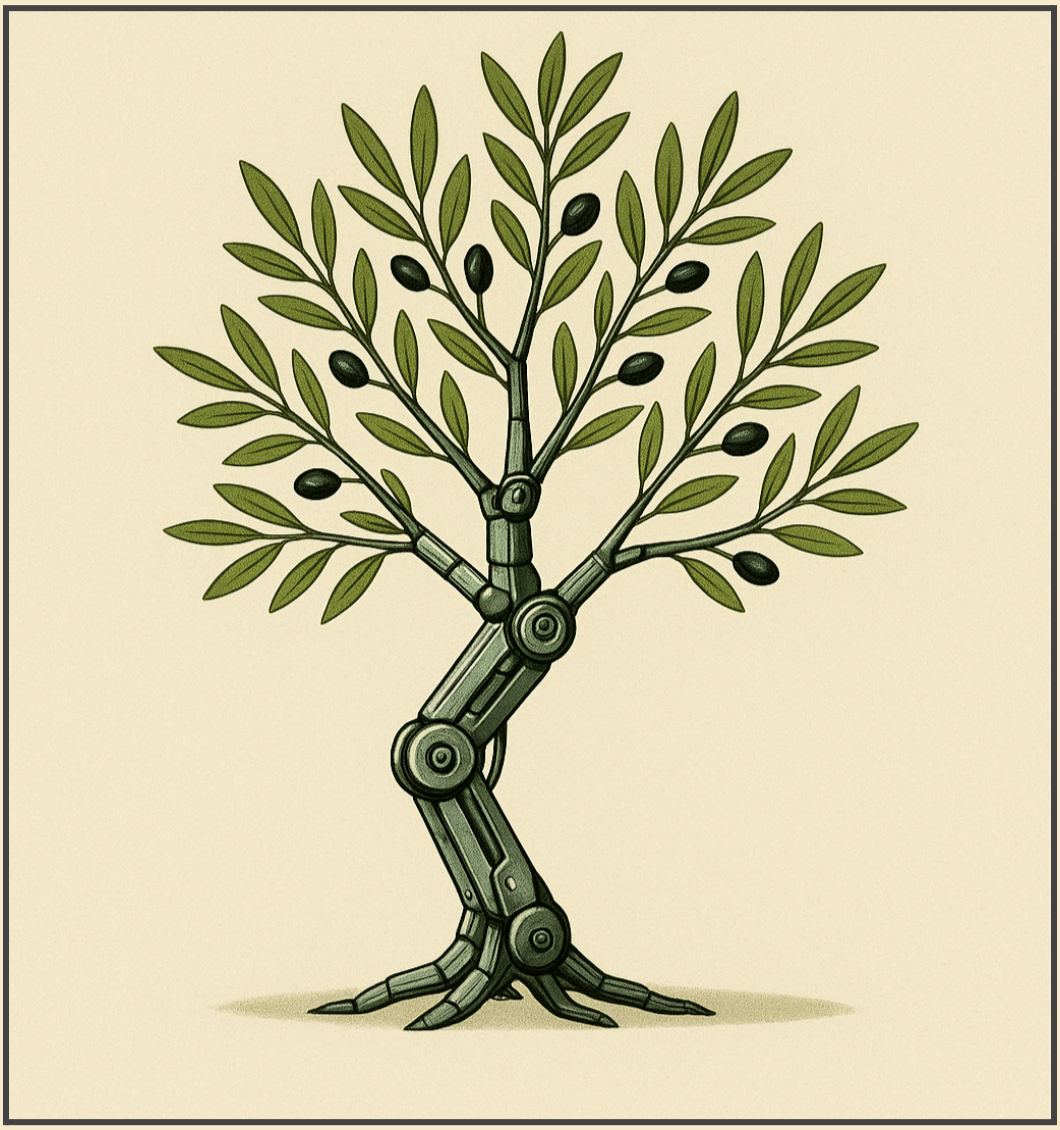
SCPS
SUSTAINABLE COOPERATION
— FOR PEACE & SECURITY —



Cyber Peacebuilding:

A Blueprint for Sustainable Security and Democratic Resilience

Cyber Peacebuilding:
A Blueprint for Sustainable Security and Democratic Resilience

Authors: F. Daniele, T. Pipis, G. Servida, L. O. Tancredi, L. E. Vernetti

Published By: Sustainable Cooperation for Peace & Security

Publication Date: 21/12/2025

DOI: 10.5281/zenodo.18020267

Foreword

We live in an age of fragmentation, where old certainties erode faster than new equilibriums emerge. The post-Cold War promise of linear openness has ceded to a *multiplex world*: a world with **no single hegemonic centre of gravity, overlapping spheres of influence**, and **a global governance architecture that is plural, fluid, and contested**. Power is now distributed and transactional: actors compete and cooperate simultaneously, shifting alliances issue by issue rather than block against block.

In this environment, competition unfolds not only between states, but among private companies, platforms, proxy groups, and ideological networks. Traditional diplomatic and security frameworks struggle to keep pace. Power no longer flows solely through armies, treaties, or borders, but through infrastructure — digital and physical — as well as through platforms, algorithms, data ownership, and narrative control. The frontier of conflict is no longer distant, and rarely declared. It sits inside the devices with which we work, the platforms where public opinion is shaped, and the technological systems that sustain our economies and democracies. The multiplex order **widens the space for strategic manoeuvre**. With blurred red lines, weak enforcement mechanisms, and high ambiguity around attribution and proportional response, **hybrid tactics become attractive tools**: low-cost, deniable, incremental, and disruptive without triggering open retaliation. This is the strategic logic under which hybrid threats thrive.

They exploit ambiguity, legal grey zones, and institutional blind spots; they weaponize connectivity, interdependence, and societal fractures. Cyberattacks, information manipulation, and disruptive influence campaigns increasingly operate below the traditional thresholds of armed conflict, and therefore below the radar of the deterrence-based security architectures that defined the 20th century. What makes these threats effective is not only their sophistication, but their ability to strike at the connective tissues of modern societies: trust, legitimacy, critical infrastructure, media ecosystems, supply chains, and civic cohesion. In such an environment, **security is no longer a domain, it is a fabric**. And fabrics tear where they are weakest: marginalised communities, under-resourced institutions, fragmented coordination mechanisms.

This demands a strategic shift. New threats require new approaches. If malign actors operating in cyberspace are multiple, distributed, and asymmetric, then our defensive capacity must be equally plural, networked, and collaborative. Governments alone cannot secure the digital domain; nor can private companies, civil society, or platforms in isolation. **The only way to address systemic risk is by cultivating systemic resilience**. This implies a true *whole-of-society* response, one that empowers journalists, educators, private companies,

platforms, local communities, researchers, and policymakers as co-producers of security rather than passive end-users of it.

Yet building resilience is not only a technical exercise. It is political, ethical and social. The digital sphere is now a political space where rights, agency, identity, inclusion, and participation are continuously negotiated. Protecting cyberspace therefore means protecting people: their dignity, their ability to participate safely in democratic life, and their access to trustworthy information and secure digital ecosystems. It requires us to think of peace not merely as the absence of conflict, but as the presence of justice, equity, and trust, what peace scholars call *positive peace*. This report embraces exactly that shift. It positions *cyber peacebuilding* as a paradigm that bridges security with human rights, defence with development, technical controls with civic empowerment, moving from tactical reaction to structural prevention.

The challenge is global. Hybrid, and cyber threats in particular, have no borders; they are transnational by definition, exploiting interconnection and jurisdictional gaps. They can only be met by frameworks capable of matching that reach, which means investing in multilateral cooperation and shared global norms. This may seem paradoxical in a time of heightened geopolitical competition and fragmented multilateralism. Yet fragmentation is precisely what makes common rules indispensable. When vulnerabilities are interconnected, security cannot be built in isolation. Cyber peacebuilding therefore requires global norms that enable coordination, accountability, and collective resilience. Peace in cyberspace is a public good – and public goods endure only when jointly upheld.

This document offers a blueprint for moving in that direction. It advances a vocabulary, a conceptual foundation, and a roadmap for thinking differently about security in the digital age: one that reorients us from defending systems to empowering societies; from reactive containment to proactive resilience; from fragmentation to cooperation; from cyber security *against* to cyber peacebuilding *with*.

The following pages are an invitation — to decision makers, policymakers, technologists, academics, entrepreneurs, civil society actors, and citizens — to reimagine digital security as an ecosystem: interdependent, participatory, and grounded in human dignity. In a time when conflict unfolds without a declaration of war, building cyber peace is not utopian and certainly not easy, but undeniably necessary. **This paper is where we start.**

Mattia Caniglia

Senior Policy and Intelligence Analyst, Co-Chair of the **FIMI-ISAC**, and Affiliate Lecturer at the **University of Glasgow** with the International Master's in *Security, Intelligence and Strategic Studies* (IMSISS).

Table of Contents

Executive Summary

This paper advances the concept of cyber peacebuilding as a comprehensive framework for addressing the complex interplay between digital and physical domains of insecurity.

Distinguishing itself from both cybersecurity and digital peacebuilding, cyber peacebuilding integrates human security, structural equity, and systemic resilience into the governance of cyberspace, calling for a new approach to peacebuilding practices that situates peace at the intersection of the digital and physical, addressing their mutual influences on stability, justice, and social cohesion. It recognises that threats such as hybrid warfare, cybercrime, and information manipulation have evolved from mere technical vulnerabilities to political, economic, and social harms. These threats are compounded by structural violence in the form of digital exclusion and inequitable access to technology, which perpetuate conflict dynamics and undermine the foundations of peace. The core thesis posits that sustainable peace in cyberspace requires preventive, inclusive, and systemic governance mechanisms.

Cyber peacebuilding is presented as an organising framework capable of aligning diverse stakeholders, namely states, platforms, civil society, media, and local communities, around shared goals of equity, trust, and accountability. It calls for moving beyond episodic crisis response toward systemic prevention and trust repair, recognising information integrity, digital and media literacy, and equitable participation as peace-enabling assets that are fundamental to democratic resilience. It integrates technological resilience with social justice, transforming cyber and information security from defensive practices into peace-enabling endeavours. By aligning technical, political, and ethical dimensions of digital governance, cyber peacebuilding establishes the foundations for durable peace in an interdependent digital-physical order.

The paper concludes with a set of policy recommendations urging governments, regional bodies, and civil society to adopt cyber peacebuilding as a guiding framework for hybrid-threat governance. This entails embedding human security metrics within national and regional strategies, fostering cross-sector collaboration, and ensuring that digital inclusion and equity are treated as security imperatives. Furthermore, it identifies persistent accountability blind spots within current regimes and argues for the development of transparent, rights-respecting processes that sustain legitimacy and trust in cyberspace.

Finally, this paper introduces a call to action for institutional entities, national and international bodies, civil society organisations, and peacebuilding actors to come together and form a coalition dedicated to further the goals, strategies, and principles of cyber peacebuilding.

Context and Problem Statement

Key Terms

Clarifying the key concepts is essential to understanding the context of cyber peacebuilding. Digital peacebuilding refers to the application of digital technologies and online platforms to traditional peacebuilding practices, ranging from diplomatic engagements and conflict mediation to supporting civil society engagement and cooperation online (Hirblinger et al., 2022). In contrast, Cyber peacebuilding adopts a broader perspective, addressing peace at the intersection between digital and physical realms and recognising the mutual impacts these domains have on peace and security. Chenou (2022) further defines cyber peace as the creation of conditions conducive to cooperative and secure coexistence in cyberspace, grounded in the principles of positive peace, including equity, justice, and sustainability. Cybersecurity, while closely related, predominantly emphasises technical and policy measures designed to protect digital infrastructure from attacks or disruptions, typically without addressing broader structural conditions or societal impacts (O'Connell, 2012). Instead, cyber peacebuilding encompasses the human and structural dimensions of insecurity, acknowledging that digital threats extend beyond virtual space and significantly affect real-world peace and stability (Chenou, 2022; Shackelford, Douzet & Ankersen, 2022).

An Evolving Threat Landscape

The proliferation of cyber warfare, cybercrime, and information warfare has significantly reshaped contemporary security threats. Advanced Persistent Threat (APT) groups, in particular, contribute to persistent instability by combining espionage, sabotage, and influence operations that undermine societal resilience (Buzatu, 2022). Cyber warfare encompasses a range of hostile activities conducted by state and non-state actors intended to disrupt, damage, or gain unauthorised access to computer systems, networks, or critical infrastructures (Azibuike, 2023). Despite the absence of direct fatalities traditionally associated with warfare, cyber operations can significantly undermine national security by disrupting essential services such as healthcare, finance, and utilities, destabilising societies economically and politically, thus undermining trust in the institutions that are supposed to provide security guarantees to citizens (Robinson et al., 2014).

Cybercrime, primarily driven by non-state actors as cybercriminal organisations, hacktivists, and individual hackers, introduces a second layer of complexity to the concept. Ransomware attacks, identity theft, and large-scale financial fraud present an additional layer of insecurity. Events such as the 2021 Colonial Pipeline ransomware attack illustrate the real-world implications of cybercrime, where attacks on digital infrastructure trigger significant disruptions and economic losses (Easterly, 2023). Moreover, cyber mercenaries and hackers-for-hire often cooperate with state actors, blurring the lines between state and non-state activity, complicating accountability and response strategies (Paganini, 2022).

Information warfare represents a distinct, yet equally disruptive threat. Characterised by the deliberate spread of misinformation and disinformation, information warfare aims to destabilise societies, manipulate public perception, and erode trust in democratic institutions. State actors often conduct coordinated disinformation campaigns to advance geopolitical interests or undermine adversaries, as seen in election interference operations. Non-state actors, including organised groups and individuals, also play a significant role, sometimes motivated by ideology, financial gain, or social disruption. Additionally, interest groups such as political parties, lobbying organisations, and even corporations may engage in information warfare to sway public opinion or promote specific policy agendas. Examples include state-sponsored disinformation campaigns targeting elections or the enactment of environmental and economic policies, as well as politically motivated misinformation spread by domestic groups during national referenda or legislative debates, all of which directly threaten societal cohesion and the integrity of democratic processes (Shackelford, Douzet, & Ankersen, 2022).

Emerging technologies such as artificial intelligence (AI), blockchain, and augmented or virtual reality (AR/VR) introduce both new opportunities and complex challenges for information resilience. While these innovations hold potential to enhance transparency, verification, and inclusivity in governance, they also expand the attack surface and exacerbate existing inequities in the digital ecosystem. AI-driven systems can support cyber defence, misinformation detection, and crisis response, yet they are equally susceptible to misuse through deepfakes, automated disinformation, and bias amplification in algorithmic decision-making. Blockchain technologies may strengthen accountability and data integrity, but their decentralised nature can also hinder oversight, enabling illicit financial flows and disinformation financing networks that undermine trust (ENISA, 2017). Likewise, the growing adoption of AR/VR platforms creates new socio-technical domains where harassment, surveillance, and psychological manipulation can occur, further blurring the boundary between digital and physical harms (Roff, 2016).

Beneath these immediate threats lies a structural layer of violence and exclusion in digital spaces. Unequal access to technology, disparities in digital literacy, and exploitative data practices reproduce patterns of marginalisation that mirror, and often amplify, real-world inequities. For many communities, digital exclusion translates into limited access to education, employment, and participation in governance. These are not merely development issues; they are peace and security challenges that entrench and deepen societal divisions (Schirch, 2020). Addressing these systemic issues is vital for establishing positive peace, a peace that is not only the absence of direct violence but also the presence of justice and equity (Galtung, 1969).

Limitations of Current Frameworks

Despite growing awareness of these risks, existing frameworks remain ill-equipped to address evolving cyber threats and the challenges they pose for human rights monitoring, protection, and oversight. Traditional cybersecurity paradigms, often state-centric and militaristic, focus primarily on negative peace (i.e. the mere absence of cyberattacks) without addressing the

underlying socio-political conditions that foster insecurity (Marlin-Bennett, 2022; O'Connell, 2012).

Similarly, digital peacebuilding typically applies traditional peacebuilding methods to virtual contexts, treating the digital space only as a tool for physical-world peacebuilding without adequately addressing the mutual influences between the digital and physical spaces (Hirblinger et al., 2022). This oversight limits the ability to recognise and respond effectively to threats that cross boundaries between digital and physical domains, potentially allowing digital conflicts to escalate into real-world instability and violence.

Recognising these limitations, scholars advocate for alternative frameworks, such as the Cyber Peacekeeping model proposed by Robinson et al. (2014), which emphasises international monitoring and intervention mechanisms to prevent and respond to cyber conflicts. Additionally, Chenou's (2022) Cyber Peace framework emphasises equitable and cooperative governance structures. Both models suggest that cyber peacebuilding requires comprehensive, multi-stakeholder approaches that incorporate both technical and socio-political strategies to foster sustainable digital and physical peace effectively.

The complexity of contemporary cyber threats necessitates a shift toward cyber peacebuilding, integrating considerations of human security, structural inequalities, and multi-dimensional cooperation. Cyber peacebuilding provides a more comprehensive, proactive framework by incorporating inclusive policies, cross-sector partnerships, and capacity-building initiatives that foster sustainable peace through systemic changes. Cyber peacebuilding not only addresses the immediate threats of cyberattacks and information manipulation but also the deeper socioeconomic conditions, such as digital exclusion and media illiteracy, that contribute to sustained insecurity across digital and physical environments (Chenou, 2022; Shackelford, Douzet, and Ankersen, 2022).

Why Cyber Peacebuilding?

The growing sophistication of cyber and informational threats reveals a simple truth: security cannot be sustained through defence alone. Cyber peacebuilding is necessary to achieve both negative peace, which reduces and deters direct digital harms, and positive peace, which builds fair, inclusive, and resilient socio-technical conditions that sustain stability (Roff, 2016; White, 2024). Traditional cybersecurity concentrates on blocking or absorbing attacks, while traditional digital peacebuilding often treats the online sphere merely as a set of tools or channels. In contrast, cyber peacebuilding recognises that infrastructures, data practices, information integrity, and social justice are interdependent and must be governed together to prevent cycles of insecurity (Shackelford, Douzet, & Ankersen, 2022; Schirch, 2020).

By introducing this approach, cyber peacebuilding aims to fill three persistent gaps in current cybersecurity and digital peace efforts. First, it clarifies what peace in cyberspace means: not only reducing direct harms but cultivating equitable access, trustworthy information,

accountable data, and inclusive participation. Second, it promotes integrated, multi-actor cooperation linking states, platforms, academia, international organisations, and civil society, aligning technical defence with community capacity and information integrity. Third, it reframes the governance of hybrid threats, ensuring that security measures safeguard human rights, social inclusion, and democratic trust. This shift moves the global conversation from reactive containment to systemic prevention.

Beyond Negative Peace

Building from the limits of purely defensive postures, limiting objectives to intrusion prevention or rapid recovery leaves intact deeper patterns that reproduce vulnerability. For example, disinformation corrodes shared factual baselines required for deliberation and peaceful dispute resolution (White, 2024; Shackelford, Douzet, & Ankersen, 2022). Recurrent yet non-kinetic attacks on health, energy, or municipal systems can degrade trust, including campaigns associated with APT actors (Buzatu, 2022), and heighten perceptions of fragility (Robinson et al., 2014). Meanwhile, data extraction, surveillance asymmetries, and exclusion from digital services act as structural violence, reinforcing unequal power relations and limiting agency for marginalised groups (Schirch, 2020; Firchow et al., 2016). Consequently, viewing security through a positive peace lens widens the protective perimeter beyond technical cyber infrastructures toward the broader ecosystem that sustains information integrity, including independent media, public interest data governance, education and digital literacy systems, inclusive civic platforms, and local knowledge networks (Roff, 2016; White, 2024; Schirch, 2020). By treating these sectors as core security and peace-enabling assets rather than peripheral soft targets, institutions cultivate redundancy, diversity, and trusted intermediaries, thereby making the information environment more resilient and resistant to manipulation (Firchow et al., 2016; Shackelford, Douzet, & Ankersen, 2022). Therefore, a narrow pursuit of quiet networks or the mere absence of disruption cannot, on its own, deliver durable societal stability. The underlying inequities, information distortions, and trust deficits must also be addressed.

Human Security at the Centre

Extending this argument from systems to people, individuals and communities experience layered harms: fraud, harassment, manipulation, privacy erosion, chilling of activism, and psychological stress (Roff, 2016; Schirch, 2020). Furthermore, militarised and state-centric frames risk overlooking diffuse, cumulative, and psychosocial impacts (O'Connell, 2012). In response, cyber peacebuilding aligns human security metrics, such as dignity, inclusion, and participation, with technical aims, including confidentiality, integrity, availability, and resilience. It pairs protective controls with social measures such as digital literacy, safe communication channels, community early warning, and restorative responses to online abuse (Grunewald & Hedges, 2020); Firchow et al., 2016). This integration reduces the risk that heavy-handed security responses inadvertently shrink civic space or silence vulnerable constituencies (O'Connell, 2012).

Fragmented Actor Landscape

The current panorama involves many actors whose efforts remain loosely connected. International and regional organisations craft norms, capacity programmes, and confidence-building measures, yet enforcement gaps and uneven inclusivity persist (Pawlak, Tikk, & Kerttunen, 2020; Robinson et al., 2014). States bring regulatory authority and coercive power but may default to deterrence logics that underplay participatory governance (O'Connell, 2012). Peacebuilding NGOs and mediators face digital spoilers without an integrated framework linking cyber hygiene and information integrity to conflict transformation (Peacemaking and New Technologies, 2018; Schirch, 2020). Fact checkers and journalists stabilise the information environment but struggle against scale and harassment (Schirch, 2020). Cybersecurity firms deliver threat intelligence and incident response, yet commercial silos fragment situational awareness (Shackelford, Douzet, & Ankersen, 2022). Major online platforms influence public debate and what content gets boosted, acting like regulators without being fully accountable to all stakeholders (Firchow et al., 2016). Local communities simultaneously absorb frontline harms and hold contextual knowledge essential for tailored resilience (Grunewald & Hedges, 2020). Consequently, cyber peacebuilding offers a shared conceptual frame to align these roles toward complementary rather than parallel or conflicting efforts.

Filling Gaps in Existing Approaches

Adjacent proposals, such as cyber peacekeeping, highlight the preventive value of neutral observation, monitoring, and reporting to de-escalate incidents and protect critical services (Robinson et al., 2014; Akatyev & James, 2019). However, peacekeeping alone does not systematically address upstream inequities or guide long-term trust repair. Emerging regional cyber conflict prevention strategies emphasise confidence-building and capacity development but continue to confront cross-sector coordination challenges (Pawlak et al., 2020). To bridge these gaps, a cyber peacebuilding lens connects structural prevention (equity and inclusion), operational prevention (resilience, monitoring, attribution), and post-incident recovery (rebuilding trust and information integrity), while avoiding path dependency toward escalation or normalised low-level hostilities (Inversini, 2020; O'Connell, 2012). In short, this shifts the focus from incident mitigation to a holistic agenda that sets the conditions for both negative and positive peace by linking immediate prevention and recovery with the structural governance needed to sustain them, and it prepares the ground for a coordinated, multi-actor practice that aligns technical resilience with rights-based, inclusive outcomes.

Strategic Value

Taken together, these shifts reveal the strategic value of the approach. Cyber peacebuilding fosters alignment between technological, social, and governance dimensions of security. By bridging these traditionally separate domains, it promotes coherent strategies that address both digital threats and their societal impacts. Digital inclusion lowers overall exposure to cyber risks, stronger information integrity reinforces electoral legitimacy, and equitable data

governance builds the trust needed for cross-border cooperation and effective threat intelligence sharing (Schirch, 2020; White, 2024). Building diverse, independent verification ecosystems is a prerequisite to such integrity and, by extension, to cyber peace (Knake & Shostack, 2022). This integrated framing enables broader coalitions and pooled investment compared to fragmented cybersecurity or narrowly tool-focused digital peace initiatives (Firchow et al., 2016; Grunewald & Hedges, 2020).

The Anatomy of Cyber Peacebuilding: Principles and Core Elements

Cyber peacebuilding derives its strength from a set of interlocking principles that move beyond the limitations of traditional cybersecurity. These principles emphasise human dignity, systemic resilience, equity, and accountability, and they require more than rhetorical commitment; they demand concrete practices, governance structures, and cross-sector collaboration. Below, the anatomy of cyber peacebuilding is defined in greater depth, with a focus on what each principle entails and how it can be realised in practice.

1. Human-Centered Security

First, cyber peacebuilding is best understood as a paradigm shift in security governance, redefining the very subject of protection. Rather than focusing primarily on states and critical infrastructures, it adopts a human-centred security approach that places individuals and communities at the heart of peace efforts. Cyber threats are experienced not only as breaches of technical systems but also as disruptions to daily life, dignity, and participation. They fracture shared factual baselines, generate fear and self-censorship, and drain time and resources from essential services as institutions are forced into perpetual crisis response (White, 2024; Schirch, 2020; Robinson et al., 2014; Easterly, 2023). For instance, targeted disinformation campaigns against women politicians or activists documented across Europe and Latin America have silenced voices in public debate and led to real-world withdrawal from political participation (Schirch, 2020). This can be seen in Brazil, where a study found that among female mayors elected in 2020, 58% reported incidents of political violence; many of these women also reported disinformation, online threats, slurs, and hate speech. False information dissemination was reported by 74% of them, while 66% faced direct online threats (Wilson Center, 2022). Over time, this cumulative psychosocial stress deepens polarisation, normalises hostility in public discourse, and erodes the trust required for cooperative problem solving (Schirch, 2020; Firchow et al., 2016; Chenou, 2022; Roff, 2016). Online harassment, fraud, disinformation, and privacy violations accumulate to shape psychosocial harms that weaken trust in institutions and corrode civic life (Roff, 2016; Schirch, 2020). By foregrounding human security, cyber peacebuilding aligns digital governance with broader values of inclusion, dignity, and empowerment, ensuring that protective measures do not inadvertently silence or marginalise vulnerable groups but instead expand their agency and resilience.

2. Holistic, Cross-Domain Governance

Second, cyber peacebuilding requires a systemic and holistic approach that bridges the technical and social domains of insecurity. Lasting security cannot be achieved by mitigating immediate technical threats alone (Marlin-Bennett, 2022). A purely reactive cybersecurity model, focused on responding to incidents such as ransomware attacks or data breaches, is insufficient because it fails to address the structural drivers of vulnerability. Cyberattacks, disinformation campaigns, and financial fraud constitute visible manifestations of insecurity, yet beneath them lie structural drivers such as inequality, exclusion, and asymmetries in access to digital resources. Addressing these underlying patterns is essential to breaking cycles of vulnerability.

Cyber peacebuilding, therefore, operates on two fronts: responding to immediate harms through resilience and monitoring, while advancing systemic transformation to reduce inequities and empower communities. This dual orientation widens the perimeter of protection beyond technical infrastructures, extending it to education, media integrity, inclusive civic platforms, and local knowledge systems (Schirch, 2020; Chenou, 2022; Shackelford, Douzet & Ankersen, 2022; Firchow et al., 2016). In the field of disinformation, rapid responses such as fact-checking and content takedowns are necessary to mitigate immediate harm. Still, they cannot, by themselves, prevent the recurrence of manipulative campaigns. Long-term resilience requires fostering digital literacy, building trust in local media, and strengthening democratic institutions. For example, the Baltic states have invested in public education programs that enhance media literacy as a defence against Russian disinformation, combining short-term technical interventions with broader civic resilience (Hirblinger et al., 2022).

Integrating digital and physical realms is central to this framework. Traditional peacebuilding often treated cyberspace as a peripheral tool for diplomacy or mediation, while cybersecurity remains confined to the technical or security domains. Cyber peacebuilding overcomes this divide by recognising that online harms spill into offline life, and offline inequities shape digital vulnerabilities. A cyberattack such as the 2017 WannaCry ransomware incident, which crippled hospital IT systems, illustrates this interdependence: its consequences extended beyond data loss to disrupt emergency response, endanger physical health, and erode public trust in institutions (Enisa, 2017; Gafur et al., 2019). Likewise, election interference campaigns are not only digital events but also attacks on democratic legitimacy in the offline sphere; disinformation distorts democratic decision-making in physical polities, just as digital exclusion entrenches pre-existing economic or political marginalisation.

Conversely, resilient local communities and equitable governance structures strengthen the capacity to withstand cyber and informational attacks: community-based media literacy and early warning networks linking local journalists, schools, civil society organisations, and municipal incident response teams can shorten detection and response cycles for coordinated phishing or disinformation surges, reducing amplification and service disruption (Firchow et al., 2016; Schirch, 2020; Robinson et al., 2014). Likewise, participatory and

equitable data governance, such as inclusive digital identity systems, multilingual reporting channels, and transparent allocation of cybersecurity resources, reduces exclusion-driven attack surfaces and builds trust that facilitates rapid collective recovery during ransomware shocks or narrative manipulation crises (Chenou, 2022; Grunewald & Hedges, 2020; Shackelford, Douzet & Ankersen, 2022). This interdependence demands governance that bridges the digital and physical, the technical and social, and the local and global dimensions, embedding structural prevention alongside operational resilience (Pawlak, Tikk & Kerttunen, 2020; Roff, 2016; O'Connell, 2012).

3. Inclusivity and Equity

Third, another fundamental principle of cyber peacebuilding is inclusivity and equity. Digital threats do not affect all groups equally: women, minority communities, LGBTQ+ groups, people with disabilities, people affected by social and economic inequalities, and those in marginalised regions often face disproportionate risks, both in terms of access and exposure to harms (CyberPeace Institute, 2024; Firchow et al., 2016). Cyber peacebuilding insists that security frameworks cannot be considered adequate or just unless they actively redress these asymmetries at their core design.

Marginalised and vulnerable groups, those often excluded from decision-making and deprived of digital access, are also those most exposed to disinformation, surveillance, and online exploitation (Schirch, 2020). Peace cannot be sustained if communities remain structurally disadvantaged. Cyber peacebuilding insists on participatory processes that prioritise voices from the periphery, whether in global governance debates, local resilience building, or platform accountability mechanisms. By embedding equity into its design, it transforms digital governance into a shared project of justice rather than a top-down imposition of control (Chenou, 2022). This inclusivity also strengthens resilience: diverse, participatory ecosystems are more adaptive, trusted, and resistant to manipulation than homogenous, centralised systems (Firchow et al., 2016, White, 2024).

Taken together, human-centred security, holistic engagement, digital-physical integration, and inclusive equity form the anatomy of cyber peacebuilding. They distinguish it from both militarised cybersecurity and tool-focused digital peace initiatives, positioning it instead as a systemic, preventive, and participatory framework. Cyber peacebuilding seeks not only to suppress digital harms but to foster the enabling conditions of sustainable peace across intertwined digital and physical orders (Chenou, 2022; Roff, 2016; White, 2024).

Strategies to Achieve Peace in Cyberspace

Implementing cyber peacebuilding requires a shift in how global actors engage in the digital realm, moving beyond mere technical compliance to concrete strategies. Cyberspace is transnational, influenced by states, corporations, international organisations, civil society, and local communities. Effective peacebuilding in this context necessitates structural reforms and

operational mechanisms that enhance security, resilience, and accountability. Key strategies include strengthening global norms and cooperation, building cyber resilience and capacity, and ensuring accountability and attribution.

Strengthening Global Norms and Cooperation

Cyber peacebuilding requires norms that recognise not only state restraint in cyberspace but also the protection of the broader information ecosystem as a peace-enabling asset (Pawlak, Tikk & Kerttunen, 2020; Robinson et al., 2014). Building on UN processes and regional initiatives, states should codify commitments that prohibit targeting electoral infrastructure and essential services, while integrating human security and information integrity into the interpretation of norms. The UN Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) consensus reports affirm that international law applies in cyberspace and set voluntary norms, including that states should not target critical infrastructure providing public services and should cooperate to mitigate malicious ICT activity originating from their territory. Regionally, OSCE confidence-building measures and the EU's cyber diplomacy toolbox operationalise these expectations through incident notification channels, points of contact, and coordinated response mechanisms (Pawlak, Tikk & Kerttunen, 2020). Housen-Couriel (2022) underscores that cross-sector information-sharing mechanisms, the development of shared situational awareness, and the establishment of trust frameworks are critical best practices for sustaining cooperation and cyber peace."

To be effective, these norms must extend beyond governments and formal institutions. Journalists, fact checkers, independent media, civil society organisations, local technologists, and community early warning networks should be recognised as components of the national information security infrastructure, alongside Computer Emergency Response Teams (CERTs) and critical service operators. National and European strategies should formalise protections for press freedom during cyber crises, establish rapid coordination channels between CERTs and media coalitions for verified public updates, and fund multilingual reporting and rumour-monitoring hotlines operated in partnership with civil society (Schirch, 2020; Firchow et al., 2016).

Operationalising these norms requires structured, routine cooperation among multistakeholders. UN and regional confidence-building measures should include joint exercises where state responders, platform policy teams, local journalists, and civil society organisations practice coordinated responses to ransomware against hospitals or disinformation surges during elections, aligning technical containment with trusted communication to limit panic and polarisation (Robinson et al., 2014; Schirch, 2020). At the European level, integrating these roles into security strategies should provide clear guidance on information sharing, incident classification, accountability, and standardised templates for cross border notifications that include a public interest communication plan, as well as regional surge teams that pair digital forensics with media literacy outreach in affected municipalities (Pawlak, Tikk & Kerttunen, 2020; Grunewald & Hedges, 2020). Including

independent technical and civic verifiers in these exercises strengthens trust in communication and reduces the risk of manipulation (Knake & Shostack, 2022).

Effective implementation also depends on formalised partnerships that make cooperation across states, civil society, the private sector, and international organisations more predictable. Tools should include standing memoranda of understanding for rapid data sharing with due process and privacy safeguards, pre-established roles for non-governmental responders in incident playbooks, and regional surge capacities such as cross-border teams that combine digital forensics, fact-checking, and local outreach to counter coordinated ransomware or disinformation. Dedicated national and regional coordination bodies (tasked with implementing norms, maintaining a common operating picture, and convening stakeholders through formal liaison mechanisms with non-governmental partners) can serve as neutral hubs that streamline decision-making and synchronise operations. Equity-oriented funding should enable under-resourced municipalities and media ecosystems to participate on equal footing (Chenou, 2022; Firchow et al., 2016). By translating high-level norms into routines, these mechanisms reduce misattribution, close coordination gaps, and accelerate trust-preserving recovery, laying the foundation for a sustainable cyber peace architecture (Housen-Couriel, 2022).

Resilience and Capacity Building

Norms alone are insufficient without operational resilience. Cyber resilience turns norms into practice by investing in infrastructure security, structured intelligence sharing, and routine public-private cooperation. Post-incident reviews show that basic controls deliver measurable gains: after WannaCry, the United Kingdom National Health Service (NHS) migrated off unsupported systems, segmented networks, and hardened backups, reducing high-severity outages and shortening recovery windows across trusts (Robinson et al., 2014). Similar patterns are reported in municipal and school ransomware cases where immutable offline backups and network segmentation enabled same-week service restoration (Grunewald & Hedges, 2020). Sector benchmarks also link well-implemented controls to lower losses: organisations aligning to risk-based frameworks such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) report lower breach costs and faster containment, driven by multifactor authentication, patch pipelines, endpoint detection and response, and tested incident playbooks (Shackelford, Douzet & Ankersen, 2022). These investments should be paired with equity-oriented funding for small hospitals, municipalities, and local media so that resilience is not confined to well-resourced actors (Firchow et al., 2016; Chenou, 2022).

Resilience does more than reduce technical disruption: it directly contributes to the peacebuilding goal of preserving trust and preventing escalation. Attacks on healthcare systems or electoral infrastructure are not merely operational interruptions but threats to human security and democratic legitimacy. By reducing the likelihood that such attacks spiral into social unrest, loss of confidence in governance, or cross-border retaliation, resilience acts

as a peace-enabling buffer that maintains both negative and positive peace in the digital domain (Schirch, 2020; Hirblinger et al., 2022).

Threat intelligence and public-private partnerships amplify these gains by speeding detection and coordinated action. Financial Sector Information Sharing and Analysis Centres (ISACs) have documented reductions in fraud losses during malware waves when members shared indicators and countermeasures in near-real time, a model replicated in health through Health-ISAC advisories during Ryuk and Conti campaigns that enabled pre-patching and earlier detections (Robinson et al., 2014). Cross-border exercises in the EU CSIRTs Network have improved notification speed and joint response to supply-chain vulnerabilities, while national partnerships such as CISA's Joint Cyber Defence Collaborative coordinated rapid mitigations for *Log4Shell* and Microsoft Exchange flaws by aligning vendors, operators, and civil society communicators (Pawlak, Tikk & Kerttunen, 2020; Grunewald & Hedges, 2020). Estonia's whole-of-society drills, supported by CCDCOE, show how integrating CERTs, local governments, and independent media sustains service continuity and trusted public updates during crises (Schirch, 2020).

True resilience, however, extends beyond infrastructure. Training local cyber volunteers, embedding digital literacy into school curricula, and integrating civil society watchdogs into national cyber strategies extend resilience beyond technical infrastructures, embedding it in social practice (Firchow et al., 2016). This participatory approach reflects peacebuilding's emphasis on inclusive processes that empower communities and strengthen the social fabric against destabilisation (Schirch, 2020).

Globally, addressing disparities in cyber capacity remains a peacebuilding imperative. Unequal access to digital assets and cybersecurity resources perpetuates vulnerabilities that can destabilise entire regions. International assistance, through European Union capacity-building initiatives, United Nations cyber resilience programs, and regional partnerships, helps close these gaps and advances a more equitable distribution of security (Chenou, 2022; White, 2024). Addressing such asymmetries is a peacebuilding imperative: without reducing structural inequalities in digital capacity, global cyberspace remains vulnerable to drivers of conflict and coercion.

To enhance societal resilience in line with this approach, it is essential to make arrangements routine through memoranda of understanding (MoUs), protected reporting, and widen the adoption of threat intelligence platforms and standards such as *Structured Threat Information Expression/Trusted Automated Exchange of Indicator Information* (STIX/TAXII), the *Malware Information Sharing Platform* (MISP), and existing killchains. Joint exercises also play a vital role in this process. A key aspect of building capacity involves identifying essential actors, including journalists, civil society organisations, and local institutions. Their active participation ensures that resilience strategies are integrated into wider security ecosystems rather than being limited to a narrow technical elite.

Accountability and Attribution

Finally, cyber peacebuilding requires credible mechanisms to identify, deter, and punish malicious behaviour. While resilience reduces the damage of attacks, accountability mechanisms are essential for deterring them in the first place. Attribution, namely the ability to identify the perpetrators of cyber incidents, has advanced significantly through both technical and political innovations. Emerging technologies such as machine-learning-driven traffic analysis and blockchain-based evidence preservation are improving forensic accuracy, while multinational cooperation has enabled joint attribution statements that raise the political costs of malicious behaviour (Pawlak, Tikk, & Kerttunen, 2020; Shackelford, Douzet, & Ankersen, 2022). Coordinated declarations by the European Union, the United States, and NATO partners attributing the *NotPetya* malware to Russian state actors in 2018 signalled a collective willingness to hold aggressors accountable and set the stage for sanctions and diplomatic responses (Roff, 2016), thereby establishing a precedent for timely, coordinated collaboration. The legitimacy of such efforts hinges on credibility and transparency: involving independent researchers, civil society, and platform experts in the attribution process enhances public confidence and limits the room for denial or deception (Knake & Shostack, 2022).

Legal frameworks also play a central role in reinforcing accountability. Internationally, instruments like the Tallinn Manual and UN OEWG discussions clarify norms of state responsibility, while the EU's Cyber Diplomacy Toolbox provides mechanisms for sanctions and coordinated responses (O'Connell, 2012). Nationally, updated criminal codes and Europol's Joint Cybercrime Action Taskforce (J-CAT) enable the dismantling of ransomware and botnet networks (Robinson et al., 2014).

Accountability mechanisms also extend to non-state actors, particularly private companies whose negligence or complicity fuels insecurity. Obligations to notify of breaches in a timely manner under the European Union's Network and Information Security (NIS2) Directive, as well as liability regimes for insecure software, create incentives for stronger corporate security practices (White, 2024). Lastly, civil society's oversight, through transparency reporting, watchdog investigations, and investigative journalism, ensures that the state does not monopolise justice and remains grounded in democratic scrutiny.

Recommendations: Advancing the Cyber Peacebuilding Agenda

Building on the principles of cyber peacebuilding, this section outlines practical strategies for translating human-centred security, resilience, and accountability into national and regional policy. By merging technical safeguards with principles of equity and inclusion into governance frameworks, institutions, and everyday practices, states and societies can prevent

digital harms, foster trust, and ensure that cyberspace becomes a foundation for sustainable peace rather than a new frontier of conflict.

Implement Cyber Peacebuilding in Regional and National Security

Governments, EU institutions, and international organisations should adopt cyber peacebuilding as a guiding framework for hybrid-threat governance. This requires recognising that technical resilience, information integrity, and social justice are interdependent pillars of security, and aligning strategies accordingly. At national and regional levels, peace and security strategies should explicitly integrate human security metrics alongside the "confidentiality, integrity, and availability" triad, ensuring that investments in controls, data governance, and crisis communication also reduce exclusion and protect vulnerable groups (Roff, 2016; White, 2024).

Existing UN and regional norms provide a foundation, but their implementation should elevate actors often excluded from security planning: journalists, civil society, local technologists, and independent media should be included as essential partners in sustaining trusted information flows during crises (Pawlak, Tikk, & Kerttunen, 2020; Robinson et al., 2014). Adoption should prioritise capacity for inclusive participation, cross-sector exercises, and equity-oriented resourcing so small municipalities, hospitals, and local media can meet baseline standards and join shared situational awareness (Firchow et al., 2016).

Embedding this framework marks a shift from incident-by-incident containment to systemic prevention and trust repair, aligning cybersecurity with democratic legitimacy and positive peace. By including cyber peacebuilding in national and regional security strategies, policymakers create a clear funding pathway. NATO's 2035 objective to reach 5% will drive a sharp rise in defence spending. That growth can be turned into an opportunity for democratic resilience. Funds can support journalists, independent media, civil society, local technologists, and community institutions. These actors are not usually treated as security stakeholders, and their budgets are already shrinking. Redirecting a share of new spending can reverse this trend rather than deepen a military-centric tilt. It also opens a practical agenda for research and coalition-building to refine metrics, roles, and evaluation consistent with human-centred security.

Facilitate Information and Knowledge Sharing and Collaboration

States, regulators, CERTs, platforms, universities, media, and civil society, through the creation of dedicated forums and agencies, should establish standing spaces for dialogue that persist beyond crises. Regular cross-sector convenings, joint scenario discussions, and shared learning reviews help align language, objectives, and expectations, reducing coordination failures seen in ransomware and disinformation surges (Pawlak, Tikk, & Kerttunen, 2020; Robinson et al., 2014). Dialogue should be inclusive by design, bringing in local journalists, community organisations, educators, and small operators who experience harms first and often lack access to expert networks (Firchow et al., 2016; Schirch, 2020). The goal is not to

draft technical playbooks here, but to build mutual understanding, map roles, and surface gaps in capacity, communication, and trust. These interactions create the social capital that later enables rapid, credible communication and cooperative response. They also support research by identifying shared metrics for human security and resilience, closing the distance between policy intent and frontline needs while reinforcing accountability and transparency.

Embed Human Security and Digital Inclusion in Cyber Peacebuilding

At the heart of cyber peacebuilding lies a simple truth: peace and resilience in the digital age cannot exist without justice and inclusion. Purely technical or policy-driven safeguards remain insufficient if they fail to address the disproportionate harms experienced by vulnerable groups such as women, minorities, journalists, and civil society actors (Schirch, 2020; Firchow et al., 2016). Digital inequalities, whether through lack of infrastructure, exclusion from governance, or targeted online harassment, entrench cycles of marginalisation and vulnerability (Chenou, 2022; Roff, 2016). To counter these dynamics, national and regional cybersecurity strategies should incorporate digital equity indicators into their assessments, ensuring that protective measures also expand access, participation, and dignity for all. Embedding inclusion into digital governance enhances systemic resilience and public trust. Beyond incident response, peacebuilding initiatives should prioritise education, digital literacy, and participatory governance structures that empower communities to detect and mitigate threats themselves (Grunewald & Hedges, 2020; White, 2024). Inclusive systems are inherently more adaptive and resistant to manipulation, while exclusion deepens susceptibility to disinformation and coercion (Hirblinger et al., 2022; Shackelford, Douzet, & Ankersen, 2022). Ultimately, prioritising human security redefines cyber peace as more than the absence of conflict; it becomes the active presence of justice, participation, and trust across digital and physical domains (Schirch, 2020; Chenou, 2022; White, 2024).

Strengthening Legal and Institutional Accountability

Despite notable progress in international norms and cooperation, accountability remains the weakest pillar of cyber governance. Current regimes often rely on voluntary norms, fragmented enforcement, and political declarations, leaving significant gaps in deterrence and justice (Pawlak, Tikk, & Kerttunen, 2020; Robinson et al., 2014). The problem is not merely the absence of law but its *incoherence*: jurisdictions overlap, evidentiary standards vary, and attribution remains politically contested and technically complex (Roff, 2016; O'Connell, 2012).

This accountability deficit undermines trust and emboldens malicious actors who exploit legal ambiguity to conduct cyberattacks, disinformation campaigns, and digital repression with near impunity (Shackelford, Douzet, & Ankersen, 2022). Non-state actors, including private companies and contractors, frequently operate in grey zones, complicating enforcement and the allocation of responsibility (Chenou, 2022; White, 2024). While technical advances in forensic attribution and international cooperation, such as joint attribution statements or

sanctions regimes, represent steps forward, they remain uneven and reactive rather than systematic (Pawlak et al., 2020).

Cyber peacebuilding requires recognition of accountability and attribution as peace-enabling functions, not merely deterrence tools. Without credible mechanisms to identify perpetrators and uphold digital justice, efforts to build trust, reconciliation, and deterrence remain incomplete. Thus, a key recommendation is to acknowledge the persistence of attribution and accountability blind spots within current cyber governance and to treat their resolution as a structural peacebuilding priority. Establishing consistent, transparent, and rights-respecting accountability processes, whether legal, technical, or diplomatic, will be essential to building a stable and peaceful cyberspace grounded in legitimacy and mutual trust (Roff, 2016; White, 2024; O'Connell, 2012).

Conclusion: Future Steps for a Resilient, Just Cyberspace

Cyber peacebuilding is not a peripheral or optional innovation but an essential condition for achieving sustainable peace in an increasingly digitalised and interdependent world. This paper has argued that neither conventional cybersecurity (focused narrowly on technical defence) nor digital peacebuilding (limited to applying online tools to traditional contexts) can adequately confront the hybrid and systemic threats that define the contemporary security landscape. Cyber peacebuilding instead reconceptualises peace in cyberspace as both negative and positive: it mitigates direct harms while addressing the underlying inequities, exclusions, and trust deficits that perpetuate digital and physical insecurity alike. By centring human security, systemic resilience, and structural equity, cyber peacebuilding transforms cyber and informational security from a reactive discipline into a proactive, peace-enabling practice. It connects technical governance to the broader social, ethical, and political infrastructures that sustain legitimacy and trust. This integrated approach positions individuals, communities, and civil society alongside states and private actors as co-producers of digital security, stability and justice.

The implications are clear: policymakers, international organisations, and private-sector leaders must embed cyber peacebuilding principles into national, regional, and global security strategies. This requires not only new mechanisms of coordination and accountability but also the political will to invest in equity, inclusion, and information integrity as core security imperatives. Building cyber peace is thus not merely a technical endeavour; it is a moral and strategic obligation. In an era where digital disruptions increasingly shape real-world conflict and cohesion, cyber peacebuilding offers a path toward a just, secure, and trustworthy digital order. Adopting this framework is a collective responsibility: to transform fragmented defences into a cooperative effort to strengthen democratic resilience, and to ensure that the digital realm becomes a foundation and not a fracture line for lasting peace.

Sustainable Cooperation for Peace & Security (SCPS) aims to create a civil society coalition to co-author a concise manifesto that articulates principles, priorities, and a public interest case for adoption in law and strategy. The manifesto will consolidate evidence from practice and scholarship, highlight equity and human security as security imperatives, and call for integration of cyber peacebuilding across national strategies and international instruments addressing hybrid threats. Rather than prescribing rigid implementations, it should set an agenda for continued research, stakeholder engagement, and monitoring without defining granular implementation, leaving space for context-specific adaptation. The coalition should then coordinate outreach to parliaments, ministries, international bodies, and standards communities, and convene public dialogues that broaden participation beyond technical and policy circles. This shared platform would strengthen advocacy coherence, raise visibility, and build the momentum needed to embed cyber peacebuilding within democratic governance and long-term security planning.

References

1. Bosco, F., & Reid, K. (2025, July 29). *Elevating AI for good: The role of peace and data security*. CyberPeace Institute. cyberpeaceinstitute.org/news/elevating-ai-for-good-the-role-of-peace-and-data-security

2. Buzatu, A. (2022). Advanced persistent threat groups increasingly destabilize peace and security in cyberspace. In *Cambridge University Press eBooks* (pp. 236–242). doi.org/10.1017/9781108954341.015

3. Chenou, J., & Bonilla-Aranzales, J. K. (2022). Cyber peace and intrastate armed conflicts. In *Cambridge University Press eBooks* (pp. 94–116). doi.org/10.1017/9781108954341.005

4. Christen, M., & Bangerter, E. (2017). Is Cyberpeace possible? In *Springer eBooks* (pp. 243–263). doi.org/10.1007/978-3-319-57123-2_13

5. *Cyber conflict uncoded*. (2025, February 6). European Union Institute for Security Studies. iss.europa.eu/publications/briefs/cyber-conflict-uncoded

6. *Disinformation and online political violence against women in Brazil*. (2023, September 19). Wilson Center. wilsoncenter.org/article/disinformation-and-online-political-violence-against-women-brazil

7. Duguin, S., Lewis, R., Bosco, F., & Crema, J. (2022). Bits and "Peaces." In *Cambridge University Press eBooks* (pp. 212–222). doi.org/10.1017/9781108954341.012

8. Easterly, J. (2023, May 7). *The attack on Colonial Pipeline: What we've learned and what we've done over the past two years*. cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

9. Firchow, P., Martin-Shields, C., Omer, A., & Mac Ginty, R. (2016). PeaceTech: The Liminal Spaces of Digital Technology in Peacebuilding. *International Studies Perspectives*, ekw007. doi.org/10.1093/isp/ekw007

10. Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *Npj Digital Medicine*, *2*(1). doi.org/10.1038/s41746-019-0161-6

11. Grunewald, P., & Hedges, M. (2020). An integrative approach to building peace using digital media. *Journal of Peacebuilding & Development*, *16*(2), 179–193. doi.org/10.1177/1542316620966256

12. Hirblinger, A. T., Hansen, J. M., Hoelscher, K., Kolås, Å., Lidén, K., & Martins, B. O. (2022). Digital Peacebuilding: A Framework for Critical–Reflexive Engagement. *International Studies Perspectives*, *24*(3), 265–284. doi.org/10.1093/isp/ekac015

13. Housen-Couriel, D. (2022). Information sharing as a critical best practice for the sustainability of cyber peace. In *Cambridge University Press eBooks* (pp. 39–63). doi.org/10.1017/9781108954341.003

14. Inversini, R. (2020). Cyber Peace: and how it can be achieved. In ˜*The œInternational library of ethics, law and technology* (pp. 259–276). doi.org/10.1007/978-3-030-29053-5_13

15. Jenny, J., Greenberg, R., Lowney, V., Banim, G., & Centre for Humanitarian Dialogue. (2018). Peacemaking and new technologies. In Jonathan Harlander (Ed.), *Mediation Practice Series*. hdcentre.org/wp-content/uploads/2018/12/MPS-8-Peacemaking-and-New-Technologies.pdf

16. Knake, R., & Shostack, A. (2022). Trust but verify: diverse verifiers are a prerequisite to cyber peace. In *Cambridge University Press eBooks* (pp. 154–169). doi.org/10.1017/9781108954341.008

17. Marlin-Bennett, R. (2022). Cyber peace. In *Cambridge University Press eBooks* (pp. 3–21). doi.org/10.1017/9781108954341.001

18. Matamis, J. (2024). Addressing international cyber peace and security. *Stimson Center*. stimson.org/2024/addressing-international-cyber-peace-and-security

19. O'Connell, M. E. (2012). Cyber Security without Cyber War. *Journal of Conflict and Security Law*, *17*(2), 187–209. doi.org/10.1093/jcsl/krs017

20. Robinson, M., Jones, K., & Janicke, H. (2014). Cyber warfare: Issues and challenges. *Computers & Security*, *49*, 70–94. doi.org/10.1016/j.cose.2014.11.007

21. Roff, H. M. & New America. (2016). *Cyber Peace: Cybersecurity through the lens of positive peace*. New America. static.newamerica.org/attachments/12554-cyber-peace/FOR%20PRINTING-Cyber_Peace_Roff.2fbbb0b16b69482e8b6312937607ad66.pdf

22. Schirch, L. (2020, September 29). *25 Spheres of Digital Peacebuilding and PeaceTech*. Toda Peace Institute. toda.org/policy-briefs-and-resources/policy-briefs/25-spheres-of-digital-peacebuilding-and-peacetech.html

23. Stifel, M., Giroud, K., & Walsh, R. (2022). Cyber hygiene can support cyber peace. In *Cambridge University Press eBooks* (pp. 223–229). doi.org/10.1017/9781108954341.013

24. Trahan, J. (2022). Contributing to cyber peace by maximizing the potential for deterrence. In *Cambridge University Press eBooks* (pp. 131–153). doi.org/10.1017/9781108954341.007

25. Valeriano, B., & Jensen, B. (2022). De-escalation pathways and disruptive technology. In *Cambridge University Press eBooks* (pp. 64–93). doi.org/10.1017/9781108954341.004

26. *WannaCry Ransomware: First ever case of cyber cooperation at EU level | ENISA*. (n.d.). enisa.europa.eu/news/enisa-news/wannacry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level

27. White, P. A. (2024). Peace and the digital revolution: Toward "cyberpeace?" *Peace & Change*, *49*(4), 393–399. doi.org/10.1111/pech.12694