Photo: Tookapic

COMMENTARY: CHILDREN AND CYBERWAR: VICTIMIZATION THROUGH PROTECTION?

By Jon Penney

Assistant Professor of Law
at Dalhousie University

Mr. O'Bright has offered an important essay on the many complex issues and questions raised by child soldiers in the information age. With an aim to supplementing his helpful discussion, this brief comment examines state obligations to prevent children from becoming involved in hostilities as I believe it raises challenges unique to cyberwarfare, while also highlighting the importance of Mr. O'Bright's central question— which international legal norms can be applied to cyberwar, and which require fundamental changes or rethinking.

International law not only prohibits enlistment of children into conflict, but also imposes positive obligations on states as well. These obligations, as O'Bright notes, most likely apply to cyberwar as well. The *Tallinn Manual* committee, and Articles in the *Convention on the Rights of the Child* and the *Convention's Optional Protocol on the Involvement of Children in Armed Conflict* arguably combine to not only prohibit such enlistment, but take positive steps to prevent such enlistment and recruitment, with Article 1 of the *UNCRC Optional Protocol* obliging state parties to make "all feasible measures" to ensure armed forces members do not take part in "direct hostilities" before 18 years of age, Article 2 prohibiting compulsory recruitment before age 18, and Article 6 mandating that states "shall take all necessary legal, administrative and other measures" to implement these obligations. While these obligations are well meaning attempts to protect children, when implemented in the context of digital war, these measures may well victimize children rather than protect them.

For example, if states must take "all feasible measures" to prevent online recruitment of children into cyberwar operations, those measures will inevitably include extensive online surveillance of children themselves. That is, in order to track, trace, monitor, and investigate any efforts to recruit child soldiers into cyberwarfare, states will have to track, trace, and monitor, perhaps on an ongoing basis, a lot of children online, as well as their activities. While such surveillance may be carried out here with good intentions and in a good faith attempt to protect the children themselves, this may nevertheless have a significant chilling effect on the children's online activities, with potentially long term negative psychological harms. Indeed, there is some evidence that younger internet users, more so than older ones, are more affected by chilling effects associated with online surveillance (Penney, 2017). Here, children are being victimized and impacted even where they are not even recruited as child soldiers.

Cyberwar's unique complexities may also lead states to unintentionally victimize or harm children in other ways as well. Given the wide availability of digital tools and means for belligerents to remain anonymous, cloak their location, and prevent tracking, tracing, and attribution, states aiming to comply with international requirements will likely take steps to render such age and location information more easy to track or collect. This may involve legal measures requiring disclosure of personal information like age and location or efforts to force public/private sector intermediaries and online service providers to collect, retain, and share

with government, such data from users. Inevitably, such measures— again aiming to protect children—may ultimately expose children to other harms, like privacy threats, reputational damage, identity theft, and, if their physical location is exposed publicly, to a whole host of personal physical threats as well.

Child soldiers are best understood as both victims and potential victimizers (Boothby, 2006). Their involvement in war and conflict mean they may victimize others; but their status as child soldiers also means they cannot lead normal lives as children— a reality often with long lasting negative psychological and physical impact (Boothby, 2009). Cyberwar is no different— but as I have argued here, there is an additional challenge whereby measures taken by states to prevent children's participation in digital conflict may harm or victimize children in other ways too. Clearly, there is still far more work to be done on this and a range of issues on child soldiery in the information age, but Mr. O'Bright's excellent essay has certainly laid a thoughtful foundation for future research, and we would do well to pursue the essential questions he has raised.

Jon is an Assistant Professor at Schulich School of Law, Dalhousie University, and a Research Fellow at the Citizen Lab, Munk School of Global Affairs, University of Toronto. In 2017-2019, he will be a research affiliate at Princeton's Center for Information Technology Policy. His interdisciplinary research focuses, among other things, on human rights, privacy, censorship, and security, especially as they intersect with information law and policy. Follow him on Twitter @jon_penney

SOURCES

Neil Boothby, "When Former Child Soldiers Grow Up: The Keys to Reintegration and Reconciliation", in Neil Boothby, Alison Strang, Michael G. Wessells (eds), A World Turned Upside Down: Social Ecological Approaches to Children in War Zones (Bloomfield, CT: Kumarian Press, 2006).

Jonathon W. Penney, "Understanding the Comparative Dimensions of Chilling Effects Online", Internet Policy Review (2017, forthcoming).