PARIS PEACE FORUM × ACCESS NOW

Toward a Digital Ceasefire?

Session by Access Now
at the 8th edition of the Paris Peace Forum

OCTOBER 2025 ■ SUMMARY REPORT

PARIS PEACE FORUM

accessnow

ACKNOWLEDGMENTS

REPORT LEAD AUTHOR

Ashiya Dewan

Laidlaw Leadership & Research Scholar

Munk School of Global Affairs and Public Policy

University of Toronto

DIGITAL CEASEFIRE PROJECT LEAD

Giulio Coppi

Senior Humanitarian Officer

Access Now

FOREWORD

Since its launch in 2018, the Paris Peace Forum has pushed, across every edition, the idea that international stability and human security do not end where the physical world does. By coordinating the Paris Call for Trust and Security in Cyberspace, it has pursued the same conviction that the edge of a network is no less a frontier of security than the edge of a territory.

Artificial intelligence is now recasting the instruments of digitized war faster than governance can follow it. At its eighth edition, in October 2025, the Forum chose to examine this transformation across the full war-to-peace continuum rather than in fragments. It set discussions on the development of emerging military technologies alongside the standing of international humanitarian law when hostilities are carried out by digital means. From there, the exchange turned to a harder question still. Does a ceasefire still hold once part of the fighting has shifted onto environments a traditional agreement does not mention?

The idea of a digital ceasefire, advanced within that exchange by Access Now, speaks directly to that absence. It takes a term inherited from the old grammar of peacemaking and asks it to name a form of conflict it was never built for. This report resumes the question where the seminar set it down.

Pablo Rice
Head of Programme,
Cyber & Emerging Technologies
Paris Peace Forum

OPENING

When guns fall silent,
digital hostilities frequently do not.

74%

of telecommunications infrastructure destroyed in **Gaza**, leaving the population with largely 2G access, making it one of the most digitally isolated regions in the world.

95

internet shutdowns imposed in **Myanmar** in 2025 alone, 76 of them by the military regime, with satellite services coming under targeted attack.

114

conflict-related shutdowns documented by Access Now across 14 countries in 2025, the highest total on record, with 70 of them coinciding with grave human rights abuses and apparent war crimes.

A conversation at the 2025 Paris Peace Forum, convened in partnership with Access Now, brought together representatives from the public and private sector, Big Tech and civil society, as well as leading NGOs to discuss **the impetus of a "digital ceasefire"**. While most experts in the room agreed on the necessity of exploring the implications of integrating digital systems into traditional ceasefire frameworks, its concrete application to modern-day conflict sparked a rich and nuanced debate. Under the moderation of Access Now, the session opened with a working definition of digital ceasefires:

> *"A digital ceasefire is the cessation of all digital hostilities conducted through or against digital systems, networks, and infrastructures through mutual agreement between parties to a conflict."*

This definition is not intended to become a new legal concept, but rather a mental model: a shared vocabulary for a dimension of conflict that ceasefire negotiations have yet to consider. A growing number of advocates are drawing attention to what it means to cease fighting in the digital age, where disinformation, cyberattacks, attacks on critical infrastructure and internet shutdowns that shroud civilians in darkness are a reality of war.

Notably, most experts agreed that the concept has both a negative and positive framing; it is not only about stopping cyber or kinetic attacks but also about preserving connectivity. A digital ceasefire, in this framework, might outline prohibited conduct alongside affirmative commitments: It calls for the cessation of internet shutdowns just as it reaffirms that populations must retain access to connectivity during and after hostilities.

OBSTACLES TO OPERATIONALIZATION

Panellists did not shy away from difficult conversations, and identified **several structural challenges that definitional efforts alone will not solve**. Cyber operations are not only deniable and devastating, but often cheaper than traditional attacks. Participants acknowledged that many practitioners view a full cessation of hostilities through cyber means as impossible: the incentive for parties to continue using these tools seems to be just too strong. Instead of pursuing the elimination of cyberattacks, some experts say, we must manage their impact and prevent escalation, foremost ensuring that a cyber incident does not become the trigger for a return to kinetic violence.

THE GEOPOLITICAL PROBLEM

Ceasefires are already extraordinarily difficult to achieve and maintain in purely kinetic situations. The current geopolitical climate favours rapid (albeit fragile) deal-making over comprehensive peace diplomacy, which makes it less likely that negotiators under pressure will take on additional, technically complex issues. In conflict zones, the perspective among those closest to their impact is blunt: cyberattacks are harmful, but stopping the bombs is the priority. Any digital ceasefire framework has to reckon with a tangible hierarchy of urgency.

THE CHALLENGE OF UNIQUE ACTORS

Traditional ceasefire negotiations assume a small number of identifiable state parties. Digital conflict is populated by atypical actors such as cybercriminals, hacktivists, bot farms, and civilian technologists, none of whom traditionally sit at the negotiating table. Reaching these actors requires parallel dialogue tracks, adding layers of logistical and diplomatic complexity, as diplomats are often not trained to engage them and frequently cannot identify them without help from the private sector. The private sector arguably has superior technical capacity for threat detection and attribution, but companies operate under different legal frameworks and incentives, facing risks like economic or judicial retaliation when they call out state actors. The creation of an independent monitoring body, to which private sector data could be fed into traditional mechanisms under treaties, was floated as a partial solution.

WHY BOTHER

Conflict-related cyber and digital operations aim to threaten civilian infrastructure, disrupt humanitarian operations and peace-building efforts, or undermine their results. Around the world, civilians face high and material stakes. Access Now's #KeepItOn campaign tracked some of the gravest harms in the past year. In Myanmar, junta forces cut internet and phone lines while conducting airstrikes on nearby villages, leaving residents unable to warn one another or coordinate shelter. Shutdowns also obstruct external response: United

Nations officials in the Democratic Republic of the Congo reported that their humanitarian intervention capacity was severely reduced as a result of a shutdown by authorities during an M23 offensive that left 700 dead. By February 2026, under the cover of Iran's most prolonged shutdown, there were 7,000 confirmed killings with at least 12,000 deaths under investigation by human rights organizations. The shutdown is actively obstructing this process of verification and accountability; a joint demand by the UN Special Rapporteur for Iran calls for the restoration of unhindered telecommunications for civilians and independent monitoring.

When populations are cut off from connectivity, they lose their ability to seek, receive, verify, and share information at critical moments. Communication is a determinant of survival in conflict-zones, critical to keeping up with announcements, contacting loved ones and finding medical help during airstrikes. Despite this, there is almost no ceasefire or peace agreement including reference to offensive cyber operations, internet shutdowns or any other contemporary weapon of digital warfare. This absence enables its continuation, as combatants retain the ability to disrupt humanitarian efforts or carry out atrocities under cover of darkness. An agreement that addresses only kinetic violence leaves civilians exposed to harms of comparable severity, while digital protections in isolation cannot substitute for the cessation of armed hostilities. The model of a digital ceasefire aims to bridge this gap by extending the basic logic of ceasefires – that civilians should not be targeted – to the technologies they now depend on.

THE ACCOUNTABILITY GAP

The current moment is one of near-total impunity in the tech sector, characterized by unprecedented concentration of corporate power, with many of the same companies embedded in state military operations. An expert noted that anything with relevance to national security operates in a general state of legal exemption, enabling unchecked experimentation with technologies that are often tested on populations least equipped to push back, such as in the Global South. The digital dimensions of modern conflicts, such as cyber operations, commercial spyware, cloud and satellite infrastructure are increasingly carried out through private-sector platforms, which complicates the question of accountability and who can be held responsible for acts in war. Participants agreed that accountability mechanisms are essential to ensure digital ceasefire frameworks are enforceable and conscious of the multiple actors shaping modern conflicts.

DESIGNING THE STRUCTURE OF A DIGITAL CEASEFIRE

The discussion converged on a few details: A digital ceasefire must be ownable and implementable by all parties, but one that attempts to cover all digital hostilities may be overly aspirational. Attribution of cyberattacks through the traditional approaches can take months or years; during a ceasefire, parties may position themselves in adversary networks that remain invisible until after the fact. The discussion posited that greater specificity in scope may improve monitoring and resolve some of the attribution challenges.

A narrower scope focusing on purely cyber operations and excluding hybrid ones, such as kinetic attacks by self-guided military drones that drop physical bombs, would be more achievable and enforceable. However, a narrower approach produces further ethical questions: Should social media posts that inflame conflict be included? Does doing so risk further blurring military and civilian distinctions and overstepping rights like freedom of expression? The scoping challenge is not only one of breadth but of depth—how far restrictions can go. The panel's consensus, to the extent one emerged, was that where to draw these lines is not for outside experts to determine, but for the parties negotiating based on what they can mutually agree, implement, and monitor.

SEPARATE OR INTEGRATED?

There is a realist concern of digital rules becoming easier to breach, which could be misused by resuming kinetic hostilities. Ceasefire architecture is traditionally minimalist by design: it asks for less, on the theory that this makes the peaceful period harder to violate. Other experts responded that existing ceasefires are already fragile instruments, constantly violated with or without digital dimensions. The deeper question is whether the absence of this dimension in agreements makes them weaker by ignoring the realities that civilians experience. This discussion begged the question of what digital ceasefires can look like in practice and whether their provisions are best encompassed by standalone agreements.

STANDALONE AGREEMENT

It needs to be agreed upon between the parties that a breach of one would not amount to a breach of another. This could insulate the kinetic ceasefire from a digital one, but would double the diplomatic effort, a new set of accountability mechanisms that do not yet exist and a harmonisation challenge.

ANNEX TO AN EXISTING AGREEMENT

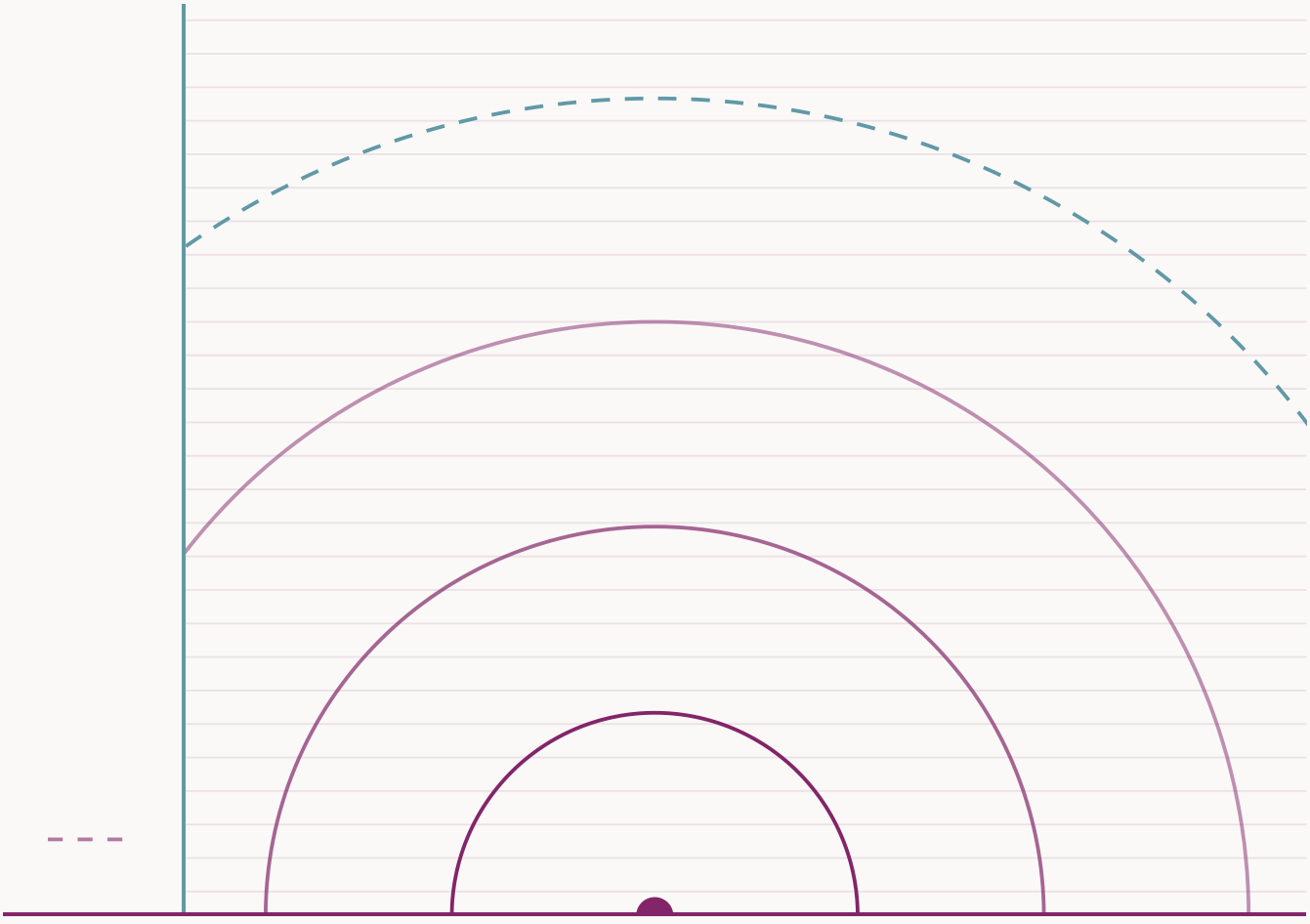
The most likely scenario in practice. It keeps the digital dimension inside instruments the parties already recognise and demands far less new machinery. It also risks overloading agreements that are fragile to begin with.

III IMPLICATIONS

There is broad consensus that "digital ceasefire" captures a tangible and urgent idea. The definition remains a strong starting point for conversation, with structural challenges that require new diplomatic approaches, new forms of sector engagement and institutional willingness to take the digital dimension of conflict as a serious matter of peace and security. The session directly informed the development of the Digital Ceasefire & Deescalation Handbook by the Human Rights Center at UC Berkeley, a model framework equipping mediators and negotiators with tools to address the digital dimensions of conflict, to be launched this year. As a participant elucidated:

> *"A ceasefire cannot be asked to do what it is not designed to do; it cannot resolve a conflict. But it can shape an understanding that there is some way forward, or out, through negotiations."*

The panel concertedly acknowledged that parties are unlikely to achieve a comprehensive peace agreement that addresses both kinetic and digital elements of conflict with equal rigour. However, those living through conflict cannot wait for perfection. The model as it stands is not meant to be copied into a treaty, but to function as a way of equipping mediators, negotiators and diplomats, many of whom are walking into conflicts saturated with digital dimensions, with the language and tools needed to prevent or mitigate harms.



KEY TAKEAWAYS

AN EMERGING GAP IN CONFLICT MANAGEMENT

The session confirmed broad consensus that the "digital ceasefire" concept addresses an emerging gap in contemporary conflict management: almost no ceasefire or peace agreement to date includes digital provisions, even as material harm is inflicted on civilian populations. The working definition proposed provides a viable starting point.

AGREEMENT ARCHITECTURE REMAINS UNRESOLVED

The question of agreement architecture – whether digital ceasefires should be standalone or integrated into existing ceasefires – was identified as a consequential choice with no clear resolution. The former offers insulation from the risk of digital breaches triggering the collapse of kinetic ceasefires, but requires more resources. Integration is more realistic but risks overloading already fragile agreements.

AN ACCOUNTABILITY DEFICIT TO CONFRONT

As there is currently no legal definition of a ceasefire, there is a fundamental accountability deficit that any digital ceasefire framework must confront. The concentration of corporate power in the technology sector, broad legal exemptions for matters of national security and tension around what level of harm to include without infringing on civilian rights are key considerations. It is suggested that these boundary decisions belong to the negotiating parties and their own specific objectives.

A CAPACITY GAP AMONG PRACTITIONERS

A capacity gap was highlighted among mediators, negotiators and diplomats, many of whom are engaging in conflicts with significant digital and cyber elements, but lack the language, technical literacy and tools to address them. The digital ceasefire concept, even in its preliminary form, is a model to provide peace practitioners with the vocabulary to name and contain digital harms within the processes they lead.

HOSTED BY THE PARIS PEACE FORUM

parispeaceforum.org