Received: 10 May 2024 | Accepted: 31 May 2024

DOI: 10.1111/pech.12694

ORIGINAL ARTICLE

PEACE & CHANGE
A Journal of Peace Research
WILEY

Peace and the digital revolution: Toward "cyberpeace?"

Paul Antony White

Leeds Beckett University, Leeds, UK

Correspondence
Paul Antony White, Leeds Beckett University, Leeds, UK.
Email: paul.a.white@leedsbeckett.ac.uk

Abstract

This article will explore challenges posed by the digital communications revolution to some long-standing concepts and assumptions around security, warfare, and peace. It will demonstrate the obsolescence of the traditional state-focused national security paradigm with regards to matters of cybersecurity, as well as the limitations of conventional collective security approaches. It will also outline the Internet's potential as a peacebuilding medium, and the crossroads we currently face between a new era of cyberwarfare or an Internet for "cyberpeace."

The field of International Relations has always drawn heavily upon the older discipline of History; we cannot hope to make sense of the modern world without understanding the linkages between present and past. Nonetheless, we also live in an era of unprecedented globalization, characterized by profound and rapid technological and societal change. In my courses on global governance and peacebuilding I argue that these developments will inevitably challenge some of our established assumptions around the nature of global politics, and this includes our understanding of some core concepts related to security, violence, war, and peace.

To truly grasp the significance of contemporary developments, it is crucial to set them in their proper historical context. The study of cyberwarfare and cyberpeace inevitably draws upon concepts and understandings that are rooted in long-standing, historically based discourses around international security, warfare, and peacemaking. This paper aims to frame these present-day phenomena in that context, highlighting long-term patterns of change and continuity at both a practical and conceptual level. It also aims to offer some brief commentary on the extent to which public policy responses in this issue-area could represent history in the making.

The rise of the Internet represents a revolutionary development in human communications. As with so many previous technological revolutions, its consequences have a dual potential to be

highly beneficial, or extremely damaging. Digital communications can be a tool of oppression, a channel for disinformation and propaganda, and even a means of waging war; but at the same time, the technology also promises immense potential as a facilitator of the peacebuilding process. The advent of the digital age thus has potentially transformative implications for multiple aspects of international security, conflict and peacebuilding.

Any attempt to define "cyberpeace" must first begin with a consideration of what is meant by "peace." A narrow definition would simply be the absence of active warfare or violent conflict, a condition we refer to as "negative peace." However, peace scholars have expanded the definition of peace to include respect for and promotion of human rights, the establishment of good governance and rule of law, the presence of democracy, power sharing, equity and social justice, and environmental protection. This expanded definition is known as "positive peace."[1] The concept of positive peace is closely linked to the idea of peacebuilding as a process of preventing and resolving conflicts by addressing their underlying causes, promoting reconciliation, and fostering sustainable peace through various social, political, and economic measures. Cyberpeace can be linked to each of these perspectives on peace and peacebuilding, as will be demonstrated below.

One aspect of cyberpeace concerns the need to deal with new and emerging threats to the security of nations, as well as that of private companies, organizations of all sizes, and individuals. Obvious direct threats include hacking attacks, cybercrime, viruses and malware, but digital communications also provide a new medium for hostile actors to disseminate propaganda and exert political and social influence. The term "information warfare" refers to attempts by state and nonstate actors to influence public opinion, and ultimately political outcomes, through selective representation (or misrepresentation) of facts and the presentation of a biased or even false narrative. Recent studies have found such practices to be on the increase.[2] Besides state actors, various terror groups have embraced the Internet as a medium for disseminating propaganda, for radicalization and recruitment,[3] for training of recruits and for planning and organizing attacks.

Modern societies, particularly advanced economies, are characterized by a high degree of dependence on interconnected computer networks, and this dependence creates direct strategic vulnerabilities. Both governmental and private infrastructures represent likely targets for damaging cyberattacks by hostile powers or groups, with potentially disastrous consequences. As a result, the online world has increasingly come to be seen as a domain of warfare in its own right, alongside land, sea, air, and space.[4] A rapidly evolving "cyber arms race" has ensued,[5] with state and nonstate actors seeking to develop sophisticated cyberwarfare techniques and cyberweapons.

Current governmental thinking around cyber-conflict is frequently based on a "national security" paradigm, rooted ultimately in "Realist" conceptualizations of security. Cyberwarfare is treated as an extension of traditional warfare, drawing upon familiar concepts such as offense and defense, deterrence and balances of power. Cyber capabilities are seen as additional instruments of offense alongside traditional military capabilities, and as coercive instruments of "power."[6] Defense against cyberattack is approached in terms of the protection of national infrastructure (virtual "territory") against incoming attacks.[7] However, applying these conventional understandings of warfare and security to cyberspace is problematic.

Realist approaches assume that states will make rational calculations based on a known international power balance. Although there have been efforts to quantify the relative "cyber-power" capabilities of various state actors,[8] in practice it can be notoriously difficult to make accurate power calculations in this area, because of the inherent uncertainties about what capabilities actors actually possess, and the fact that these capabilities can change rapidly. Alongside states, various nonstate actors may possess credible capabilities, the extent of which may be difficult to ascertain.[9] Furthermore, the notion of defending a "national" cyberspace in terms of constructing

the digital equivalent of a "Maginot Line" may be largely meaningless in an insecure and borderless global cyber environment. The targets of a cyberattack may include a myriad of different organizations, many operating across national borders. Meaningful digital security requires the active participation of these organizations, and is not something that we can look to national militaries or other state agencies to manage alone.

The difficulties of defending against an incoming cyberattack may seem to favor an offensive strategy. The temptation to strike first may be increased by the prospect of "plausible deniability," since the inherent difficulties of attribution may lead a government (or nonstate actor) to believe that it can "get away" with a cyberattack, without the reprisals that would surely follow an attributable conventional attack.[10] This weakens the prospect of effective deterrence. Such offensive-minded thinking, though, is dangerous and potentially destabilizing. Since there are no clearly established norms around what constitutes a proportionate response to a cyberattack, there is a real danger that governments might, under some circumstances, opt for a conventional military response, which may not have been anticipated by the attacker. There is thus a very real possibility of miscalculation leading to escalation into conventional kinetic warfare. These uncertainties mean that an offensive cyber-strategy might be dangerously destabilizing for the international system.

The alternative might appear to be some kind of "collective cybersecurity" approach, through initiatives to establish international norms and thus create more certainty and stability, such as an international convention on cyberwarfare, together with an arms control regime for cyberweapons. In practice, though, this may not be workable. Terms like "cyberweapon" are notoriously difficult to define, which may preclude a legally watertight treaty. Furthermore, such capabilities cannot easily be checked for, making verification processes of the sort that underpin conventional arms control regimes extremely difficult if not impossible.[11] It also seems unlikely that nonstate actors, which may be significant players in the cyber-arms race, would be party to any intergovernmental agreement or inclined to abide by its rules. For these reasons, a purely intergovernmental approach to online collective security is unlikely to be workable.

Cyberpeace is not concerned solely with cybersecurity, but also with the positive potential of digital communications as a peacebuilding channel. In the midst of conflict, the absence of communication links between belligerent parties equals a lack of channels for constructive dialogue, and creates the conditions for opposing groups to demonize one another through propaganda. Belligerent leaders on each side will attempt to control the narrative and present their own perspective and version of events, while censoring others. The Internet can provide a channel to circumvent such controls. Information censored in one location remains available in other jurisdictions, and accessible globally, offering opportunities for peace activists to counter official warlike narratives and propaganda and disseminate alternative perspectives. Attempts to restrict access through filters and similar controls can often be fairly easily circumvented by use of proxy servers and virtual private networks.[12] The Internet thus acts as a repository of alternative information that the belligerent parties cannot control or censor. It also provides a channel for alerting the world to conflict, its consequences, and the need for intervention. With the advent of social media, ordinary people caught in the midst of conflict are able not only to recount their experiences online, but also, in many cases, to actually evidence their stories by uploading high-quality photographs and video. If the conflicts of the late twentieth century were the first "TV wars," the conflicts of today are increasingly played out to a worldwide social media audience. The ongoing conflict in Ukraine offers an example of how war crimes can be documented and publicized through such channels.[13] The gathering of such evidence may even eventually assist

international prosecution.[14] Evidence gathered in the case of the Ukraine war is already being used to aid prosecution in Ukrainian courts.[15]

The Internet also offers opportunities for direct communication across hostile lines, providing a forum for dialogue, a neutral meeting place where there is no physical danger to participants. Here grievances can be aired and discussed, and people and communities on opposing sides of a conflict can come to better understand each other's point of view, building understanding and ultimately trust. One instructive early example that may be of interest to peace historians concerns the *Zamir Transnational Net* (ZTN), an ad hoc Internet connection created in 1991 by peace activists to restore communications between Serbs and Croats, and between Serbia and the outside world, during the conflict in former Yugoslavia. ZTN is credited with enabling a range of peace and humanitarian efforts, and facilitating an avenue for dialogue and civic discourse that would not otherwise have existed.[16] Other examples of online platforms credited with the advancement of peace initiatives have been identified with regard to conflicts in Cyprus, Burundi, Libya, Kenya, and elsewhere.[17] In terms of long-term post-conflict peacebuilding, the online medium may facilitate development of a lasting peace culture, offering opportunities for peace education and the continued dissemination of peaceable values and norms. It can also provide a means of scrutinizing electoral processes and officials, thus increasing transparency and aiding in the establishment of stable democracy in the aftermath of conflict.[18]

While digital communications technologies can facilitate the cause of peace, they can also be utilized by those seeking to suppress peace movements. One area of interest for peace historians to consider would be to examine how cyberattacks on those working toward the cause of peace can undermine the building of a more peaceful world. Authoritarian regimes may use various tactics to target and silence human rights campaigners and peace activists, including the use of Internet surveillance to identify and target dissenters; the restriction of access to content that promotes peace activism; and the use of cyberattacks and online harassment to disrupt the work of peace activists or to intimidate and silence them. One obvious example would be the use of digital surveillance technologies to suppress the activities and impact of democracy campaigners within China. As a more specific case study, the case of the Filipino journalist Maria Ressa can serve as an excellent starting point that historians can use to expand the dimensions of peace history in relationship to cyberbullying by authoritarian figures seeking to silence writers opposed to violence and oppression. Ressa was subjected to a 5-year campaign of state-sponsored online harassment and was subsequently convicted in the Philippines on "cyberlibel" charges, in reprisal for her critical investigation into President Rodrigo Duterte.[19]

Thus, like so many human inventions, the Internet can potentially be a force for good or for ill, for conflict and oppression or for peace. Which of these it becomes may depend, very largely, on the type of regimes that are set up to govern it. Internet governance continues to be an evolving issue-area, and deals with a new domain of human interaction, one where old rules and assumptions may not necessarily be applicable or helpful. As outlined above, a purely intergovernmental approach to Internet governance is probably unworkable. Security in cyberspace cannot be provided by governments acting alone, or indeed by any one single body or organization. Instead, we must look to the multistakeholder approach that has characterized Internet governance to date, based on a recognition that a borderless global medium cannot be effectively governed by territorial states with their narrow perceptions of "national interest." Similar multistakeholder principles must be applied to the construction of a regime for collective security in cyberspace. This will require broadening our understanding of "collective security" from its origins in purely intergovernmental organizations, toward a new definition that embraces a more complex array of partnerships and mechanisms for cooperation and coordination among a broad range of state

and nonstate stakeholders. Such partnerships must facilitate the sharing of technical knowledge and practice, identification of threats and countermeasures, and the coordination of responses, policies and strategies, all on an ongoing basis in the context of rapidly advancing technology and a dynamically evolving environment.

Initial concrete steps toward the development of such a regime could be led by the International Telecommunications Union, fostering discussions through existing public-private structures such as the Internet Governance Forum. The upcoming WSIS+20 discussions due to take place in 2025 may be the opportune moment to begin serious negotiations.[20] This would constitute a significant broadening of the scope of "Internet governance" beyond its original bounds (as understood at the first World Summit on the Information Society in 2003–2005). In the past, partly due to the sensitivities of states around "security" issues, there has often been a separation between discussions of Internet governance and discussions around cybersecurity. Although the historiography in this area is just beginning, works such as Samantha Bradshaw and Philip N. Howard, *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*, Joseph S. Nye, *The Future of Power*, and Gregory J. Rattray and Jason Healey, *Non-State Actors and Cyber Conflict* are helpful in advancing our understanding of the complexities surrounding "Internet governance." Collectively, they argue, as I do, that as we move forward there must be a recognition that the two areas are linked and inseparable, and this understanding must inform the evolution of future multistakeholder Internet governance arrangements.

It is perhaps not an exaggeration to say that the emergence of cyberspace as a new and distinct domain of human interaction has challenged the foundations of the traditional Westphalian system (or at, least, certain aspects of it). In the online world, traditional conceptualizations of "national interest," geopolitics and security are outmoded. Progress toward the establishment of an effective "cyberpeace" will require movement away from traditional statist and "national interest" thinking, and toward the establishment of a new kind of collective security regime. This post-Westphalian approach to security will necessitate a paradigm shift not just beyond traditional "Realist" thinking but also beyond the purely intergovernmental basis of conventional collective security, embracing instead the multistakeholder principles that have characterized other aspects of Internet governance. Such a shift may well meet with resistance at both the practical and conceptual level, from policymakers and scholars alike, The alternative, however, is to continue pursuing a "national interest" approach to cybersecurity that may have dangerously destabilizing effects on the broader international system. Both the academic and Internet communities should be mindful of the potential historic significance of developments in this area, and their importance for the broader cause of global peace and stability.

Historians, in particular, will recognize that human societies, and the international system itself, are not static but evolve over time. An understanding of history not merely as a series of events, but as an ongoing process of evolution in human societies, helps us to appreciate that the future of international relations, along with the future of peacebuilding, will not necessarily always revolve exclusively around the interactions of nation-states or the types of intergovernmental diplomatic processes that characterized peacemaking in the nineteenth and twentieth centuries. Cyberpeace represents a new chapter in the long history of peacebuilding, which present-day and future peace historians will need to document and set in a broader long-term context. This will involve examination of a number of issues and themes. Firstly, future historians should investigate the role of information warfare, cyberwarfare, and cyberespionage in reshaping international relations, and the effects of these phenomena on the international system. Secondly, they should explore the establishment and evolution of principles, norms, and institutions related to Internet governance and cyberpeace, and

in particular the roles played by nonstate actors. Linked to this, historians should explore the emergence of cyberpeace movements, civil society organizations, and advocacy groups working to promote peace and security in cyberspace, as well as the obstacles to their work presented by state-sponsored campaigns of harassment and censorship. Finally, historians should consider the values and ethical considerations associated with cybersecurity practices, and the balance between security and individual rights in the digital age. In exploring these and related issues, scholars will give appropriate recognition to the significance of cyberpeace as a new frontier in peace history.

ENDNOTES

[1] See Johan Galtung. 1969. "Violence, Peace, and Peace Research." *Journal of Peace Research* 6(3): 167–91.

[2] Samantha Bradshaw and Philip N. Howard. 2019. *The Global Disinformation Order: 2019 Global Inventory of Organized Social Media Manipulation*. Oxford: Oxford Internet Institute, https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf.

[3] Charlie Winter et al. 2020. "Online Extremism: Research Trends in Internet Activism, Radicalization, and Counter-Strategies." *International Journal of Conflict and Violence* 14(2).

[4] NATO, Warsaw Summit Communiqué, paragraphs 70 and 71, Accessed July 14, 2023. https://www.nato.int/cps/en/natohq/events_132023.htm.

[5] Jarno Limnéll. 2016. "The Cyber Arms Race is Accelerating – what are the consequences?" *Journal of Cyber Policy* 1(1): 50–60.

[6] Joseph S. Nye. 2011. *The Future of Power*. New York: Public Affairs, 123.

[7] James Andrew Lewis and Götz Neuneck. 2013. *The Cyber Index: International Security Trends and Realities*. New York and Geneva: UNIDIR, 3.

[8] See IISS. 2021. *Cyber Capabilities and National Power: A Net Assessment*. London: International Institute for Strategic Studies. https://www.iiss.org/-/media/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---a-net-assessment___.pdf?la=en&hash=832036F094A4C489C313AC617643369E07FAE9F8.

[9] Gregory J. Rattray and Jason Healey. 2011. *Non-State Actors and Cyber Conflict*. Washington, DC: Center for a New American Security, 68.

[10] See Kenneth Geers. 2010. "The Challenge of Cyber Attack Deterrence." *Computer Law & Security Review* 26(3): 298–303.

[11] Przemysław Roguski. 2021. "An Inspection Regime for Cyber Weapons: A Challenge Too Far?" *American Journal of International Law Unbound* 115: 111–15.

[12] Cormac Callanan et al. 2011. *Leaping over the Firewall: A Review of Censorship Circumvention Tools*. Washington, DC: Freedom House. https://freedomhouse.org/sites/default/files/inline_images/Censorship.pdf.

[13] *The New York Times*, "Documenting Atrocities in the War in Ukraine," May 5, 2022, Accessed February 28, 2023. https://www.nytimes.com/interactive/2022/05/22/world/europe/ukraine-war-crimes.html.

[14] Lorenzo Tondo, Emma Graham-Harrison and Isobel Koshiw, "Crimes Against Civilians: Documenting the Scale of Abuse in Ukraine," *The Guardian*, June 20, 2022, Accessed February 28, 2023. https://www.theguardian.com/world/2022/jun/20/crimes-against-civilians-documenting-scale-abuse-ukraine.

[15] Lily Hyde, "Meet the Ukrainians Documenting Russian War Crimes, in Real-Time," *Politico*, May 19, 2022, last accessed February 28, 2023. https://www.politico.eu/article/ukraines-sprawling-unprecedented-campaign-to-document-russian-war-crimes/.

[16] Amy Herron and Eric Bachman. 2000. "Zamir Transnational Net: Computer Mediated Communication and Resistance Music in Bosnia-Herzegovina, Croatia and the Federal Republic of Yugoslavia." In *Culture and*

Technology in the New Europe: Civic Discourse in Transformation in Post-Communist Nations, edited by Laura B. Lengel, 273–92. Stamford, CT: Ablex Publishing Corporation.

[17] See Paul White. 2019. "Cyberpeace: Why Internet Governance Matters for Global Peace and Stability." *Peace and Change* 44(4): 454–56.

[18] Ibid, 441–67.

[19] Julie Posetti, Diana Maynard and Kalina Bontcheva. 2021. *Maria Ressa: Fighting an Onslaught of marmacpower* 1@gmail.comOnline *Violence*. Washington, DC: International Center for Journalists.

[20] See International Telecommunications Union, "High–Level Dialogue: WSIS +20 – WSIS Beyond 2025," Accessed February 28, 2023. https://www.itu.int/net4/wsis/forum/2022/Agenda/Session/476.

AUTHOR BIOGRAPHY

Paul Antony White is a Lecturer in Politics and International Relations at Leeds Beckett University (UK). He has previously taught at the University of Derby and the University of Huddersfield. His primary research interests lie in the area of global governance (with a particular focus on Internet governance), security and peacebuilding, and global inequalities.

How to cite this article: White, Paul Antony. 2024. "Peace and the Digital Revolution: Toward "cyberpeace?" *Peace & Change* 49(4): 393–399. https://doi.org/10.1111/pech.12694.