National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

ARE DIGITAL BLUE HELMET FIRES RED: HOW THE UN NEEDS TO THINK BIOLOGICALLY ABOUT ITS CYBER CAPABILITY DEVELOPMENT

Major Travis Hanes

JCSP 46

Solo Flight

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2020.

PCEMI 46

Solo Flight

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de la Défense nationale, 2020.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 46 – PCEMI 46
2019 – 2020

SOLO FLIGHT

ARE DIGITAL BLUE HELMET FIRES RED: HOW THE UN NEEDS TO THINK BIOLOGICALLY ABOUT ITS CYBER CAPABILITY DEVELOPMENT

By Major Travis Hanes

"This paper was written by a candidate attending the Canadian Forces College in fulfillment of one of the requirements of the Course of Studies. The paper is an academic document, and thus contains facts and opinions which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defense. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defense. "

Word Count: 5,800

"La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale."

Nombre de mots : 5.800

ARE DIGITAL BLUE HELMET FIRES RED: HOW THE UN NEEDS TO THINK BIOLOGICALLY ABOUT ITS CYBER CAPABILITY DEVELOPMENT

> *David: "They're trajectories for multi-impact reentry vehicles."*
> *Jennifer: "What does that mean."*
> *David: I don't know, but it's great.*
> - *Quote from the film 'WarGames'*
>
> *"When you plant a fertile meme in my mind your literally parasitize my brain, turning it into a vehicle for the meme's propagation in just the way that a virus may parasitize the genetic mechanism of a host cell."*
>
> - *The Selfish Gene. Richard Dawkins*[1]

INTRODUCTION

A bellicose characterization to cyberspace is not new. One need only look at Hollywood's depiction of it in the movie WarGames with a young Matthew Broderick. The movie came out in 1983. And though 80's kitsch might not seem an appropriate foil to International Relations (IR) gravitas, it is worth recalling that upon completion of watching WarGames at Camp David, Ronald Reagan turned to his staff for immediate solutions to the existential threat to the nation.[2] Paradoxically, on the one hand, cyberspace is about interconnectivity, and "recreating the world in the image of a global village,"[3] but it also divides through disinformation, is infused by hype cycles,[4] and compounded by pundits' habit to

[1] Richard Dawkins. *The Selfish Gene. 40th Anniversary Edition*. (Oxford: Oxford University Press, 2016). 440

[2] Ep.50 - Cyber Yesterday. *Defence One Radio. 29 Jul 19* https://www.defenseone.com/ideas/2019/07/ep-50-cyberwarfare-yesterday/158750/?oref=d-channelriver

[3] Marshal McLuhan. *The Gutenberg Galaxy*. (University of Toronto Press, 2011) 213

[4] Gardner Hype Cycle: "a graphical depiction of a common pattern that arises with each new technology or other innovation. Each year, Gartner creates more than 90 Hype Cycles in various domains as a way for clients to track technology maturity and future potential. The five phases in the Hype Cycle are Technology Trigger, Peak of Inflated Expectations, Trough of Disillusionment, Slope of Enlightenment and Plateau of Productivity." https://www.gartner.com/en/information-technology/glossary/hype-cycle

fetishize threats to exotic hazards.[5] It almost goes without saying, and much quoted in military writing, that it is only a matter of time before a "cyber Pearl Harbour Event" strikes the United States.[6] Yet, the trouble with this narrative thread is twofold: (1) there is little room for thinking about peace and de-escalation since the imagery of the conflict is haunted by first strike Cold War nuclear détente discourse, that fails to revisit the assumptions behind its own security dilemma;[7] and, (2) it is an overly simplistic militarization of what cyberspace is, failing to address the interconnected reality of a cyber ontology that shares much in common with its biological cousin.

This has very real consequences for peacekeeping operations, especially as they straddle the divide between peace and war. Modern belligerents present a mix of high-tech informational reach vis-à-vis the cyber domain, and the very real world of ultra-violence[8] (imagine the story of Cain and Able but with Snapchat and DeepFakes). Take internet saturation in sub-Sahara Africa for instance; 77% of Africans under 35 have access to a smartphone, as cheap Chinese variants hit the market[9], and only further complicated by telecommunications giant Huawei's expansion of internet infrastructure. "Rapid connectivity," in the views of Citizen Labs founder Ron Deibert is taking place in a context of chronic unemployment, disease… and failed or failing states." As all countries orient themselves to the realities of 'virtual war' so to has the United

[5] Erik Gartzke. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down To Earth." *International Security*, Vol. 38, No. 2 (Fall 2013) 51.

[6] Elisabeth Bumiller, Thom Shanker, "Penetta Warns of Dire Threat of Cyberattack." *New York Times*.(11 Oct 2012).

[7] Charles. L. Glaser. "The Security Dilemma Revisted." *World Politics,* Vol. 50, Iss 1(Special Issue) (Fall 1997). 199

[8] Anthony Burgess. A Clockwork Orange: The Restored Edition. Penguin Classics:). 225. Burgess' view on violence is reproduced here. "I don't just mean torture and killing: but violence done to the stability of the community through such devices as inflation, and the more terrible enacted in the name of technological progress, done to the environment. We have all comes to terms with violence: it is our daily news and our nightly entertainment."

[9] Antonio Cascais. "How China Benefits from Africa's Smartphone Boom." *Deutche Welle* (28 Oct 2019) https://www.dw.com/en/how-china-benefits-from-africas-smartphone-boom/a-51016346

Nations (UN), as it seeks to fulfil its core mandate, and as the organization that shelters many of the non-United States (U.S.) standardization agencies that seek to govern the internet: the International Telecommunications Union (ITU), Internet Society (ISOC), World Summit on the Information Society (WSIS), the Internet Governance Forum (IGF) and the UN Institute for Disarmament Research (UNIDIR). The UN has recently emerged as "the most important cog" in the international system for coordinating internet management.[10]

RESEARCH QUESTION, APPROACH, MAIN ARGUMENT

This paper is looking for a way to protect peacekeepers. For many Canadian officers, and organizations like Citizen Labs, the failures of the Canadian lead mission to Rwanda were game changers. The prominent place that media had in the genocide[11] were pre-adaptations that evolved into fake news, disinformation, and truth decay. In the effort to protect peacekeeping, there has been two questions that have driven research on this topic. (1) In the rapidly developing field of cyber warfare, how can the UN field relevant cyber capabilities at either the operational or tactical level without a resolution, binding norms[12] of behaviour, or a convention that authorizes or constrains the use of these weapons? (2) Is there a framework of pre-existing norms similar enough to cyber warfare that can be grafted unto it, in lieu of higher strategic policy, so that the UN can move forward? To answer these questions, the paper will review the current

[10] Christopher Whyte, Brian Mazanec. *Understanding Cyber Warfare: Politics, Policy and Strategy*. (New York: Routledge, 2019).43

[11] Robert. J. Deibert. *Black Code*. (Toronto: Signal, 2013).169

[12] This paper has used the definition of norm as used in Information & Communications Technology (ICT) discussions in the UN: "10. . . . . Norms reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States. Norms can help to prevent conflict in the ICT environment and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development." Source: Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174. Page 7.

debate regarding the UN's quixotic development of international cyber constraining norms, and the consequences for developing digital blue helmets.

Counterintuitively the paper will use biological warfare (BW) development as a case study to make the argument that UN constraining norms are sufficient to field cyber peacekeeping capabilities. A number of reasons make this possible: the commonality of the two environments and their attributes, the longitudinal evidence of constraining norms within BW, and the shared biological lexicon. As well, recent consilience between the biological and cyber environments have bridged the divide between disciplines, and are a valuable framework in developing "expectations for how norms for cyber warfare will develop."[13] From this, the paper will demonstrate what capabilities can be developed under a force protection concept for digital blue helmets. It will do this in two distinct ways: (1) tactical applications that can be enacted now and in which UN training architecture can be created; and (2) where the UN needs to integrate operational cyber capabilities into peacekeeping operations. Finally, the goal is to provide a path for modernizing peacekeeping operations with cyber tools, within the limited construct that BW allows. Ultimately this paper is arguing that cyber warfare should be viewed not just in proprietorial terms or covert action. If this remains the fact, it will ignore the reality of its everyday pedestrian use by proxy forces, terrorists, criminals, and private military contractors (PMC): a deadly alchemy for peacekeepers. In the end, the UN needs to view cyber capabilities as an extension of self-defence and force protection, much like vaccination and personal protective equipment (PPE), so that it can request and build cyber capabilities commensurate to the requirements of modern peacekeeping.

[13] Brian M. Mazanec. *The Evolution of Cyber War*. (Nebraska: Potomac Press, 2015).37

THE HISTORY OF CYBER WITHIN THE UN

It has only been since the late 1990's that cyber constraining norms beyond technical standards have been a topic of debate: in either the UN Security Council (UNSC), or specialized agencies of the UN.[14] The Russians initially signalling to limit the use of cyber weapons.[15] It is interesting to note the inseparable nature of cyber and information operations of early Russian efforts to limit war within the internet. American, and Canadian doctrine retaining the division, have chosen to see them as different entities; however for both Russia and China these capabilities remain one.[16] These differing notions of warfare's boundaries no doubt have root in their communist revolutionary past, but regardless of this, it leads to very different views of internet freedom.[17] As a result, UN resolutions put forth by Russia and supported by China generally endeavour to constrain the internet as a vehicle for informations operations within sovereign states. Discourse is focused on state control within hardened borders looking in.[18] It is the digital manifestation of the same analog frontier borders that Russia still maintains with Norway.[19] By the mid 2000s, signalling of intent lead to a draft resolution being submitted to the UNSC only to stagnate. However by 2015, a UN resolution was submitted by Russia and

[14] This is an important distinction to make. The evolution of cyber norms has deeply embedded encoding memes, originating from the technical telecommunications and signals intelligence fields. For a more detailed description, history and the structural constraints and their impacts, see the academic compilation "Opening Standards: The Global Politics of Interoperability, ed Laura DeNardis.

[15] Tim Maurer. "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber Security." *Balfour School for Science and International Studies Discussion Paper*. (Harvard: 2011). 5 https://www.belfercenter.org/sites/default/files/legacy/files/maurer-cyber-norm-dp-2011-11-final.pdf

[16] David. E. Sanger. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. (New York: Broadway Books, 2018), 87.

[17] Kristine Lee, Alexander Sullivan. "People's Republic of the United Nations." *Center for New American Security*. (May 2019). 4. https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-China-IO-final-web-b.pdf?mtime=20190513092354.

[18] Peter Singer, Allan Friedman. "What You Need to Know: Cybersecurity and Cyberwar." (Oxford: Oxford University Press, 2014). 435

[19] David KilCullen, *Dragons and Snakes: How the Rest Learned to Defeat the West.* (New York: Oxford University Press, 2020). 238

seconded by China, containing binding agreements to regulate cyber weapons and their use.[20] U.S. views differed however, having vetoed these initiatives, seeing it as a ploy to (1) limit U.S. cyber superiority, in order to better launch attacks below the threshold of armed conflict; and (2) the likely realization of the real practical reality that 70% of global bot nets are sheltered in China, and their collusion with their tech industry to steal U.S. intellectual property.[21] That being said, a UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security was convened, and in 2015 produced a road map for non-binding normative rules, including the responsibilities of states to control cybercrime and terrorism within their borders. It never achieved consensus and was disbanded; there are now two competing normative orders: a Sino-Russian state sovereign system, and a Western free market, decentralized/distributed system.[22]

The Sino-Russian order has been lobbying at the ITU and ISOC. As mentioned, both are part of the UN; however, the extension of their mandate has rapidly grown to include internet regulation standards with a capacity building arm for developing countries.[23] Together these two developments have important consequences for the establishment of digital blue helmets. Firstly, it highlights two competing trends that make the devolution of peacekeeping authorities and capabilities difficult and muddled with development initiatives. On the one hand, stalled UNSC consensus makes it difficult to employ capabilities with the authorities required to make them useful. Delegating authorities to peacekeeping formations that are a mix of nations, regardless if

[20] Sino-Russian Cybersecurity Agreement 2015 https://carnegieendowment.org/publications/interactive/cybernorms

[21] James Fellows, "Cyber Warriors." The Atlantic 2010 https://www.theatlantic.com/magazine/archive/2010/03/cyber-warriors/307917/

[22] Alex Grigsby. "Unpacking The Competing Russian and U.S. Cyberspace Resolutions at the United Nations." *The Council For Foreign Relations Blog.* (29 Oct 2018) https://www.cfr.org/blog/unpacking-competing-russian-and-us-cyberspace-resolutions-united-nations

[23] The Plenipotentiary Conference of International Telecommunications Union Internet. *RES 101: Internet-Protocol Based Networks* (Dubai, 2018). https://www.itu.int/en/action/internet/Documents/Res%20101.pdf

the actions are at the hardware layer, or more properly located in the persona layer (the medium in which information operations are conveyed) only increases already extant issues with respect to information exchange and classification.[24] On the other hand, many of the structural standardization norms, are adopted due to economic incentives, which allow information exchange to be conducted and have the force of de facto and de jure laws.[25] This highlights how the inertia of policy generation are juxtaposed with the fast-moving economic drivers which also influence normative behaviours. Even cyber capability leaders are struggling with understanding what is permissible or should not be.[26] Banal seeming these standardization norms are, they are evolving outside any conscious control of the UNSC. It is unclear if the de facto norms are positive or negative. It cannot be assumed the norms will be liberal in design or will protect human rights. Specifically, autocratic regimes are targeting these technical UN open standards organizations as a means to further an illiberal agenda that has been frustrated at the UNSC by western countries.[27]

For the peacekeeping force facing a Future Operating Environment (FOE) that is characterized by intense competition on the ground but also in cyber space, these seem insurmountable obstacles to building effective force protection measures. There is only incremental movement forward on disarmament or control of cyber-based weapons, and a slow

[24] Canada, Department of National Defence. *JDN 2017-02. Joint Doctrine Note: Cyber Operations. (*Ottawa 2017). 2-2

[25] Rishab Ghosh, "An Economic Basis for Open Standards." Stacy Baird "The Government at the Standards Bazaar." *Opening Standards: The Global Politics of Interoperability.* Editor Laura DeNardis. (Cambridge: Massachusetts Institute of Technology, 2011). 67. Rishab Ghosh, "An Economic Basis for Open Standards." *Opening Standards: The Global Politics of Interoperability.* Editor Laura DeNardis. (Cambridge: Massachusetts Institute of Technology, 2011). 202

[26] David. E. Sanger. "The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age" (New York: Broadway Books, 2018), 87.

[27] Madhumita Murgia, Anne Gross. Inside China's Controversial Mission to Reinvent the Internet. *Financial Times. (27 May 2020) https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f*

movement forward to arm peacekeepers within an environment that is being contested in the halls of Geneva. However, what this paper would like to suggest, is that it is an incorrect framing of the problem; a failure to build upon the successes made to solve similar problems with respect to BWs. A reframe from more of a biological PPE perspective is an effective way of confidence building measures and aligning capabilities for incorporating the UN uniformed requirements registry.

AN ALTERNATIVE FRAMEWORK: A BIOLOGICAL PERSPECTIVE.

The UN has conceptually and structurally organized cyber security into a political/military and cybercrime model. Starting in 1998, a series of General Assembly resolutions aligned and assigned roles to subcommittees and organizations.[28] Fig 1 depicts the streams, showing how there is little crossover between organizational platforms tasked with very specific mandates within their respective terms of reference.

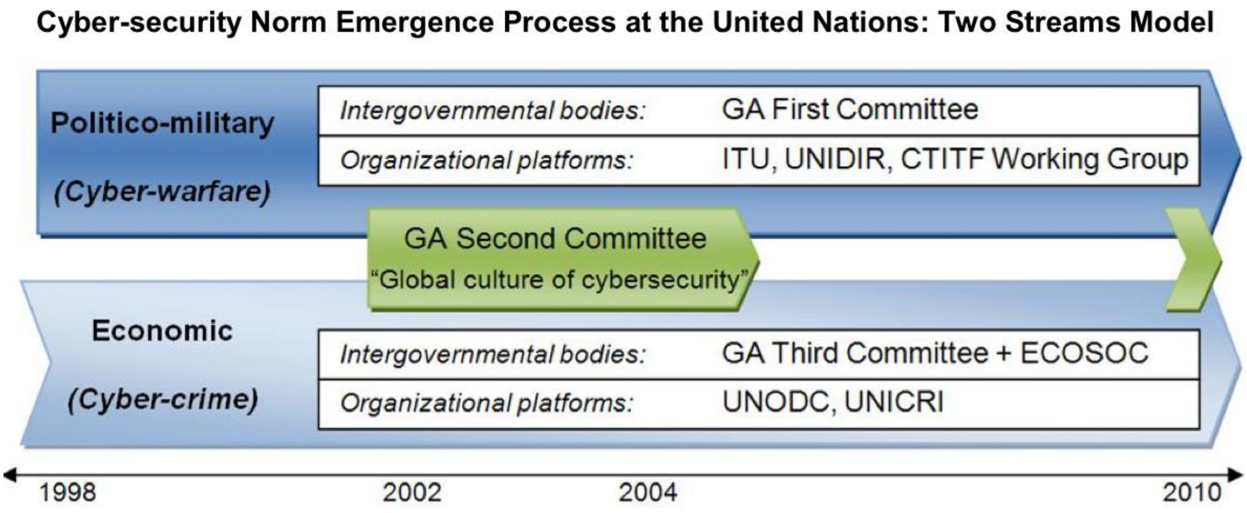
Cyber-security Norm Emergence Process at the United Nations: Two Streams Model
Politico-military
(Cyber-warfare)
Intergovernmental bodies:
GA First Committee
Organizational platforms:
ITU, UNIDIR, CTITF Working Group
GA Second Committee
"Global culture of cybersecurity"
Economic
(Cyber-crime)
Intergovernmental bodies:
GA Third Committee + ECOSOC
Organizational platforms:
UNODC, UNICRI
1998
2002
2004
2010

Fig 1. Two Stream UN Model

[28] Tim Maurer. "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber Security." *Balfour School for Science and International Studies Discussion Paper.* (Harvard: 2011). 15 https://www.belfercenter.org/sites/default/files/legacy/files/maurer-cyber-norm-dp-2011-11-final.pdf

This division makes sense for a number of reasons, yet it comes at a cost. It has been a hinderance to developing or fielding cyber capabilities during peacekeeping operations.[29] It also conceptually divides something that (a) is tightly coupled, and (b) militarizing or criminalizing cyber operations. Either is an oversimplification and ignores how interoperability, knowledge sharing, and cooperation of Other Government Departments, Non-Governmental Organizations, and an industry consisting of over 5000 internet service providers (ISPs) makes up the internet.[30] Of note in Fig 1 is the absence of an organization responsible for sabotage and espionage threats outside the dichotomy, instead it is divided across streams. Scholars like Thomas Rid have argued that cyber attacks are not forms of warfare at all but examples of espionage.[31] If he is correct the combining of the political and the military has a high potential of being an anchoring bias that ignores key features of the problem. It is not geopolitical framework in which to build consensus; it is much more of a technological one.[32]

However, an alternative view has emerged over the last few years that uses a biological perspective. In Cybersecurity and Cyberwar, RAND analyst Peter Singer and Allan Friedman look at the Centres for Disease Control (CDC) and their methods of coordinating global responses to public health threats. It is an effort to reframe and go beyond traditional dichotomies that ignore the distributed nature of cyber. They point to a commonality of terms like virus, inoculation, pandemic, incubation, and virality as more than coincidence; it is an indicator that they share a similar discursive environment characterized by evolution and adaptation.

[29] Internet Governance Forum. “CyberSecurity Agreements: Final BPF Output Report.” *Best Practice Forum on Cybersecurity.* (20 Jan 2020). 25-27
[30] Peter Singer, Allan Friedman. “What You Need to Know: Cybersecurity and Cyberwar.” (Oxford: Oxford University Press, 2014). 407
[31] Thomas Rid Rid. “Cyber War Will Not Take Place.” *Journal of Strategic Studies*. Vol. 35:1, 2012. 6
[32] David. E. Sanger. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. (New York: Broadway Books, 2018). 27

This new frame of reference has been made possible by the recent IR work of former BW specialists Gregory Koblentz and Brian Mazanec. In a comparison to a much longer BW history with an analysis of cyber weapons development, they have mapped out the commonalities, "drawing out *meaningful insights* for the *development of international constraining norms*."[33] Fig 2 is a visualization of key biological and cyber events along a historical timeline. It categorizes (a) the specific use, differentiating between a conventional, espionage or non-state attack, and (b) conventions or agreements.

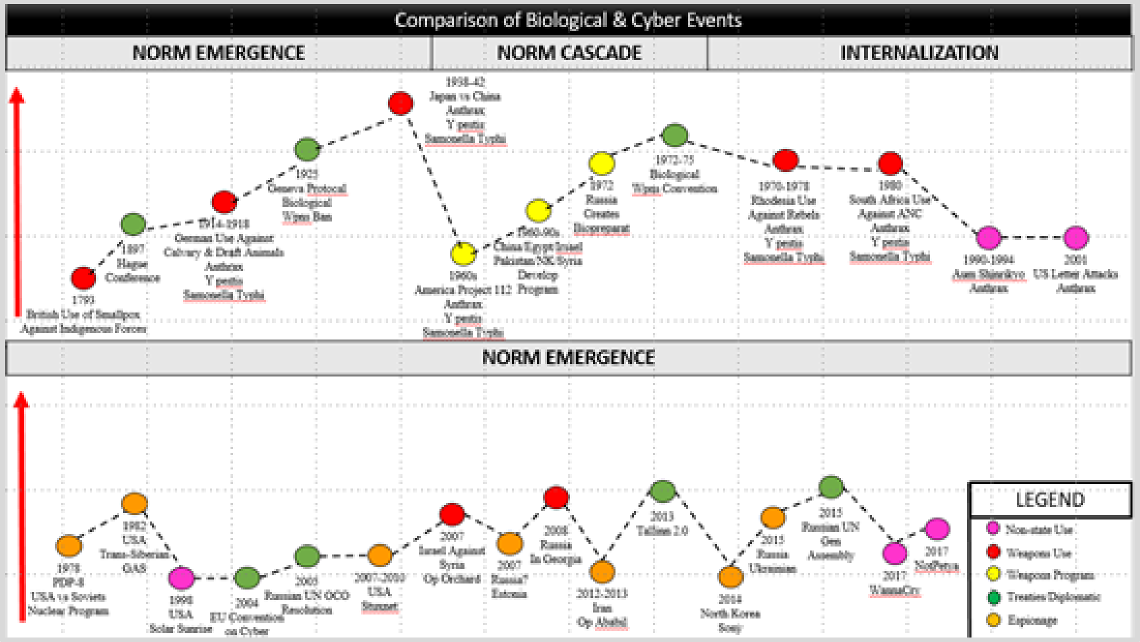

Fig 2. Comparison of Biological and Cyber events

Though the timelines are not the same duration, they demonstrate an oscillation of peaks and troughs, revolving around conflict. The higher frequency of cyber events collaborates much of the incorrectly termed 'Gerasimov doctrine'[34] or escalate to deescalate. What one is able to

[33] Gregory Koblentz & Brin Mazanec. "Viral Warfare: The Security Implications of Cyber and Biological Weapons." *Comparative Strategy. Vol 32:5, 2013. 418*

[34] Mark Galeotti. "I am Sorry for 'Creating the Gerasimov Doctrine." *Foreign Policy*. (05 Mar 18) https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

observe is that they share similar evolutionary non-linear paths. Keeping in mind, both are emerging technologies that are fundamentally reorganizing society: from gene editing to meme editing and the convergence of the two.[35] As alluded to above, both have most recently been employed in non-state use, though this is somewhat misleading considering the classification of non-state use and espionage is dependant very much on intent, which is difficult to determine in the cyber domain. This places peacekeepers in a particularly difficult position of being digitally vulnerable to state and non-state entities. It is the equivalent of not inoculating soldiers for tropical diseases or malaria. One need only recall the debate around mefloquine, the risks to physical and mental health in its use, and the decision to move forward with its use during operations in Somalia and Afghanistan, to see how politically charged this space is.[36]

GRAFTING THE BIOLOGICAL TO THE CYBER

To begin, it will be helpful to acknowledge the paper's reliance on Norm Evolution Theory, and the concept of grafting norms from different disciplines. This is a similar concept to how virus' transition through species.[37] This paper makes the assumption in line with this theory that norms, genes and memes are all codes that guide behaviour,[38] and that successful replication of adaptations are grafted and evolve from previous ones.[39] Grafting will be more successful the more shared are the attributes between them. Multi-use technologies share this feature, and

[35] Ep. 232. *COVID-19 and the Future of Bio-Security with Dr. Giordano*. The Mad Scientist Iniative: The Convergence Podcast. https://madsciblog.tradoc.army.mil/232-the-convergence-covid-19-and-the-future-of-bio-security-with-dr-giordano/

[36] Avery Haines. *Canadian Veterans Suing Government Over Anti-Malarial Drug's Adverse Effects.* Global News(*30 Apr 19)* https://www.ctvnews.ca/w5/canadian-veterans-suing-government-over-anti-malarial-drug-s-adverse-effects-1.4402691

[37] Graham ReadFearn"*How did Coronavirus Start and Where Did It Come From? Was it Really Wuhan's Animal Market?* The Guardian. (27 Apr 20) https://www.theguardian.com/world/2020/apr/28/how-did-the-coronavirus-start-where-did-it-come-from-how-did-it-spread-humans-was-it-really-bats-pangolins-wuhan-animal-market?CMP=Share_iOSApp_Other

[38] Brian M. Mazanec. *The Evolution of Cyber War*. (Nebraska: Potomac Press, 2015). 21

[39] Ibid. 40

ability to flip over to either civilian or military applications. The commonality is what allows for crossover. In the case of cyber, Peter Singer & Emerson Brooking in their book LikeWar look at four qualities that make this possible: Attribution, Low-Cost Entry, Technological Overmatch, and Virality vs Veracity. In the case of biological warfare, Gregory Koblentz, in Living Weapons, uses a strategic lens, categorizing biological weapons qualities by their strategic characteristics: Biological Warfare Favours the Attacker (the problem of defence for both the attacker & defender); Use as a Force Multiplier; Ill-suited for Strategic Deterrence; and Potential Normative Constraint Erosion. Both cyber and BW share many cross-cutting themes that are graftable. What this paper will suggest, to avoid being decisively engaged by this debate, is to submit a repackaging of characterization, one based on paradoxes shared between the two, emphasizing grafting qualities, and pulled from both works. The following 5 paradoxes are essential concepts in order to graft biological warfare constraining norms to cyber warfare, as a necessary step in justifying precedence and applying it to digital blue helmets.

1. *The Multi-Use Paradox.* In biological and cyber applications are both a military weapon and underlying structural code that makes the internet function, or in the case of biological, gene replication possible. Both share the common practice of creating virus' in order test their vaccines, which then in turn is a potential weapon.[40] Both have the potential of high infectivity rates. Paradoxically you need to create a very dangerous meme or gene to develop an anti-viral or anti-meme. Since both are multi-use technologies many of the virus live on, ready to be reengineered. This is not a

[40] Peter Singer, Max Brooking. *LikeWar*. (New York: HMHCO Publishing Company, 2018) 129; Gregory Koblentz. *Living Weapons: Biological Warfare and International Security*. (Ithaca: Cornel University Press, 2009). 23-40

superfluous fear: one needs to only look at issues surrounding the use of smallpox and recent creation if it in a lab to see the dangers associated with this technology.[41] One through the creation of Generative Adversarial Networks (GAN) for iterative testing, which allows for algorithm (memes) to evolve. The other through a sophisticated network of pharmaceutical companies, research universities, and military research organizations like DARPA. It is not coincidental that DARPA recently partnered with the U.S Food and Drug Administration, repurposing a military application to a COVID-19 blood test that can identify the virus days before patients become infectious.[42] The risks this paradox presents peacekeepers is mitigated through the issuing of anti-virals, inoculations, hygiene, and preventive and crisis responsive medicine. A recent example is the deployment of Canadian Armed Forces field hospital to stop the Ebola epidemic in Sierra Leone.[43] These protections currently do not exist within the cyber domain - though confidence building measures and capacity building programs are identified by both the IGF and ITU.[44]

2. *The Openness Paradox.* Both are openly traded technology reliant on an interconnected network of researchers and publicly traded companies where adversaries can hide anywhere, but also a place of governmental secrecy and covert operations. Big Pharma is

[41] The Spectre of Smallpox. Nature. (13 Aug 18) https://www.nature.com/articles/d41586-018-05936-x

[42] Natalie Rahhal. *US Military scientists working on germ warfare develop new test that can detect COVID-19 within 24 hours - before carriers display symptoms or are infectious* The Daily Mail (01 May20). https://www.dailymail.co.uk/health/article-8279461/US-Military-scientists-working-germ-warfare-make-COVID-19-test.html

[43] The Canadian Press. *Canadian military medical staff end six-month Ebola mission in Sierra Leone*. Macleans (20 Jun 15) https://www.macleans.ca/news/canada/canadian-military-medical-staff-end-six-month-ebola-mission-in-sierra-leone/

[44] Internet Governance Forum. “Towards an Inclusive Cyber Security Capacity Building Approach.” Organization of American States Working Group. (21 Dec 2017) https://www.intgovforum.org/multilingual/content/igf-2017-day-4-room-xi-ws118-towards-an-inclusive-cybersecurity-capacity-building-approach

constantly fighting generic drug manufacturers as a form of intellectual property. Universities produce variants of very lethal bacteria that can be used for attacks, as seen post 9/11 with the anthrax letters attacks. These two trends together allowed Iraq in the 1990s to build their biological weapons program – all from open source and university information exchanges.[45] The same relationship exists with cyber code that is carried within everyday software and mimics the fomites that have spread virus' like colds to bubonic plague. The threat to peacekeepers in the cyber domain is the ability to reframe the informational narrative using disinformation, deep fakes and/or fake news. This is what happened to Israeli in 2014. Hamas created fake attacks with casualties to undermine IDF operations.[46] The ability to use open-source imagery and embedded it with a counter message is a particularly pernicious threat to UN stability operations. It is critical to the protection of individual peacekeepers, and mission success that UN equities such are credibility and legitimacy are maintained.

3. *The Deterrence/Decisive Point Strategy Paradox.* In a journal article for Comparative Strategy, Brian Koblentz and Brian Mazenac identify how neither biological nor cyber weapons are suited for deterrence by either control or denial. The attractiveness of non attribution is paradoxically why it is an ineffective strategy for deterrence; it lacks many of the intention signalling required to deter an adversary. Embedded as well, is the hype that characterizes SCADA attacks as a decisive form of warfare. However, it is no more decisive as pearl harbour. Consequentially, it is a tactic of below threshold armed conflict

[45] Gregory d. Koblentz. *Living Weapons: Biological Warfare and International Security*. (Ithaca: Cornel University Press, 2009), 12.

[46] Peter Singer, Max Brooking. *LikeWar*. (New York: HMHCO Publishing Company, 2018). 430

fighting, a space in which peacekeepers by definition conduct operations. Peacekeeping or enforcing is the future of phase zero operations.

4. *High Cost/Low Entry Paradox*. It is very expensive to generate and maintain technological overmatch in either the biological or cyber domain. The maintenance and manufacturing of vaccination and ability to identify new biological threats and develop counter measures is expense, as witnessed during the Covid-19 crisis. So, to is cyber security and the development of anti-viral software and monitoring. Both have high start up costs, but in combination with the other paradox's has low entry costs once used and released within cyberspace to be picked up by PMCs in collaboration with with cyber criminals.

Ultimately, these paradoxes are why grafting of norms is possible: on the one hand, protection measures are normative behaviours that are universally agreed upon and designed to be employed at the forward edge of the battle area; on the other, they are limited in their military application, bounded by the scope of their application. By changing the discourse away from either a politico/military or cybercrime paradigm to one akin to that language of public health and force protection is a means of getting past the inertia of committee debates - digitally 'arming' UN peacekeepers to win their fights against a growing threat. It is to both inoculate the peacekeepers for there own personal safety, and the means to build herd immunization, contesting belligerent's freedom of movement within the cyber domain.

MOVING FORWARD WITHOUT A CONVENTION?

There has been much publicity and grassroots action calling for a Cyber Weapons Convention. As recent as 2018, a consortium of over 30 global technology companies signed a non-binding Geneva-type accord.[47] Though in one sense tangential to the real debates happening in Geneva (the signatories are all western companies), these specific companies are inseparable and irreplaceable from the open standards organizations that govern the internet. They are major contributors in both developing software, and developing the standards that make the software interoperable with everything.[48] However, if the evolution of BW is any indication, the formal will lag behind the informal structuring norms, and most recently acknowledged in a speech by UN Secretary General Antonio Gutteres in 2018.[49] The Biological Warfare Convention (BWC) is unique. Any cyber convention will share many of the same limitations the BWC had to have in order for it to be signed and ratified: (1) the absence of a UN body monitoring signatory nations; and (2) no verification process like all the other weapons bans.[50] This is a result of the paradoxical nature inherent to both biological and cyber weapons; they are deeply intertwined with health issues/business. There has even been attempts have by NGOs to start an Internet Health Organization, mirroring the World Health Organization.[51] This requirement to modernize force protection can be seen in The Department of Peacekeeping Operations/Department of Operational Support (DPO-DOS) Action Plan to Improve the Security of United Nations Peacekeepers.[52] The plan focuses on the need for enhanced performance across the board to improve the safety and security of peacekeepers. The IGF has also identified that agreements can

[47] Alex Hearn. “Facebook among tech firms to sign 'digital Geneva convention” *The Guardian*. (18 May 2018) https://www.theguardian.com/technology/2018/apr/18/tech-firms-including-facebook-sign-up-to-digital-geneva-convention?CMP=Share_iOSApp_Other

[48] From Open Standards

[49] Andrei Khalip. U.N. Chief Urges Global Rules for Cyber Warfare. (Reuter: Technology Review, 19 Feb 2018). https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4

[50] Gregory d. Koblentz. *Living Weapons: Biological Warfare and International Security*. (Ithaca: Cornel University Press, 2009). 20

[51] Robert. J. Deibert. *Black Code*. (Toronto: Signal, 2013). 523

[52] United Nations Department of Peacekeeping/ The Department of Peacekeeping Operations. *Improving Security of United Nations Peacekeepers Action Plan for Implementation of Fatalities Report Part 1: Actions Taken at The Field Level. (07 Apr 1)* https://peacekeeping.un.org/sites/default/files/180406_action_plan_revised.pdf

have the adverse effect of being counterproductive, and placing personal and private information of peacekeepers at risk.[53]

WHAT DIGITAL BLUE HELMETS COULD LOOK LIKE

While norms continue to develop at the strategic and technical level of the UN, operational and tactical force protection measures implementation can happen now. What this will look like will depend on the theatre of operations, mission profile, and composition of Troop Contributing Nations (TCNs). The precedence set by biological force protection capabilities grafted to cyber will be acceptable to TCNs concerned about an absence of overarching politico/military policy. It also has the consequence of being scalable and address the risks associated with the paradoxes listed above. Finally, it will (a) address current cyber gaps in UN missions with respect to force protection; and (b) enable mission success by providing umbrella operational enablers to fielded peacekeepers. The following cyber capabilities, grafting on biological warfare force protections are fieldable now, and should be included in future uniformed capability requirements for UN peacekeeping as follows:

1. *Operational Cyber Task Force (TF)*: Bespoke cyber TFs either in the form of a coalition TF ARES like organization[54], or unilateral TCN but framed as a task to establish cyber 'quarantines'[55] to (a) separate belligerents and their social engineering narratives (b) protect peacekeepers going into an infected space. By definition this would differentiate itself from offensive cyber operations (OCO) conducted by TF

[53] Internet Governance Forum https://www.intgovforum.org/multilingual/filedepot_download/8395/1896#page24

[54] Dina Temple-Raston. "How the US Hacked ISIS.*" How I See things. NPR. (26 Sept 19)* https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis

[55] Put in here the military DefenseOne definitionof quarantine

ARES by drawing a clear line between an essentially passive defensive cyber operation (DCO) and offensive cyber operations (OCO). The potential counter-narrative that a digital quarantine is a euphemism for a digital concentration camp must be considered and that is essentially dependent on maintaining an information assurance and defensive posture versus offensive measures division. The benefit of operational enabler support is that the capability does not need to be housed in theatre but can be remote from TCN home country. This approach has the advantage of establishing a cordon with minimum information exchange, mitigating security classification concerns inherent to a coalition.

2. *Awareness.* Digital awareness is a prerequisite to immediacy of crisis response - before contagions achieve critical mass, and in order to flatten the curve/deescalate conflicts. Identifying subversive disinformation or adversary attack vectors through cyber data mining, has its corollary in pandemic horizon scanning in preventive medicine and a key tenet of bio-security.[56] This would include sousveillance and surveillance of active social media fields.[57] Like a cyber TF, this capability can exist in home country.

3. *Preparation.* Already identified by the IGF and ITU with nascent program development earmarked for countries most requiring it, the UN has mostly focused on information assurance. Again, due to the paradoxical attributes of cyber technology effort at developing DCO and OCO capabilities is highly unlikely. However, if viewed as a form of inoculation and preemptive medicine, there is much that can be

[56] 232. “The Convergence” – COVID-19 and the Future of Bio-Security with Dr. Giordano https://madsciblog.tradoc.army.mil/232-the-convergence-covid-19-and-the-future-of-bio-security-with-dr-giordano/

[57] Jennifer Kavanagh, Samantha Cheney, Hilary Reininger, Norah Griffin. “Fighting Disinformation Online: Building the Database of Online Tools.” *RAND Report*, 2020

done with relatively little investment by TCNs. As the UN expert Dr. Dorn has written, the establishment of peace support training centres are required to build capacity building in peacekeepers.[58] An institution like this could also provide cyber security force capacity building (SFCB), instructing on higher end tactics, techniques, procedures (TTPs) in open source investigatory techniques and intelligence gathering; the conduct of digital hygiene; and overall increasing of digital literacy. This is the functional equivalent of chemical, biological, radiological, and nuclear (CBRN) investigators, and CBRN reconnaissance conducted by specialized army soldiers within the armoured & infantry corps, or to higher level in Special Operations Forces. Capacity building could include incorporation Cubic simulators and WarGaming, replicating almost real time peacekeeping areas of operations. Inexpensive options such as the UN publishing its equivalent of the U.S. Army Social Media Handbook tailored to regions is also a necessary first step.

4. *Response*. This is the most important capability that needs to be fielded at the tactical level. There has to be immediate action drills to triage disinformation casualties after an attack. The information battle happens in the cyber domain. This would protect the force from catfishing and other social engineering attack. North Atlantic Treaty Organization has gone as far as conducting catfishing on their own soldiers during exercises as a form of inoculation.[59] The purpose to highlight the need to protect personal information in today's conflicts.

[58] Walter Dorn. "Back in the Game: Recommended Canadian Contributions to UN Peace Operations." *World Federalists Movement Canada. (*24 April 2018). 2

[59] Issie Lapowsky. "NATO Group Catfished Soldiers to Prove a Point About Privacy." *Wired*. (18 Feb 2019). https://www.wired.com/story/nato-stratcom-catfished-soldiers-social-media/

CONCLUSION

In his recent book, Only the Dead, Bear Braumoeller, argues that international orders and the cooperative systems they create, reduce certain violence, but at the expense of others, because all international orders "values something more than it values peace."[60] One of the ways of mitigating these behaviours has been peacekeeping as a mechanism to (a) deescalate conflicts in process or (b) as a form of quarantining violence from spreading during intractable

conflicts .[61] This paper has worked under the assumption that peacekeeping, while strategic level constraining norms evolve, will need to continue in cyberspace, and that the best way to do this is to graft norms from the biological space onto cyberspace operations. This reframing recognizes the requirement for digital first aid on peacekeeping or making operations. It treats disinformation for what it is: a meme that requires inoculation in order to build immunity in our peacekeeping, acknowledging that historically disease transmission coming out of conflict zones are high, regardless if it is in an analogy or digital form. What no one wants is a digital version of the Spanish Flu to infect civilians post conflict.[62] Not all aspects of cyber and biological environments map over. This paper makes no claim to resolving the very real world frictions behind offensive cyber operations and the authorities required to approve attacks or share tightly held technological capabilities. To finish with a final thought: no two technologies have

[60] Bear Broemoeller. Only the Dead. (New York: Oxford University Press: 2019). 474

[61] Page Fortna. "Has Violence Declined in World Politics? A Discussion of Joshua S. Goldstein's Winning the War on War: The Decline of Armed Conflict Worldwide." *Perspectives on Politics* Vol. 11/No. 2. (Jun 2013). 568 https://polisci.columbia.edu/sites/default/files/content/pdfs/Publications/Fortna/Journal%20Articles/Goldstein%20symposium%20PoP%202013.pdf

[62] Ep. 66: The 1918 flu and the U.S. military. Defence One Radio. https://www.defenseone.com/ideas/2020/04/ep-66-1918-flu-and-us-military/164559/

undergone such disruption transformation in the last 30 years.[63] Unfortunately, it is a truism that the pace of change is not the same as the tempo of consensus. Grafting the biologically grounded norms unto cyber is an interim solution - an instrumental way of looking at peacekeeping that begins the conservation. If this does not happen, the edge will develop ad hoc solutions that will have iatrogenic impacts, where the curative will be worse than the memes.

[63] Ep. 232. *COVID-19 and the Future of Bio-Security with Dr. Giordano*. The Mad Scientist Iniative: The Convergence Podcast. https://madsciblog.tradoc.army.mil/232-the-convergence-covid-19-and-the-future-of-bio-security-with-dr-giordano/

BIBLIOGRAPHY

Books

Richard Dawkins. *The Selfish Gene.' 40th Anniversary Edition*. (Oxford: Oxford University Press, 2016)

Koblentz, Gregory. *Living Weapons: Biological Warfare and International Security*. Ithaca: Cornel University Press, 2009.

Broemoeller, Bear Only the Dead. New York: Oxford University Press: 2019.

Deibert. Robert *Black Code*. Toronto: Signal Publishing, 2013.

DeNardis, Laura. Ed. *Opening Standards: The Global Politics of Interoperability.* Editor Laura DeNardis. (Cambridge: Massachusetts Institute of Technology, 2011)

McKeown, Ryder and Wilner, Alex. "Deterrence in Space and Cyberspace." *Canadian Defence Policy in Theory and Practice*. Ed by Thomas Juneau, Phillipe Lagasse, Srdjan Vucetic. Ottawa: Palgrave MacMillan:2019.

Sanger, David. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York: Broadway Books, 2018.

Singer, Peter and Friedman Allan. *What You Need to Know: Cybersecurity and Cyberwar.* Oxford: Oxford University Press, 2014.

Singer, Peter, and Max Brookings. *LikeWar: The Weaponization of Social Media*. New York: HMH Publishing Co, 2018.

Mazanec, Brian. *The Evolution of Cyber War*. Nebraska: Potomac Press, 2015.

McLuhan, Marshall. *The Gutenberg Galaxy*. University of Toronto Press, 2011.

Whyte, Christopher, and Mazanec, Brian. *Understanding Cyber Warfare: Politics, Policy and Strategy*. New York: Routledge, 2019.

Winterfred, Steve and Jason Andreas. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice.* Waltham: Elsevier Publishing, 2013.

Journals & Media

Biller, Jeffrey, and Schmitt, Michael. "Classification of Cyber Capabilities and Operations as weapons, Means, or Methods of Warfare." *International Law Studies.* Vol 95, 2019.

Walter Dorn. "Back in the Game: Recommended Canadian Contributions to UN Peace Operations." World Federalists Movement Canada. (24 April 2018). 2

Fortna, Page. "Has Violence Declined in World Politics? A Discussion of Joshua S. Goldstein's Winning the War on War: The Decline of Armed Conflict Worldwide." Perspectives on Politics Vol. 11/No. 2. (Jun 2013)

Hear, Alex. "Facebook among tech firms to sign 'digital Geneva convention" *The Guardian*. (18 May 2018) https://www.theguardian.com/technology/2018/apr/18/tech-firms-including-facebook-sign-up-to-digital-geneva-convention?CMP=Share_iOSApp_Other

Galeotti. "I am Sorry for 'Creating the Gerasimov Doctrine." *Foreign Policy*. (05 Mar 18) https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

Grigsby, Alex. "Unpacking The Competing Russian and U.S. Cyberspace Resolutions at the United Nations." The Council For Foreign Relations Blog. (29 Oct 2018

Khalip. Andrei "U.N. Chief Urges Global Rules for Cyber Warfare." *Reuter: Technology Review*, 19 Feb 2018). https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4

Koblentz, Gregory and Mazanec, Brian. "Viral Warfare: The Security Implications of cyber and Biological Weapons. *Comparative Strategy*. Nov 2013.

KilCullen, David. *Dragons and Snakes: How the Rest Learned to Defeat the West.* New York: Oxford University Press, 2020.

Lee, Kristine and Sullivan, Alexander. "People's Republic of the United Nations." *Center for New American Security*. (May 2019). 4. https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-China-IO-final-web-b.pdf?mtime=20190513092354

Mazarr, Michael, Ryan Michael Bauer, Abigail Casey, Sarah Anita Heintz, Luke .J. Matthews. "The Emerging Risk of Virtual Societal Warfare: Social Manipulation In a Changing Information Environment." RAND:2019)

Rahhal, Natalie. *US Military scientists working on germ warfare develop new test that can detect COVID-19 within 24 hours - before carriers display symptoms or are infectious* The Daily Mail (01 May20). https://www.dailymail.co.uk/health/article-8279461/US-Military-scientists-working-germ-warfare-make-COVID-19-test.html

ReadFearn, Graham. "*How did Coronavirus Start and Where Did It Come From? Was it Really Wuhan's Animal Market?* The Guardian. (27 Apr 20) https://www.theguardian.com/world/2020/apr/28/how-did-the-coronavirus-start-where-did-it-come-from-how-did-it-spread-humans-was-it-really-bats-pangolins-wuhan-animal-market?CMP=Share_iOSApp_Other

Rid Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies*. 2012, 35:1, 5-32

.

Shuya, Mason. "Russian Cyber Aggression and the New Cold War." *Journal of Strategic Security* 11, no. 1 (2018)

Temple-Raston, Tina. "How the US Hacked ISIS*." How I See things. NPR. (26 Sept 19)* https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis

The Canadian Press. *Canadian military medical staff end six-month Ebola mission in Sierra Leone.* Macleans (20 Jun 15) https://www.macleans.ca/news/canada/canadian-military-medical-staff-end-six-month-ebola-mission-in-sierra-leone/

Electronic Sources

Banach, Steve. "Virtual War – A Revolution in Human Affairs." Small Wars Journal 5. https://smallwarsjournal.com/index.php/jrnl/art/virtual-war-revolution-human-affairs

Cascais, Antonio. "How China Benefits from Africa's Smartphone Boom." *Deutche Welle* (28 Oct 2019) https://www.dw.com/en/how-china-benefits-from-africas-smartphone-boom/a-51016346

Donavan, Joan. "How Memes got Weaponized: A short History." (MIT Technology Review: 24 Oct 2019) https://www.technologyreview.com/s/614572/political-war-memes-disinformation/

Fellows, James "Cyber Warriors." *The Atlantic* 2010 https://www.theatlantic.com/magazine/archive/2010/03/cyber-warriors/307917/

Murgia, Madhumita Anne Gross. Inside China's Controversial Mission to Reinvent the Internet. *Financial Times. (27 May 2020) https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f*

Ep. 66: The 1918 flu and the U.S. military. Defence One Radio. https://www.defenseone.com/ideas/2020/04/ep-66-1918-flu-and-us-military/164559/

Ep. 84 – The future of Cyber Conflict, with Lt.Gen. Stephen Fogarty, Commander of U.S. Army Cyber Command," *The Modern War Institute,* Sep. 6, 2019. https://mwi.usma.edu/mwi-podcast-future-cyber-conflict-lt-gen-stephen-fogarty-commander-us-army-cyber-command/

Ep. 48 - Cyberwarfare Today." *Defence One Radio*. 12 Jul 19. https://www.defenseone.com/ideas/2019/07/ep-48-cyberwarfare-today/158387/?oref=d-channelriver

Ep.50 - Cyber Yesterday. *Defence One Radio. 29 Jul 19* https://www.defenseone.com/ideas/2019/07/ep-50-cyberwarfare-yesterday/158750/?oref=d-channelriver

Ep 232. "The Convergence" – COVID-19 and the Future of Bio-Security with Dr. Giordano https://madsciblog.tradoc.army.mil/232-the-convergence-covid-19-and-the-future-of-bio-security-with-dr-giordano/

Doctrine

Canada, Public Safety Canada. *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*. Ottawa: Canada Communications Group, 2018.

Canada, Department of National Defence. JDN 2017-02. *Joint Doctrine Note: Cyber Operations Joint*. Ottawa: 2017.

UN Resources

Internet Governance Forum Website https://www.intgovforum.org/multilingual/filedepot_download/8395/1896#page24

Internet Governance Forum. "CyberSecurity Agreements: Final BPF Output Report." *Best Practice Forum on Cybersecurity*. (20 Jan 2020)

Internet Governance Forum. "Towards an Inclusive Cyber Security Capacity Building Approach." Organization of American States Working Group. (21 Dec 2017) https://www.intgovforum.org/multilingual/content/igf-2017-day-4-room-xi-ws118-towards-an-inclusive-cybersecurity-capacity-building-approach

Maurer, Tim. "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber Security." *Balfour School for Science and International Studies Discussion Paper*. (Harvard: 2011). 15 https://www.belfercenter.org/sites/default/files/legacy/files/maurer-cyber-norm-dp-2011-11-final.pdf

United Nations Department of Peacekeeping/ The Department of Peacekeeping Operations. *Improving Security of United Nations Peacekeepers Action Plan for Implementation of Fatalities Report Part 1: Actions Taken at The Field Level. (07 Apr 18)* https://peacekeeping.un.org/sites/default/files/180406_action_plan_revised.pdf