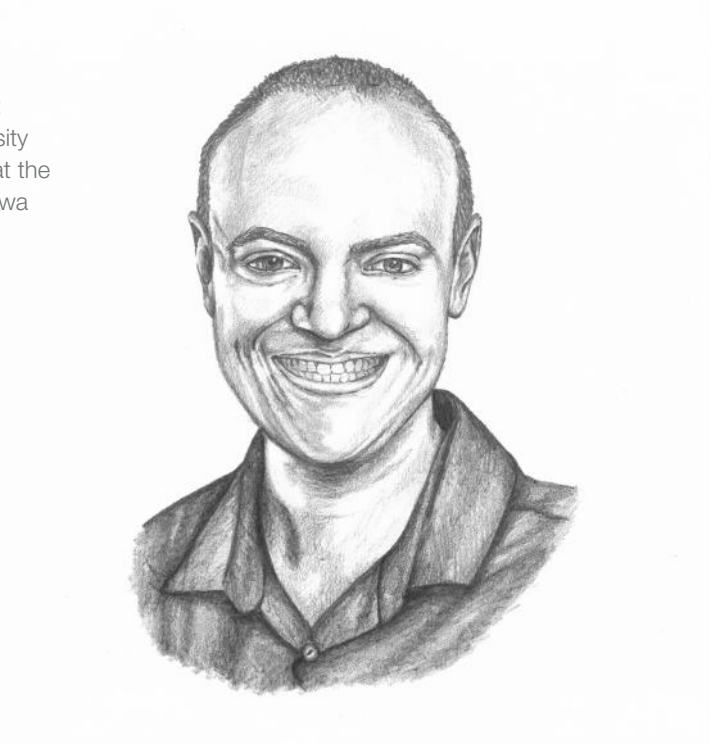
Photo: Luis Llerena

CHILD SOLDIERY IN THE INFORMATION AGE

By Ben O'Bright

PhD candidate at
Dalhousie University
and Researcher at the
University of Ottawa



INTRODUCTION

In 2007, Estonia was the victim of a significant, coordinated cyberattack, which crippled government communications, newspaper websites, banks and other connected entities in Europe's most Internet-saturated country. At the time, leading theories suggested that Russia, or at the very least elements of its intelligence community, might be somehow involved, spurred by the physical symbolism of Estonia removing Soviet-era monuments from city squares and public spaces (Davis, 2007). Indeed, in an attempt to visibly remove its history of engagement as part of the Soviet Union, Estonian authorities and political figures had become determined to demolish and destroy remaining statues erected pre-1990. Two years after the cyberattack, an event that Wired Magazine colloquially termed "Web War One," further details of the unexpected perpetrators would begin to emerge. According to reports by the Financial Times and Reuters, Nashi, a pro-Kremlin youth group with an estimated membership of 150,000, claimed responsibility for the digital assault against Estonia; they described to authorities a strategy of repeated denial-of-service (DoS) attacks, (Clover, 2009; Lowe, 2009). Nashi members, based on different sources, range between the ages of 17 and 25 (Knight, 2007).

According to international law, and in particular the *Paris Principles on Children Associated with Armed Forces or Armed Groups* and the *Optional Protocol on the Involvement of Children in Armed Conflict* affixed to the *United Nations Convention on the Rights of the Child*, a child soldier is "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 who has taken a direct part in hostilities" (UNICEF, 2007, 7; UNOHC, 2000). While the world continues to work towards the goal of ending the use of thousands of remaining children engaged by state military forces, the rise of non-conventional armed conflict, both in terms of actors and spaces, has created a unique challenge largely unanticipated by the drafters of those Conventions, Principles and Protocols noted above: how to define, characterize, and understand a child soldier in the context of contemporary 'battlefields'?

Thanks in part to former U.S. President George Bush's global *War on Terror*, and our current knowledge of child use by emerging extremist organizations including Daesh and Boko Haram, the academic community has begun to place research and evaluative emphasis on exploring the "armed group" affiliation, rather than armed force, component of a contemporary child soldier's existence. But for the large part, these agents remain operative in a physical space, causing physical harm to a physically present opposing force: a child hidden in the underbrush with an AK-47; a girl abused after capture by an insurgent group; or, boy told to martyr himself for a cause. In removing these physical characteristics and

replacing them with the digital, however, are we, or should we, still (be) discussing child soldiery? This paper will endeavour to explore the definitional conundrum facing academics and policymakers regarding the participation of exceptionally connected and digitally literate children and young people in state-backed and non-state instances of cyber attacks or cyber warfare. Indeed, against the backdrop of endemic difficulties in delimiting a threshold in international law beyond which cyber attacks merit hard power responses by states, and the public policy dilemma of appropriate response to young person-led black hat groups, this paper will attempt to begin a conversation deemed by this author as critically necessary for the answering of the questions identified above: what is a child soldier in the digital age?

To begin, this paper will explore the challenge of warfare in our connected, cyber-society, including the difficulties of delineating the beginning and end points of such conflict outside a physical space. Second, the paper will briefly overview and subsequently consider three distinct categories of conflict-actors in the digital age, and how their existence should prompt the academic and policymaker communities to reengage with existing definitions of child soldiers: state-sponsored agents; black hat and 'hacker' groups; and, lone wolves. Finally, the paper will conclude with a proposed series of definitional categories for digital child soldiers and outline future directions for research. As noted, the purpose of this paper is not to provide a final verdict on the applicability of child soldier or related group "types" international law tenets to scenarios of cyber war, but to offer route markers, in the form of conundrums and questions at the end of each case discussion section, for initiating a robust conversation in this regard.

CHILDREN AND WAR IN THE DIGITAL AGE

Generally, war throughout contemporary history has been governed by the collective international *Law of Armed Conflict,* a combination of dozens of treaties from the United Nations Charter and the Geneva Conventions, to the specific banning of chemical weapons and cluster munitions, among others. The challenge, however, has arisen with the emergence of digital and telecommunications technologies in the 20th and 21st centuries: do these agreements and their respective core principles require adjustment or replacement? The academic debate in this regard has been robust. Some, including Lewis suggest that if we approach cyberwarfare as simply involving the application of new technology to gain an advantage over an opposing force, then existing regimes may well continue to be appropriate with adjustments to terminological definitions of combatants, force, and sovereignty (Lewis, 2010, 1). Schmitt, echoing Lewis, proposes that any cyber operation that amounts to an attack, as defined by existing international humanitarian law can qualify as "armed" conflict, by virtue of the former's very real ability to cause meaningful, physical harm outside the digital sphere (2012, 250-252).

The patch of the United States Cyber Command (Department of Defense Photo/Marvin Lynchard)

Additionally, the International Committee of the Red Cross (ICRC)[1] argues that cyber activities which disable a designated object, regardless of consequential physical damage or harm equally constitute an armed attack, although Schmitt suggests that a minimal threshold should be designated, for the shut down of a single computer that performs non-essential functions may not qualify (Schmitt, 2012, 252).

In practical application, organizations including the North Atlantic Treaty Organization (NATO) and the U.S. Department of Defense have moved to apply their own criteria to war in the digital age. The Wall Street Journal reported in 2011 that the Pentagon had drafted a strategic directive indicating that computer-related or computer-driven acts of maleficence and sabotage derived from another state-entity could constitute an act of war, the response to which would be driven by notions of equivalency and proportionality guided by the existing *Law of Armed Conflict* (Gorman and Barnes, 2011). This approach is based on a reported assumption by officials at the time that the most sophisticated attacks on American digital infrastructures and computer systems would require the resource backing of a government (Gorman and Barnes, 2011).

---

[1] In cyberwarfare, the differential between jus in bello and jus ad bellum remains vague and ill-defined, despite heroic efforts by some researchers to fit the rapid and often unanticipated developments in new information technology into existing international law parameters. In the case of ICRC definitions of armed attack in the context of conflict, challenges continue in the fundamental definition of what an armed conflict as such actually entails in the context of the cyber. For our purposes here, quoted material is used simply to reflect the continuing issues related to applying traditional understandings of child soldiery in the digital sphere.

The most prominent of these state-driven definitional framing efforts has been the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, published by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCE) in 2013. Reflective of the on-going debate regarding cyberwarfare in the international law of armed conflict, the Tallinn Manual not only defines for NATO members the acceptable criteria for both *jus ad bello and jus in bello* components for armed conflict, but it provides the first meaningful references to the use of children in this regard. In regarding the Manual, we find indirect linkages to the proposed three form categorization of the manner by which children participate as "soldiers" in cyber warfare: as state-sponsored agents; as formal or informal groups of associated participants, colloquially referred to as black hats or hacker groups; and as lone wolf actors.

STATE-SPONSORED AGENTS

Unanswered queries readily and immediately form the basis of academic scholarship in any discipline. They are not something to be feared but to be embraced. As graduate students, we are taught that being unable to answer a posed question provides us with almost as much value for research as responding to a defined hypothesis. Taking this one step further, I would argue that the investigation to discover those questions, those hypotheses, is of equal merit for scholarly activity. As such, each of the following sections below will work to enable future research avenues by beginning to broach the applicability of international law and definitional characterizations of child soldiers in a contemporary age.

The Tallinn Manual's expert drafting committee suggests that current international law, including the *Convention on the Rights of the Child* Article 38, and Articles 1, 2, and 4 the *Convention's Optional Protocol on the Involvement of Children in Armed Conflict* provides a basis for strongly prohibiting the enlistment by state military organizations of children for the purposes of cyber warfare (Schmitt, 2013, 179). Beginning with the UNCRC Optional Protocol, its drafters mandated that, as in other laws related to armed conflict, state parties make all feasible efforts to ensure that members of an armed force do not take part in direct hostilities until reaching 18 years of age (childrenandarmedconflict.un.org, 2000). In cyberwarfare research, the challenge of defining the notion of direct hostilities in particular has yet to be remedied. Delerue argues that cyberspace offers the opportunity for civilians to easily access a fluid cast of digital "weapons" (from blogs to malicious worms) and participate in armed conflict without ever having set foot in the territory of belligerent parties (2014, 1, 14). Digital warfare also invokes the challenge of online collaboration without a clear understanding of a possible end result (as was demonstrated in 2014 with Reddit and the Boston bombing), as well as "weapons" being slaved by outside parties for the purposes of an attack or conflict contribution (Delerue, 2014, 15). Turns adds that notions of direct participation in hostilities as applied to cyberwarfare are equally hampered by a continuing belief by applicants, that so long as cyber-elements of conflict perpetrated by civilians do not cause direct physical damage

to a person or object, as was the case referenced in this paper's introduction in Estonia, they fail to meet the threshold needed for constituting direct participation (? 2012, 287). Indeed, the Tallinn Manual process contributed to expanding the above question by leaving open several caveats to their recommendation on the prevention of "child soldiers" in digital conflict. The authors note that contributing experts were unable to agree as to whether international law had evolved to the point at which there is consensus on 18 years of age as the basement threshold for appropriate military recruitment, as defined by the UNCRC's Optional Protocol (Schmitt, 2013, 179). The threshold in this regard becomes critical for future discussion for we know from previous research that both in physical and digital armed conflict[2], those able to wield a weapon of war are found under both proposed benchmarks of 15 and 18 years of age.

Additionally, according to the *International Criminal Tribunal for the Former Yugoslavia* (ICTY) and subsequent analysis thereof, there are several approaches by which actions by private individuals can become linked to the authority of the state. First, related to the ICTY case of *Prosecutor v. Tadic*, it was determined that "private individuals acting within the framework of, or in connection with, armed forces, or in collusion with State authorities may be regarded as de facto State organs." (Schmitt, 2012, 253). Second, cyber attacks carried out by individuals whose actions are facilitated by existing law, albeit not as a direct agent of the state, may also be enough to be considered as if launched by state organs themselves (Schmitt, 2012, 252-253). Third, if a state endorses and encourages the perpetuation of cyber attacks from its territory onto others, by formal or informal groups, Schmitt suggests that such activity meets the criterion of state-sponsored armed cyber conflict and a group can be considered a state organ (2012, 253). Under the logic above, tenets of international law on child soldiers do become muddied. With the latter case, there are numerous examples of digital hacking groups which have the de facto support of government entities, including the Syrian Electronic Army (SEA), Iran's Tarh Andishan, APT28, Unit 61398, and Axiom, among others. If any one of these organizations uses the participation of children under the age of 18 or 15, the subsequent causal chain could suggest state-support for child soldiers, if all other definitions on the latter hold true. But, for example, if a young person under the age of 15 retweets messages from the SEA and pledges their electronic support for the organization's objectives despite not being a formal member, is that individual a "child soldier" following the logic above? If "state-sponsorship" in the case of a child soldier in the digital sphere is

---

[2] According to reports by the United Kingdom's National Crime Agency, the average age for perpetrators of "cyber crime" had dropped below 17 years old as of 2015. Reports of those 15 years of age or younger conducting similar activities elsewhere in the world are equally prevalent. See National Crime Agency, "Campaign Target's UK's Youngest Cyber Criminals," Government of the United Kingdom 8 Dec 2015 <http://www.nationalcrimeagency.gov.uk/news/765-campaign-targets-uk-s-youngest-cyber-criminals>, and Emil Protalinski, "15-Year-Old Arrested for Hacking 259 Companies," Zdnet.com 17 Apr 2012 <http://www.zdnet.com/article/15-year-old-arrested-for-hacking-259-companies/>.

A Ukrainian D-30 howitzer. An app used by Ukrainian forces to aid in aiming them is suspected to have been hacked by Russian-backed agents to help separatist forces target them. (DTRA photo).

interpreted as loosely as the proscriptions of the Paris Principles (i.e. the use of a child directly or indirectly), the use of a child directly or indirectly, then nearly all young people indirectly contributing to the 'conflict' objectives of a state-sanctioned, state-sponsored, or state-supported hacking group could well fall into this definition. Recalling the *Paris Principles* view of a child 'soldier' as being any person below the age of 18 who has been or is recruited and/or used by an armed force or group, directly or indirectly as part of hostilities, we return to the paper's original question: can existing understandings of international law be used without fundamental changes to core ideas in order to negotiate this particular case of state-sponsored agents within the changing landscape of armed conflict in the digital age? As with the academic discussion of direct participation in hostilities in regards to cyberwarfare, so long as applicants of international law are comfortable with the broad interpretation of some definitions and the tailoring of others within the context of child soldiers, I suggest that existing legal templates may remain effective. To do so, there should be a recognition that weapons or arms in the digital sphere can be any implement that has either a kinetic or non-kinetic force impact on a designated target.

> **A cyber 'attack' by a person under the age of 15 does not need to blow up a pipeline to have a measurable effect on a conflict.**

Indeed, the definition of a weapon wielded by a child soldier must be redefined for the digital age so as to avoid states using its hard-and-fast physical representations as a workaround for their providing direct and indirect support to digital conflict groups.

The above, however, does not preclude a host of remaining questions, issues, and areas requiring troubleshooting. As was expected, the broaching of child soldier definitions and protections within cyber environments will require the response to a number of lingering issues:

1. What constitutes direct and indirect participation in hostilities pertinent to the use of children in armed conflict?

2. How should state *sponsorship* and state *recruitment* be delineated for discussions on cyber child soldiers?

3. Upon definition, does indirect cyber participation, both knowingly and unknowingly, in an armed conflict by military members under the age of 18 constitute a breach of the UNCRC and its Optional Protocol on Child Soldiers?

4. Does state sponsorship of an independent cyber warfare group or unit constitute a breach of international law related to the use of child soldiers, if the former employs them directly or indirectly in their activities?

5. Does digital warfare and the participation in it by children and young people under state-sponsorship require an adjustment to the minimal age of armed conflict participation as defined by the UNCRC, and if so, what might that age be?

INDEPENDENT HACKER GROUPS

Black hat or independent hacker groups have repeatedly made headlines in recent years, their organizational names becoming synonymous in the public environment with online criminality and cyber armed conflict. Some, like those referenced above, are believed to be in some way sponsored by governments or state entities. But others, including Anonymous, LulzSec, and the Lizard Squad, have typically avoided at any meaningful, mutually supportive relationship with national authorities, operating instead based on their own objectives and external to state apparatuses.

Article 4 of the *UNCRC Optional Protocol on the Involvement of Children in Armed Conflict* highlights that states must take all feasible measures to prevent the "recruitment" or use of children under the age of 18 in armed groups distinct from officially designated armed forces (childrenandarmedconflict.un.org, 2000). This same position is reflected in the Tallinn Manual's language as it limits prevention of recruitment recommendations to state-sponsored entities or any other "organized armed group." According to Margulies, Additional Protocol II of the 1949 Geneva Conventions defined an organized armed group narrowly as characterized by control under a responsible command, exercising control over part of a territory enabling

them to carry out sustained military operations (2013, 55). Precedent setting case law, including *Prosecutor v Limaj* argues that without a headquarters, unified chain of command, and a military police(-like) unit to arrest malefactors, a group is simply a criminal band or assemblage of individuals engaged in the perpetration of unrest (Margulies, 2013, 60-61). Other cases, including *Abella v. Argentina* argue that groups must only demonstrate a "relative" level of organization, although perpetrated acts must be more than riots, banditry and unorganized or short-lived rebellion (Margulies, 2013, 63). In contrast, the *International Committee of the Red Cross's Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* affords "organized armed groups" a distinctive third categorization beyond civilians and state-militaries: individuals in these groups provide a continuous combat, rather than support function, the latter of whom remain civilians (Watkins, 2009, 643).

Therefore, with the above in mind, we must first ask whether hacker groups do indeed recruit individuals under the age of 18 for the purposes of 'armed conflict'? The short and simple answer is most likely, a supposition based on limited after-the-fact police reporting. In 2015, the United Kingdom arrested several members of the Lizard Squad, who had been targeting online gaming platforms with distributed denial of service (DDoS) attacks in order to collapse by overload the company servers (Good, 2015). According to the report by Polygon, all those taken into custody were between 15 and 18 years of age (Good, 2015; Turton, 2015). In Canada, a 12-year-old Anonymous affiliate conducted similar DDoS attacks, as well as illicit entry of government and police services and webpage vandalism in Quebec, Chile and elsewhere (Cline, 2013). This small sample above does indicate that members below the age of 18 are indeed recruited and used by independent black hat organizations for the purposes of cyber conflict on corporations and government.

That said, however, are these young people participating in the child soldier-related international law definitions of an "armed group"?

> **This question returns to my ponderings above as to whether young people in this regard are considered armed; can computers and related black hat tools be considered weapons of war?**

According to Farwell and Rohozinski, the use of the Stuxnet virus against Iranian nuclear facilities and botnet attacks on Georgian government systems during the 2007 conflict with Russia both effectively represent why computers should be considered weapons of war when use thereof can cause physical, real-world damage or injury to another party (2011, 30). Babbin, for his part, is unequivocal in his determination that whether used by one state party against another, or by an

The Natanz nuclear facility in Iran, where uranium enrichment centrifuges were targeted by the Stuxnet computer worm (Photo: Hamed Saber).

armed group against a national entity, computers should be considered weapons of war based on a yet-to-be-determined definition of proportionality beyond the colloquially expounded idea that when a young person sends a virus in an email, the author says, that is not an act of war (2011, 24). The *Paris Principles* and the *UNCRC Optional Protocol on the Involvement of Children in Armed Conflict* make the case that an armed group is distinct from the military of a nation-state. Therefore, provided that these broad interpretations are held true, then a hacker group independent of state-sponsorship could be perceived as an armed group, in that they do occasionally target entities of economic, commercial, and political consequence via computers used as weapons of war.

Additionally, armed groups (according to strict readings of definitions in international law) should demonstrate a form of organization. Traditionally, and in parallel to segmented organizational structures of terrorist organizations, hacker groups have often been perceived in public narratives as headless, anarchic and decentralized organisms that grow and evolve without forms of centralized control needed to be defined as an armed group. Haaster, Gevers, and Sprengers contend, however, that this understanding is fundamentally untrue – hacker groups are instead hierarchically organized around knowledge, skills, and expertise, with those harbouring the most of each forming the leadership nucleus of a given entity (2016, 11). Bussolati terms this a "double-layered" structure, with the nucleus acting as administrators for a given organizational platform, and affiliates both demonstrating varying degrees of loyalty and ceding operational command to the administrators (2015, 112). This hypothesis is tentatively confirmed by a Guardian investigation in 2010 which identified a core-periphery hierarchy present in Anonymous, organized and defined around knowledge and expertise of users (Halliday and Arthur, 2010).

As such, it would appear that at least in principle, existing international law on the involvement of children in armed conflict could be definitionally expanded to comfortably account for young people involved in independent hacker groups. Continuing this logic chain, if hacker groups are to be considered armed groups, then international law would provide that government must take all feasible measures to prevent the recruitment of children as either willing or unwilling "soldiers" of a hacker group. That said, the digital age provides an interesting third categorization beyond these latter two soldier types: the unknowing participant in armed conflict. In October 2016, the world witnessed one of the largest cyber-attacks ever recorded, one which caused a host of popular internet websites, including Twitter and Paypal, to be inaccessible. Subsequent analysis revealed that hackers had slaved thousands of pieces of the Internet-of-Things (online connected devices, from webcams to digital video recorders) as part of a weaponised botnet to initiate a potent DDoS attack, all unbeknownst to everyday users (Blumenthal and Weise, 2016; Thielman and Hunt, 2016). Many of these articles and items would have been owned and operated by individuals under the age of 18 years old. Thus, a question for future research, among others, is whether these persons would be considered as part of a third category of cyber child soldiers: the unknowing participant?

As with state-sponsored hacker groups, this investigation of independent black hat organizations leaves us with a number of critical questions that should be answered as research continues this conversation regarding child soldiery in the digital age:

1. Can independent hacker groups truly wage "armed conflict" on a government using only non-kinetic tools and weapons (i.e. computers)? Or is what they are performing simply an extension of criminality?

2. Can computers and computer-technology be appropriately classified as "weapons of war"? What are the repercussions of this reclassification?

3. Do hacker groups, independent of state support, fall under the mandate of existing humanitarian law and the treatment of enemy combatants, or are they to be considered mercenaries? How do these differential label applications affect the protection of young people as cyber child soldiers?

4. Could hacker groups be considered *levée en masse*, as per international humanitarian law, and does this require a certain threshold of participant numbers in order to apply?

5. Is the double-layered structure found in independent hacker groups enough to be considered an organized armed group as per provisions of international law?

6. What feasible measures must a government pursue to prevent all three approaches to digital child soldier recruitment: voluntary, involuntary, unknowing participant?

LONE WOLVES

Thus far, existing international law on armed conflict and on the involvement of children in such a scenario appears to be worded broadly enough to allow for a digital evolution of sorts, in which young people are drawn into conflict directly and indirectly via information and communications technology, provided that certain provisions noted above are reworked and remaining queries answered. That said, the connected nature of human existence which defines our world today brings with it the interesting category of lone wolves.

Contemporary legal approaches to child soldiers refer to them in the context of their recruitment and participation in a military or non-state actor armed group, inside (internal) or outside (external) of a country in question. The Tallinn Manual, however, does make reference to lone wolves, albeit only in regards to the state's responsibility in the prevention of children being involved in "hostilities"; another semantic challenge for cyber conflict scholars (Schmitt, 2013, 179-180). Indeed, it is a rare case in which a child soldier is referenced as an individual entity, one without affiliation to an organized, hierarchical group. One of the reasons for this is the inability for a child soldier thus far to wield enough destructive force to cause wide-ranging damage to a country's critical infrastructure, economic and commercial systems, or political institutions relative to an armed group. Until the moment arises when an individual or a singular actor is able to match the kinetic impact potential of a collective, the terms 'child soldier' and 'armed group' will likely remain synonymous.

But the digital world, including the advent of hyperconnectivity through pervasive telecommunications technology and a rapid diffusion of technical knowledge throws a wrench into this linkage between individual and group, because it does allow for lone wolves to match the potential non-kinetic impact of an armed group. For example, in 2014, a 14-year-old British teen was arrested for conducting effective cyber-attacks on a number of government agencies and servers, including the Iraqi Ministry of Foreign Affairs, the Thai Department of Agriculture and the Chinese Ministry of Security, as well as various corporate entities (Evans, 2016). In 2015, three independent young hackers were able to penetrate the email account of CIA Director John Brennan (Zetter, 2015). Finally, in 2016, a report surfaced that a teen hacker was able to access hundreds of sensitive data file-transfer protocol servers operated by the U.S. government, collecting from them millions of social security numbers (Parrish, 2016).

As is the challenge in negotiating levee en masse with regards to thousands of indirect participants in conflict unbounded by geopolitical borders, I would argue that it is time for a revitalization of child soldier definitions in recognition that one may not need to be recruited and used by either an armed group or military to act, and perhaps more importantly, impact like an (un)armed child combatant in conflict.

Photo: Thomas Kvistholt

> **But does a young person conducting these types of cyber-attacks, independent of a group, warrant the classic label of child soldier or criminal?**

As it often does, I would argue that context plays an important role in this regard. To perpetrate a cyber-attack outside the confines (non-geographical confines due to the transborder nature of the Internet) of an armed conflict, I believe, would warrant the label of 'crime.' Although the UNCRC's Optional Protocol and the Paris Principles do not define armed conflict within the context of children's rights specifically, the International Committee of the Red Cross feels that two definitions exist: international armed conflict between two or more states; and, non-international armed conflicts between a state and an armed group, or two or more armed groups on a designated territory (2008, 5). I would suggest that a designation of 'conflict' as such can be applied by any one participating or observing party.

Inside the context of an armed conflict, however, young people unaligned with either combative actor, but participating under their own right and for the achievement of their own self-designated objectives (whether such objectives align to a combative party or not) should be afforded the same protections as any other child soldier would under the parameters of international law. There should be a disaggregation of the implied condition that a young person as child soldier has become a conflict participant for one organized side or another. In the digital age, a child combatant can engage in an armed conflict and affect change on their own accord, to perhaps the same degree as an organized group. As such, I propose that the academic and practitioner communities begin to consider a series alternative definitional categories for the "digital child soldier," A combatant may be affiliated or unaffiliated with an organized armed group or party to a conflict. Additionally, and as noted, thanks to the global nature of modern telecommunications, a child participant may be internal or external to the territory upon which physical conflict is occurring.

Four such broad categories, based on the information above, can be proposed, with the expectation that they will be substantially changed as research progresses. First is the *Affiliated Digital Child Soldier*, or a young person, as defined by the UNCRC and Paris Principles, operating under the purview, voluntarily or forcibly, of a state party, military, or state-affiliated armed group engaged or preparing to engage in kinetic or non-kinetic armed conflict. Second is the *Unaffiliated Digital Child Soldier*, or a young person, as defined by the UNCRC and Paris Principles, operating outside the purview of participant actors in a kinetic or non-kinetic armed conflict, for self-defined objectives that may or may not align to those of the conflict's actor groups. Third, I propose a category termed the Internal Digital Child Soldier, a young person, as defined by the UNCRC and Paris Principles, involved directly or indirectly with an existing armed conflict from within the designated physical territory upon which or about which a conflict pertains. Finally, in contrast to the third, there is the *External Digital Child Soldier*, a young person, as defined by the UNCRC and Paris Principles, involved directly or indirectly with an existing armed conflict from without (outside) the designated physical territory upon which or about which a conflict pertains.

It is encouraged that future research explore the various combinations of the above definitions, from External Affiliated Digital Child Soldiers, to Internal Unaffiliated Digital Child Soldiers. As well, this work could add additional characterization categories to the above, refining and narrowing existing definitions so as to adequately reflect the changing nature of child participation in conflict whilst preventing the "digital" from weakening or blurring the protections afforded to young people trapped within the confines of war. Indeed, this should include a focused effort at preventative measures in regards to the radicalization of young people prior to recruitment by an armed group.

CONCLUSION

Humans are not infallible deliverers of anticipatory policymaking, especially at the international level. To expect those drafters of original laws of armed conflict and the involvement of children in such to have effectively authored text to encompass the monumental changes arising from the digital age is likely too much. Instead, as a society, we must be willing to adjust, as appropriate and when needed, the core documentation and common principles that underline our regulatory environment when they can no longer adequately encompass contemporary challenges.

In this paper, I hoped to begin a conversation in this regard, advocating for the emergence of a digital child soldiery definition in some unprecedented cases. First, I investigated the applicability of existing international law to state-sponsored child agents of cyber warfare, concluding that with minor expansion, both the UNCRC and the Paris Principles, as well as leading armed conflict manuals, are well equipped to broach this new category of actor.

Similar conclusions were reached in the exploration of independent hacking groups, with the caveat that a number of remaining queries must be addressed. Finally, I proposed that real definitional change in international law must come so as to negotiate the emergence of lone wolf actors, each of whom may have their own objectives and can potentially wield as much non-kinetic force as an armed group or military. In this section, I offered a two-columned definitional nexus to guide future efforts in approaching lone wolf digital child soldiery, one I hope other researchers can continue to add to, expand upon, or narrow.

Barring an unexpected cataclysmic event, digital child soldiery will only continue to grow in strength, potential and complexity. As such, it is critical we begin this conversation now, for fear of being unable to effectively direct this trend in the near future. Especially as digital connectivity increases each year in every corner of the globe, including the developing world which has seen some of the highest levels of ICT diffusion and adoption, it would be naïve to assume those legal proscriptions authored for a young person with an AK-47 would be adequately equipped to face the threat of cyberwarfare. I can only hope that others will take this call to heart; let us begin to collectively interrogate the notions of child soldiery in the digital age.

Ben received his Masters of Science degree from the London School of Economics and Political Science in the Politics and Government of the European Union. His dissertation focused on the reflection of European Union core institutional values, particularly the respect for human rights, in member state digital media policies. Today, Ben is a PhD candidate at Dalhousie University where he studies the politics and policies around emergent technologies, particularly the causes of chosen governance approaches for new science and technology innovation. Currently, Ben works as a Researcher with the Centre on Governance at the University of Ottawa, as an international consultant for several organizations including UNICEF, the African Mineral Development Center, the United Nations Economic Commission for Africa, and the Qatar Foundation, and as a doctoral researcher on (digital) human rights with the Roméo Dallaire Child Soldiers Initiative.

BIBLIOGRAPHY

Babbin, Jed. 2011. "Computers Are Weapons of War." The American Spectator, August.

Barnes, Siobhan Gorman And Julian E. 2011. "Cyber Combat: Act of War." Wall Street Journal, May 31, sec. Tech. http://www.wsj.com/articles/SB10001424052702304563104576355623135782718.

Cline, Alex. 2013. "This 12-Year-Old Just Got Busted For Hacking For Anonymous." Mic. October 28. https://mic.com/articles/70489/this-12-year-old-just-got-busted-for-hacking-for-anonymous.

Delerue, François. 2014. "Civilian Direct Participation in Cyber Hostilities." Revista D'Internet, Dret I Política, no. 19 (October): 1–17.

Evans, Martin. 17:14. "Teenager Who Hacked Governments Worldwide Is Spared Jail." The Telegraph, sec. 2016. http://www.telegraph.co.uk/news/2016/07/20 teenage-hacker/.

Farwell, James P., and Rafal Rohozinski. 2011. "Stuxnet and the Future of Cyber War." Survival 53 (1): 23–40. doi:10.1080/00396338.2011.555586.

Gavin Knight. 2007. "The Alarming Spread of Fascism in Putin's Russia." The New Statesman, July 24. http://www.newstatesman.com/politics/2007/07/putin-russia-nashi-soviet.

Good, Owen S. 2015. "British Cops Arrest Six in Connection with Lizard Squad Christmas Attacks on Xbox, PSN." Polygon. August 29. http://www.polygon.com/2015/8/29/9224813/lizard-squad-arrests-hacker-attacks-ddos.

Haaster, Jelle Van, Rickey Gevers, and Martijn Sprengers. 2016. Cyber Guerilla. Syngress.

"Hacked Home Devices Caused Massive Internet Outage." 2016. USA TODAY. Accessed October 26. http://www.usatoday.com/story/tech/2016/10/21/cyber-attack-takes-down-east-coast-netflix-spotify-twitter/92507806/.

Halliday, Josh, and Charles Arthur. 2010. "WikiLeaks: Anonymous Hierarchy Emerges." The Guardian, December 16, sec. Media. https://www.theguardian.com/media/2010/dec/16/wikileaks-anonymous-hierarchy-emerges.

Hunt, Sam Thielman Elle. 2016. "Cyber Attack: Hackers 'Weaponised' Everyday Devices with Malware to Mount Assault." The Guardian, October 22, sec. Technology. https://www.theguardian.com/technology/2016/oct/22/cyber-attack-hackers-weaponised-everyday-devices-with-malware-to-mount-assault.

International Committee of the Red Cross. 2008. "How Is the Term 'Armed Conflict' Defined International Humanitarian Law?" Opinion Paper. Geneva: International Committee of the Red Cross. https://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf.

"Lizard Squad Member Convicted of 50,000 Counts of Computer Hacking." 2015. The Daily Dot. July 7. http://www.dailydot.com/crime/lizard-squad-indicted-julius-kivimaki/.

Lowe, Christian. 2009. "Kremlin Loyalist Says Launched Estonia Cyber-Attack." Reuters, March 13. http://www.reuters.com/article/us-russia-estonia-cyber space-idUSTRE52B4D820090313.

Margulies, Peter. n.d. "Networks of Noninternational Armed Conflicts: Crossing Borders and Defining 'Organized Armed Group.'" International Law Studies 84: 54–74.

"National Crime Agency - Campaign Targets UK's Youngest Cyber Criminals." 2016. Accessed October 25. http://www.nationalcrimeagency.gov.uk/news/765-campaign-targets-uk-s-youngest-cyber-criminals.

Ohlin, Jens David, Kevin Govern, and Claire Finkelstein. 2015. Cyber War: Law and Ethics for Virtual Conflicts. OUP Oxford.

"Optional Protocol to the Convention on the Rights of the Child." 2016. Accessed October 4. http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPACCRC.aspx.

Parrish, Kevin. 2016. "Multiple FTP Servers Owned by the U.S. Government Were Accessed by a Teen Hacker." Digital Trends. September 19. http://www.digitaltrends.com/computing/teen-hacker-ftp-servers-usa-government/.

Protalinski, Emil. 2016. "15-Year-Old Arrested for Hacking 259 Companies." ZDNet. Accessed October 25. http://www.zdnet.com/article/15-year-old-arrested-for-hacking-259-companies/.

Schmitt, Michael. 2012. "Classification of Cyber Conflict." Journal of Conflict and Security Law 17 (2): 245–60. doi:10.1093/jcsl/krs018.

Security, Author: Kim Zetter Kim Zetter. 2016. "Teen Who Hacked CIA Director's Email Tells How He Did It." WIRED. Accessed October 27. https://www.wired.com/2015/10/hacker-who-broke-into-cia-director-john-brennan-email-tells-how-he-did-it/.

Turns, David. 2012. "Cyber Warfare and the Notion of Direct Participation in Hostilities." Journal of Conflict and Security Law 17 (2): 279–97. doi:10.1093/jcsl/krs021.

UNICEF. 2007. "The Paris Principles: Principles and Guidelines on Children Associated with Armed Forces or Armed Groups." Paris: UNICEF.

Watkin, Kenneth. 2009. "Opportunity Lost: Organized Armed Groups and the ICRC Direct Participation in Hostilities Interpretive Guidance." New York University Journal of International Law and Politics 42: 641