
CYBER ATTA
CYBER ATTA
NEWS NEWS NEWS
CYBER Att

The P3 equation: cyber warfare shaping peace, power & perception

by Sarra Hannachi

Cybersecurity: the human in the cyber

Human security as a concept has always been disputed, largely because every new "security" context in history has contributed to its meaning. Traditionally, human security has been understood in terms of physical violence and instability, associated with being protected from armed conflict, crime, terrorism, and extremism, while framing security within the boundaries of military-state paradigms.

Today, that concept has evolved because we live in a digitally transformative era defined by rapid technological development that is accessible both intellectually and financially. Like any resource in the world, its utility is determined by how humans deploy it. This is how the duality of technology manifests in an era of rising geopolitical tensions, crimes, and violations. As much as digital technologies in cyberspace can serve infrastructure and the public sector, they can also be weaponized – like chemicals or steel. There is no human security without cybersecurity.[1]

Peace under digital siege

Peacebuilding and peacekeeping efforts for human security continue to be threatened by

1 Fukuda-Parr, S., & Messineo, C. (2012, January). Human Security: A Critical Review of the Literature (Working Paper No. 11). Centre for Research on Peace and Development (CRPD). https://sakikofukudaparr.net/wp-content/uploads/2013/01/HumanSecurityCriticalReview2012.pdf

a digital siege composed of cyberattacks, surveillance spyware, data theft and manipulation, digitally generated or disseminated disinformation campaigns, and other misleading operations. Peace efforts have been undermined by such threats, including, for example, intentional digital infrastructure sabotage – such as the attacks in Ukraine that disrupted telecommunications and Internet connectivity[2] – as well as recent ransomware incidents in Iran, which stole and gradually leaked sensitive public-sector and banking data.[3]

These cyberattack operations play a role in cyberwarfare and cyber terrorism and can jeopardize peace agreements during war, as well as due-diligence processes in digital security.

Cyber warfare creates a self-reinforcing cycle capable of disrupting peace without leaving physical traces or legally binding evidence in some cases, making accountability for cyber operations during war significantly more complex and dividing stakeholder perspectives

When digital forensics reveal that what once appeared to be fact is a manipulated narrative, it becomes significantly more difficult to undertake diplomatic tasks such as mediation or drafting terms for accountability, peace, or ceasefire agreements. It is also difficult when human security assessments cannot effectively take place because cyberattacks damage infrastructure, mobility, resources, and vital sectors.

Power dynamics in cyber weaponization

State actors are no longer the only entities using their technological advancement for dig-

2 Frąckiewicz, M. (2025, June 21). Telecommunications Infrastructure in Ukraine (2022–2025): Destruction and Resilience. TS2 Space. https://ts2.tech/en/telecommunications-infrastructure-in-ukraine-2022-2025-destruction-and-resilience/

3 Olney, M. (2025, June 30). 5 of the biggest cyber-attacks of 2025 (So far). Industry Trends & Insights. https://insights.integrity360.com/5-of-the-biggest-cyber-attacks-of-2025-so-far

ital deterrence and non-physical control of the battlefield alongside traditional military forces. Non-state actors involved in cyber operations during war or conflict can also obstruct the international community's pursuit of peace and justice by deliberately threatening the human security of both combatants and civilians aligned with the opposing party.[4]

It shows how fragile global peace and security are in digital spaces, and unpredictable diplomatic outcomes can be in this environment. Furthermore, cyber operations may not be entirely dependent on technical experts due to the rapid availability of open-access intelligence and technologies, but they remain dependent on digital tools.

Weaponizing these tools and transforming cyberspace into a battlefield have significantly influenced the outcomes of warfare and become highly contingent on the digital economy.[5] The political size of actors matters less as cyber tactics alone can redefine leverage.

> **State actors are no longer the only entities using their technological advancement for digital deterrence and non-physical control of the battlefield alongside traditional military forces**

@UN Photo/ Evan Schneider

4 Borghard, E. D., & Lonergan, S. W. (2019). Cyber Operations as Imperfect Tools of Escalation. Strategic Studies Quarterly, 13(3), 122–145. Available at: https://www.jstor.org/stable/26760131

5 Rojas, V., & Lissette, A. (2023, September 22). The Rise of Net-States in the Cyberspace: Cyber Power Dynamics and the Disruption of International Security. Digitální Repozitář UK. https://dspace.cuni.cz/handle/20.500.11956/187380


Credit: UNFICYP

Perception as a trust-building factor

Historically, there are methods for building trust and confidence between states and their military units, which include Confidence and Security Building Measures (CSBMs). They are traditional tools used to foster trust between states and their military units. The Organization for Security and Co-operation in Europe (OSCE) leads confidence-building efforts among its participating states,[6] while other international organizations such as the United Nations Office for Disarmament Affairs (UNODA) also implement CBMs in the broader context of arms control and global security [7] to ensure new developments in capacities – such as biological or technological innovation – are not additionally exploited for the modernization and proliferation of arms.

While CBMs have proven effective for some states by allowing yearly field visits, regular military information exchanges, and other commitments, transparency in information exchange cannot be guaranteed because visits remain limited to physical military spaces, resources, and equipment, disregarding the intangible developments that may result in cyberwarfare. This leads to trust built on a perception rather than on full compliance with international frameworks.

Pathways to cyber-enabled justice & security

Cyber warfare creates a self-reinforcing cycle capable of disrupting peace without leaving physical traces or legally binding evidence in some cases, making accountability for cyber operations during war significantly more complex and dividing stakeholder perspectives.[8]

Integrated approaches are therefore key to global stability, cybercrime mitigation and human security. Combining technology, diplomacy, and security can provide all the information and resources needed to mediate peace, de-escalate tensions, seek justice for actions that machines cannot be held responsible for, and balance geopolitical and

6 History and Background of Confidence- and Security-Building Measures (CSBMs) in the OSCE. (2004). OSCE. https://www.osce.org/fsc/40035

7 Military confidence building measures | United Nations Office for Disarmament Affairs. https://disarmament.unoda.org/en/our-work/cross-cutting-issues/military-confidence-building-measures

8 Roudani, C. (2025, June 18). Cyber Deterrence and Digital Resilience: Towards a New Doctrine of Global Defense. Modern Diplomacy. https://moderndiplomacy.eu/2025/06/18/cyber-deterrence-and-digital-resilience-towards-a-new-doctrine-of-global-defense/

cyber-power dynamics.[9] This is achieved not only through multi-stakeholder strategies in peacebuilding processes, ethical technology deployment during conflict, and cyber defense mechanisms, but also through far-sighted planning. Hence, it is important to invest in proactive CBMs in cyberspace and digital platforms as much as in physical weaponry and systems, to prevent conflict escalation and the spread of disinformation.

Overall, embedding cyber resilience into broader peace and security frameworks to ensure justice, stability, and trust forms the core of what this article refers to as the P3 equation.

> **State actors are no longer the only entities using their technological advancement for digital deterrence and non-physical control of the battlefield alongside traditional military forces**

ABOUT THE AUTHOR

Sarra Hannachi is a Mozilla Fellow and a member of the Coalition for Independent Technology Research. She collaborates with non-governmental organizations and think tanks to advance peace and security through the ethical development, use and policymaking of AI and emerging technologies. Sarra specializes in evidence-based research and technology policy, particularly in border security and contexts of war and armed conflict, drawing on experience in the Middle East and North Africa (MENA) region and Africa to provide strategic recommendations on responsible AI in security settings. For youth representation and empowerment, Sarra also serves as a member of the African Union-European Union (AU-EU) Youth Lab Advisory Board with the AU-EU Youth Voices Lab initiative.

9 Van der Meer, S. (2015). Enhancing International Cyber Security: A Key Role for Diplomacy. Security and Human Rights, 26(2–4), 193–205. https://doi.org/10.1163/18750230-02602004