, and the Case of Syria", Global Responsibility to Protect, 10:1-2, 2018, 239-259, DOI: 10.1163/1875984x-01001012.

[25] NATO RTO, RTO-TR-SAS-087 NATO Guide for Judgement-Based Operational Analysis in Defence Decision Making, June 2012, p. 2-2.

[26] Ibid., ch. 6.