12

Bits and "Peaces"

Solving the Jigsaw to Secure Cyberspace

Stéphane Duguin, Rebekah Lewis, Francesca Bosco, and Juliana Crema[*]

1 INTRODUCTION

Efforts to create peace in cyberspace can, at times, be much like trying to assemble a 1,000 piece jigsaw puzzle without a picture of the finished product, full of important, related elements, but lacking an overall strategy. Much like the missing picture on the puzzle box, the absence of a mutually agreed-upon definition of "cyber peace" is itself one of the fundamental challenges to achieving it. Without a common understanding – a common vision – it is difficult to come together and work collectively toward a common goal. While agreeing on a universal definition of any truly global concept is inherently challenging (witness the ongoing debates surrounding "sustainability"), due to the sheer number and diversity of perspectives involved establishing a shared understanding of cyber peace is particularly difficult due to the complex and evolving nature of cyberspace, and the nature and meaning of peace itself. By taking a more operational perspective in this chapter and building from the work of others throughout this edited volume, our hope is to advance the discussion on cyber peace beyond this uncertainty – in essence, to transcend it.

First, we will set forth a "light-weight" operational definition of cyber peace that we believe is compatible with more theoretical formulations of the concept, while providing a guiding compass point for both strategic and tactical activities. To be impactful, we argue that any approach to cyber peace must, above all, be concerned with human well-being and, therefore, contemplate the integrated, multidimensional components of the human experience. As outlined in the first chapter of this volume, there are various interpretations of cyber peace. Some understand it solely as a concept to be theorised, whereas others consider it to be a set of practices

[*] The CyberPeace Institute is an independent, nonprofit organization headquartered in Geneva that works to enhance the stability of cyberspace by decreasing the frequency, impact, and scale of destructive cyberattacks against civilians. The Institute promotes transparency about such attacks and holds malicious actors to account for the harm they cause on vulnerable communities and populations. To this end, the Institute's mission is to ensure a human-centric and evidence-led response to cyber operations.

https://doi.org/10.1017/9781108954341.012 Published online by Cambridge University Press

that can be employed (Marlin-Bennett, 2022, pp. 4–6). With this work in mind, we will build upon Marlin-Bennett's conception of cyber peace as a practice in order to better understand the human role and the related impact we can have to promote cyber peace and accountability in cyberspace. Second, we will highlight two key challenges that we believe must be overcome on the road to cyber peace. In assessing these challenges, we also seek to bring to the fore a broader geopolitical issue, the growing and fundamental redistribution of power that is not supported by a complementary redistribution of oversight and accountability. Lastly, we will argue that the principle of accountability – as a generally applicable concept and a key component of literature on institutional analysis such as the Ostrom Design Principles – provides a flexible and durable means to pursue cyber peace. By taking into account this operational understanding of cyber peace and by using current examples to illustrate how they apply can help to further guide the path toward a sustainable cyber peace framework.

2 DEFINING CYBER PEACE

In an effort to highlight the necessary collective approach to achieve cyber peace, we have built our operational understanding of cyber peace around previous work, but have adjusted the focus to ensure that it is human-centric. As discussed in the Preface and first chapter of this edited volume, discussions of cyberspace, operations, security, and peace have come from a variety of actors in a move toward a multistakeholder approach to cyberspace and away from the previous focus upon state-centered security models (Shackelford, 2022, p. xxv). The state as a focal point makes sense in a Westphalian world order in which national territory and governments serve as the primary mechanisms for protection of rights and preservation of stability and order. But the scope of cyberspace – as a "notional environment" defined by connected networks and devices – is rapidly expanding (Delerue, 2020, p. 29). Today, from a micro-level perspective, computers, networks, and, information and communication technologies – "cyber" – is woven into almost every aspect of human life. Equally important to recognize is the macro-level perspective in order to understand how the complexities of our digital life are nestled into broader societal and geopolitical contexts. Accordingly, we assert that any efforts to achieve cyber peace should and must, as a moral imperative, be centered around and motivated by a concern for the well-being of *individual human beings* in order to achieve a peace beyond the mere absence of war (Diehl, 2019, pp. 2–3). Echoing Heather Roff (2016, p. 8), we believe that the individual human should be the main referent for a guiding conception of cyber peace. In keeping with this singular focus on the human being as the center point of a peaceful cyberspace, we propose that *cyber peace exists when human security, dignity, and equity are ensured in digital ecosystems.*

This formulation of cyber peace is intended to be highly actionable at an operational level and, we believe, is complementary to and compatible with existing

https://doi.org/10.1017/9781108954341.012 Published online by Cambridge University Press

related scholarship which has been previously discussed in this volume.[1] For those seeking to actively pursue cyber peace, the definition is intended to be instructive on a number of practical levels and works to approach these issues from a human perspective from the start. In this way, we can begin to address the challenges and obstacles in achieving accountability in cyberspace. In an effort to clarify each element of cyber peace listed above, there are specific criteria and questions to consider. For example, we believe that human security exists in cyberspace when services essential to human life and related critical infrastructure are protected. Based on this definition, we can begin to think through cyber-related topics by using a human-centric lens, and by questioning which rights and freedoms have been violated such as, "… the right to life, liberty and security of person" (United Nations, 2015, p. 8). Some questions to think about include whether there has been an obstruction to essential resources and services; this line of critical thinking will also begin to highlight the question of accountability, and in cases of attacks against healthcare facilities; for example, who holds responsibility for the failure to protect the element of human security.

Moreover, following the foundation laid out by human security, in the cyberspace context human dignity presents a mutually reinforcing concept as these associated rights rest upon the fulfillment of security in cyberspace. With this in mind, human dignity exists in cyberspace when individual's beliefs, cultural rights, and ability to participate in society are protected. Human dignity is unique to the individual's experience and context-specific to their everyday realities. Rights relating to this definition include, but are not limited to, civil and political rights, along with freedom of expression and assembly, as well as cultural and indigenous rights. Furthermore, human equity exists in cyberspace when individuals are protected against discrimination, bias, prejudice, and inequality. The importance of human equity in cyberspace stems from the reality that not everyone is starting at the same position in life and that these discrepancies need to be rectified in order for cyber peace to exist. This understanding follows the first and key tenant from the Universal Declaration of Human Rights, which emphasizes that "all human beings are born free and equal in dignity and rights" (United Nations, 2015, p. 4). This definition helps to get to the root problems that need to be addressed in order to resolve inequalities and can include issues such as political or developmental barriers to equity, or social constructions which inhibit upon one's rights. This holistic and proactive approach is needed to ensure that these barriers are eliminated for people and communities everywhere. We view cyberpeace as encompassing three distinct elements: human security, dignity, and equity. These key elements relate to various dimensions of the human experience, including political, economic, and social considerations,

[1] For example, this definition comports with the four pillars of a positive cyber peace "…as a system that: (1) respects human rights and freedoms; (2) spreads Internet access along with cybersecurity best practices, (3) strengthens governance mechanisms by fostering multi-stakeholder collaboration, and (4) promotes stability and relatedly sustainable development" (Shackelford, 2020, pp. 15–16).

and in this way are closely linked with human rights. To be clear, these three key elements are intertwined, interdependent, and intersectional as a necessary effort to achieve cyber peace. The human rights specifically encompassed by human security, dignity, and equity build upon and reinforce each other, as is relevant for each individual's experience.

Keeping these concepts in mind, but further building upon our understanding of cyber peace, the role of accountability becomes much more apparent. By grounding these definitions in rights and freedoms, and while maintaining a human-centric perspective, we can further question the intersection of the virtual and physical worlds, and the role that each actor plays in these ecosystems. Having a clearer understanding of the roles and responsibilities, both on and offline, will help to rectify the accountability deficit we currently face due to the rapid evolution and convergence of disruptions in technology, geopolitics, and human behavior.

One example of the operationalization of our approach toward cyber peace is the focus we have been devoting to the healthcare sector. As the extent of people relying on health services for necessary human needs increases, the potential harm to human security and dignity are immense. Malicious cyber operations against healthcare facilities put human lives in jeopardy and require immediate action. To this end, we supported a call on the world's governments to collaboratively work to stop cyberattacks against healthcare facilities and related critical infrastructure entities. Then, considering the increasing gap reported between the variation and sophistication of cyberattacks and the ability for healthcare sector entities to protect themselves from such attacks, we set up Cyber 4 Healthcare. This initiative is a global matchmaking service to partner civil society organizations and healthcare providers with private sector actors to individually assist them in protecting their services in order to decrease their vulnerability to cyberattacks, while considering their local context. The personalized advice and discussions through Cyber 4 Healthcare is just one example of how cyber peace, as it encompasses human security, dignity, and equity, must truly span the globe, inside and out, while maintaining contextual relevance.

3 KEY CHALLENGES ON THE ROAD TO CYBER PEACE

In order to further unpack the goal of cyber peace through accountability, we must be cognizant of the challenges and obstacles in this realm. In order to illustrate this, we have identified two deeply rooted and largely false assumptions about the nature of cyberspace itself that must be debunked and counteracted in order to make meaningful progress toward cyber peace. First, we must recognize the unequal and disproportionate access and engagement with cyberspace around the world, and address this issue in the discourse around responsibilities and responsible behavior in cyberspace. Second, we must acknowledge and tackle head-on, through creative, out-of-the-box thinking, the persistent tensions and gaps in the existing ecosystem of laws, norms, and principles governing cyberspace, and the use of information and

communications technologies (ICTs). By analyzing these issues through a cyber peace lens, we can begin to address them on the basis of rights and freedoms afforded to all in international treaties and declarations.

3.1 *Access and Security in Cyberspace*

Keeping in mind the definition of cyber peace and its corresponding elements, access and security in cyberspace remains a prominent challenge. Communities around the world are in vastly different stages of development and implementation when it comes to cyberspace infrastructure and technology, which thus leads to questions of human equity and the impact that this discrepancy in development has upon end-users and citizens of the world more generally. Bias and subjectivity are hard-wired problems in technology, though access to this technology is in itself unevenly distributed, which deepens existing inequalities. In order to keep this issue in a global context, it is also highlighted by the UN's Sustainable Development Goals, particularly goal number 9, which is to "build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation" (United Nations Department of Economic and Social Affairs, 2020, p. 42). Specifically in relation to access to the Internet, the UN cites that, "in 2019, almost the entire world population (97%) lived within reach of a mobile cellular signal, and 93% lived within reach of a mobile-broadband signal" (United Nations Department of Economic and Social Affairs, 2020, p. 43). However, despite this high percentage of coverage the UN found that, "most of the offline population live in LDCs, where only 19% use the Internet …" (United Nations Department of Economic and Social Affairs, 2020, p. 43). Moreover, the 2019 Human Development Report emphasizes this point and warns that, "… while access to basic technologies is converging, there is a growing divergence in the use of advanced ones …" leading to a growing concern about a so-called New Great Divergence, following the first divergence created by the Industrial Revolution (United Nations Development Programme, 2019, pp. 200–203). With a greater emphasis placed upon the question of human equity and an active approach to facilitate the participation of all in cyberspace, concerns about the digital divide can begin to be addressed. As stated in the Sustainable Development Goals, bridging the digital divide by providing Internet access to the 3.6 billion people – nearly half of the world's population – in the developing world who are not online "is crucial to ensure equal access to information and knowledge, as well as foster innovation and entrepreneurship" (United Nations Development Programme, n.d., para. 3). Moreover, disparate levels of exposure and access to technology mean communities have vastly different experiences upon which to form mature policy positions, significantly affecting their ability to participate meaningfully in global fora, and therefore harming their overall security as a citizen and as a person.

To be clear, getting online is only one piece of the puzzle. While infrastructure is a first and crucial step to access, it is not enough simply to invest in the installation

of fiber or cell towers, or even to foster an ecosystem of service providers. Once online, users must be able to engage and act without threat to their privacy, freedom of speech, and financial or physical security. Such threats, in the form of online discrimination, censorship, manipulation, and surveillance are faced by vulnerable populations around the world, but manifest differently depending on the relevant technology and context specific to them. In order to be sustainable and effective, a cyber peace framework must, therefore, acknowledge and account for the distinct ways that cyberattacks impact different populations depending on their context and unique situations, and therefore threaten their human security. The role of accountability becomes clearer in this context, because by recognizing threats to an individual's opinion or their privacy, the behavior of states, industry, civil society, and end users becomes more apparent.

The healthcare sector in the context of the COVID-19 pandemic presents one such case where vulnerable communities, whose ability to access and securely engage in cyberspace, have been severely compromised as a result of specific circumstances and characteristics. Long before the coronavirus outbreak, the healthcare sector's dependence on digital technology and connectivity had skyrocketed. This dependence, combined with the sensitive data and services under its purview, put the healthcare sector at high-risk to cyberattacks, such as ransomware or data breaches. Following the declaration of a global pandemic and the sudden increase in demand for medical facilities and services, this community became even more vulnerable to existing security threats as they scrambled to set up field hospitals and testing centers, produce and procure equipment, and reshuffle staff and schedules. A well-publicized attack against a hospital in Düsseldorf, Germany, forced the hospital to turn away patients, including a woman who later died, due to a ransomware attack that encrypted thirty of the hospital's servers (Goodin, 2020). In cases like this, by disrupting healthcare operations, such attacks have a very real and tangible impact on the health and well-being of its staff, patients, and the broader community the healthcare sector serves. It shows how questions and concerns over human security should be at the forefront of cyber peace since, at the end of the day, events such as cyberattacks against hospitals have an impact on human lives and their overall well-being.

In addition, the COVID-19 infodemic is another closely related example of the unique impact of cyberattacks on specific communities. These communities are often not defined by any geographic or territorial boundaries, but are still protected under the concepts of human security, dignity, and equity. Due to the nature of the COVID-19 outbreak:

> … communities are relying on online resources to be informed, and are producing information on their own. This leads to a massive generation of online content, blending information coming from official channels (media outlets, international organization bodies, governments), private communication entities and user's generated content (CyberPeace Institute, n.d., para 1).

https://doi.org/10.1017/9781108954341.012 Published online by Cambridge University Press

The World Health Organization (WHO) has identified this "blending of information" as an "infodemic," defined as, "… an over-abundance of information – some accurate and some not – that makes it hard for people to find trustworthy sources and reliable guidance when they need it" (World Health Organization, 2020, p. 2). For example, as an increasing number of people turn to online resources to work and study from home, malicious actors are taking advantage of this influx of online activity. In one case, the WHO itself was hacked and phishing emails that mimicked the organization's internal email system were sent out by a malicious actor (Satter et al., 2020).

These kinds of attacks not only weaken public trust in authoritative institutions like the WHO, but also cause these organizations to divert staff resources away from their usual activities to respond to attacks and mitigate their effects.[2] Beyond the community of institutions like the WHO, this infodemic greatly impacts the broader community of so-called "netizens" – engaged and responsible online users – by eroding their sense of trust and security on the Internet itself. Without a sense of security online, those who are already vulnerable to attacks or influence are left more vulnerable, and any sense of accountability is lost. These are just two specific examples of how global events and changing circumstances, even those – like the COVID-19 pandemic – with no direct relationship to digital technology, can quickly create new vulnerabilities and threats to online access and security. In pursuing cyber peace, we must account for this volatility and incorporate mechanisms to protect vulnerable populations as they arise in a rapidly changing global landscape.

4 THE ECOSYSTEM OF LAWS AND NORMS

The current ecosystem of international law and norms surrounding cybersecurity is complex to say the least. While these complexities present many areas of interesting debate, specifically about polycentric engagement, those in pursuit of cyber peace must work to identify and address the gaps and ambiguities that have the greatest impact on civilian life and human well-being with relation to human security, dignity, and equity. The COVID-19 pandemic again provides a powerful recent example of some of the impact of such gaps and ambiguities.

Cyberattacks against hospitals, such as the one in Düsseldorf as previously discussed, and other facilities during the pandemic emphasize the importance of protecting essential services – especially (but not only) during times of crisis when the civilian population is particularly dependent upon them and their security is at risk. However, both international law and norms present hurdles. Related to international law, the question of attribution presents a foundational issue regarding the ability to track adherence to specific responsibilities and bring claims against specific states. In

[2] See the following public service announcement as an example: www.who.int/about/communications/cyber-security.

https://doi.org/10.1017/9781108954341.012 Published online by Cambridge University Press

addition, ongoing debate regarding relevant thresholds for violations of obligations related to territorial sovereignty and due diligence also frustrates the ability to bring substantiated claims (Open Ended Working Group, 2020, p. 5). Voluntary nonbinding norms that have been proposed to support or complement existing legal obligations are also challenged by ambiguity regarding the meaning of certain key terms, including critical civilian infrastructure – as evidenced by debates and comments at the Open Ended Working Group (OEWG) and discussions regarding a new norm prohibiting attacks against medical facilities further underline this ambiguity (International Committee of the Red Cross, 2020).

This latter issue regarding critical infrastructure is highlighted by the norms outlined in the 2015 report by the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) (United Nations General Assembly, 2015). Two of these norms address the protection of "critical infrastructure," which is of particular importance to discussion and analysis of the implications of cyberattacks against the healthcare sector, and specifically in how they relate to human security, dignity, and equity:

> (f) A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.
> (g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions … (United Nations General Assembly, 2015, p. 8).

Not only is the definition of critical infrastructure itself the subject of much debate, the question of what constitutes "appropriate measures" in the context of norm (g) is also unclear. This snapshot of how the existing legal and normative framework for cyberspace applies to a specific sector in a time of acute crisis demonstrates some of the current gaps between conceptualization and on-the-ground reality. Without clarity regarding these foundational components, the effectiveness of law and norms as mechanisms for change and accountability will be limited. In the meantime, the human cost and impact of these attacks continue to rise as individual's security, dignity, and equity is threatened as the pandemic rages on.

5 ACHIEVING CYBER PEACE

In keeping with the notion of cyber peace as a multidimensional concept, adopting a general theory of change rather than attempting to enumerate specific measures will maximize operational flexibility, durability, innovation and, ultimately, impact. In critiquing the World Federation of Scientist's Erice Declaration, which

https://doi.org/10.1017/9781108954341.012 Published online by Cambridge University Press

applies a top–down governance solution to cyber peace, Heather Roff notes that "by framing the issue this way, the Scientists discount problems associated with unjust social structures, as well as the unsatisfactory nature of the entire international legal framework" (2016, p. 5–6). This is but one example of how prescribing specific approaches – in this case, peace through legal governance, may discount important issues that specifically relate to human security, dignity, and equity. Another point of reference to consider are the principles put forth by Ostrom which show "… in many places around the world how communities devise ways to govern the commons to assure its survival for their needs and future generations" (Walljasper, 2011). These principles can be used to form sustainable and equitable governance systems in communities which form an integral part of the polycentric governance model discussed previously in this edited volume. In essence, the principles put forth by Ostrom are a way to assess one's responsibility to act in their community, so that future generations may also enjoy the same natural resources; for example (Walljasper, 2011).

As applied to cyberspace, we believe a general theory of accountability can provide the needed flexibility and durability to serve as a foundation for a globally applicable methodology for achieving cyber peace. Such a theory of *accountability* is not synonymous with *attribution* or so-called "naming and shaming." Rather, we recommend a very practical understanding of accountability as used in a variety of everyday settings, from the hyper-local to the international, building upon the polycentric approach discussed throughout this volume. For example, in the maintenance of a dwelling, training of a sports team, or employees at a coffee shop – in all these settings, specific actors have clear responsibilities and roles aimed at achieving a common goal and each are held accountable for these actions through various mechanisms. Accountability requires an evolving understanding of relevant stakeholders and responsibilities. More specifically, at the CyberPeace Institute, we believe that a systematic approach to accountability involves the following key steps for each stakeholder; identification of relevant responsibilities, confirmation of commitment to these responsibilities, tracking or measurement of adherence to these responsibilities, and analysis and implementation of effective measures to ensure or increase adherence. We believe that these four steps complement existing work on the topic of cyber peace by advocating for both a bottom–up approach to governance, as outlined in the polycentric model, but by also promoting a simultaneous top–down approach in governance to ensure that appropriate regulation and oversight works to promote accountability of all stakeholders in cyberspace.

6 CONCLUSION

The key challenges above expose an underlying redistribution of power as a result of changing digital ecosystems; a redistribution that is not accompanied by equally robust mechanisms for accountability that can be leveraged to protect individual human beings and their rights and freedoms, both on and offline. By defining cyber

https://doi.org/10.1017/9781108954341.012 Published online by Cambridge University Press

peace around human security, dignity, and equity we can take direct aim at this systemic problem and begin to address the human impact of infringements upon these fundamental building blocks of peace.

As we move into a brave new world, we want to actively and deliberately design our future. Cyber peace is a way to articulate the desired contours of that future and provide clear compass points toward a destination that will benefit all. Recognizing again that common action requires common understanding and a common goal, we must be clear about what we are after and why. The CyberPeace Institute is committed to further operationalize the concept of cyber peace. Such operationalization does not require consensus regarding a finite list of the specific means to achieve our end goal. With the rough contours and a working theory of accountability, we can move forward in a common pursuit of cyber peace.

REFERENCES

CyberPeace Institute. (n.d.). What is the infodemic? Retrieved from: https://cyberpeaceinstitute.org/blog/2020-03-25-what-is-the-infodemic

Delerue, F. (2020). *Cyber operations and international law*. Cambridge University Press. DOI: 10.1017/9781108780605

Diehl, P. F. (2019). *Peace: A conceptual survey*. Oxford Research Encyclopedia of International Studies. Oxford University Press. https://doi.org/10.1093/acrefore/9780190846626.013.515

Goodin, D. (2020, September 19). A patient dies after a ransomware attack hits a hospital. *Wired*. Retrieved from: www.wired.com/story/a-patient-dies-after-a-ransomware-attack-hits-a-hospital/

International Committee of the Red Cross. (2020, February 11). Norms for responsible State behavior on cyber operations should build on international law. Retrieved from: www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-build-international-law

Marlin-Bennett, R. (2022). Cyber Peace: Is that a thing? In S. J. Shackelford, F. Douzet & C. Ankersen (Eds.), *Cyber Peace: Charting a path toward a sustainable, stable, and secure cyberspace* (pp. 3–21). Cambridge University Press.

Open Ended Working Group on developments in the field of information and telecommunications in the context of international security. (2020, May 27). Second "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. Retrieved from: https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf

Roff, H. M. (2016). Cyber Peace: Cybersecurity through the lens of positive peace. *New America*. Retrieved from: https://static.newamerica.org/attachments/12554-cyber-peace/FOR%20PRINTING-Cyber_Peace_Roff.2fbbb0b16b69482e8b631293760 7ad66.pdf

Satter, R., Stubbs, J., & Bing, C. (2020, March 23). Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike. *Reuters*. Retrieved from: www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN

Shackelford, S. J. (2020). Inside the global drive for Cyber Peace: Unpacking the implications for practitioners and policymakers. SSRN. Retrieved from: https://ssrn.com/abstract=3577161 or http://dx.doi.org/10.2139/ssrn.3577161

Shackelford, S. J. (2022). Introduction. In S. J. Shackelford, F. Douzet, & C. Ankersen (Eds.), *Cyber Peace: Charting a path toward a sustainable, stable, and secure cyberspace* (pp. xix–xxxi). Cambridge University Press.

United Nations Department of Economic and Social Affairs. (2020). The Sustainable Development Goals Report 2020. Retrieved from: https://unstats.un.org/sdgs/report/2020/

United Nations Development Programme. (2019). Human Development Report 2019: Beyond income, beyond averages, beyond today: Inequalities in human development in the 21st century. Retrieved from: http://hdr.undp.org/sites/default/files/hdr2019.pdf

United Nations Development Programme. (n.d.). Goal 9: Industry, innovation and infrastructure. Retrieved from: www.undp.org/content/undp/en/home/sustainable-development-goals/goal-9-industry-innovation-and-infrastructure.html

United Nations, General Assembly. (2015, July 22). Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security, A/70/174. Retrieved from: https://undocs.org/A/70/174

Walljasper, J. (2011, October 2). Elinor Ostrom's 8 Principles for Managing a Commons. *On the Commons*. Retrieved from: www.onthecommons.org/magazine/elinor-ostroms-8-principles-managing-commmons

World Health Organization. (2020). Novel Coronavirus (2019-nCoV): Situation Report – 13. Retrieved from: www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf?sfvrsn=195f4010_6