WORKING PAPER

Global PeaceTech: Unlocking the Better Angels of our Techne

Kalypso Nicolaidis and Michele Giovanardi

European University Institute
Robert Schuman Centre for Advanced Studies
Global Governance Programme

Global PeaceTech: Unlocking the Better Angels of our Techne

Kalypso Nicolaidis and Michele Giovanardi

Views expressed in this publication reflect the opinion of individual author(s) and not those of the European University Institute.

Robert Schuman Centre for Advanced Studies

The Robert Schuman Centre for Advanced Studies, created in 1992 and currently directed by Professor Erik Jones, aims to develop inter-disciplinary and comparative research on the major issues facing the process of European integration, European societies and Europe's place in 21st century global politics.

The Centre is home to a large post-doctoral programme and hosts major research programmes, projects and data sets, in addition to a range of working groups and ad hoc initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration, the expanding membership of the European Union, developments in Europe's neighbourhood and the wider world.

For more information: http://eui.eu/rscas

The EUI and the RSC are not responsible for the opinion expressed by the author(s).

The Global Governance Programme

The Global Governance Programme is one of the flagship programmes of the Robert Schuman Centre. It is a community of outstanding professors and scholars, that produces high quality research and engages with the world of practice through policy dialogue. Established and early-career scholars work on issues of global governance within and beyond academia, focusing on four broad and interdisciplinary areas: Global Economics, Europe in the World, Cultural Pluralism and Global Citizenship.

The Programme also aims to contribute to the fostering of present and future generations of policy and decision makers through its executive training programme: the Academy of Global Governance, where theory and 'real world' experience meet and where leading academics, top-level officials, heads of international organisations and senior executives discuss on topical issues relating to global governance.

For more information: http://globalgovernanceprogramme.eui.eu/

Abstract

The double-edged nature of technology pervades human history. Today, the potential for peace offered by the internet, social networks, mobile devices, digital identities, AI, blockchain, big data, geospatial information, is matched by the risks of disinformation, polarisation, online violence, surveillance, data privacy, cyber-attacks, and power concentration. Faced with this knife-edge between the bright and dark sides of disruptive technologies, how do we conjure up the better angels of our nature? Many agents for change around the world have sought to employ and regulate new technologies to foster peaceful processes under the aegis of "PeaceTech" initiatives. This paper introduces "Global PeaceTech" as a new field of social inquiry in the context of International Relations and Global Affairs, with the aim of analysing the global context in which these initiatives are embedded and interconnected, in order to draw prescriptive lessons. The deployment of technology for peace entails legal, political, economic, and ethical dilemmas that transcend national borders and require new models of transnational governance. By bringing together the world of "tech-for-good" and the field of international studies broadly defined as the study of patterns of global change, "Global PeaceTech" fills a gap at the intersection between peace studies and global governance and promotes policy innovation at the transnational level. The paper offers an overview of this agenda in four parts: Part I starts from the IR literature and explores the relationship between technology, peace and war. Part II defines the main differences between PeaceTech and Global PeaceTech. Part III sets out a new research agenda in Global PeaceTech, introducing core analytical concepts and research methods, and discussing its potential political and societal impact. In Part IV, we conclude by presenting a series of example of relevant research areas as a reference for further research in Global PeaceTech.

Keywords

Acknowledgements

Contents

List of Figures and Tables

Introduction: Technology at a crossroad: how can we use new technologies for a more peaceful world?

The latest developments in Ukraine have been a wakeup call for western public opinion. European citizens, and especially young generations, realize more starkly than ever that peace is not forever, but instead a delicate business entrusted to all, from the highest echelons of government to every citizen. Beyond the more than sixty active conflicts in the world in 2022 (ACLED 2022), our global economic and political order has become increasingly fragile and fragmented, heralding the emergence of a multi-order world.

But all is not bleak. To different layers of power struggles and governance correspond different opportunities for peacebuilding initiatives. Here we argue that emerging technologies represent unprecedented opportunities to empower citizens and build transnational processes of peace from the micro to the macro levels, and that these opportunities come with crucial challenges that we need to study and address in order to mitigate the risks and unleash the disruptive potentials of emerging technologies for peace. We label this agenda 'Global PeaceTech.'

The diffusion of technologies to connect people worldwide in the last thirty years brought with it great hopes for democratisation, emancipation, transparency, freedom, education, and peace. Tech-optimism defined the first wave of expansion of the internet in the late nineties and early two-thousands, culminating in the Arab Spring, mass protests in Israel and Spain and the global diffusion of the Occupy movement initiated in New York (Khondker 2011). Yet, already at this stage some observers realised that this was a double-edged sword. In his book 'The Net Delusion: How Not to Liberate the World', Evgeny Morozov argues that the hopes for the democratizing power of the Internet were being replaced by its effective use by authoritarian governments to suppress free speech, hone their surveillance techniques, disseminate cutting-edge propaganda, and pacify their populations with digital entertainment (Moroviz 2011). The optimistic attitude towards the digital's potential for peace and democratisation gave way to more pessimistic accounts. The very same digital platforms that were supposed to enhance peace by connecting people, democratising information, fighting stereotypes and creating communities of trust across borders, turned out to foster institutional mistrust, disinformation, discrimination, polarisation, hate speech, online and offline violence, organised crime and transnational terrorism (Conway 2017).

The twinned opportunities and risks of technologies pervade the history of humanity. Today, besides the use of digital platforms for peacebuilding, mediation, and grassroot participation in peace processes, tech-for-peace across borders includes a wide variety of functions, such as the employment of digital application for early warning systems, the use of digital identities and matching algorithms for refugees' management, big data and predictive analytics for conflict prevention, satellites and drones' deployment for smart border control, blockchain, crypto or smart contracts for humanitarian aid.

The potential is even greater when we consider the social impact of emerging technologies at large. Supported by new techniques in deep learning and multi-layer convolutional neural networks, the harnessing of big data and artificial intelligence (AI) has recently enabled researchers to develop technologies of unprecedented power, including computer vision, speech recognition and natural language processing. The potential benefits of these technologies for society include the possibility of reshaping political structures and the human condition itself, leading some to label their emergence a fourth revolution and the dawn of a new era for humanity. Facial recognition algorithms could significantly increase the general level of security, improving the efficiency of police forces to arrest criminal fugitives or find kidnapped children. Pattern recognition solutions are expected to enable autonomous vehicles, resulting in fewer road fatalities together with more efficient, inclusive and ecological mobility. Embedded in personal connected objects or combined with medical apparatus, stochastic algorithms and image processing solutions also promise great advancements in predictive medicine, allowing more efficiency and personalization in medical care. Other valuable social benefits

include the identification of distressed people on social networks, the promotion of empathy in human-computer interactions (especially between senior people in retirement homes and embodied robots) thought emotion recognition solutions, automated translations promoting easier interactions between peoples and cultures thanks to natural language processing software and personal virtual assistants for cheaper, more efficient and personalized public services.

Against this backdrop, pundits and members of the publics alike have recently become more acutely aware of the dark side of tech, voicing an aspiration everywhere to "take back control." (Innerarity 2021, 2022). For one, a number of scandals have recently revealed the extent of the dangers underlying these new technologies. While Cambridge Analytica showed how large-scale automated misinformation campaigns often orchestrated from abroad could permit powerful political interference and hit democracies at their heart, in many countries, platforms like Facebook have helped spread hate speech – as with mobilisation against Rohingya Muslims uncovered by the UN's investigation in Myanmar (Solon 2018). Yilun Wang and Michal Kosinski's "gaydar" can be used by any government of the 73 countries considering homosexuality as a crime (in 13 of which it is a capital offence) for discriminatory ends. Deepfake's montages raise concerns about identity theft, from which massive trust issues in public information may ultimately result, as no photo, video or sound record can any longer be trusted. Other notorious examples include Northpointe's racially-biased algorithm COMPASS, used by US courts to assess a defendant's likelihood to backslide. No wonder that techno-optimism has turn into techno-pessimism.

The issues at stake are numerous and complex, distributed across the innovation circuit from fundamental research, and the management of data bases (consent in the data collection, control over its access, portability, and erasure, etc.) to the development of algorithmic systems (biases, minimum accepted rate of accuracy, system's integrity and safety, etc.), as well as their intended or unintended applications (emotional recognition for psychological manipulation, facial recognition for mass surveillance, etc.), and the indirect consequences they may have on individuals and societies (public trust weathering, filter bubbles, algorithmic governmentality, etc.).

In sum, ever more sophisticated manipulation techniques seem to herald the advent of a world replete with the 'mining of our lives' (Zuboff, 2020) and the 'hijacking of our minds' (as 'Time well spent' founder Tristan Harris would have it). The increasing concentration of power, be it corporate or political, created by technological advantages and the absence of adequate regulation to govern the interactions they allow will ultimately lead to the loss of our individual sovereignty. Taken together, our innovative techne allows for an unprecedented coup from above, an assault on democracy by way of subverting the very idea of what it means to be an individual (Zuboff 2019, Moroviz 2013, Wu 2017, O'Neil 2016, Pasquale 2015, Maragh-Lloyd 2020, Turkle 2016). These patterns are heightened when the military-defence and intelligence industries develop products that not only will be out of our control (as with lethal autonomous weapons systems – LAWS) but also progressively infiltrate our daily lives, as when the biggest arms sellers to the Middle East and North Africa also produce the surveillance technology used to monitor borders, and the IT infrastructure to track population movements (Akkerman 2016).

We are thus at a turning point. Publics are increasingly pressuring democratically elected governments to address these dangers, increasingly cooperatively, including through regulation (Renda 2019, 2020, Bleyer-Simon 2021). But traditional institutions struggle to address these issues for several reasons. First, the challenge of regulating a set of very recent and fast changing technologies with potential applications in a vast range of domains, which hampers the delimitation of a precise regulatory scope. Premature regulation could then end up being quickly outdated and inefficient. Second, the high level of technicality of the field calls for a strong expertise that regulators do not possess. Third, the great power of technology companies undermines the capacity of states to enforce national regulation without international coordination, resulting in "law shopping", and a loss of states' sovereignty. Finally, the motivation for states to regulate suffers from a critical dilemma. While governments recognize their duty to establish an appropriate regulatory framework to protect

their citizens' rights, they also understand the necessity to support the development of these technologies, including by exercising caution against over-regulation within the context of a fierce international race – and nowhere is this race fiercer than in the realm where quantum technology, AI and big data intersect. A fear of hampering national research and haemorrhaging researchers pervades domestic regulatory approaches.

In this context, a fierce debate has emerged over who may be the most legitimate authority to regulate the spectrum of issues related to new technologies. Even as we recognize the need for regulation, we also need to consider the risks of overregulation and abusive paternalism. Although valuable freedoms that people still enjoy on the internet proceed from the failure to reach an international consensus over a common governance, Lawrence Lessig and others have argued that the diversity of regulatory modes necessary includes not only national and international laws, but also encompasses mechanisms such as social pressure, financial signals and may be embedded into computer code themselves (Lessig 2009).

But in contrast with the early promise of 'tech' to effect change without the state and institutions, it has become clear that institutions and the real people who steer them will be central to redressing the balance between the benefits and risks of new technologies (e.g., vaccinations aren't effective at preventing outbreaks without a public health service to educate and administer; laptops in classrooms aren't effective without teachers; digital labour is exploitative without unions and regulation). This is all the truer at the international level as we consider the ambivalent transnational political effect of emerging technologies, and in particular their effect on transnational processes of peace and conflict. Are emerging technologies contributing to more peaceful interactions between societies across borders? How can emerging technologies contribute to global peace? What are the main obstacles to unleashing their potential?

We argue that while it is evident that connectivity instead of bringing us together in a globalised world is in fact tearing us apart and weaponised as a tool of power politics (Kello 2021, Leonard 2021), this is not the end of the story. Technologies can be employed and regulated to foster peaceful processes in numerous ways as exemplified by the numerous PeaceTech initiatives around the world. By introducing Global PeaceTech as a new field of social inquiry in the context of International Relations and Global Affairs, we aim to analyse the global context in which these initiatives are embedded and interconnected in order to draw prescriptive lessons.

This paper offers an overview of this agenda in four parts: Part I starts from the IR literature and explores the relationship between technology, peace and war therein. Part II defines for the reader what we see as the difference between PeaceTech and Global PeaceTech. Part III sets out a new research agenda in Global PeaceTech, introducing core analytical concepts and research methods, and discussing its potential political and societal impact. In Part IV, we conclude by presenting a series of example of relevant research areas as a reference for further research in Global PeaceTech.

I. Disciplinary Landscape: IR Meets PeaceTech

War and Peace studies are at the heart of IR. Yet technology-for-peace is still an understudied subject. New technologies have profound transformative effect on global politics, can help optimise the allocation of scarce resources, connect people and groups across borders, and help relocate power from corporations and states to communities and individuals. Henry Kissinger in his "World Order" argues that emerging technologies can outdo both strategy and doctrine of foreign policy in a way that will dramatically change the nature of leadership and capacity to solve problems by humans. It will have both negative and positive consequences of which we are not even aware. Much of the literature on the global impact of 'digital DNA' focuses on the global governance of the internet or of the side effects of the information and production disruption (IPD) created by AI or blockchain, or on the offensive side of the equation, such as impact of cyber weapons (Cowhey and Aronson, 2017) . In spite of much rhetoric, governments have not been able to find ways of dealing with these issues

together, aside from some forays in e-commerce and initial strategic discussions on developments such as LAWS. Nor have they considered systematically the implications of technological disruption for peace and development efforts.

An IR approach to technology and peace will provide the necessary analytical framework to examining the power struggles, social movements, norms and outcomes of the use of technology in shifting from negative peace to positive peace. This is also significant because peace is an elastic concept with different meanings for different communities, societies and geographies based on the political and historical background of a given case. In examining the relationship between peace, war and technology in International Relations, we offer an alternative to the three dominant approaches, which broadly correspond to the traditional schools of thought in the discipline: realism, liberalism, constructivism. Each approach oscillates between technological determinism and technological instrumentalism. Technological determinism has been defined as an approach that identifies technology, or technological advances, as the central causal element in processes of social change, such as considering advancement in telecommunication as a driving force of globalization beyond the will of the actors involved (Croteau and Hoynes 2013). Tech-instrumentalism refers to a conception of technology as a neutral instrument that actors use to achieve their own ends. According to this second approach, technology is not considered a key explanatory factor of social change, but only a means to achieve the (political) will of the actors.

Realists approaches to technology and international politics fall under one of two schools of thought: tech-instrumentalism or tech-determinism. On the first and dominant instrumental count, realism's rational ontology focused on state actors and their material power and influence regards technological innovation as a "force multiplier" or material capability contributing to state economic power and thus ultimately military. In this view, technology does not have a transformative role on international relations but is just another means of power politics. It can change, but the nature of international relations remains unaltered, fundamentally based on uncertainty and anarchy, balance of power and states' political aims ultimately driven by overwhelming security concerns. Even in the case of nuclear weapons, security or power are considered the ultimate goal and nuclear weapons only an instrument in the hand of states' security politics, whose acquisition might be useful or detrimental to security depending on distribution of power, strategic balance, and political aims behind it. On the other hand, there are other studies generally associated with realism, focusing on security dilemmas and game theory, which can be seen as techno-determinist. This is the case of the offense-defence balance theory (Jervis 1978, Fearon 1995, Van Evera 1998), that treats technology as an independent variable explaining the outbreak of war, depending on the nature of the weapons utilised (offensive or defensive). Here, technology is seen as a casual factor potentially worsening power competition and conflict, as in the case of the famous insecurity spiral generated by technological innovation and the arms race. While highly influential in the academic debate in security studies, this theory was persuasively criticised by other realist scholars for core problems of distinguishability and underestimation of the role of military doctrine and war plans (e.g., the cult of the offensive in the First World War) (Lynn-Jones, 1995).

In contrast with mainstream realists, liberal approaches to technology and IR tend towards tech-determinism albeit from different premises than the rationalists or defensive realists of the offense-defense school. While they share a rationalist ontology with realists, liberals consider a plurality of actors, including non-state actors, and a plurality of interactions and processes involving them, like complex interdependence, globalisation, institutionalism, domestic politics. While, as illustrated in the introduction, liberals and adherents of modernisation theory, initially viewed technology-induced global connectivity with optimism (Keohane and Nye 1998, Nye 2004), this gave way to a second wave of "liberal pessimism." Far from contributing to transnational peace, cybersecurity and cyberwarfare, surveillance capitalism, disinformation, all pointed to the false promises of the digital age and a global risk society (Friis and Ringsmose 2016, McCarthy 2017). In both cases, however, liberals tend to converge with realists in their technological determinism, considering technology as

an independent variable that drives political change, for better or worse.

In contrast, constructivist approaches to IR and technology criticise tech-determinism or what they call tech-essentialism, emphasising the way in which interests and preferences are shaped by the identities of actors, which are in turn influenced by the norms and shared understanding of the political world. In this context "500 UK nuclear weapons are less threatening than 5 North Korean, because the British are friends. Amity and enmity are functions of shared understanding" (Wendt 1995). The common denominator of constructivist contributions on IR and technology, sometimes labelled as "Social Construction of Technology Studies" is that technology, like any other social product, has no predefined "essential" meaning, but its transformative effect will depend on the shared meanings that actors give it (Klein and Kleinman 2002, Bijker 2012, Eriksson and Giacomello 2007). Technology is what actors make of it and is thus never "politically neutral", depending instead on its mediation by social norms. In short, constructivists can be thought of as tech-instrumentalists, but an instrumentalism that is governed by norms rather than power differentials.

While we recognise the value of these traditional approaches, we situate our analysis both in the middle ground between tech-determinism and tech instrumentalism, and on a separate dimension, namely the endogenous or exogenous character of the technologies at stake (Fig 1). Our conceptual approach is in keeping with a series of works grouped under the label of "technopolitics" for which tech is neither good, bad, nor neutral but 'deeply political' (Kurban et al. 2017). Most importantly, "technology is an ambivalent endogenous core component of the global system" as technology and politics shape and reshape each other in complex and unpredictable ways. (Fritsch 2014). Accordingly, paradigm of technopolitics seeks to "cover the desert between tech-determinism and human agency" (Mayer et al. 2014). If technologies affect social behaviours and interactions in predictable ways we can study, actors still have agency and can mitigate their negative effects. Our one contribution to technopolitics is to bring this understanding of agency to the global level to ask how we can influence these processes though both individual awareness and collective regulation.

Figure 1. The role of technology in explaining peace and war in IR theory

The study of Global PeaceTech as part of IR studies raises multiple questions. Some involve examining "what do technologies do". One compelling approach, for example, is to think about information technologies as changing space and time (Schwanen and Kwan, 2008). Things that are far seem close. Things that used to take a long time are fast. What happens when decision-making in conflict speeds up? What happens when national groups are able to form transnational networks? What happens if issues can't be hidden or ignored? As Floridi (2007) has argued, the increase in common publicly accessible knowledge makes leaders more morally accountable for actions. This focus on action – what technology does – is also a way of avoiding simplistic discussions of technology as 'good' or 'bad' or getting to wrapped up in a single innovation. Duffield's work (2012, 2014) is also focused on the shrinking of space through the use of surveillance and remote technologies. He argues this creates a false sense of 'knowing' from a distance and, as Fisher (2018) argues, this has furthered the 'bunkerisation' of aid. This idea of knowing from afar is also at the heart of critiques of reporting platforms like Ushahidi – what does this data actually show? Burns (2014, 2015) notes that in the case of Hurricane Sandy 'if responders had looked only at Big Data they would assume the hardest-hit areas were wealthy Manhattan neighborhoods.' There is a lot of work now on the role of both social media and VR in immersion and persuasion such as the work by Graham and Zook (2013) on ideas of augmented reality (e.g., maps) in creating worlds that overlap – or not – with others; this is a physical embodiment of a filter bubble. Toyama (2011) speaks of amplification. Beniger (2009) works on control. This could all have interesting implications for connecting tech and conflict.

The role of technology in the relationship between security and peace can be also elaborated from the perspective of empowerment and surveillance. The relationship of new technology and the rise of what Agamben, following Carl Schmitt, referred to as 'politics of a permanent state of exception' is significant to analyse from a PeaceTech perspective. According to Agamben, western politics has essentially become a permanent state of exception in the aftermath of 9/11. This refers to a routine use of exceptional powers and measures (ever increasing surveillance, profiling, and suspension of individual rights for specific categories of people) which leads to their normalization; or, as Didier Bigo has argued, we live in a permanent 'state of unease' in which those who claim to 'know the truth' (security service officials and various experts) successfully justify the use of various measures that threaten or undermine various freedoms. As a matter of fact, smart border and the rights of migrants and asylum seekers are issues that are clearly related to this (Agamben 2005, Bigo 2002).

Another area of concern will be the potential of new technology to enhance resistance such as the notion of 'sousveillance' or 'watching the watchers'. For instance ACLU and CopWatch developed apps to film and fight police brutality in the USA; indigenous peoples have also used similar technologies to fight against abuses. That raises the question about the ambivalence of new technology in peoples' struggle against authoritarian states. On the one hand, it has never been easier to overcome collective action problems through the use of the internet and peer-to-peer technology (encrypted messaging apps, proxy servers, anonymous online platforms, etc.). On the other hand, powerful states have the technological means to monitor almost all telecommunication streams, censor and use AI to anticipate people at risk of engaging in 'state subversion'. Thus, the question is what consequences have arisen – and will arise in the future - from advanced technology for activists in dictatorships? And what might be strategies to circumvent some of the 'new' obstacles for 'liberation' campaigns?

Arguably, the current stage of capitalism can be characterised as 'precarious capitalism' e.g., a transformation of neoliberalism into a system of relations generating insecurity for a greater number of citizens. Conversely, security (including the literature on physical security, economic security, environmental security, and food security) is a must for a stable peace, but the security-oriented approach might also reproduce conflict and violence with the help of frontier and digital technologies. Although the number of interstate and civil wars has declined, violence related to local disputes, organised crime and political repression has increased (Caplan 2019). Therefore, we should not

focus only on peacebuilding process in post-conflict areas such as supporting 'resilient societies' of conflict-affected countries but also analyse various forms of violence and peace including gender violence and peaceful coexistence between local and migrant-refugee communities.

Technology does not need to be the only starting point. We can build on excellent work on peace literature, and we see ways for technologies to play a role in these functions (e.g., empathy building, trust/verification, network building, information sharing, decentralisation, responsive governance). This provides a way of unpacking current PeaceTech initiatives: Do they all focus on similar functions or peacebuilding practices? If so, why is that? If available infrastructures (e.g., Facebook, mobiles) help to drive the shape of these innovations, are there path dependencies? This also goes to the question of how the use of technologies affects interactions (e.g., how people interact, which people interact). In the promise of using technologies to support peace and peacebuilding, we also have to think about how tools shape behaviour (e.g., online dialogue the same as an in person one?) and how ideas shape these tools.

II. What is Global PeaceTech?

From PeaceTech…

The term PeaceTech first emerged in the context of peacebuilding and referred mainly to the use of digital platforms and applications to support peacebuilding strategies. Sheldon Himelfarb, CEO and Founder of the "PeaceTech Lab", a Washington based NGO affiliated to the U.S. Institute of Peace, described PeaceTech as "a movement aimed at effective grassroots conflict prevention made possible by ground-breaking amounts of data for early warning, the ability to mobilize through digital networks, and new private sector resources invested in fragile and emerging countries" (PeaceTech Lab 2022). On the NGO's website we can find a further characterization of PeaceTech as "products and services that help foster relationships between groups, protect people from the effects of violent conflict, disrupt the tactics of violence, or respond to the root causes of conflict" and again "tools that foster positive outcomes like enhanced social well-being, sustainable economies, stable governance, rule of law, and safe and secure environments". More synthetically, the PeaceTech Lab defines PeaceTech as "technology to tackle the drivers of conflict, promote stability, and build peace". Whilst the definition is kept intentionally broad to include any kind of technology that can potentially contribute to conflict prevention and peacebuilding, the cases presented are mostly referred to mobile applications for early warning systems, data gathering and analytics, and the use of digital platforms for peacebuilding campaigns to fighting online violence, misinformation, and radicalization.

Another definition is provided by the NGO "Build-Up" which defines PeaceTech as "an emerging body of peacebuilding practice which includes a technological component that is of strategic importance to its objective(s)". Here the focus is on peacebuilding activities enhanced by the strategic use of digital technologies, distinguished from the general use of technology for organization management, like the use of emails, websites, social media, as most civil society actors do. (British Council 2016). This 'use with purpose' includes data collection, analysis, and visualization, strategic communication to promote alternative narratives and information sharing, gaming, and engagement tools to create new ways for people to influence or act in their communities (Larrauri 2013; British Council 2016). More recently Cottray and Larrauri (2017) expanded this definition by including more tools: in addition to databases, smartphone apps, messaging services and cameras, and video games, also unmanned aerial vehicles, virtual reality, and geographic information systems (GIS) are considered PeaceTech.

...to Global PeaceTech

With the study of Global PeaceTech we aim to contribute to the debates on the definition of PeaceTech from an international relations approach where Firchow and Martin-Shields (2017) have said that PeaceTech is in a state of liminality and ambiguity, with many of its roles and boundaries being established and negotiated. In its simplest form, we can accept a broad definition of PeaceTech as 'technologies built or used to achieve peace'. However, this minimalist definition requires a clarification on what we mean by 'technology' and what we mean by 'peace' within the proposed definition.

When it comes to 'technology', we propose adopting an inclusive approach that does not exclude any kind of emerging technology. A provisional list of technologies for which the potential for peace can be assessed includes connectivity infrastructure (e.g., fixed line, wireless 4G/5G, satellite, undersea cables), open internet and social networks (including metaverse), distributed ledger technologies (e.g., blockchain), digital identity and biometrics, digital government, artificial intelligence and machine learning, internet of things (including sensors, extended reality support, wearable or implanted devices), virtual reality and gamification, edge/cloud infrastructure, big data analytics, satellite imagery and space technology, robotics. This list may expand in the future to include quantum and other technologies that we do not currently foresee.

The definition of 'peace' is somewhat more complex. There is no generally agreed term on the definition of peace, and the peace literature includes various theories. We understand the peace agenda to encompass the prevention and resolution of conflict among and within nations via non-violent solutions and create necessary conditions for sustainable peace through empowerment of people. As the Global PeaceTech proposal links the peace technologies with empowerment, we will consider both classical 'negative' peace and 'positive' peace theories where negative peace is the absence of the violent conflict and positive peace is the presence of harmonious relations, social justice and empowerment of communities through a systematic change as stated by Johan Galtung (1964). Global PeaceTech will point out the strategical significance of technology in shifting from negative peace to positive peace and strengthen the peace at the flawed situations to ensure the stability and sustainability of peace through creating new avenues of participation for inclusive dialogue and interaction between societies, communities, and individuals.

In view of the aforementioned definitions of technology and peace, we can therefore define Global PeaceTech as the following:

Global PeaceTech is a field of analysis applied to all processes connecting local and global practices aimed at achieving social and political peace through the responsible use of frontier technologies.

This inquiry involves a wide range of actors at all levels of action and governance and lies at the intersection of different analytical levels and disciplines. Some examples of PeaceTech include the use of data collaboratives and predictive analytics for peace, the use of digital platforms for mediation, grassroot participation to peace processes, fighting stereotypes and building transnational communities of trust, the use of application, satellites, and drones for early warning and response systems, employment of space technologies for geo-localisation and smart boarder control, the use of blockchain technology both for digital identities and financial applications, like smart contracts and cryptocurrencies, to transform democratic interactions and financial aid. A distinguishing feature of Global PeaceTech is that it focuses not only on applications and use cases, but also on how these technologies influence transnational political processes and can be managed and regulated collectively to promote responsible, human rights-friendly and peace-enhancing use. A non-exhaustive list of Global PeaceTech use-cases and examples is provided in the table below. Further Global PeaceTech examples, research questions, and themes are provided in section IV.

III. Global PeaceTech: a new research agenda

Much of the IR literature has focused on how the spread of new technologies affects the conduct and dynamics of war. Our aim is to shift the focus to how technology can influence global peace patterns, promoting a paradigm shift from technology-for-war to technology-for-peace. The deployment of technology for peace entails legal, political, economic, and ethical dilemmas that transcend national borders and require new models of transnational governance. Our aim is to study these models, highlight existing practices, and propose concrete solutions to promote the responsible use of technologies such as Artificial intelligence, the Internet of Things, blockchain, technical architectures for e-identity, and many more, in support of peace. The expected result is a novel academic framework centred on the new concept of "Global PeaceTech" which brings together the world of "tech-for-good" and the field of international studies broadly defined as the study of patterns of global change. This will fill a gap at the intersection between peace studies and global governance and promoting policy innovation at the transnational level.

Aim

Research exists on the dilemmas and regulatory possibilities related to specific technological applications. For instance, we have seen a wave of studies on cyberspace and cyber regulation, and we are witnessing a similar trend with AI governance (Bullock et al. 2022). However, these technologies and dilemmas are rarely studied together in their interaction and combined impact on global affairs, while an approach that treats these challenges separately is often privileged. Moreover, the specific effects of disruptive technologies on peace are hardly considered systematically. The Gobal PeaceTech research agenda intends to go beyond this 'silo mentality' to embrace a comprehensive approach in which it is impossible to separate one technology from the other in the study of the transnational construction of global peace. In fact, emerging technologies present common challenges and effects, which can be studied by referring to similar nomenclature and concepts when evaluating their socio-political impact.

The promise of the Global PeaceTech research agenda is to develop new ideas and analytical frameworks to better understand, monitor and enrich "the better angels of our techne" while being cognisant of all their potential pitfalls. This new research agenda matches the vision of putting the human being and human rights at the centre of the technological revolution. A human-centric approach is vital so as not to leave decision-making processes to algorithms and demystify the hype around frontier technologies. Moreover, it will help to build an inclusive tech-base for peace, exploiting the potential of new technologies to address the root causes of conflicts and create conditions for peace by promoting good governance, citizen participation, socio-economic wellbeing and inclusion, and shared values and non-discrimination. Finally, it will go in the direction of promoting a collectively reflexive use of new technologies, given the possible unintended harms or risks to human beings and society at large, and in particular to vulnerable communities such as refugees, focusing on power struggles and conflicting interests, and adding to the many initiatives that seek to define principled guidelines for digital ecosystems.

The expected impact of this new research agenda is threefold. Firstly, it will contribute to models of governance and regulations of technology for peaceful purposes. Secondly, it will orient impactful investments in sustainable PeaceTech solutions that work. Thirdly, it will accelerate new ideas on applications of technologies for peace, by investing in new research project that apply technology and social sciences to solve common problems and devise solutions for peace.

An interdisciplinary project

There is no denying that the scope of our research is exceptionally wide. As mentioned, we are looking to broader trends to assess the impact technology can have on global peace. A wholistic approach to peace starts with acknowledging the continuum between security and the humanitarian field, the latter and development, development and trade, and thus the intersection of the spaces of diplomacy, development, conflict resolution and social media. Our research interest in Global PeaceTech is not limited to the local dimension of conflict and how technology can contribute to local peacebuilding efforts, but the extent to which local conflicts are interconnected transnationally in a globalised world and how peace can be built with technology in across-borders actions and interactions. This includes different levels of analysis and different actors.

Figure 2. An interdisciplinary project
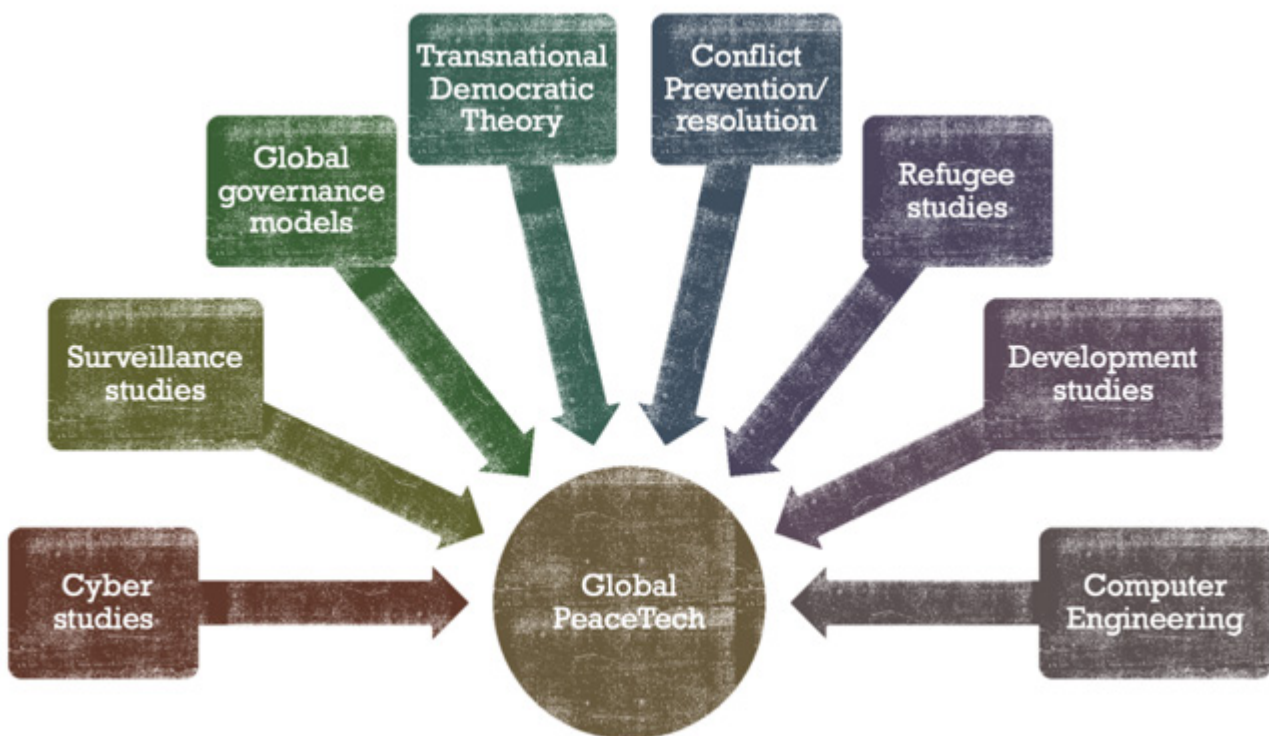
The issue nexus

When people refer to technological innovations to serve peace, they may be thinking of different levels: the individual level, in which technologies can empower human potential and fulfilment; the local level, where technologies can be deployed to prevent conflict or the recurrence of conflict as well as to help create environments conducive to peace; the transnational sphere where connections between individuals and groups across borders can be consider as the social foundation for peace; the global level where both public and private actors seek to shape the rules of the game which may or may not be conducive to peaceful competition and innovation. Our ambition is to connect these various levels – in particular, by assessing both the vertical dimension (e.g., ways of connecting individuals and the global through technology) and the horizontal dimension which connects various types of actors horizontally across borders – be they non-state or state actors, be they individual as citizens, activists, or corporate employees, be they experts or politicians. In doing so, we will aim to simultaneously analyse the economic and political spheres where these developments are played out. Ultimately, however, we are interested in the point where these different spheres meet and are redefined by technological disruptions – a point we call "the nexus"

Figure 3. The Issue Nexus

Macro-Global

Corporate Regulation & Tech Geopolitics

Regional & Global governance clusters. Global algorithmics

Economics

The Nexus

Politics

Eg Social Media for Social good and cross border action

Eg Transnational Citizenship and democratic empowerment

Micro-Individual
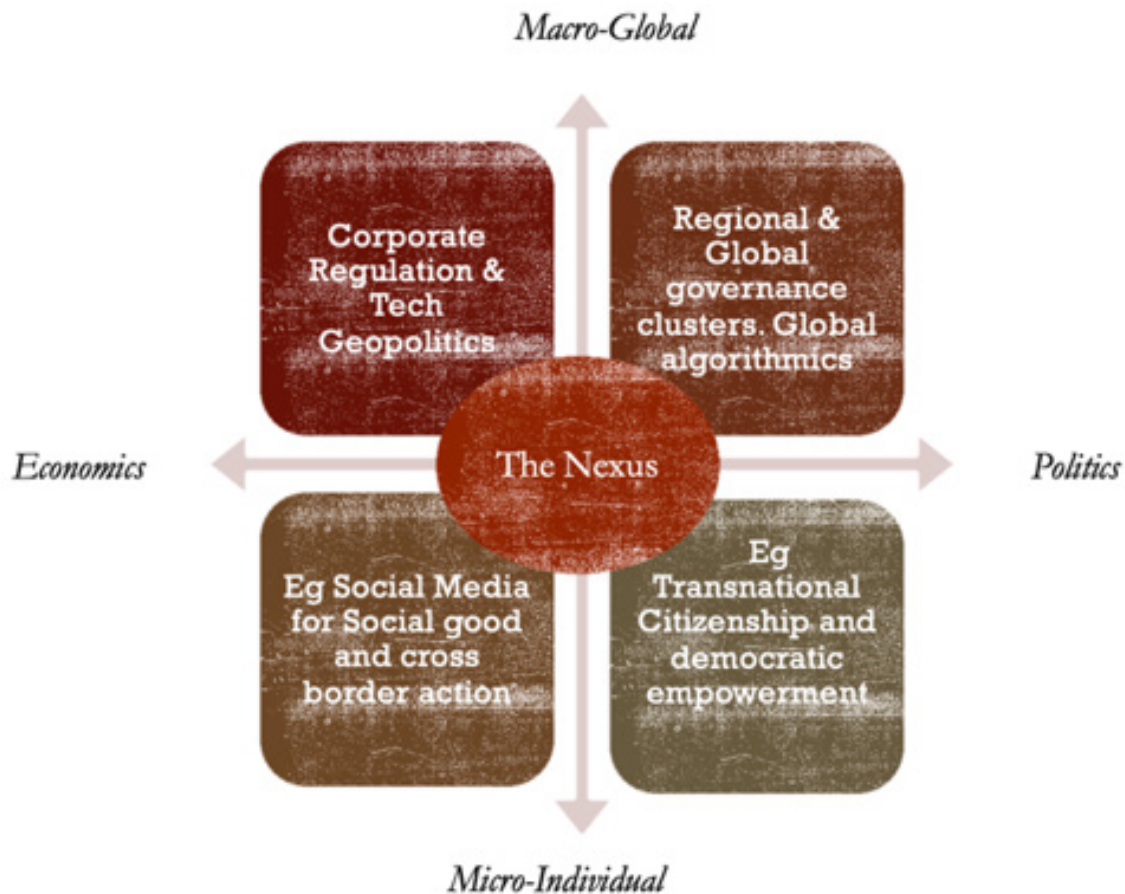
The PeaceTech tipping model

To navigate this vast landscape, we suggest a simple heuristic which we refer to as the "PeaceTech tipping model" grounded on the widespread sense that our human predicament at the beginning of the XXI century is on a knife-edge, with the bright and dark sides of disruptive technologies battling for our future. The great hopes for democratisation and peace that accompanied the diffusion of the open internet, were abruptly reversed with the rise of online violence, hate speech, and radicalisation. The potentials of social networks and telepresence for trust and empathy building across transnational communities of citizens are now confronted with deep-fake, disinformation, and polarisation. The opportunities for new democratic participatory processes and financial emancipation offered by digital identities and blockchain technology are confronted with issues of data ownership and power concentration. The potentials for peace of digital applications, satellites, drones for smart border control and early warning system are jeopardised by the shadow of surveillance state and surveillance capitalism. The unprecedent opportunities of the internet of things is undermined by the vulnerabilities of the cyber. The list goes on.

Figure 4. The PeaceTech Tipping Model
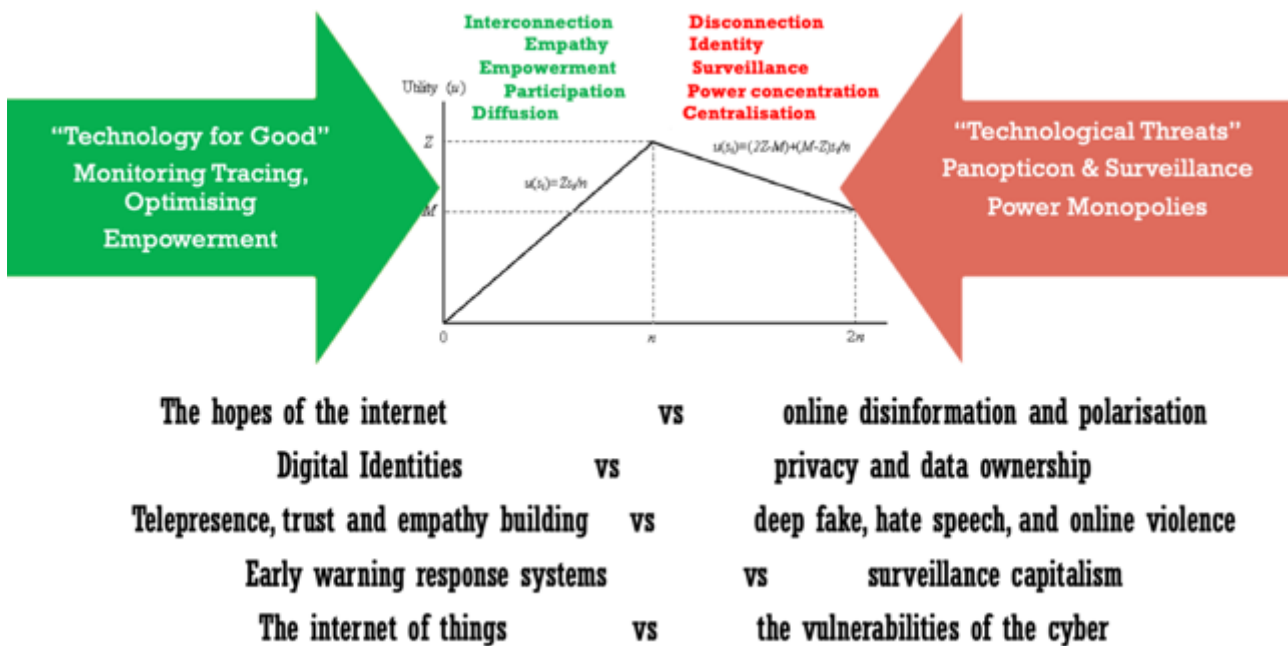
The tipping model captures a non-linear dynamic and tension in the societal effects of emerging technologies between positive and negative. This duality has to do with the dual face of power which is particularly present in this field and corresponds to the two faces of technology, e.g., technology-for-good, and technological threat. On one hand, technology can be the key to empowering individuals around the world and the weaker parties in conflicts or those kept outside the formal institutions of power. They can provide ubiquitous access to material and cognitive resources which in turn can strengthen peace by creating transnational communities of trust. On the other hand, technologies can be a means of power politics and cyberwarfare, and if appropriated by a few actors, can lead to a concentration of power benefitting certain firms or sectors or indeed certain countries to the exclusion of others. To the promise of unprecedented empowerment corresponds a fear of unprecedented power grab. Such dynamics may result from profit motives or a drive towards monopolising markets but can also be the result of expediency. Moreover, the hope that technology may offer bottom-up solutions to otherwise intractable problems at the local level ought to be balanced by the risks of generalised surveillance. Technological solutions simultaneously support the distribution of power throughout society (e.g., through diffuse networks), while also fostering its concentration (e.g., through intrusive surveillance).

We express this tension through the PeaceTech tipping model, where we ask, on the analytical level, what factors may lead to "tipping" technologies' potential for good as opposed to negative effects, and, on the prescriptive level, what strategies and regulations are best able to counter these effects and avoid the technological application to tip to the technological threat side. We call this the "tipping challenge". As mentioned, we believe technology is not neutral but deeply political. That is why a political approach to understanding and using technology is crucial in overcoming technology-associated challenges and promoting the wellbeing of societies.

The tipping model serves to highlight a number of risks and thus challenges to address. It also serves three additional purposes. First, it helps avoiding "tech-essentialising". While the world is full of new technological innovations that may become tools to solve conflicts peacefully, tools are not necessarily magic keys. This is related to tendencies of technological determinism already mentioned – the just-add-tech perspective that sees tech as independently driving social relations/structures.

This was a core issue in lots of early ICT-for-development thinking (e.g., laptops = education). We must assume that if human wellbeing can be promoted with the help of technology it can also be destroyed by it. What we need to ask is what is their tipping point: when and how can such and such technology be harnessed in ways conducive to peace and development rather than in ways that threaten human advancement?

Secondly, the tipping model emphasises complex thinking and avoiding incredible certitude, e.g., the routine tendency to offer exact predictions of policy outcomes, to shy away from expressions of uncertainty as if estimates did not usually rest on unsubstantiated assumptions and limited data. Because all actors operate under conditions of bounded rationality, we need to communicate the bounds of knowledge in the language of probability and sensitivity analysis thus mitigating the tendency to overselling. This is especially true when dealing with long-term impacts and policies.

Thirdly, the tipping model is useful tool to addressing unmitigated risks, e.g., the societal risks associated with the dual nature of power discussed above and the associated risks of surveillance, arbitrariness and the denial of self- government. Ubiquitous surveillance in particular often lurks behind efforts at monitoring conflict flares. Machine arbitrariness is a more subtle threat whereby our efforts to do away with human arbitrariness (say in allocating refugees from warzone across and within countries) are leading to the creation of algorithms powered by AI which may in turn lead to layers of decision-making protocol that lie beyond human comprehension. While we will be seeking to identify positive trends and contributions, we will always systematically assess the risks associated with the technologies we discuss. It is thus under the long shadow of such heightened risks that we propose to ask how new technologies can be used to create, support, and improve the quality of peace within and between nations.

Studying Global PeaceTech: mapping, analysis, action

Our approach to the development of the Global PeaceTech research agenda is based on three main steps: (1) mapping, (2) analysis and assessment, (3) action and policy recommendations. PeaceTech is not only an academic discipline but an ecosystem of start-ups, private companies, NGOs. The first step will be a rigorous mapping of all these initiatives in different domains, on a global scale.   Mapping can go both geographical and by technology type. The mapping will also organise the PeaceTech use cases and initiatives along the lines of negative or short-term peace and positive or long-term peace, to facilitate the study of policy responses in different time-horizons and domains.

The second research step will be an in-depth analysis and critical assessment of the PeaceTech use cases identified in the mapping. In order to do so, we need to investigate existing and alternative technologies and their corresponding modes of regulation. This will entail analysing not only the technical but also the political, legal, and ethical issues underlying the development of the tech-constellation, including the development and deployment of technologies on the ground, and the behaviour of actors involved. This will lead to an assessment of current regulatory models that mediate the interaction between tech-use and tech-user, and to the prescription of a coherent consolidated regulatory framework at the local, regional, and global level.

The analysis step should focus on three core elements as summarised in **Figure 7. Tech-use, tech-users, and tech-regulation.** Regarding tech-use, research can examine the potential as well as the risks associated with the use of certain technologies and how they contribute to key functions identified by the peace literature, such as empathy building, trust and verification, network building, information sharing, decentralisation, responsive governance. When examining tech-users, research can focus on how the use of technologies affects actors' behaviours (e.g., how people interact, which people interact). In the promise of using technologies to support peace and peacebuilding, we also have to think about how tools shape behaviour and how ideas shape these tools.

As for tech-regulation, a wide range of governance modes shall be reviewed, from no regulation, auto-regulation and self-regulation to political regulation, inter-regulation, and co-regulation, assessed on various levels (local, national, international, global). This includes questions related to the coherence of their structure (centralized, hierarchically decentralized, distributed, etc.), the relevance of their legal status (public institutions, non-governmental organizations, inter-governmental organizations, international alliances, independent agencies, etc.), and the legitimacy of their decision-making structures (uniform deciding body of policy-makers, multi-stakeholder committees, etc.). Particular attention should also be paid to the efficiency of their normative mechanisms: from industry common standards and shared good practices to soft law mechanisms (guidelines, directives and non-binding rules), hard law instruments (norms, binding laws providing for financial sanctions and individual prison sentences, sectorial and public-private agreements including independent observation bodies with sanction powers, etc.) and unconventional mechanisms (nudge strategies leveraging financial incentives, public opinion affecting companies' image and sales, strategic collaboration opportunities, etc.).

The last step will consist in translating the analysis into political action, with clear guidelines on best-practices and policy recommendations. The reasons for lack of action in this field may be multiple. Ideas may be incipient and not yet translated into action, through lack or resources and design capacity. Or a given technology may fail to spread and be adapted to different contexts, requiring intervention to diffuse peace innovations. Connections between analysts, activists and entrepreneurs need to be made and sustained. We must ask about unimagined possibilities, and what it will take for us to do the imagining and turn it into deeds. Ultimately, we aim to suggest action and policies to uncover and unleash the untapped potential associated with new technologies. Action can happen at different level. Some examples can be grassroot social campaigns, awareness and education initiatives, public investments in PeaceTech transnational projects. At the political level, change can be fostered through international policy dialogues, lobbying and civic engagement aimed at promoting the adoption of rules and regulations in favour of applications of technology for peace. More directly, we hope to contribute to building up a local, national and global PeaceTech movement, that can support organisations, tech businesses and start-ups that contribute to socio-economic development and peace through their activities both on the ground and through affecting governance.

IV. Areas, themes, and research questions

In this last section we outline some possible areas of research in Global PeaceTech that go beyond a narrow definition of PeaceTech as the employment of digital tools for peacebuilding. These areas lie at the heart of transnational politics, where research and debates are being fostered on how technology and its governance can play a key role in building the conditions for transnational peace. Some of these areas relate to what has been defined above as 'positive peace', i.e., the conditions for a stable transnational peace, and partly overlap with the sustainable development goals defined by the United Nations. Development and peace are closely intertwined (Zannier 2015). Not only peace and security are prerequisites for achieving sustainable development, but sustainable development provides the pathway to peaceful societies, and that is where innovation and sustainable technologies for peace can play a disruptive role in accelerating the achievement of SDGs. Global PeaceTech embeds the discussion on power distribution, inequalities, global citizenship, respect of human and individual rights, into the PeaceTech debate from the outset. This generates a new research agenda with new research questions at the intersection of peace studies and global governance, but it also goes in the direction of ensuring issues of fairness, inclusivity, and democracy remain salient in the study of PeaceTech. Below is a list of possible thematic focuses and research questions as proposal for further research in Global PeaceTech.

Theme 1. The Socio-Economics of Peace: Inclusivity And Sustainability

While Global PeaceTech starts from the ground up to assess and promote the use of new technologies at the local level, we ask how Peace is in part related to development and economic growth. A great part of the current research and practice on PeaceTech focuses on data gathering, mobilization and communications, while the uses of PeaceTech to support economic development is understudied. In an ideal world, digital and frontier technologies should enable us to deliver SDGs more effectively and help tackle global poverty for all so that no one is left behind (UNCTAD 2018, United Nations 2019). For this purpose, mainstreaming new technologies among ordinary users is essential. One example is the initiative led by the EPLF EssentialTech Center in Losanna, aimed at harnessing science and technology to drive sustainable development, humanitarian action and peace. The idea is to incorporate principles of sustainability and accessibility by design, so that technologies can be equally accessible in low- and high-income communities. A shift from technology that is designed for the West and "will be fine for the rest" to technology that is "designed for the rest" and is good for the West, being it cheaper and more sustainable, leading to a "globalization of good solutions" .

Technology cannot be the only focus in addressing problems. The opportunities afforded by innovation are accompanied by risks of greater inequality and exploitation which are great threats to peace. Leadership and cooperation are needed to overcome current inequalities in accessing frontier-digital tech. While some communities are living in a 5G world, many others can access only 2G. In many developing countries, only the most privileged people can access digital services. A big divide can be observed in the world's access to the most advanced technology. The current digital divide and its future manifestations are not driven by technological capability. It is possible to connect every person to the internet cheaply and easily; failure to do so is a consequence of political decisions and economic interests. This is significant because smartphones, satellites, and sensors allow people to observe the world from different perspectives and foster inter-dependence globally. This sense of inter-connectedness and inter-dependence shapes people's behaviour and changes business model. In addition to affordability, upgrading digital skills is crucial to enable people to get the maximum benefit from the new technological revolution. As a consequence of the digital divide, "urban, professional men experience an amplification of their existing privilege, whilst rural, disabled women experience an amplification of their relative disadvantage" (Hernandez and Roberts 2018). In addition to access and costs, safety is also a vital aspect of making technology available for all. People should feel safe and secure when engaging online. For instance, off-line violence can travel on-line in a way that further drives exclusion.

Possessing advanced technology in itself is creating or will create economical imbalance between countries. Concentrated AI/ML capability in the hands of corporations/countries will shift power balances. AI may change global economic power structures. Benioff argues that "today only a few countries and companies have access to the best AI in the world. And those who have it will be smarter, healthier, richer and of course their warfare will be significantly more advanced. (…) Those without AI will be less educated, weaker, poorer and sicker" (Butcher 2019). The digital divide both between developed and developing countries, and even within societies, is already one of the biggest obstacles for digital economy to flourish. It concerns both access to general services, e-commerce platforms and legal frameworks. Even the most developed countries experience huge gaps in data collection. Robotics, which is well on the rise, is highly concentrated in just few countries. Inequality in the world can be speed up by technological revolution in many policy areas: economic, financial, environmental. For developing countries a big challenge would create re-shoring production back to advanced economies in consequence of use of new technologies. Cheap labor force, which is their key comparative advantage, would lose its competitive edge. There are big gaps between high-income economies and those less-developed in all measures of innovation input and output, which will likely not diminish in the future. The lines of division clearly mark imbalances between different regions. According to Global Innovation Index, countries who are richer are more likely to have higher scores of innovation then the rest. The winner-takes-all dynamic, or 'the best vs. the rest',

is evidently on the rise. The IMF has already found out that in most of the countries only the most dynamic, productive and innovative firms could have risen their markups while the others did not. The OECD noted productivity boom among the top best firms, while the others have stagnated. It will have profound consequences for the global system and may cause more conflicts and a sense of injustice.

International Organizations are well aware of this problem (UNCTAD 2018). For example WTO Aid for Trade initiative is directed now to alleviate the digital divide. WTO countries decided not to impose custom duties on electronic transmissions until 2019, reduced tariffs on ICT products if a country concerned is a member of the WTO Information Technology Agreement, and within the framework of WTO Trade Facilitation Agreement inserted provisions on digital technologies. Most of the work of new technologies in trade is however done at the level of regional trade agreements. They are very different in their scope of regulation; The UNGA called for establishment of Commission on Science and Technology for Development. It has also established Inter-agency Task Team on Science, Technology and Innovation for the Sustainable Development Goals and launched Technology Facilitation Mechanism which was the result of the Addis Ababa Action Agenda for of the 2015 Third International Conference on Financing for Development. Science Technology and Innovation became also important component of the Paris Agreement on Climate Change regarding mitigation and adaptation efforts; Digital economy became also the subject of every G20 presidency, including separate ministerial conference; The OECD member countries plus number of others have signed Ministerial Declaration on the Digital Economy, Innovation, Growth and Social Prosperity. Among others it commits them to: reduction of barriers to investment and adoption of digital technology in all sectors, development of global technical standards that enable interoperability and a secure, stable, open and accessible Internet, adoption of technologically neutral frameworks that promote competition, use of open, transparent and inclusive processes to shape global Internet governance, reduction impediments to e-commerce within and across borders. Former NATO Secretary General, A.F.Rasmussen is currently promoting the idea to launch the World Data Organization based on the example of the WTO.

Rapid technological progress in AI and blockchain is about to transform existing business models. Companies are beginning to use new technologies to help manage their human resources, attract and promote the loyalty of clients and customers, and increase transparency in their supply chains. Application of AI and blockchain by companies to their operations provide better visibility and predictability; however, these efforts do not yet include human rights in their design. The mainstream business model where companies seek to lower prices at any cost to be competitive has caused "a race to the bottom" for their suppliers, who are generally located in the Global South, by increasing the productivity of the labour force and decreasing wages. This model has intensified the exploitation of children, enabled instances of modern slavery, and undermined health and safety conditions. There are even fewer initiatives that focus on sustainability, and these have largely been directed at environmental sustainability; so far little attention has been paid to the potential of AI to address labour and human rights issues. Here, the corporate power of giant tech companies which act as monopolies in commercialising the data created by masses will be examined for sustainable peace (Puschmann and Burgess 2013).

For instance, Tech/Peace/Development nexus Blockchain technology can be employed in many ways to improve international trade: to substantially reduce different trade costs; make trade paperless; facilitate business-to-government and government-to-government processes at the national level and thus open new opportunities in number of WTO areas; allow to rise new generation of services; impact insurance and e-commerce areas; help administer intellectual property rights and help fighting with counterfeits; track the origin of products; enhance government procurement process; build trust and enhance the transparency of supply chains; open up new opportunities for micro, small and medium-sized enterprises and small producers from developing countries. Thanks to blockchain technology cost reduction in the financial sector and the shipping industry range between 15 and

30 percent while the removal of barriers is estimated on more than 1 trillion USD of new trade in the next decade. These opportunities may only be realized if important technical issues like scalability, interoperability and legal challenges are addressed. Additionally, International Finance Cooperation sees Blockchain role in promoting financial inclusion, which creates opportunities for developing countries to leapfrog older technologies (Ganne 2018).

There has been much research on factors affecting peace and development and therefore the leverage point for tech-for-peace, including the need to include marginalized sections of society in order to address people's socio-economic grievances, promote social inclusion and raise the 'opportunity cost' of war and violence. Ultimately, we need to ask: what transnational material and regulatory infrastructures are needed to sustain and enable these innovations?

Concrete examples and questions include:

- How can digital and frontier technologies be used to facilitate poverty reduction, while ensuring that the benefits are accessible to all and that no one is left behind?

- As emerging technologies enable a revolution in how we collect and use data for humanitarian development, what are the big opportunities and challenges ahead?

- Assessing the untapped potentials of blockchain to provide financial access to populations in developing and conflict-prone regions, including the promotion of investments in local businesses (a form of micro credit without intermediaries).

- Using digital product identification and blockchain technology to establish transparent supply chains and make sure that no financial support is provided to local 'warlords', 'blood diamond' production and the like.

- Exploring the potential of decentralised and sustainable 'circular economies' through digital platforms (matching needs and demands). When products are designed, manufactured, distributed and eventually re-used in a 'cycle' this not only increases a society's resilience against financial and economic crises by making it less dependent on external resources, but also promotes its long-term sustainable development.

Theme 2. Peace and People on the Move: Humanitarian Responses to Refugees and Migration

Frontier technologies such as blockchain and AI have increasingly featured in various projects in recent years implemented by the UN agencies and humanitarian NGOs. This has been accompanied by biometric identification, mobile applications, and the analysis of data collected from mobile phones and social media. Humanitarian organisations working with the United Nations and its associated institutions have been at the forefront of these initiatives, with the encouragement of donor states and other agencies that provide funds. Examining the impact of the new transformative technologies in "empowering" people on the move is crucial. According to the UNHCR, there are 68.5 million forcibly displaced people worldwide. Of these, 4 million are internally displaced people, 25.4 million are refugees and 3.1 million are asylum seekers. There are also 10 million stateless people. Developing countries host 85 % of the world's displaced people. Various projects are currently underway to address the challenges arising from migratory movements and states' surveillance strategies. These include:

- Initiatives to provide refugees with digital identities;

- Research on the role of social media and mobile phone applications for the survival strategies of refugees, and for state surveillance/verification of asylum claims;

- Efforts to develop AI to predict migratory movements and guide authorities in the resettlement of

refugees;

• Drones for humanitarian purposes and border control;

• Facial recognition as a supply mechanism for biometrics and also for finding missing people and matching siblings, and;

• Mobile banking for cash transfers.

Refugees and migrants are increasingly making use of new technology to support their journeys. Yet there are concerns about the privacy of refugees, where the data is stored and how to avoid negative outcomes including the tracing of digital footprints of refugees to use against them. It is therefore crucial to ask how and when technological empowerment can have perverse effects. This raises concerns about how migrant and refugee data is being collected, where it is being stored, how people in vital need of assistance give their consent, how to establish data confidentiality, and what measures are taken to prevent people's data from being used against them. These serious political, ethical, and social questions have still not received a satisfying response.

The relationship between UN agencies and tech corporations is an essential topic of debate. From one hand, giant tech companies such as Google, Microsoft, Palantir, Mastercard collaborate with the UN agencies to provide digital infrastructure as could be seen in the agreement between UN World Food Programme and Palantir. On the other hand, there are many and mostly failed start-ups which aims to provide digital solutions for migrants and refugees through hackathons and other initiatives. For the giant tech corporations, their relations with intelligence and military industry/bureaucracy raise concerns, and transparency and accountability of these agreements are questioned to protect privacy and rights of vulnerable communities. For start-ups, majority of over 1500 applications for migrants and refugees are hardly used (Madianou 2019).

In many cases, there is no clarity about the outcomes of these technologies. Pilot projects are important to learn from these technologies. Most importantly, the dissemination of project findings, impact assessment, transparency, and collaboration are necessary if progress is to be made. These projects should be transparent, and the results of the pilot projects must be clear, measurable, and open to independent review. This is significant because sophisticated data mining techniques can be used for humanitarian purposes, however, as Letouzé, Meier and Vinck (2013) underlines, "relying primarily on biased-and-messy-data analysis by number crunchers who may have never set foot in the field to inform sensitive policy and programmatic decisions in conflict-prone or -affected contexts would indeed be like pouring hot oil on burning ashes". In other words, the concern is that "rushing to apply Big Data in such volatile and dangerous environments without fully understanding and addressing the associated risks and challenges—the non-representativeness of the data, the difficulty in separating 'the signal from the noise,' the larger challenge of modeling human behaviour, even the risk of misuse of such tools by oppressive regimes—may well end up spurring rather than preventing the spread of conflict" (Letouzé et al. 2013).

To simplify and address more specific lines of research, we can further subdivide this thematic area into three sub-areas pertaining Digital IDs, Smart Boarder Management Systems, and Blockchain for Refugees.

A) Identification and Digital IDs

Identifying people is one of the main challenges both in developing countries and in the humanitarian context. Over one billion people are estimated to not have an official identity and their lack of any identification hinders their access to basic services such as health and education as well as rendering them unable to open bank accounts and access the SIM cards necessary to benefit from new technologies. The utilization of blockchain, biometrics, and crypto technologies promotes globally verifiable information that can be used for the registration of births, voters, and refugees alike. It can

also be used to maintain education records and process financial transactions, among other uses. The 'right to a legal identity' is implied by the Universal Declaration of Human Rights and achieving this for all is a part of SDG 16.9. A legal identity promises to help individuals become 'bankable' and to access social and medical care, police protection, and other services. In the context of forced migration, identification is a primary means of population management. But question remains about what the best approaches to such digital identities are given the risk of appropriation of control by more powerful actors.

B)   Smart Border Management Systems

New technologies and border management is an emerging topic particularly in forced migration studies. Digital and frontier technologies are used to manage borders and control migratory movements by states, and the defence-military-intelligence industry provides high-tech tools to manage borders. The biggest arms sellers of the EU also offer "smart" border management tools (Akkerman 2016). "Smart border" constructed by the US at Mexico border (Ghaffary 2019) and the EU's digitalised border-management systems, including Eurosur and Eurodac, are of great interest in this regard. As satellites, drones and big data analyses push physical borders outwards, biometrics push borders inwards. The use of algorithms and artificial intelligence to decide on the asylum applications and confiscation of mobile phones of asylum-seekers and checkingtheir social media accounts at the border to verify their applications has become a daily routine of border management in the US and the EU. It becomes thus key to analyse the contradiction between the tech used by migrants for survival strategies and states for surveillance.

C)   Blockchain for Refugees

Various pilot projects are starting to make use of blockchain to support refugees. A particular focus of such initiatives is to provide services rapidly and to cheaply to facilitate payments and data protection and to support local businesses through cryptographic security without intermediaries, while also offering transparency and accountability. For instance, The United Nations World Food Programme (WFP) has introduced a pilot project called 'Blockchain against Hunger', deploying blockchain technology in Jordan's Azraq camp to make cash-based transfers to 10,000 refugees. WFP relies on biometric registration data provided by the UNHCR and refugees can shop from local supermarkets using iris scans; the system confirms the identity of the refugee in this way, checks their account balance and confirms the purchase. However, despite these claims, these projects are criticised as occurring in relative secrecy, not being transparent and open source. Also "the removal of intermediaries and altered power dynamics may result in unintended consequences that could endanger end users as well as future projects. Accountability may also be undermined through a lack of meaningful consent and engagement in project design from end users, which could exacerbate power imbalances between aid organisations and their beneficiaries and facilitate a surveillance-type system that could be used to harm, rather than help, vulnerable populations" (Coppi and Fast 2019).

Concrete examples and research questions in the area Tech for Humanitarian Responses, Refugees, and Migration are:

•   How can international donors, UN agencies, NGOs, and corporations work together to best understand the human security needs of various segments of migrants and refugee populations?

•   How can the international community work together to safely deploy digital and frontier technologies in humanitarian contexts and what are the best use cases for this purpose?

•   Technological progress may help to reach and track any person in need. It may offer them digital identities, mobile numbers, and bank accounts. But does this mean that people are empowered? Do all this progress provide a solution to poverty? And what are the risks?

Theme 3. The Politics of Peace: Power and Conflict

Fair and effective economic strategies sustained by economic innovation are not good enough. We know that peace rests on empowerment, citizen participation and ownership and ultimately, the amorphous concept of "good governance". Good governance in turn calls for both responsiveness, accountability and ultimately a democratic ethos on one hand, and responsibility, accountability and effectiveness on the other. In the end, peace and democracy are deeply inter-related in complex and subtle way discussed in normative IR and ranging from the way in which the peaceful resolution of disputes sustains or subverts existing orders to the way in which democracy is the core pre-requisite to peace. We aim to explore how new technologies can be used to open up new paths of constructive, non-violent change through democratic citizen participation and citizenship across borders. For instance, in recent years, many countries have released their official strategies on artificial intelligence (AI). This trend started with the US in 2016, followed by the United Kingdom (UK), Germany, France, the EU, Russia, Japan, China and United Arab Emirates (UAE). One shared concern of these official documents is the fear of "missing the boat" as technological progress brings rapid changes to society that are likely to affect directly the global balance of power, military strength, economic wealth, and social structures (Wentworth 2018). Thus, all these global powers focus on the areas in which they have a comparative advantage so as not to lose their superiority or permit others to overtake them in these areas—with little regard to the human rights risks of these actions. A clear approach to working with different stakeholders is crucial because governments are allocating millions of dollars to the promotion of AI systems and planned actions will be conducted through close cooperation between corporations, universities and states without any clear, legally binding ethical and social principles.

An IR perspective will also help the Global PeaceTech to examine the role of giant tech corporations in promoting peace technologies. The tech giants have been introducing themselves not only for-profit corporations but also as foreign policy players or humanitarian actors. Such an analysis is vital for peace promotion because corporations like Google, Microsoft, Shell send millions of Euros annually for lobbying activities and many tech corporations also have commercial links with security, military, and intelligence departments of various states (Gorwa and Peez 2019). As many of these tech corporations have higher revenues than many countries' GDP, the Global PeaceTech will examine these developments from the perspective of global negotiations to promote peace and dialogue. Global negotiations can be evaluated from different perspectives: inter-state relations between global North and South; corporation-state relations (e.g., Denmark's tech ambassador to Silicon Valley); and also, for societies to strengthen global civil society and the public sphere. For instance, the constitutional referendum in Iceland in 2008 was the first crowdsourced constitution where citizens engaged policy debates and offered proposals via Facebook and Twitter. The role of frontier and digital technologies also open new spaces for international and supranational organisations such as the UN and the EU to convince and mobilise states and corporations for the peaceful solution of conflicts and violence. However, peacebuilding processes face four major problems. These are the early warning problems, gaining local support for mediation of disputes, promoting reconciliation, and understanding across groups and promoting peaceful change under authoritarian settings. Peace should bring justice and social change. Technology can support the peacebuilding process to overcome these challenges if there is a political will.

Concrete examples and questions include:

A)   Conflict Prevention and Conflict Resolution

- Assess and compare the use of technology for early warning networks (see for instance WANEP and their WARN project in West Africa). Questions include: what data and data interpretation is most relevant for such systems? What are the repressive risks in aggregating information from the ground into coherent patterns? Who is responsible for acting on such information? Is the capacity there? What are the channels from warning to action and, crucially, to action by whom? Which existing networks and technologies can be re-purposed be- tween different categories of humanitarian emergencies, including epidemics as well as emergent conflict risks? How do you input mobile data in these contexts?

- Use of satellite imagery, drones, mapping, and AI for responding more effectively to emergency situations caused by armed conflicts or natural disasters. Establish safe and quick distribution systems of humanitarian aid, including food, water, medicine, and shelter, and coordinate the distribution of such basic goods with the help of AI for increased efficiency and effectiveness.

- Combine the intelligence of AI and (voluntary) citizens in the identification of fake news, hate speech, government propaganda etc. on social media outlets to restore public trust in the political system and/or peace process.

- Exploit the potential of digital platforms that use of crowdsourcing and geospatial information for conflict monitoring and the prevention of violence, such as violence before or after elections, fundamental human rights abuses, gender-based violence, and war crimes, based on direct digital reporting by its victims or bystanders.

- Use AI to analyse a variety of data sources from traditional and social media, reports, public speeches, and debates, etc. to predict the outbreak of armed conflicts and identify situations and political developments that present a considerable risk to human safety and the respect for fundamental human rights.

- Satellite surveillance and employment of drones for the monitoring of ceasefire agreements and humanitarian response in conflict zones.

- Investigate the use of digital platforms for increased citizen participation in peace negotiations: Making the peace negotiation process, i.e., selection of key negotiators, agreement of a time frame and formal procedures to follow and agenda setting, more transparent and participatory to increase its legitimacy and chances of successful implementation. Technologies that could assist mediators in supporting conflict resolution shall be examined as well.

B)   Strategic Environment

- The use of blockchain technology to create financial transparency of public income & spending. Fighting corruption and the complicity of state authorities with 'warlords' or criminal organizations and ultimately making governments accountable to their own citizens and international donors in how they spend their money (Orgad 2018, Reijers et al. 2022).

- The potential of AI and blockchain to increase transparency and the efficient use of natural resources by public and private enterprises. This may serve to prevent internal and cross-border resource conflicts (e.g., water, land, oil, minerals, etc.). Depending on the concrete case (e.g., Nile water conflict), satellite images and data could be employed for close monitoring and tracking of resource utilization; and AI could help in determining the resource's most 'intelligent' use and distribution. In the case of land ownership disputes, blockchain could create a transparent and fraud-resistant system and satellite monitoring could detect forceful resettlement of communities

and prevent the destruction of indigenous peoples' habitats.

Theme 4. Peace Mindsets: Trust and Awareness Across Borders

In the end, and coming back to the "Nexus", we need to go back to the individual level – across the socio-economic and political realm – and to the premise that peace starts in habits of the mind. Democracy may be the core foundation of peace but both democracy and peace in turn depend not only on institutions but on deep social foundations. Here, we propose to engage with the flourishing field of techno-democracy – grassroots transnationalism as it were, and connect insights from peaceful and peacebuilding societies. Much of the sustainability of peace depends on the extent to which parties can learn to trust each other – trust being perhaps the most precious yet elusive commodity on the planet. It is not enough to call for tolerance and the kind of 'truth seeking' and genuine empathy that are vital for peaceful coexistence. The question is how such trust is created and sustained. Peace education, the strengthening of international organizations, monitoring and control of ceasefire agreements and respect for fundamental human rights in fragile contexts are all key aspects to prevent the outbreak of violence and reconcile former enemy groups after conflicts. Ideally, people would trust in the peace process, often, however, control is necessary to restore lost trust. But issues of trust are also important closer to home in our western societies: trust is predicated on knowing each other and engaging in face-to-face conversations, shared experiences and struggles. How can we go back and forth between what we learn from polarization studies in western societies and dynamics in war-prone societies elsewhere?

Concrete examples and questions in this area include:

A)   Democratic Politics and the Rule of Law

- Use technology to empower citizens who seek to enforce the rule of law against corruption, suppression, and abuse of power.

- Make the participation in elections more transparent and physically safe through e-voting (you can vote from your home or abroad) to prevent voter intimidation, election violence and fraud. We will use the Estonian case as a template. Also, European donors promote biometric voter registrations (BVR) in Africa for liberal democracy promotion, which is supposed to provide free, fair and credible elections. Twenty-eight countries in Africa already use BVR (Jacobsen 2019).

- Explore the potential of digital direct democracy, i.e., electronic voting upstream on matters such as education, health care, infrastructure projects, spending of the public budget, the approval of new laws and regulations etc. to channel potentially violent dissent into political reforms and the search for compromises. The issue here is the balance between consultative and mandatory referenda as well as between upstream consultations about citizens' preferences vs specific outcomes.

B)   Peace and Democratic Mind-Sets

- Use technology to mobilize public support for peace by employing AI to analyse what 'enemy' groups share and what connects them with each other in spite of all the differences and disagreements across conflict lines.

- Regulate the use of frontier technologies such as AI, facial recognition, and automated data analytics to predict terrorist activities and strengthen counterterrorism capabilities of states to alleviate concerns about the limits of these measures to protect fundamental human rights (McKendrick 2019).

- Connect studies of political polarization in democratically established countries with the challenges of 'living with the enemies' in countries where peacebuilding is incipient. In the former, explore

the use of technology to de-polarize debate. In the later, give local people living in the conflict zones from both sides of the conflict the opportunity to tell their 'stories' through social media and memory banks on-line and how the conflict affects their daily lives to overcome ignorance and re-humanise 'the enemy'. Disseminate 'success stories' from other regions where reconciliation was possible (restore belief in the possibility of peace).

• Virtual reality and global awareness: Using virtual reality immersion for the purpose of global and sustainable peace. Research will analyse how Immersive Experience (using Virtual Reality and Augmented Reality Technology) can be used for futures foresight, and the making of agreements to promote peace.

• Performance games and the theatre of transformation: Train creative and non-violent conflict-solving and negotiation skills, create empathy for the 'enemy' through virtual role switching.

C) Transnational and Global Citizenship

• Beyond local theatres of peacebuilding assess the various ways in which social media and Apps/algorithm can help sustain agonistic (e.g., conflictual but not antagonistic) democracy by connecting individuals and groups with different world views across borders, thus creating the embryo of transnational democracy.

• Explore products/apps that help connect individual or local group action to macro-goals in particular the Sustainable Development goals.

• (Mathematical) Model(s) of Demoicracy and Peace Measurement Modelling frameworks: game theory, social network analysis, agent-based modelling, simulations (Schelling 1969). Can we prove, using a model, that demoicracy and peace models are more resistant (or susceptible) to network effect of (acceleration of) concentration of power?

Theme 5. Global Governance for Peace: Corporations, Governments and Capacity Building

Capacity building is a crucial component of harnessing digital and other frontier technologies in development efforts. Simply distributing laptops in a remote village in Peru is not a solution. Supporting teachers, receiving feedback from them, and building capacities will bring long-term results. It is necessary to focus on tailoring services to create an ecosystem for widespread uptake of technology. Here, bringing governments into the conversation is crucial if various barriers in regulation and governance-related issues are to be overcome. Digital can then be used as a leverage to accelerate inclusion. There is a need to be careful about government outsourcing and giving over responsibility to one large partner. Estonia, New Zealand and Singapore are great examples of government leading technology application and working well with the private sector to promote innovation-boosting economic competition. Importantly, these governments have developed internal expertise and mainstreamed it across their departments.

Cooperation between governments is a necessity. Even advanced countries face difficulties in dealing with global technology corporations—developing countries face a challenge of many orders of magnitude in this respect. Also, inter-connectedness might have a negative effect when fake, provocative news spreads among communities. Additionally, it is necessary to challenge various governments' attempts to control and limit peoples' access to digital technologies. Regulation can, after all, also lead to political control. For instance, a social media tax could be implemented for political purposes, and such a tax might hinder poor women from accessing online services. Here, digital diplomacy is gaining more importance in international politics.

Capacity building and cooperation require collaboration with the private sector as well. Governments need to up-skill themselves to the level needed to engage productively with the private sector. New business models can be introduced as a result of new technologies to connect people with others. The private sector is good at driving innovation for first adopters, but not necessarily for those most excluded (e.g., women or the poor). Incentives are a significant way to bring services to regions with insufficient infrastructure.

Ultimately, we want to ask about the global dimension of peace-through-tech. Of course, global norms and rules are no longer the purview of governments alone making decisions in closed off conclaves away for the scrutiny of citizens. Further research and analysis questions include:

- Do different organisations have unique roles to play in digital and frontier technology innovation in development and where should we focus our collaborative efforts?

- What should be the main principles to manage the relationship between tech corporations and governments/the UN agencies?

- How can the global governance of Tech support efforts at sustaining post-conflict peace as stated in the UN's SDGs?

- What is the role played by private enterprises and bottom-up market dynamics in shaping regional and global governance? Through what mechanisms and pathways do these actors' preferences percolate upwards to change the prevailing rules of the game? Qui bono – whose interests and values are best served by these emerging patterns of influence and how are these translated into new rules of the game?

- Most broadly, what kind of global governance – across international institutions - can best serve the needs of PeaceTech actors identified above?

Conclusion

Our aim in this paper is to inspire a new strand of research on what we label "Global PeaceTech," which will address the political effects that the innovative use and regulation of disruptive technologies can have in influencing patterns of global peace. Further research in Global PeaceTech, investigating the connection between emerging technologies and peace initiatives - from empirical and normative as well as technical and scientific perspectives- can help policy makers, companies and civil society expand their knowledge and expertise and suggest applied technological solutions for enhancing peace.

The expected social impact of the Global PeaceTech research agenda will also contribute to the UN's Sustainable Development Goals. We know that the UN is spearheading efforts to put new technologies at the service of its 17 Sustainable Development Goals, including the most amorphous one – peace - and has recently set up a blockchain committee for SDGs for instance. One of the UN core concerns is to ask what makes peace initiatives investable – whether they have a financial return or "only" a social return, and how such factors can be measured. This is a promising venue of application of the Global PeaceTech research.

One common objection is that the main factor affecting any given political process is the political will behind it, whereby technology is only an instrument, a tool to be or not to be used. We argue that tech is more than a tool, it is not neutral but deeply political and it influences users and political process as much as it is influenced by them. Emerging technologies (AI, big data, blockchain, digital identities, space tech) bear with them risks and opportunities for peace beyond the state. Ours is non-deterministic journey encountering emergent patterns that will affect us for decades to come.

Global PeaceTech promises to produce innovative research to better assess how to tap into the better angles of our nature and from there provide guidelines for policy decisions and regulations. Our hope is to inspire innovative research, in the sense of a 'laboratory' where new ideas and solutions can be incubated, and practice-oriented knowledge, through our 'scientific support centre' that makes research outputs readily available to professionals from the private and public sector, civil society, and policymakers in their respective fields of work. It will take many new ideas and initiative to create conditions truly conducive to peace on a local, national, and global scale worldwide. Global PeaceTech, we hope, will play its part.

References

ACLED. 2022. 'The Armed Conflict Location & Event Data Project' - https://acleddata.com/data-export-tool/, Retrieved 10 May 2022.

Agamben, G. 2005. *State of exception*. Chicago: University of Chicago Press

Akkerman, M. 2016. *Border wars: the arms dealers profiting from Europe's refugee tragedy.* Transnational Institute and Stop Wapenhandel.

Beniger, J. 2009. The control revolution: Technological and economic origins of the information society. Harvard university press.

Bigo, D. 2002. 'Security and immigration: Toward a critique of the governmentality of unease'. *Alternatives* 27(1_suppl): 63-92.

Bijker, W. E. 2012. *Social construction of technology* MIT Press.

Bleyer-Simon, K. 2021. 'Policies to tackle disinformation in EU member states'. European Digital Media Observatory.

British Council. 2016. 'Build Up. Innovative Peacebuilding in Syria. A Scoping Study of the Strategic Use of Technology to Build Peace in the Syrian Context' - http://creativeconomy.britishcouncil.org/media/uploads/files/Peacetech_Report_Web_En.pdf, Retrieved 24 May 2020.

British Council. 2018. 'Peace and Beyond: Reflections on building inclusive and sustainable peace' - https://www.britishcouncil.org/sites/default/files/j063_peace_and_beyond_essays_final_web_new_0.pdf.

Build Up. 2018. 'The Commons: Pilot Methodology for Addressing Polarization Online'. Build Up and MISTI

Build Up. 2019. 'Analysing refugee-host community narratives on social media in Lebanon'. Build Up and UNDP, Feb 2019

Build Up and British Council. 2016. 'Innovative Peacebuilding in Syria, A Scoping Study of the Strategic Use of Technology to Build Peace in the Syrian Context'. British Council.

Build Up and British Council. 2018. 'Innovative Peacebuilding in Syria 2, An Update on the Strategic Use of Technology to Build Peace in the Syrian Context'. British Council.

Bullock, J., Chen, Y.-C., Himmelreich, J., Hudson, V. M., Korinek, A., Young , M., & Zhang, B. (Eds.). 2022. *The Oxford Handbook of AI Governance*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780197579329.001.0001

Burns, R. 2014. Moments of closure in the knowledge politics of digital humanitarianism. *Geoforum* 53: 51-62.

Burns, R. 2015. 'Rethinking big data in digital humanitarianism: Practices, epistemologies, and social relations'. *GeoJournal*, 80(4): 477-490.

Butcher, M. 2019. World Economic Forum warns of Ai's potential to worsen global inequality. TechCrunch - https://techcrunch.com/2019/01/23/world-economic-forum-warns-of-ais-potential-to-worsen-global-inequality/?guccounter=1&guce_referrer_us=aHR0cHM6Ly90LmNvL1Q3Q2tOUkVzeEE&guce_referrer_cs=1zfSzsooZtS4pWgfDZQtiA, Retrieved September 14, 2022,

Castells, M. 2011. T*he rise of the network society.* John wiley & sons.

Caplan, R. 2019. M*easuring peace: principles, practices, and politics*. Oxford University Press, USA.

Cerf and Himelfarb. 2018. 'Can the peacetech industry save the internet?', 29/09/2018 - https://edition.cnn.com/2018/09/29/opinions/technology-harm-better-application-help-world/index.html. Retrieved 20 May 2022

Christoff, Z., & Grossi, D. 2017. 'Binary voting with delegable proxy: An analysis of liquid democracy'. *Proceedings of the 16th Conference on Theoretical Aspects of Rationality and Knowledge* (TARK): 134–150;

Cottray, O., & Puig Larrauri, H. 2017. 'Technology at the service of peace' - *https://www.sipri.org/commentary/blog/2017/technology-service-peace* .

Conway, M. 2017. 'Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research'. *Studies in Conflict & Terrorism* 40(1): 77-98.

Coppi, G., & Fast, L. 2019. 'Blockchain and distributed ledger technologies in the humanitarian sector'. HPG Commissioned Report.

Cowhey, P. F., & Aronson, J. D. 2017. *Digital DNA: disruption and the challenges for global governance*. Oxford University Press.

Croteau, D., & Hoynes, W. 2013. *Media/society: Industries, images, and audiences*. Sage Publications.

Cummings, M. L., Roff, H. M., Cukier, K., Parakilas, J., & Bryce, H. 2018. *Artificial Intelligence and International Affairs*. Chatham House Report, 7-18.

Eriksson, J., & Giacomello, G. (Eds.). 2007. *International relations and security in the digital age* (Vol. 52). London: Routledge.

Del Vicario, M., Zollo, F., Caldarelli, G., Scala, A., & Quattrociocchi, W. 2017. 'Mapping social dynamics on Facebook: The Brexit debate'. *Social Networks* (50): 6-16.

Duffield, M. 2012. 'Challenging environments: Danger, resilience and the aid industry'. S*ecurity dialogue* 43(5): 475-492.

Duffield, M. 2014. 'From immersion to simulation: remote methodologies and the decline of area studies'. *Review of African Political Economy* 41(sup1): S75-S94.

Fearon, J. D. 1995. 'The offense-defense balance and war since 1648'. *Annual meeting of the International Studies Association*, Chicago: 379-414.

Fisher, J. 2017. 'Reproducing remoteness? States, internationals and the co-constitution of aid 'bunkerization'in the East African periphery'. *Journal of Intervention and Statebuilding* 11(1): 98-119.

Firchow, P., Martin-Shields, C., Omer, A., & Ginty, R. M. 2017. 'PeaceTech: The liminal spaces of digital technology in peacebuilding'. *International Studies Perspectives* 18(1): 4-42.

Floridi, L. 2007. 'A look into the future impact of ICT on our lives'. *The information society* 23(1): 59-64.

Friis, K., & Ringsmose, J. (Eds.). 2016. *Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives*. Routledge.

Fritsch, S. 2014. 'Conceptualizing the ambivalent role of technology in international relations: Between systemic change and continuity'. *The Global Politics of Science and Technology* (1): 115-138. Springer, Berlin, Heidelberg.

Fritsch, S. 2011. 'Technology and global affairs'. *International Studies Perspectives* 12(1): 27-45.

Galtung, J. 1964. 'An Editorial'. J*ournal of Peace Research* 1(1).

Ganne, E. 2018. *Can Blockchain revolutionize international trade?* Geneva: World Trade Organization.

Ghaffary, S. 2019. 'The "smarter" wall: how drones, sensors, and AI are patrolling the border'. Obtenido de Recode - https://www.vox.com/recode/2019/5/16/18511583/smart-border-walldrones-sensors-ai.

Gorwa, R., & Peez, A. 2018. 'Big Tech Hits the Diplomatic Circuit: Norm Entrepreneurship, Policy Advocacy, and Microsoft's Cybersecurity Tech Accord'.

Graham, M., & Zook, M. 2013. 'Augmented realities and uneven geographies: exploring the geolinguistic contours of the web'. *Environment and Planning A*, 45(1): 77-99.

Guadagno, R. E., Nelson, M., & Lock Lee, L. 2018. 'Peace data standard: A practical and theoretical framework for using technology to examine intergroup interactions'. *Frontiers in Psychology*, 734.

Haidt, J., & Bail, C. 2022. *Social media and political dysfunction: A collaborative review*. Unpublished manuscript, New York University.

Hernandez, K., & Roberts, T. 2018. 'Leaving no one behind in a digital world'.

Himelfarb 2016. 'Girls, Tech, and the Sustainable Development Goals' - https://www.linkedin.com/pulse/girls-tech-sustainable-development-goals-sheldon-himelfarb/, 12/05/2016, Retrieved 20 May 2022

Hyman, P. 2014. '"Peace Technologies" enable eyewitness reporting when disasters strike'.

Innerarity, D. 2021. 'Making the black box society transparent'. *AI & SOCIETY* 36(3): 975-981.

Innerarity, D. 2022. *Controlling the Desire for Control: Machines, Institutions and Democracy. In Democratic Institutions and Practices*. Springer, Cham.

Jacobsen, K. L. 2020. 'Biometric voter registration: A new modality of democracy assistance?'. *Cooperation and Conflict* 55(1): 127-148.

Jervis, R. 1978. 'Cooperation under the security dilemma'. *World politics* 30(2): 167-214.

JustPeace Labs. 2017. 'Ethical Guidelines for PeaceTech' - https://justpeacelabs.org/services/ethics/

Kahng, A., Mackenzie, S., & Procaccia, A. 2021. 'Liquid democracy: An algorithmic perspective'. *Journal of Artificial Intelligence Research* (70): 1223-1252.

Kello, L. 2018. *Cyber threats*. In The Oxford Handbook on the United Nations.

Kello, L. 2021. 'Cyber legalism: why it fails and what to do about it'. *Journal of Cybersecurity* 7(1) tyab014: 1-15.

Keohane, R. O., & Nye Jr, J. S. 1998. 'Power and interdependence in the information age'. *Foreign Affairs* 77 (5): 81-94.

Khondker, H.H. 2011. 'Role of the new media in the Arab Spring'. *Globalizations* 8(5): 675-679.

Kissinger, H. 2014. *World order* (Vol. 9). New York: Penguin Press.

Klein, H. K., & Kleinman, D. L. 2002. The social construction of technology'. *Structural considerations. Science, Technology, & Human Values* 27(1): 28-52.

Kurban, C., Peña-López, I., & Haberer, M. 2017. 'What is technopolitics? A conceptual schema for understanding politics in the digital age'. *IDP. Revista de Internet, Derecho y Política* (24): 3-20.

Larrauri, H. P., & Kahl, A. 2013. 'Technology for peacebuilding. Stability'. I*nternational Journal of Security and Development*, 2(3): 1-15.

Letouzé, E., Meier, P., & Vinck, P. 2013. 'Big data for conflict prevention: New oil and old fires'. *New technology and the prevention of violence and conflict*: 4-27.

Leonard, M. 2021. *The Age of Unpeace: How Connectivity Causes Conflict.* Random House.

Lessig, L. 2009. 'Code: And other laws of cyberspace' - ReadHowYouWant.com.

Lynn-Jones, S. M. 1995. 'Offense-defense theory and its critics'. *Security studies* 4(4): 660-691.

Madianou, M. 2019. 'Technocolonialism: Digital innovation and data practices in the humanitarian response to refugee crises'. *Social media+ society* 5(3): 2056305119863146.

Mancini, F., Letouze, E. F., Meier, P., Vinck, P., Musila, G. M., Muggah, R., & O'Reilly, M. 2013. 'New technology and the prevention of violence and conflict'. International Peace Institute, UNDP, USAID (2013).

Maragh-Lloyd, R. 2020. *Safiya Umoja Noble, Algorithms of oppression.* NYU Press

Maxmen 2019, 'Can tracking people through phone-call data improve lives?'. *Nature,* 29/05/2019, https://www.nature.com/articles/d41586-019-01679-5 Accessed 20/05/2022.

Mayer, M., Carpes, M., & Knoblich, R. 2014. 'A toolbox for studying the global politics of science and technology'. *The Global Politics of Science and Technology* (2): 1-17. Springer, Berlin, Heidelberg.

McCarthy, D. R. (Ed.). 2017. *Technology and world politics: An introduction.* Routledge.

McKendrick, K. 2019. 'Artificial intelligence prediction and counterterrorism'. London: The Royal Institute of International Affairs-Chatham House, 9.

Meier, P. 2012. 'Do "liberation technologies" change the balance of power between repressive states and civil society?' (Doctoral dissertation, Fletcher School of Law and Diplomacy, Tufts University).

Miklian, J., & Hoelscher, K. 2018. 'A new research approach for peace innovation'. *Innovation and Development* 8(2): 189-207.

Morozov, E. 2011. *The net delusion: How not to liberate the world*. Penguin UK.

Morozov, E. 2013. *To save everything, click here: The folly of technological solutionism.* Public Affairs.

Niforos, M., Ramachandran, V., & Rehermann, T. 2017. 'Block Chain: Opportunities for Private Enterprises in Emerging Market'. Washington, DC. International Finance Corporation - https://openknowledge. worldbank. org/handle/10986/28962.

Nicolaïdis, K. 2017. 'Sustainable Integration in a Demoicratic Polity: A New (or not so new) Ambition For the European Union after Brexit. Brexit and Beyond', 212-221.

Nicolaïdis, K. 2019. 'Sustainable integration: The silver lining of a democratically challenged EU'. *Twelve Stars*: 117-126.

Nye, J. S. 2004. *Power in the global information age: From realism to globalization.* Routledge.

Nye, J. S. 2011. *The future of power.* Public Affairs.

O'Neil, C. 2016. *Weapons of math destruction: How big data increases inequality and threatens democracy*. Broadway Books.

Orgad, L. 2018. 'Cloud communities: the dawn of global citizenship?' *Debating transformations of national citizenship*. Springer, Cham, 251-260.

Pasquale, F. 2015. *The black box society. In The Black Box Society*. Harvard University Press.

PeaceTech Lab. 2022. 'What is peacetech' - https://www.peacetechlab.org/what-is-peacetech. Retrieved 17 May 2022

Pierskalla, Jan, And Florian M. Hollenbach. 2013. 'Technology And Collective Action: The Effect Of Cell Phone Coverage on Political Violence in Africa'. *American Political Science Review* 107: 207–24.

Puschmann, C., & Burgess, J. 2013. 'The politics of Twitter data'.

Reijers, W. Orgad, L., & De Filippi, P. 2022. 'The rise of cybernetic citizenship'. *Citizenship Studies*: 1-20.

Quihuis, M., Nelson, M., & Guttieri, K. 2015. 'Peace technology: scope, scale, and cautions'. *Building Peace* 5: 14-16.

Renda, A. 2019. 'Artificial intelligence: Ethics, governance and policy challenges'. CEPS Task Force Report.

Renda, A. 2020. 'Europe: Toward a Policy Framework for Trustworthy AI', in Markus D. Dubber, Frank Pasquale, and Sunit Das (eds), *The Oxford Handbook of Ethics of AI* (2020; online edn, Oxford Academic, 9 July 2020).

Searle, J. R., & Willis, Y. S. 1995. *The construction of social reality*. Simon and Schuster.

Schaub, M., & Morisi, D. 2020. 'Voter mobilisation in the echo chamber: Broadband internet and the rise of populism in Europe'. *European Journal of Political Research* 59(4): 752-773.

Schelling, T. C. 1969. 'Models of segregation'. *The American economic review* 59(2): 488-493.

Schwanen, T., & Kwan, M. P. 2008. 'The Internet, mobile phone and space-time constraints'. *Geoforum* 39(3): 1362-1377.

Schwarz, E. 2019. 'Günther Anders in Silicon Valley: Artificial intelligence and moral atrophy'. *Thesis Eleven*,153(1): 94-112.

Searle, J. R., & Willis, Y. S. 1995. *The construction of social reality*. Simon and Schuster.

Solon. 2018. 'Facebook struggling to end hate speech in Myanmar, investigation finds'. *Guardian,* 16/08/2018 - *https://www.theguardian.com/technology/2018/aug/15/facebook-myanmar-rohingya-hate-speech-investigation*.

Stauffacher, D., Drake, W., Currion, P., & Steinberger, J. 2005. 'Information and communication technology for peace: The role of ICT in preventing, responding to and recovering from conflict'. United Nations/ICT Task Force.

Toyama, K. 2011. 'Technology as amplifier in international development'. *Proceedings of the 2011 iConference:* 75-82.

Turkle, S. 2016. *Reclaiming conversation: The power of talk in a digital age*. Penguin.

United Nations. 2019. 'The impact of rapid technological change on sustainable development'. Report of the Secretary-General, ECN.16/2019/2, 4.03.2019

UNCTAD. 2018. 'Technology and Innovation Report', 2018. Harnessing Frontier Technologies for Sustainable Development, United Nations Conference on Trade and Development, Geneva..

Van Evera, S. 1998. 'Offense, defense, and the causes of war'. *International Security* 22(4): 5-43.

Weidmann, Nils B. 2015. "Communication Networks and the Transnational Spread of Ethnic Conflict'. *Journal of Peace Research* 52: 285–96.

Wendt, A. (1995). Constructing international politics. International security, 20(1), 71-81.

Wentworth J., Kenny C., Harriss L., Miller J., Border P., Bunn S., Saleh Z., 2018. 'Topics of interest', 2018, House of Parliament PostBrief, Number 27, January 2018 - https://researchbriefings.files.parliament.uk/documents/POST-PB-0027/POST-PB-0027.pdf. Retrieved 14 September 2022,

Wu, T. 2017. *The attention merchants: The epic scramble to get inside our heads*. Vintage.

Zannier. 2015. 'Fostering Peace and Sustainable Development', United Nations - https://www.un.org/en/chronicle/article/fostering-peace-and-sustainable-development. Retrieved 24 June 2022].

Zuboff, S. 2019. *The age of surveillance capitalism: The fight for a human future at the new frontier of power*: Barack Obama's books of 2019. Profile books.

Table 1. Examples of (Global) PeaceTech applications

Use of cell phones and social media to increase communication and achieve "inter-group bridging" (e.g. PeaceDirect's Platform4Dialogue)	Data aggregation/visualization to report human rights abuses (e.g. Syria Tracker; Eyes on Darfur)
Use of web platforms to crowdseed information on existing conflicts and to fight disinformation	AI-powered conversational bots to enable peacebuilding in war zones.
Use of drones for de-mining	Smart Border Management Systems
Deployment of AI in cyberwarfare, to launch/ prevent cyberattacks on civilian and military targets	Big Data for Network Analysis of terrorist groups
Machine learning to detect and police violence in the online environment..	Use of digital technology to protect civilians in conflict zones
AI-assisted consultations for peace processes.	Open-data access for peacebuilders
Blockchain technology and smart contracts for humanitarian aid	Digital Education and computer gaming for peace
Network analysis for intelligence and conflict resolution. For example, Kate Keator, Manager of the Syria Conflict Mapping Team at The Carter Center, ran big data through an open source social network analysis software Gephi to model the complex relationships of armed groups in Syria's Aleppo Governorate	. Use of big data and facial recognition to identify potential terrorists; reliance on machine learning algorithms for predictive peacekeeping (e.g., SAGE), predictive policing and prevention/anticipation of violence or social unrest
Use of web-based platforms to increase political accountability and monitor/report corruption (e.g., Ushahidi in Kenya and Indonesia)	Web-based platforms oriented towards promoting peace-oriented innovation (e.g., PeaceTech Exchange, or PTX)
Use of content moderation to prioritize conciliatory messages over hate speech and enable sentiment analysis (e.g., "peace bots"). As an example, the Data-Pop Alliance used machine learning algorithms to analyse Facebook data and determine how residents of Botswana feel about the police and corruption	Use of big data exchanges for humanitarian purposes. A good example is the the Humanitarian Data Exchange. Big data analytics for mediation. The UN reports that data analytics tools currently used in mediation contexts include Crimson Hexagon, Crowdtangle, DataminR, Europe Media Monitor, Factr, Google Analytics, Hootsuite, Storyful, Sysomos, Talkwalker and Twitterfall
Early Warning Systems against violence and abuses	Satellite imagery for smart border control and human rights protection
Telepresence and digital communication for empathy and trust building across borders	Matching algorithms for asylum seekers management

Table 2. The expected impact of the Global PeaceTech research agenda

Research	Output	Actions	Application
Mapping of PeaceTech use cases Tech/PeaceTech Assement	Identification of PeaceTech that works	Investments	Private and Public Investors
Regulatory options assessment Forecast and simulations with different regulatory models Study of other normative instruments, educational activities and awareness campaigns	Study of the options to regulate tech in a way that favours peace	Regulation	Institutions / Policymakers
Pilot project proposals Prototyping and scale	New ideas for innovative use of tech for peace	Transformation	Industry / companies / civil society

Table 3. Analysis and assessment of peace technologies

Objects of analysis	Level of analysis	Description
Tech-Use	Technical	Development and deployment of technologies for peace on the ground
Tech-Users	Behavioural/Ethical	The behaviour of actors involved and emergent ethical and political dilemmas
Tech-Regulation	Legal/Normative	A coherent consolidated regulatory framework at the local, regional and global level

Authors

Prof Kalysp Nicolaidis

Chair of Global Affairs

School of Transnational Governance (EUI)

kalypso.nicolaidis@eui.eu

Michele Giovanardi

Coordinator of the Global PeaceTech Hub

School of Transnational Governance (EUI)

michele.giovanardi@eui.eu