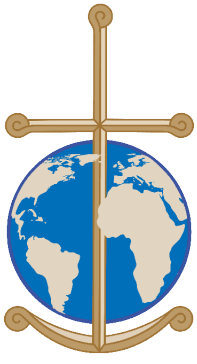
THE CARITAS IN VERITATE FOUNDATION WORKING PAPERS
"The City of God in the Palace of Nations"

Human Fraternity in Cyberspace

Ethical Challenges and Opportunities



With a selection of recent documents on the Church's engagement on cyberspace

www.fciv.org
Editors: Alice de La Rochefoucauld and Stefano Saldi
Electronic document preparation by Margarete Hahnen
Published by FCIV
16 chemin du Vengeron, CH-1292 Chambésy

ISBN: 978-2-8399-3461-9

EDITORIAL

AMBASSADOR AMANDEEP SINGH GILL
Project Director/Chief Executive Officer, International Digital Health & AI Research Collaborative (I-DAIR)
Former Executive Director of the United Nations High-Level Panel on Digital Cooperation

In his Encyclical Letter *Laudato Si'* of 2015, Pope Francis recalled Saint Francis of Assisi's care for Mother Earth, "our common home", akin to a "family" with whom we share our life.[1] This notion rhymes across many cultures and spiritual traditions. In the ancient Indian dictum "*Vasudhaiva Kutumbakam*", the sage declares: "the whole world is my family".[2] The first astronauts, who looked out of the porthole at the beautiful blue dot that is our planet, must have felt a similar emotion of oneness and belonging. All of humanity shares a common living space along with the wonders and vulnerabilities that go with this inescapable fact.

All of humanity shares a common living space along with the wonders and vulnerabilities that go with this inescapable fact.

Historically, this idea of "commonness" has been practically divided into specific domains: pastures and fallow lands shared by rural communities, river waters shared across borders, maritime commons beyond the reach of cannon balls, and so on. A rich body of knowledge, law and practical guidance has developed around each of these "commons" and their lay users and expert practitioners routinely and systematically feel its normative effect. Mishaps, for example ships running into each other, and mischief, such as sewage being discharged into water sources, are discouraged while responsible use is promoted under the rationale of common good.

In modern times, the laws of the commons for outer space and the seas have grown in sophistication and importance as has the need for impartial normative frameworks. International conventions and bodies such as the UN Convention on the Law of the Sea (UNCLOS) and the International Tribunal on the Law of the Sea (ITLOS) have come into being. Promotional work and capacity building for the good use of the commons has become a priority, for instance through the UN Committee on the Peaceful Uses of Outer Space (UNCOPUOS) in Vienna.

In parallel, a global consciousness has developed as means of communications and transport have brought people living in different parts of the world much closer. News channels beam images of tragedies and triumphs from across the globe into our living rooms. We can feel the ripple effects of faraway events on our pension funds, on our weather and on our health. Civic action, for long a very local phenomenon, has developed a transboundary character through movements such as the climate change related Extinction Rebellion.

Even though it is manmade, an interesting candidate for joining the ranks of global commons is the digital realm.

In sum, we live amidst a number of commons, some more tangible than the others, almost all bestowed on us by nature. Even though it is manmade,

an interesting candidate for joining the ranks of global commons is the digital realm. Its importance has grown exponentially since the internet protocols were invented in the 1970s and especially since the World Wide Web was offered by CERN scientists as a global public good in 1989. Our lives are unimaginable today without the countless services facilitated by digital networks and devices. The COVID-19 pandemic was a stark reminder of this dependency.

Our lives are unimaginable today without the countless services facilitated by digital networks and devices. The COVID-19 pandemic was a stark reminder of this dependency.

In military parlance (unfortunately) cyber has already joined land, air, sea and space as a domain for offensive and defensive actions. Societally, we have become used to meeting people 'on Internet' and working or playing with them. The virtual metaverses imagined by the Silicon Valley tech giants might still be decades away but there is no denying that a significant global population spends a large part of its waking hours roaming this domain.

The digital world is also witnessing a familiar tragedy of the commons. In the manner of the badly governed commons of the past, criminals and buccaneers of all sorts abound. Digital pirates cross boundaries to wreak havoc at will. Data is extracted and exploited unfairly and personal privacy and wellbeing is subordinated to commercial advantage. States are often helpless or clueless about what goes on in the digital realm and how to police it. The regulatory tools at their disposal were designed for a pre-digital world and are either ineffective or too blunt. Truth be told some actors do not actually mind a degree of lawlessness as they pursue narrow or monopolistic goals even if this poisons the well for everyone in the long run.

As this publication powerfully argues, a global commons approach to the digital realm makes eminent sense to prevent lawlessness and promote good use.

As this publication powerfully argues, a global commons approach to the digital realm makes eminent sense to prevent lawlessness and promote good use. There is a lofty ambition in Article 1 of the 1967 Outer Space Treaty - "The exploration and use of outer space […] shall be the province of all mankind."[3] Could this guiding principle be extended to the digital realm, which in many ways is already the province of all mankind?

Could we take another leaf from that book? The international community took an important preventive step through the Outer Space Treaty by banning nuclear weapons and other weapons of mass destruction from outer space. This prevented terrestrial conflict from extending into outer space. While efforts to prevent an arms race above our planet continue, they rest, at the very least, on a solid foundation.

While it might be too late to uninvent cyber weapons, there might be value in restricting their use, say against critical civilian infrastructure and electoral institutions, and declaring certain parts of the digital commons as sanctuaries protected from cyber conflict. It might also be valuable to turn humanity away from developing autonomous weapons systems that can take life on their own without human control and accountability. This precautionary principle is inspired not only by the outer space commons but also by others from the environmental and health domains.

What ultimately makes a commons is the aspect of use. A commons walled off to everyone will soon be a ruin. And walled gardens for the select few are clubs and not commons. Therefore, in addition to the regulatory and control aspects, we must pay attention to promoting common benefit as well as inclusiveness in the use of the digital commons. We need both guard rails and common rails in the form of public goods.[4] In practical terms it means bringing "missing" users and information into the commons, and avoiding "missed" use due to lack of interoperability and other enablers in addition to preventing "misuse" through norms and other rules of the road.

At its most basic level, the "3 Ms" approach requires a renewed effort to bridge the digital divide.[5] The half of humanity that does not have access to cyber space must be enabled to participate in the digital commons. This access must be affordable and meaningful. If the next billion to come online from Africa, Asia and Latin America can only use social media, games and entertainment on their devices, they would not be able to truly benefit from the transformative power of the digital domain. They will remain forever trapped in a low-value segment of the digital economy as mere consumers of content made by others for the benefit of others.

Beyond meaningful and affordable access, we also need agency over the data economy. This means going beyond the data protection paradigm to a data empowerment paradigm.[6] The protective effect of giving informed consent to data collection at the outset of signing up for a digital service gets eroded if consent for data sharing with third parties is collected in advance and in broad terms. Separating consent to collect from consent to share can open new avenues for citizens to participate in the digital economy. This can also help startups and small firms reach a more equal footing with the big tech giants.

The digital commons of the future would also require distributed digital architectures and data infrastructures that level the playing field for all users. Today, bar a handful of tech companies and research institutions in high income countries, researchers working with large data sets and artificial intelligence (AI) have limited access to high performance computing and cloud capacity. A federated infrastructure that would help develop capacities closer to where the use is, promotes collaboration and allows local data to first serve local needs will be critical.[7]

Ultimately, building an inclusive digital future requires that the opportunity to build be also inclusive. Leveling the knowledge-making playing field is the real test of our intentions and rhetoric on inclusiveness, diversity and equal opportunities. If knowledge-making remains limited to a few, if 'problem-solvers' take data from 'problem-owners' to develop solutions, the digital commons we are hoping to build will fall short of Pope Francis' touchstone of the human family. In a family, no one gets left behind. We build others to build ourselves because in their strength is our strength.

If knowledge-making remains limited to a few, if 'problem-solvers' take data from 'problem-owners' to develop solutions, the digital commons we are hoping to build will fall short of Pope Francis' touchstone of the human family.

Mahatma Gandhi gave us a talisman years ago to weigh our actions when in doubt. Recall the face of the weakest, the most wretched person you know, and ask yourself if what you do will help that person. Then act. As we set out to build the digital commons it is worthwhile asking who we are building it for, why and with whom.

This publication presents some outstanding reflections to get us started. It eschews the "technocratic paradigm" and fosters the "culture of encounter and interdisciplinary dialogue." It is hopeful about a better world "thanks to technological progress, if this is accompanied by an ethic inspired by a vision of the common good, an ethic of freedom, responsibility and fraternity, capable of fostering the full development of people in relation to others and to the whole of creation."[8]

It is hopeful about a better world "thanks to technological progress, if this is accompanied by an ethic inspired by a vision of the common good, an ethic of freedom, responsibility and fraternity, capable of fostering the full development of people in relation to others and to the whole of creation."

Notes

1. Pope Francis, Encyclical Letter *Laudato Si'*, 24 May 2015
2. Maha Upanishad, date unknown
3. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, UN General Assembly Resolution 2222 (XXI), 19 December 1966
4. Amandeep S. Gill, "Imagining the AI Future", *The Survival Editors Blog*, 2 January 2020
5. Amandeep S. Gill and Stefan Germann, "Conceptual and Normative Approaches to AI governance for a global digital ecosystem supportive of the UN Sustainable Development Goals (SDGs)", *AI and Ethics*, 6 May 2021
6. Vikas Kathuria, "Data Empowerment and Protection: Concept and Assessment", Observer Research Foundation. *ORF Issue Brief* No. 487, 12 August 2021
7. Amandeep S Gill, "Realising the promise of digitally-enabled health", *Globe*, 6 April 2020
8. Pope Francis, Address to the participants at the meeting on "Common Good in the Digital Age", 27 September 2019

METHODOLOGICAL NOTE

ALICE DE LA ROCHEFOUCAULD
Former Director, Caritas in Veritate Foundation
STEFANO SALDI
Attaché for International Security and Disarmament, Permanent Mission of the Holy See to the United Nations and Other International Organizations in Geneva

Cyberspace represents a relatively new domain for interactions among peoples and among States. As the line between security and peace, as well as between civilian and military applications, becomes increasingly blurred, it would be opportune and beneficial to agree at the international level on shared norms to guide actions in cyberspace.

In the first part of this publication, the ethical challenges and opportunities of creating forms of human fraternity in cyberspace are presented. In particular, the concept of "common heritages of mankind", just as it is found under international law in relations to cultural patrimonies, biodiversity, outer space, seabed and ocean floors, is proposed as relevant and useful for characterizing the cyber domain.

In this regard, it is proposed that it would be helpful to think of cyberspace as a kind of global commons, where all of us enjoy certain basic rights. Here as elsewhere, we also have responsibilities; there are fundamental limits that must be observed in the interests of our common humanity. To this end it can be instructive to reflect for a moment on the norms that by international agreement guide our activities in other, related common domains.

This is particularly important as cyberspace is increasingly becoming another ground of confrontation among States. What would be preferable is that cyberspace remains a "safe haven" reserved exclusively for peaceful purposes, cooperation and mutual enrichment at the service of the common good. In this regard, this publication suggests that these noble objectives would only be achievable if cyberspace is shaped by a solid normative framework rooted in international law and ethics.

Challenges, both from the perspective of the *jus in bello* as well as the *jus ad bellum*, are addressed, as well as the complexity of agreeing on common definitions. For these reasons, the clarification of existing norms or the elaboration of new laws is urgent, but this process has to be rooted in a solid ethical background. Without it, this task would be blind or motivated merely by the logic of utility or particular interests.

The second part of the publication, instead, focuses on the engagement of the Catholic Church and its institutions vis-à-vis the issues raised by the emergence of digital technologies. While the "digital world" we live

in is the product of extraordinary achievements brought about by human ingenuity, it is urgent for States to establish a normative legal framework to develop a culture of responsibility as well as an ethics of fraternity and peaceful interactions in the context of cyberspace, so as to foster intellectual growth, access to education, peace and mutual enrichment.

Lastly, in the conclusions, without forgetting the cyber divide experienced by too many people in the world on a daily basis, and the need of capacity building, it is reiterated that cyberspace truly is a new territory and a virtual sovereign space, within which relationships are woven, bonds and obligations are established and policies are outlined. What is most concerning, however, is that what was initially experienced as an expression of freedom and relationship, has resulted in a field characterized by expansion without verification and possibility of control, limitless sharing of volumes of information, the fear for maintaining the integrity of one's identity, the risk of losing personal data, and the primacy of technology over knowledge.

Indeed, once again, it would be highly desirable, and to the benefit of all humankind, to consider cyberspace as a neutral ground or a global commons, that could contribute to mutual understanding among peoples by promoting dialogue and a culture of encounter. In this regard, by building bridges of relationships, the Church can continue to offer its expertise, not by standing in judgment of society, but rather by helping unite people.

SECTION I - HUMAN FRATERNITY IN CYBERSPACE: ETHICAL REFLECTIONS ON THE CHALLENGES AND OPPORTUNITIES

HUMAN FRATERNITY IN CYBERSPACE: ETHICAL CHALLENGES AND OPPORTUNITIES

A *Caritas in Veritate* Foundation Report

PROF. DOMINIQUE LAMBERT, UNIVERSITY OF NAMUR
PROF. GREGORY M. REICHBERG, PEACE RESEARCH INSTITUTE OSLO
DR. EVA THELISSON, AI TRANSPARENCY INSTITUTE
REV. FR. ANTOINE ABI GHANEM

1. Introduction

Since the advent of digital media,[1] it has become customary to speak of "cyberspace", namely as a sphere (or domain) in which human beings communicate with one another via computer-to-computer electronic transmissions. The World Wide Web (Internet) is most closely associated with this flow of communication, but other digital connections are also operative: proprietary communication networks, memory devices that are physically transported by human agents from computer to computer, wireless transmission via satellites, etc. The flow of electronic data has two main purposes: to facilitate the exchange of thought between human beings and to enable remote human control over physical systems (e.g., electrical power grids, manufacturing processes, household appliances, mobile telephone systems, to name just a few of the many applications which range from the mundane to the cutting edge of science).

In every corner of the globe, human beings have increasingly become dependent on digital media to manage their daily lives. Because digital communications are now the *lingua franca* of contemporary knowledge-sharing, commerce, and social relations more generally, it is vitally important that all people have access to this technology. The Internet can make a significant contribution to human life. It can foster prosperity and peace, inspire intellectual growth, contribute to mutual understanding among peoples. The benefits are many, but so too are the actual and prospective harms.

The Internet can make a significant contribution to human life. It can foster prosperity and peace, inspire intellectual growth, contribute to mutual understanding among peoples. The benefits are many, but so too are the actual and prospective harms.

Digital surveillance platforms infringe on the privacy and security of individuals and communities, while the circulation of disinformation and hate speech have found a potent means of transmission in cyberspace. Perhaps most worrisome, a new arena for competition and conflict has emerged. Military professionals now speak of "cyberspace" as a battlefield "domain" alongside the traditional domains of land, sea, air, and outer space. While it might have been hoped that cyberspace could be preserved as a global common for peaceful interactions, this regrettably has not happened.

Furthermore, there are no agreed upon "rules of engagement" in this new and nebulous form of warfare. Much as we might wish to turn the clock back, we cannot ignore this new form of militarized confrontation. Here, as elsewhere, the requisites of our shared humanity, of ethics and peace, make it imperative that together we recognize what norms are applicable in this domain. Reaching a global consensus on how best to limit the grave risks of cyberconflict is in the clear interest of us all, wherever on the globe we might find ourselves. The reflections that follow have for aim to foster better understanding of these risks and to encourage concerted action toward their reduction.

Reaching a global consensus on how best to limit the grave risks of cyberconflict is in the clear interest of us all, wherever on the globe we might find ourselves. The reflections that follow have for aim to foster better understanding of these risks and to encourage concerted action toward their reduction.

Reflecting on knowledge-seeking as a collective pursuit, seven hundred years ago the poet-philosopher Dante postulated that peace is the pre-requisite for achieving our full potential in this domain. "Humankind," he wrote, "readily attends to this activity [of seeking knowledge] in the calm or tranquility of peace."[2] Our minds are so constituted that no one individual or social group, however culturally refined they may be, can achieve, without the others, the perfection of which we are humanly capable. Dante thus conceptualizes the optimal condition of humanity as a state in which knowledge is freely communicated among all members of our kind. Peace is at once the condition and the outcome of this sharing.

In the inaugural Post-Synodal Apostolic Exhortation of his Pontificate, *Evangelii Gaudium*, Pope Francis said that "progress in building a people in peace, justice and fraternity depends on four principles related to constant tensions present in every social reality" (§221). One of these principles is particularly important for our purpose: "unity prevails over conflict" (§226 et sq.). How to maintain unity within – and between – the manifold communities that make up our world is of paramount importance today, especially when powerful forces of polarization are pulling us apart. How our communications in cyberspace can enhance fraternity across the globe, and what should be done to forestall destructive uses of these same technologies, is what motivates the ethical reflections that follow.

How to maintain unity within – and between – the manifold communities that make up our world is of paramount importance today, especially when powerful forces of polarization are pulling us apart. How our communications in cyberspace can enhance fraternity across the globe, and what should be done to forestall destructive uses of these same technologies, is what motivates the ethical reflections that follow.

2. Towards a Cyber Commons for Humankind

Cyberspace represents a new domain for human interaction.[3] Our interactions will prove to be beneficial in the measure that we can agree on shared norms to guide us in this domain. It can be helpful to think of cyberspace as a kind of global commons, where all of us enjoy certain basic rights. Here as elsewhere we also have responsibilities; there are fundamental limits that must be observed in the interests of our common humanity. To this end, it can be instructive to reflect for a moment on the norms that by international agreement guide our activities in other, related "common" domains.

The Preamble of the 1982 United Nations Convention on the Law of the Sea reaffirms what the UN General Assembly had already declared (Cf. Resolution 2749 (XXV) of 17 December 1970), "that the area of the seabed and ocean floor and the subsoil thereof, beyond the limits of national jurisdiction, as well as its resources, are the common heritage of mankind, the exploration and exploitation of which shall be carried out for the benefit of mankind as a whole, irrespective of the geographical location of States" (Cfr. Preamble UNCLOS). Furthermore, Art. 136 of the same Convention further reinforced the idea of "common heritage of mankind".

Under international law, similar concepts to that of "common heritage of mankind" are present in several other fields: cultural patrimonies, natural biodiversity, outer space etc. For instance, Art. 1 of the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies affirms that "the exploration and use of outer space, including the moon and other celestial bodies, shall be carried out for the benefit and in the interests of all countries, irrespective of their degree of economic or scientific development, and shall be the province of all mankind" and that "outer space, including the moon and other celestial bodies, shall be free for exploration and use by all States without discrimination of any kind, on a basis of equality and in accordance with international law, and there shall be free access to all areas of celestial bodies."

It would be highly desirable if, in similar fashion, this notion of a "common heritage of humankind" could be made applicable to the cyber domain. Preserving this domain from intrusions of war and aggression will be to the mutual benefit of all. Working toward this goal should stand as a high priority for civil society and the diplomatic community.

It would be highly desirable if, in a similar fashion, this notion of a "common heritage of humankind" could be made applicable to the cyber domain.

Working toward this goal should stand as a high priority for civil society and the diplomatic community.

In his recent Address to the United Nations General Assembly on 25 September 2020, Pope Francis warned that "we need to break with the present climate of distrust. At present, we are witnessing an erosion of multilateralism, which is all the more serious in light of the development of new forms of military technology, such as lethal autonomous weapons systems (LAWS) which irreversibly alter the nature of warfare, detaching it further from human agency".

This very same warning rings all the truer in cyberspace, as rapidly developing technology increasingly makes it another layer of confrontation among States rather than a domain reserved for peaceful purposes and cooperation at the service of the common good. These positive ends will prevail only when this domain is shaped by the normative framework of international law.

In his most recent Encyclical, *Fratelli tutti* (released on 3 October 2020 in Assisi), Pope Francis describes how "in the face of present-day attempts to eliminate or ignore others, we may prove capable of responding with a new vision of fraternity and social friendship that will not remain at the

level of words" (§6). More specifically, Pope Francis affirms that "courage and generosity are needed in order freely to establish shared goals and to ensure the worldwide observance of certain essential norms. For this to be truly useful, it is essential to uphold "the need to be faithful to agreements undertaken (*pacta sunt servanda*)" and to avoid the "temptation to appeal to the law of force rather than to the force of law". This means reinforcing the "normative instruments for the peaceful resolution of controversies... so as to strengthen their scope and binding force" (§ 174).

The fundamental question is: how can we promote a fraternity between individuals and among States within cyberspace and thus prevent it becoming another ground for divisive competition and conflict?

The fundamental question is: how can we promote a fraternity between individuals and among States within cyberspace and thus prevent it becoming another ground for divisive competition and conflict?

3. Challenges

Regarding our interactions in cyberspace, challenges emerge not only at the interpersonal level, but in relations between States. The latter are indeed the main focus of this contribution.

While digital platforms have enhanced the efficiency of our communications, the quality of our online interactions remains a function of our virtues and vices. Good initiatives, including access to sound information, are amplified thereby, but so too are the bad. Peace can be fostered or undermined by our behaviour in cyberspace. All who participate in cyber interactions – whether individuals, groups, organizations, and even States – have a moral obligation to exhibit probity therein. The fact that these interactions are often anonymized in no way absolves us from the basic requirements of decency, honesty, civility, and respect for human dignity and the rule of law.

All who participate in cyber interactions – whether individuals, groups, organizations, and even States – have a moral obligation to exhibit probity therein. The fact that these interactions are often anonymized in no way absolves us from the basic requirements of decency, honesty, civility, and respect for human dignity and the rule of law.

Every day it becomes more apparent that serious challenges lie in the way of achieving the positive vision adumbrated above. Paradoxically, despite our becoming increasingly interconnected, individualism, indifference, and the relentless pursuit of advantage over others, are fast becoming a dominant ideology.

Cyber interactions are often carried out in anonymity. The absence of attribution – whether of individual persons or of States – can make it appear as though no one bears responsibility for what is said and done. Malicious speech easily multiples in such an environment. Removing human agency from the moral equation is problematic not only from the point of view of ethics, but also from the point of view of the foundation of law. Indeed, the bedrock principle of legal systems is the recognition of human persons as responsible subjects who may be sanctioned for their wrongdoing and obliged to provide redress for the harms they have caused. Responsibility originates from the profound reality of the human person as a free and rational being.

Even States must act as moral persons. All actions undertaken by States in cyberspace presuppose prior decisions that are made by individuals in positions of authority. The fact that the identities of these individuals often remain hidden provides no excuse to evade the fundamental claims of conscience. It is true that cyber interactions, given their high speed and volume, are increasingly guided by computerized forms of non-human agency – in other words, by what now falls under the umbrella expression "artificial intelligence" (AI).[4]

The utilization of AI as a tool within cyberoperations[5] has exacerbated three problems: (i) inadvertent escalation, insofar as AI-enabled autonomous interactions without "humans in the loop" are resistant to normal measures of supervision and control; (ii) proliferation, insofar as AI reduces the human personnel needed for cyberoperations, thereby decreasing the cost of these operations; and (iii) with lowered costs more actors (state and non-state) are able to engage in cyberoperations, and with the multiplication of these actors the attribution problem can be expected to grow proportionately. Despite these challenges we must nonetheless recognize that whatever happens through AI ultimately remains subject to human responsibility. AI designers and operators are accountable for what they set in motion, wittingly and unwittingly.

While cyberspace opens new opportunities for societal improvement, it carries a risk that individual human beings will be treated as mere data points on a screen. Cyberspace enables us to communicate and to share our thoughts and feelings on displays and devices, yet at times, they also shield us from direct contact with the pain, fears and joys of others. This can cause isolation and promote a dangerous insensitivity toward the consequences of our actions on others. Concerns have rightly been raised over ownership of our personal data and how this data will be used by corporations, States, and other powerful social actors. Often, we want to be part of the dataflow, even if that means giving up our privacy, because connecting to the system seems to have become a primary source of meaning in our lives. Real costs have emerged with respect to our civil liberties. The very same data that enables us to communicate with one another in cyberspace can also serve as a strategic asset, enabling dominant actors, often guided by narrow interests, to use our personal and community data for questionable purposes. There is a growing concern that such data is increasingly controlled by a small number of private actors and States. Individuals are often not aware that their personal data has been violated – until it is too late and the harm has become irreversible. Even if Terms of Agreement for computer software/services exist, they are often long and technical, and even those who take the time to read them have difficulty understanding them. People are thus led to share their private data without understanding the full implications. This is not "consent" in the proper sense of the term.

Moreover, it must not be forgotten that not everyone has access to cyberspace. Extensive digital infrastructure is lacking within many States. For instance, the International Telecommunications Union estimated that at the end of 2019, 53.6 per cent of the global population, or 4.1 billion people, are using the Internet, leaving nearly half of the globe without this resource (the so-called digital divide). It is important that access to cyberspace does not become another source of inequality, leading to further marginalization of our most vulnerable brothers and sisters. Marginalization is visible in the current Covid-19 pandemic, as teleworking and e-commerce have become, in many countries, the only viable option for continuing human productivity.

It is important that access to cyberspace does not become another source of inequality, leading to further marginalization of our most vulnerable brothers and sisters.

There is evidence that countries are increasingly investing in offensive cyber capabilities. As the United Nations Secretary General Antonio Guterres affirmed, episodes of cyberwarfare between states already exist. Making matters worse, no regulatory scheme for that type of warfare exists. There is currently little or no consensus on the extent to which the existing international humanitarian laws – built around the principles of humanity, necessity, proportionality, and distinction – apply to State interactions in cyberspace. For instance, might a cyber-offensive be considered a violation of UN Charter, Art. 2 (4), thereby justifying self-defensive military action in response (Art. 51)?[6] Risks that might be contained within an international rule of law are fast becoming unmanageable, leading to worrisome scenarios in which seemingly minor intrusions are misinterpreted so that larger conflicts involving conventional weapons become more frequent. This we can little afford in a world already beset by food shortages, environmental catastrophes, and other burdens that fall disproportionately on the poor and disadvantaged.

There is currently little or no consensus on the extent to which the existing international humanitarian laws – built around the principles of humanity, necessity, proportionality, and distinction – apply to State interactions in cyberspace.

Finally, we must not forget that much of the world's communication infrastructure jointly enables both civilian and military functions. In the event of armed hostilities between States, even on a relatively small scale, it is likely that this infrastructure will be targeted, leading to severe disruptions of essential civilian services, including banking, transport, water supplies, and health care facilities. Due to the interconnectedness of people and things via the Internet, civilian life has become vulnerable in new ways to outbreaks of armed conflict that may occur even in faraway places. As the line between the civilian and military spheres becomes ever more blurred, it becomes increasingly harder to live our lives free from threats of violence.

This penetration of cyber technology within the fabric of society entails a grave risk that the effects of warfare will likewise spread throughout society. Most military command and control systems operate via the same fiber optic connections that are used by civilian networks. The dual use capabilities that are characteristic of cyber networks thus represent an enormous liability in wartime, because an attack on "legitimate" military targets will involve, almost inevitably, attacks on civilian objects as well.[7]

The extension of the battlefield into the civic space – the "civilianization of conflict" as some have called it – is among the most troubling trends confronting our world today.

Under these conditions, it is becoming progressively harder to maintain the core principle of international humanitarian law that civilian life and property should be spared from direct harm in wartime. The extension of the battlefield into the civic space – the "civilianization of conflict" as some have called it – is among the most troubling trends confronting our world today. Finding ways to face this challenge through mutual recognition of norms to be observed by States in their cyber confrontations is an imperative of our age.

4. The Applicability of International Humanitarian Law to Cyberconflict

As has already been noted, it is difficult to apply classical International Humanitarian Law (IHL) in the context of a cyberconflict. This is first of all related to definitions: it is not at all easy to define what a cyberwar is, what cyberaggression and cyberconflict are; it is likewise challenging to determine when, if ever, a cyberattack might count as an employment of "armed force, such that the fundamental right of self-defense would apply. And even assuming this is so, there remains the difficult question whether solely a cyber response would be allowable or, alternatively, whether this defense could justifiably engage conventional military force.

Furthermore, new technologies are developing extremely rapidly. Hence, it is sometimes presumed that the rules of application of IHL, having been framed in another era, are now out-of-date. In fact, this could well be the case if the application of such a framework would be unable to develop itself organically, namely by adapting effectively to new situations while still preserving its core values (ethical guidelines or "moral horizon"). However, if we succeed in dynamically articulating the IHL framework, within its ethical horizon, it then becomes possible to adapt this framework to new situations (which occur frequently in the field of technology) while simultaneously maintaining its fundamental principles (distinction, proportionality, precaution).

However, if we succeed in dynamically articulating the IHL framework, within its ethical horizon, it then becomes possible to adapt this framework to new situations (which occurs frequently in the field of technology!) while simultaneously maintaining its fundamental principles (distinction, proportionality, precaution).

This understanding of "organic development" in legal principles is not new. For example, we know that in situations where legal frameworks have been lacking to tackle problems related to new military technologies, the "Martens Clause"[8] has proven useful. This clause expresses "elementary considerations of humanity". It ensures that in the process of building new legal framework or of adapting classical ones, the references to human dignity and to the dictates of public conscience are to be preserved. This enables us to fill legal gaps, but in a precise non-arbitrary manner, thereby respecting our shared humanity and inherent dignity.

Another challenge arises from the fact that cyberconflict modifies our common notions of space and time. In cyberconflicts, the targets of attack

are no longer localized as in conventional military action; moreover, the speed of engagements far surpasses what was previously imaginable in standard warfare. Furthermore, the chain of causality (and thus the identification of the accountable persons and nations) is itself highly perturbed. For example, physical damage can be produced by very indirect and distributed non-physical causes.

In alluding to these characteristics of cyberconflict, our aim is to indicate how careful thought needs to be directed toward clarifying and enhancing IHL so that these technological shifts receive adequate legal regulation. This theme has been fruitfully considered by numerous authors[9] and we encourage further reflection along these same lines. In the present instance, we content ourselves with mentioning a few basic principles that are of particular importance.

The IHL norms regarding *Ius ad Bellum* require identification of the party directly responsible for an attack. In cyber interactions this is often impossible to achieve, in what has come to be called the "attribution problem". Given the complexity of today's communications networks, the party responsible for an aggression will often remain hidden. This anonymity has several damaging effects. The costs associated with starting a conflict will be lowered, as the initiating party will not risk reprisal and legal penalties. Also, the victims of such attacks can readily misidentify the cause of their suffering, leading them to retaliate against an uninvolved third party. The occasions for the escalation of conflicts will increase, exacerbating already existing geopolitical tensions in an already highly vulnerable world such as ours. If ways could be found, through international collaboration, to identify the sources of cyberattacks, this would have a restraining influence on would-be aggressors, and the already dangerously high levels of inter-state mistrust would decrease.

With respect to *Ius in Bello*, the imperative in IHL of preserving non-combatants from direct harm (the principle of distinction or non-combatant immunity) represents a grave challenge, in light of the dual-use functions of the modern communications infrastructure. It could also be difficult to apply the principles of proportionality and precaution due to the impossibility of foreseeing with precision the consequences of a cyberattack on complex networks. The effects of such attack on cyber-dependent civilian infrastructure (e.g., water supply, electrical grids, medical infrastructures), and the further impact of these damages on the health, food supply, and financial well-being of the civilian population, are extremely difficult to predict.

It could also be difficult to apply the principles of proportionality and precaution due to the impossibility of foreseeing with precision the consequences of a cyberattack on complex networks.

With the widespread development of cyberweapons, their proliferation has become a persistent danger. Malicious codes that are developed by states for purposes of cyberattack can, by accident or malevolent intent, be released into civilian computer networks and used to extort large sums of money from organizations whose access to their own computer data has

been blocked. The examples could easily be multiplied. This proliferation of cyberweapons to criminal and other non-state actors can have devasting implications for civilians. Such malware has been used, for instance, to paralyze hospitals, airports, and even factories that produce critical vaccines. Unlike standard military hardware, which can be difficult to transport and conceal, cyberweapons, which are no more than a few lines of code, can be readily and rapidly disseminated far and wide. Here again, introducing a new weapon type with the intent of reducing the destructiveness of war, has unwittingly rendered civilians vulnerable to new and extensive forms of harm.

In summary, many of the difficulties in the application of the IHL arise from: the complexity of cyberspace that hides, distances, and "dilutes" the responsible agents; the deep entanglement of civilian and military networks, making determinations of collateral damage difficult to calculate *a priori*; and the emergence of new and potential risks of proliferation, given that cyber interactions are constituted by lines of code that are easy to conceal. But these difficulties do not mean that the basic principles of the IHL are inapplicable. On the contrary it shows that due care must be shown in the use of cyberweapons if these those principles are to be observed.

5. Ethics in the Context of Cyberconflict

Why Refer to Ethical Guidelines?

Today, legal frameworks, as well as international regulations, are absolutely necessary in the context of the completely new cyberthreats, conflicts or wars. But the creation of new laws and norms cannot be conceived without a preliminary clarification of the ethical background that guides their elaboration. Otherwise, this task would be blind or motivated merely by the logic of utility and particular interest.

Some Possible Guidelines

What are the values that could be used to serve as moral guidelines for such an elaboration?

One can call into question the choice of our ethical guidelines. Therefore, it is first and foremost necessary to motivate their use. In fact, as Professor Yves Poullet[10] noted in his study on ethics in our digital society, there is a relatively broad consensus (even amongst international institutions like UNESCO for example) to adopt the principles initially described by Beauchamps and Childress in the bioethics context: respect of dignity, of autonomy, social justice and non-maleficence ("do not harm"), with a corresponding affirmation of beneficence ("do good"), solidarity, and justice. The application of these principles in the context of the civilian

digital sphere invites us to go a step further, showing their legitimacy and applicability in the military cyberspace.

We will also use another principle that is of particular relevance today. We are accustomed to the need to respect our natural environment, our common home, and we are aware of the importance of avoiding activities that would pollute it. Indeed, this is a necessary condition for the survival of the human race and respect for future generations. We know that we are not living only in a natural sphere, but in a "noosphere", a cybersphere. Our interrelation and interdependence, in this artificial environment, are now becoming as real as in the physical world. In this context, it is perfectly justified to propose the protection of this new environment as a normative principle which, properly understood, serves the promotion of fraternity and human flourishing.

We know that we are not living only in a natural sphere, but in a "noosphere", a cybersphere. Our interrelation and interdependence, in this artificial environment, are now becoming as real as in the physical world.

Principle 1. The Fundamental Respect of Dignity, and Autonomy

Dignity is what we have in common and what we ultimately share as human persons. It constitutes, in particular, the foundation for Human Rights, and all the principles we will propose could be in fact derived from the underlying respect of human dignity. The reason justifying the choice of all the principles we will use here is rooted in the respect of the humanity we share, independent of our culture, our country, our health condition, etc.

The problems relating to the respect of human dignity in the new cyberenvironment are manifold. Cyberspace indeed opens many possibilities of intrusion into personal lives, in confidential areas, etc. The respect of dignity implies a correlative respect of privacy.

Cyberspace and its cybertools can be used to influence (fake news, propaganda, etc.) and to enslave people or nations (by destabilization, etc.). This limits or destroys the capacity of the person and even the self-determination and the sovereignty of a nation, thereby violating the right of individual and collective autonomy.

To respect the values of dignity and autonomy, it is very important to put certain limits on the use of technologies, such as deep data mining and electronic surveillance. While these can be useful to prevent malware and cyberattacks, they could also amount to private and public intrusions. This ethical principle has to guide legal regulations in an analogous way, by reference to what is done in the civilian sphere vis-à-vis rules for the protection of personal data. Regulations that limit electronic intrusions could be modelled on limits nations impose on the activities of their intelligence services (activities that are not always consistent with established law).[11]

Principle 2. The Need to Protect Vulnerable Persons, Infrastructures and Nations

The question of the protection of vulnerable persons is crucial. This is also a consequence of the principle of protection of human dignity. We are all equal in rights and dignity. Therefore, we have a moral and ethical responsibility to protect our brothers and sisters, in particular the most vulnerable ones.

In the global landscape, there are States or groups of persons who are particularly vulnerable to cyberattacks, "cyberharassment", etc. Harassment of minorities, targeting hospital networks, targeting power supply networks of poor nations, etc., should be blocked by legal protections based on the ethical principles originating in the respect of the dignity of vulnerable persons.

Solidarity with these persons and nations implies a special attention and protection against cyberattacks and more generally speaking cybersurveillance. At an international level, it would be extremely valuable to initiate a reflection on how to protect the persons and groups most at risk with regard to the harm that could be caused by cybermeans. The nations with a high level of experience in cyberprotection could share their knowledge with the more vulnerable ones.

Principle 3. The Need for Justice

It is important that all cyberactions carried out by States are motivated by a "just" cause. Of course, in each case, we have to define what a "just" cause is, but this ideal is important in order to adequately assess the legitimacy of the use of cyberweapons. The requirement of justice also implies knowledge-sharing in order to avoid extreme technological inequalities and gaps, which weaken the global equilibrium.

Principle 4. The Need for Clearly Attributed Responsible Action and Actors

Of particular concern is the dehumanization and the rejection of the responsibility associated with criminal acts committed in cyberspace, where perpetrators are not even aware of the far-reaching consequences their "actions" may entail, decoupling the inextricable nexus between action and responsibility.

This is of particular concern as States are increasingly investing in cybersecurity and cyberdefense capabilities that can also be used offensively. This race for technological progress could well be a source of increasing instability and a new arms race.

We need also to have a clear identification of who is acting in and through cyberspace, especially if the action in question involves a risk of harming, killing or destroying. The traceability of cyber military action

Responsibility and accountability are essential elements of the legal and ethical assessment of an action. This is evident from the fact that the human person has to be and to remain the moral and legal agent of his or her actions.

is of fundamental importance because it allows to pinpoint the actors responsible. Responsibility and accountability are essential elements in the legal and ethical assessment of actions.[12] This is evident from the fact that human persons must retain moral and legal agency over their actions. When human life is at stake, we have to maintain the centrality of human agency and responsibility (and notably the ability to respond in case of damage, etc.)

Very often in cyberattacks, the action cannot be easily attributed to a specific nation or organization. Such attacks proceed from distributed causes that are hidden within a complex and intricate network. This gives rise to many perplexities in the application of ethics to this new kind of conflict. Yet it is crucial to require, for all moral and legal military cyberaction (used in self-defense for example), a clear attribution of the human subject of the action. A systematic lack of transparency in cyberoperations and the lack of causal attribution opens cyberspace to countless risks and the reduction of inhibitions and accountability.

This principle is also connected to a requirement of truth. It is not admissible to fuel conflicts or to keep the fire of violence hidden. Truth and responsibility, in fact, go hand in hand.

Principle 5. The Need for Transparency of Intentions

In the case of cyberattacks, the clear attribution of a responsible person or organization is not sufficient. It is important to clearly identify the operative intention. This is an essential part of the moral assessment of an action. The morality of such attacks, as well as in conventional ones, is partly determined by the content of the intention. Naturally, it is always difficult to establish an intention, mainly in this network complexity, but we have to maintain this requirement at the core of our ethical reflection. Intention reflects what a person or a nation really and deeply wants when performing an action.

Principle 6. Not losing sight of the physical reality

A key problem in the use of cyberdevices, as well as of all techniques handling tools in the virtual world, is the risk we will lose a sense of their consequences in the physical and real world. With purely digital actions (introduction of malware software in a computer for example) we can induce directly or more often indirectly many real physical harms, thus creating victims. We can see this clearly, for example, in the case where young people propagate inaccurate or incomplete information on the web, without being conscious of what they are doing. But here, in the military context, it assumes a greater importance with sometimes disastrous consequences. For this reason, the ethical obligation of taking into account the real effects of virtual actions must be emphasized. This could also be considered as another facet of the principle of responsibility.

Principle 7. Cyberspace as a Common Good, a Common Home and an Environment to be Protected

From the outset, we must acknowledge that an adequate moral assessment of military cyber operations should be considered at the global level. Cyberspace exceeds all traditional borders, in particular those of nations. Cyberspace has established a dense and global network of connections, relating to nearly everyone. That deep interdependence has to be taken into consideration and it induces a corresponding responsibility on the part of users. Cyberspace constitutes a commons where actions, good and bad, can be spread very rapidly throughout the nodes and edges of the networks. It can be used to unite people and nations, but it can also be used, on the contrary, to provoke and enhance divisions. Like a natural environment, it can also be polluted by many "poisons": in this case, hate, discrimination, violence, suspicion, etc. As is the case within a natural or a social network, electronic viruses and worms can be spread rapidly in cyberspace (and at higher speed than in biological networks). The horizon of our moral reflection must be rooted in a conception of cyberspace as a common shared environment of a new kind, that should provide unity between people, and thereby favor peace and human flourishing. This idea is consonant with what was initially proposed, around 1925, by Fr. Pierre Teilhard de Chardin, together with Edouard Leroy, when they spoke about the "Noosphere", a domain emerging from growing networks generated by human intelligence and actions. According to Teilhard,[13] this "Noosphere" is built from an intensification of relations between human beings, led by the emergence of new technological devices enabling interaction and communicate between them, and this can survive only if human beings are moved by a deep love and a strong hope. This so-called "Noosphere" is built on what Pope Francis has called an "ethics of fraternity". Cyberspace can be used to promote fraternity or to destroy it. Teilhard emphasized the fact that the increasing interrelations between people has to correspond to respect for the personality and the autonomy of each human being. Authentic forms of human unity and "social networking" are not truly possible without a great respect for what characterizes the specific differences and the inner wealth of each person or social group. The respect of such intrinsic personal wealth can be translated into the classical protection of human dignity, integrity and of the correlative autonomy of the person. Therefore, this last principle is deeply connected with the first and fundamental one requiring the respect for human dignity.

Cyberspace constitutes a common place where actions, good or bad, can be spread very rapidly throughout the nodes and edges of the networks. It could be used to unite people and nations, but it could be used, on the contrary, to provoke and enhance divisions.

The horizon of our moral reflection has to be rooted in a conception of cyberspace as a common shared environment of a new kind, that has to be used to keep unity between people and to favor peace and human flourishing.

Our natural environment is considered today as a common home, shared by everyone on Earth, to be protected for the wellbeing of the entire human family. The preservation of this common good, and all its natural resources, is a vital necessity and very often also a condition for peace. In a similar way, we have to keep in mind that this artificial environment, this cyberspace, conceived as a common good, has to be protected by

the positive responsibility of the States, via global initiatives that strive to ensure its legitimate function of uniting people, preserving human dignity and digital integrity in cyberspace, while avoiding that this common good become a place for expressing violence, barbarity, discrimination, etc. By definition, cyberspace is a global network, and its protection necessitates global, transnational actions and regulations.

This principle can be translated immediately into the following requirements:

(1) to refuse to use cyberspace as a place to launch unjust military actions, but to use it in order to promote peace, unity, mutual dialogue and understanding between people and nations. This implies a commitment to use cyberspace to do good and not to harm, to paraphrase two famous principles of bioethics.

(2) to refuse to "pollute" the cyberspace environment with viruses, worms, and other cybertools designed to directly or indirectly harm people or to destroy national or individual assets. It is worth noting that like biological weapons, electronic viruses can backfire on the one who has used them, leading to a totally counterproductive and useless action. We know that electronic viruses can behave as biological ones, exposing even their designers to the risk of "infection".[14] In this context, introducing such viruses, with the risk of perturbing cyberspace for a long time, implies a high level of accountability.

In this context, even the sole use of cyberweapons in a defensive context, and only in order to restore cyberspace as a common home, still presents certain risks and moral implications.

6. The Way Forward

It will be important for States to establish a normative legal framework to develop a culture of responsibility as well as an ethics of fraternity and peaceful interactions in cyberspace.

It is essential that we affirm the applicability of IHL to conflicts within cyberspace. Appealing to the novelty of this technology cannot serve as an excuse to escape the law in force and of basic ethical requirements of our humanity. Article 36 of Additional Protocol I to the Geneva Conventions of August 12, 1949, concerning the process of review of a new weapon, means or methods of warfare, remains fully valid in the present instance. Moreover, the Martens Clause remains a last resort to guide interstate conduct, here as elsewhere, should the current law appear to provide insufficient guidance. States, in all circumstances, are ethically and legally responsible for their

actions. All must abide by international humanitarian law and cooperate in the development of this law when the need arises.

With technological progress and in the absence of certainty about the intentions, military preparations, and actions of other States, there is a grave risk that a climate of hostility will last over time and be viewed as a "normal" state-of-affairs. In this case, the absence of open conflict does not mean that it is a time of peace. Transparency and a set of verifiable rules accepted by all are the sine qua non for building peace on solid foundations. Here there is no need to start from scratch as important lessons have already been learned in other areas. Mention may be made of the Comprehensive Test-Ban Treaty and its infrastructure and verification's system. We can also cite the confidence-building measures that are affirmed in numerous treaties and declarations. In a positive vision of peace based on the unity of the human family, States, international organizations, and civil society are called upon to cooperate urgently to reap the authentic benefits of cyber technologies and prevent them from undermining our shared hope in the construction of a real and lasting peace. An educational effort at all levels is essential. Policymakers, civilian and military alike, are always aware of the short- and long-term consequences, limitations and risks associated with cyber weapons systems, algorithms, and artificial intelligence. A critical education into the potential and risks of these technologies would do a great service for humanity.

In a positive vision of peace based on the unity of the human family, States, international organizations, and civil society are called upon to cooperate urgently to reap the authentic benefits of cyber technologies and prevent them from undermining our shared hope in the construction of a real and lasting peace.

An atmosphere of hostility is inevitably reinforced by uncertainty about the strength of one's own defense systems, especially when it affects fundamental values of a society, such as the integrity of the electoral process in a democracy. The temptation is often great to exert some sort of deterrence vis-à-vis a potential adversary, by positioning oneself to carry out an attack, and in so doing to demonstrate the high cost of resorting to cyberattacks. The dangers of escalation are real and grave. We must find ways of refraining from such activity. In the best interest of all parties, dialogue with a view to strictly respecting the existing rules of international humanitarian law and the negotiation of new rules, when necessary, is the only viable solution to avoid falling into a vicious circle where there will be only losers.

In the best interest of all parties, dialogue with a view to strictly respecting the existing rules of international humanitarian law and the negotiation of new rules, when necessary, is the only viable solution to avoid falling into a vicious circle where there will be only losers.

It will be important to promote national policies to effectively protect civilians in recognizing a fundamental right for their digital integrity as natural persons. This right is an extension of physical and psychological integrity already enshrined in many legislations and constitutions. This right to digital integrity could also be extended to critical infrastructures and essential services like hospitals.

In an increasingly opaque field where the stakes are vital for us all, adopting robust measures for building confidence between States is a necessity. Trust can be promoted unilaterally, bilaterally and multilaterally. This is the only way to reduce if not avoid confrontations that ultimately

Trust can be promoted unilaterally, bilaterally and multilaterally.

none will win. A policy of trust and cooperation would be the expression of an ethic of fraternity which offers a positive vision of a peaceful humanity, where each person and nation can grow and flourish. Cyberspace, oceans, environment, outer space are the places where the ethic of fraternity is most tested and where the future of all mankind is at stake. Prevention through transparency and cooperation is the narrow way to avoid a cyber arms race and its proliferation, which would inevitably lead to catastrophic consequences. In the face of global problems which affect the fundamental interests of the entire human family, it is essential to establish a subsidiarity that supports, in a harmonious and equitable manner, authentic national and universal interests.

There is no doubt that with the rise of the Digital Age, AI and related technologies will continue to transform the way we live. Yet, this does not mean that social polarization individualism, and indifference will necessarily result. Technology is only a means and not an end. It can be used to tackle the most pressing challenges the world faces today, as described in the sustainable development goals, with special focus on alleviation of climate change, reduction of poverty, as well as access to healthcare and education. As suggested by Pope Francis, "we have to broaden our vision. We have the freedom needed to limit and direct technology; we can put it at the service of another type of progress, one which is healthier, more human, more social, more integral […] When technology disregards the great ethical principles, it ends up considering any practice whatsoever as licit." (Pope Francis, Encyclical Letter, *Laudato Si'*, 47.)

Pope Francis, "we have to broaden our vision. We have the freedom needed to limit and direct technology; we can put it at the service of another type of progress, one which is healthier, more human, more social, more integral […] When technology disregards the great ethical principles, it ends up considering any practice whatsoever as licit."

In order to address in an effective manner the particular challenges facing the global community, it is necessary, as Pope Francis has mentioned in *Fratelli tutti*, to present an analysis of the situation with concrete proposals for a way forward. "A wide variety of practical proposals and diverse experiences can help achieve shared objectives and serve the common good. The problems that a society is experiencing need to be clearly identified, so that the existence of different ways of understanding and resolving them can be appreciated" (§228). This paper has sought to offer such a perspective, by outlining the complexity of the cyber question, indicating the intricacies and nuances of this new global common space. We have seen that, despite the particular and novel nature of many of today's innovative technologies, it is still legitimate and necessary to approach and evaluate human (inter) action from the perspective of classical principles of ethics, responsibility and accountability. Ultimately, the basis for such an approach is justified in the conviction that "the inherent dignity and […] the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world." (*Universal Declaration of Human Rights*, 1948, Preamble).

From this perspective, it is the hope of the authors that the observations made above might serve as a concrete contribution to extend humanity's

common pursuit of peace to cyberspace.[15] Such a goal, considering the many challenges mentioned above, is both daunting and demanding. "Courage and generosity are needed in order freely to establish shared goals and to ensure the worldwide observance of certain essential norms" (Pope Francis, *Fratelli tutti*, n° 174). For this reason, it is absolutely essential to approach the cybersecurity debate with intentionality and perseverance. Without the active and sincere engagement of authorities at all levels – local, national, regional and global - it will be impossible to develop a comprehensive and systematic legal framework, that adequately accounts for the many dimensions of cyberspace.

Without the active and sincere engagement of authorities at all levels – local, national, regional and global - it will be impossible to develop a comprehensive and systematic legal framework, that adequately accounts for the many dimensions of cyberspace.

As has been noted above, in order to ensure that such efforts remain at the service of the human person and the common good, it will be necessary to stress the value of cooperation over competition. To this end, the call of Pope Francis, echoing the words of Pope John Paul II, to seek human fraternity over egoistic self-interests (whether of individuals, groups or nations) presents its full force and effectiveness: "If there is no transcendent truth, in obedience to which man achieves his full identity, then there is no sure principle for guaranteeing just relations between people. Their self-interest as a class, group or nation would inevitably set them in opposition to one another" (cf. Pope Francis, *Fratelli tutti*, n° 273).[16]

Notes

1. "Digital" describes electronic signals or data that are communicated in sequences of positive and negative states (the digits 0 and 1). "Computer" designates a machine that follows digital instructions. All computer-to-computer communications are based on a transference of signals in digital form. "Cyber" refers more loosely to matters "relating to, or involving computers or computer networks (such as the Internet)" (*Merriam Webster Dictionary*).

2. Dante, *Monarchia*, I, iv.

3. For an overview of discussions about the cybersphere as a distinctive "domain", see Roland Deibert, "Trajectories for Future Cybersecurity Research, in *The Oxford Handbook of International Security*, Alexandra Gheciu and William C. Wohlforth, eds. (Oxford : Oxford University Press, 2018), pp. 531-546.

4. There exists no standard definition of "artificial intelligence – AI"; different authors attach contrasting meanings to the term. First coined in 1955 by computer scientist John McCarthy, AI is an umbrella term designating a variety of technologies (most notably "expert systems" and "machine learning") that enable machines to simulate cognitive functions (found in humans and some other animals), including perception, memory, reasoning, problem-solving, planning, deciding, language use and transfer of knowledge. For an overview, see "What is Artificial Intelligence?" chap. 2 of Virginia Dignum, *Responsible Artificial Intelligence* (Cham, Switzerland : Springer, 2019), pp. 9-34.

5. See Danks, David and Joseph H. Danks (2013), "The Moral Permissibility of Automated Responses during Cyberwarfare", *Journal of Military Ethics* 13.1: 18-33.

6. Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *The Yale Journal of International Law* 36, pp. 421-459.

7. This trend has now been extended even to outer space; insofar as dual use satellite-based communications are essential to the functioning of earth-based weapon systems, satellites can themselves be made the target of attack. The weaponization of outer space will be the inevitable result as cyber military interactions become more pervasive.

8. Rupert Ticehurst, "The Martens Clause and the Laws of Armed Conflict", *International Review of the Red Cross*, No. 317 (30-04-1997).

9. See, for instance, Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge: Cambridge University Press, 2012); Michael M. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

10. Y. Poullet, *Ethique et droits de l'homme dans notre société du numérique* (Brussels : Académie Royale de Belgique, 2020).

11. Cfr The Schrems 2 decision by the European Court of Justice which considers that the intrusions of Intelligence Services inside the personal data of the citizens constitute a violation of the GDPR. We could consider that the surveillance and intelligent information programs have to be limited to what is needed for the national security (principle of proportionality).

12. Cf. the Ethics Guidelines for Trustworthy AI of the High-Level Expert Group on AI) which goes in this direction stating that AI has to be governed by human beings: "Develop, deploy and use AI systems in a way that adheres to the ethical principles of: respect for human autonomy, prevention of harm, fairness and explicability" (document available on the site of the European Commission).

13. Pierre Teilhard de Chardin, *The Human Phenomenon*, Sarah Appleton-Weber, translator and editor, with a Foreword by Brian Swimme, (Brighton: Sussex Academic Press, 1999), pp. 122-125.

14. For a comparison of biological and digital weaponry, and the grave dangers attendant upon each, see Richard Danzig, *Technology Roulette: Managing Loss of Control as many Militaries Pursue Technological Superiority*, Center for New American Security; June 2018.

15. The notion of cyberspace also includes the datasphere, i.e., the total circulation of data at a global scale, as suggested in this research paper: Bergé, Jean-Sylvestre and Grumbach, Stephane and Zeno-Zencovich, Vincenzo, The 'Datasphere', Data Flows Beyond Control, and the Challenges for Law and Governance (March 28, 2018). *European Journal of Comparative Law and Governance*, Vol. 5, Issue 2, 2018, Available at SSRN: https://ssrn.com/abstract=3185943.)

16. Pope Francis, *Fratelli tutti*, n° 273

SECTION II - HUMAN FRATERNITY IN CYBERSPACE: THE ENGAGEMENT OF THE CHURCH

INTRODUCTION

CARDINAL PETER K. A. TURKSON
Prefect of the Dicastery for Promoting Integral Human Development, Holy See

I am very pleased to have the opportunity to introduce the following selection of texts which highlight the engagement of the Church with the issues raised by the emergence of digital technologies. What we find in this collection are the key insights that are shaping the Church's response to the specific themes that are related with the development and application of digital technologies in the different *fora* and contexts.

We are, indeed, living in a world that we could hardly have imagined even a few years ago. We refer to this global experience of digital technologies with two simple words: "digital age". The particular domain of its development and application is referred to as "cyberspace"; and it is the product of extraordinary achievements in science and in data-processing technology brought about by human ingenuity. As a result, cyberspace now plays and will continue to play an increasingly important role in the social, economic, cultural and political aspects of our lives. and the internet is poised to foster prosperity and peace, intellectual growth, access to educational resources, and to contribute to mutual understanding among peoples by promoting dialogue and a culture of encounter.

True to her resolve at the Vatican Council II, to "show solidarity and respectful affection for the human family, and to enter into dialogue with it about all its problems",[1] the Church, ever since the internet and digital technology first became available, has always sought to promote its use in the service of the encounter between persons, and of solidarity among all.[2]

The Church, ever since the internet and digital technology first became available, has always sought to promote its use in the service of the encounter between persons, and of solidarity among all.

In so doing, the Church's primary consideration is to recognise the extra-ordinary developments that have been made in science and technology in general, and in information and digital technologies in particular. As Pope Francis reminds us in *Laudato Sì:* It is right to rejoice in these advances and to be excited by the immense possibilities which they continue to open up before us, for "science and technology are wonderful products of a God-given human creativity."[3] This is an important starting point: It is appropriate to recognise and celebrate the life-enhancing potential of new technologies. This is necessary if we are to escape from the unfair but lingering suspicion that the Church is somehow opposed to science and progress. It also legitimizes our concern to ensure that the potential for goodness of the technologies is put at the service of all humans. For, technological progress has unquestionably brought enormous benefits; yet the dangers lurking in the "dark side" of our new digital world must not

be ignored. Besides the problem of an inclusive access to the technology, such as the internet, and its uses,[4] this immense technological development has not been accompanied by a development in human responsibility and values; and it has no safeguards for human freedom.[5]

This is a concern that is shared, not only by the Church, but also by many who are active in governments and civil society. For Pope Francis, "humanity has entered a new era in which our technical progress has brought us to a crossroads."[6] Thus, while "we are beneficiaries of two centuries of enormous waves of change", the outcome of which has triggered a new digital era which has countless benefits for humanity,"[7] the power of technology, regrettably, is often associated with financial and economic powers. Those who hold this increasing and overwhelming power over humanity and nature are not necessarily "trained to use power well."[8] Similarly, the Report of the UN Secretary-General's High-level Panel on Digital Cooperation[9] does not only recognize how "Digital technologies are rapidly transforming society, simultaneously allowing for unprecedented advances in the human condition and giving rise to profound new challenges." It also observes that the "growing opportunities created by the application of digital technologies are paralleled by stark abuses and unintended consequences. Digital dividends co-exist with digital divides. And, as technological change has accelerated, the mechanisms for cooperation and governance of this landscape have failed to keep pace."

Ethics and Individual Agency

Before these concerns, we must not yield to resignation. We should take up the invitation of Pope Francis to broaden our vision. For, "we have the freedom needed to limit and direct technology; we can put it at the service of another type of progress, one which is healthier, more human, more social, more integral […] When technology disregards the great ethical principles, it ends up considering any practice whatsoever as licit."[10]

There is, thus, a growing awareness of the need for a focussed ethical consideration of new technologies, especially as we see the emergence of systems of machine learning and artificial intelligence.

There is, thus, a growing awareness of the need for a focussed ethical consideration of new technologies, especially as we see the emergence of systems of machine learning and artificial intelligence. This concern for ethics, and the determination to ensure that the positive impact of technologies on humans and human society becomes the true measure of progress, is to be welcomed. The ethical analysis of the technologies often starts with a consideration of the potential 'dual use' of the technologies. This involves an ethical reflection on the responsibilities of end users for the purposes for which they employ the technologies and on issues of moral agency. Particular attention needs to focus on the ethical responsibility of those who are directly involved in the development of the digital technologies. They are required to be attentive to the impact

and consequences of the technologies they are designing. Many of those working in the area of artificial intelligence have committed to seeking to ensure that the technologies are 'ethical by design' and they are committed to development processes that are intentionally focussed on being inclusive, objective and in service of human goods. This is true both of individuals (many young programmers are refusing to work on projects they view as being ethically objectionable), and of professional associations, which are seeking to outline standards and frameworks to ensure the correct use of the skills and specializations of their members. One example of this is the Global Initiative for Ethical Considerations in Artificial Intelligence Systems of the IEEE (Institute of Electrical and Electronics Engineers) which has as its mission to "ensure every technologist is educated, trained, and empowered to prioritize ethical considerations."[11] It is also worth noting that many of the entrepreneurs who were involved in the development of digital technologies and platforms are now more attentive to the role of 'bad actors' and are focussed on ensuring that future technologies are not vulnerable to exploitation by those who would use them for evil.

Ethics and Structural Contexts

A dual use analysis, however, will not be sufficient. Technologies cannot be viewed simply as neutral. In light of this, mere training in the correct use of new technologies will not prove sufficient. As Pope Francis has said: "As instruments or tools, these are not "neutral", for, as we have seen, they shape the world and engage consciences on the level of values. We need a broader educational effort. Solid reasons need to be developed to promote perseverance in the pursuit of the common good, even when no immediate advantage is apparent. There is a political dimension to the production and use of artificial intelligence, which has to do with more than the expanding of its individual and purely functional benefits. In other words, it is not enough simply to trust in the moral sense of researchers and developers of devices and algorithms."[12] This requires us to be more attentive to the existing political and economic conditions within which the new technologies are being developed and the need to be alert as to how those conditions can determine the whole process which will decide which technologies are developed and how they will eventually be employed. Will the emerging technologies be employed to solve global problems, or will they be focussed on meeting and, in some cases, stimulating less urgent but more immediately profitable ends? There is an acute awareness within the technology sector of the influence of the data that is used to train machine learning programmes and the likelihood that these programmes ultimately magnify the biases and the prejudices that shape the datasets.[13] In a world of enormous inequality, can we ensure that the new technologies will not exacerbate the inequalities by concentrating

In other words, it is not enough simply to trust in the moral sense of researchers and developers of devices and algorithms.

material wealth and political influence in the hands of an ever-smaller elite? How can the global community seek to regulate these technologies when the relevant scientific expertise, technical capacities and the financial resources are controlled by a small number of commercial actors which operate transnationally?

Rehabilitating Dialogue

Addressing these questions will require a global and inclusive conversation. The words of Pope Francis as articulated in the context of the environmental crisis appeal equally to the question of the future of digital technologies: "I urgently appeal, then, for a new dialogue about how we are shaping the future of our planet. We need a conversation which includes everyone, since the environmental challenge we are undergoing, and its human roots, concern and affect us all."[14] The type of dialogue required to achieve true consensus is ultimately a human achievement rather than something that will emerge simply through the use of communication technologies. We are obliged to be attentive to the damage that has been done to public discourse by some of the forms of communication fostered by digital technologies and the impact of the increased polarization particularly associated with social media. In this context, dialogue must be fostered as a true effort to generate mutual understanding and to build that trust which is required for a global consensus to emerge on how best to ensure that technology serves the interests of all. As Pope Francis says of digital communications: "Efforts need to be made to help these media become sources of new cultural progress for humanity and not a threat to our deepest riches. True wisdom, as the fruit of self-examination, dialogue and generous encounter between persons, is not acquired by a mere accumulation of data which eventually leads to overload and confusion, a sort of mental pollution."[15]

The type of dialogue required to achieve true consensus is ultimately a human achievement rather than something that will emerge simply through the use of communication technologies.

Dialogue in its most meaningful sense will help us to nurture a culture of encounter where people learn to trust and to listen to each other, and to see difference as enrichening rather than threatening. When people listen to the "other" and allow his or her voice to breach their defensiveness, they open themselves to growth in understanding. If they are willing to listen to others, they will learn to see the world with different eyes and will grow in appreciation of the richness of the human experience as revealed in other cultures and traditions. The more people grow in knowledge of others, the more they grow also in self-knowledge. "We have to be able to dialogue with the men and women of today …. We are challenged to be people of depth, attentive to what is happening around us and spiritually alert. To dialogue means to believe that the "other" has something worthwhile to say, and to entertain his or her point of view and perspective."[16] Engagement with others alerts people

Dialogue in its most meaningful sense will help us to nurture a culture of encounter where people learn to trust and to listen to each other, and to see difference as enrichening rather than threatening.

to those basic desires to love and be loved, for protection and security, for meaning and purpose that are shared by all humans. Attentiveness to the human condition, and to the one world which we all share, highlights the truth that these desires can only be satisfied fully if people construct a society that is committed to a shared concern for the well-being of all rather than to an ethos of unbridled competition where the happiness of some can only be achieved at the expense of others. In this sense the introduction of the concept of "global commons" in Part 1 of this document becomes very useful and meaningful.

Fake News

Almost 20 years ago, the British philosopher, Onora O'Neill, warned of the damage done to politics and the common good by what we might now call 'fake news': "If the media mislead, or if readers cannot assess their reporting, the wells of public discourse and public life are poisoned. The new information technologies may be anti-authoritarian, but curiously they are often used in ways that are also anti-democratic. They undermine our capacities to judge others' claims and to place our trust."[17] Concerns about fake news are receiving much attention both at national and international levels. Many believe that there is a need for national governments to have more oversight over the various actors who are responsible for the dissemination of news and information and to establish standards to protect the public. Increased attention has been focussed on the role of the social media companies in providing platforms for those who are intentionally seeking to spread misinformation, to manipulate public opinion and to promote conflict and division. Much effort is being expended by these companies to monitor their platforms and exclude hate speech and falsities. In particular, they are looking to develop algorithms capable of identifying and removing such types of communications. The intention to prevent the harm caused by such types of communication to the public discourse and to those who are being targeted is admirable, but questions arise as to who will be the arbiters of what is acceptable or true and as to whether technical solutions can be sufficiently alert to the ambiguity of human communication.

Increased attention has been focussed on the role of the social media companies in providing platforms for those who are intentionally seeking to spread misinformation, to manipulate public opinion and to promote conflict and division.

It is important also to address the question of the responsibility of the wider public, and to invite all people to be attentive to their own practises in order to foster good and constructive habits which will promote discourse. This is particularly important in the context of social media where the traditional distinctions between the consumers and the producers of content are not so clear. Commentators frequently speak of user generated content with reference to the social networks, but it is important to recognise that the very culture of the social networks is user generated. If the networks are to be spaces where good positive communications can help to promote

individual and social well-being then the users, the people who make up the networks, need to be attentive to the type of content they are creating and sharing – they need to monitor the veracity of the news they share and the impact it may have on others.

In this regard, the Church can contribute with ethical reflections on how to promote and develop human fraternity also in the cyberspace and truly put it at the service of an integral human development. A starting point would be to define the idea of peace in the cyberspace: peace centered on the person and extending to inter-State relations. Since the proper functioning of the cyberspace is the result of the shared responsibility of various actors in their respective roles, an ethics of fraternity which is rooted in "love in truth" can help "lead people to opt for courageous and generous engagements in the field of justice and of peace."[18]

Cyberwarfare

It is clear that the employment of artificial intelligence and robots has the capacity not only to radically change the nature of warfare; it also renders the traditional just war theory of St. Thomas Aquinas inadequate. While the application of artificial intelligence to warfare is a developing area and one where much further reflection is required, I am inclined to share the conclusion of the Pontifical Academy of Sciences: "International standards are urgently needed. Ideally, these would regulate the use of AI with respect to military planning (where AI risks to encourage pre-emptive strategies), cyberattack/defence as well as the kinetic battlefields of land, air, sea, undersea, and outer space. With respect to lethal autonomous weapon systems, given the present state of technical competence (and for the foreseeable future), no systems should be deployed that function in unsupervised mode. Whatever the battlefield—cyber or kinetic—human accountability must be maintained, so that adherence to internationally recognized laws of war can be assured and violations sanctioned."[19]

But more desirable and to the mutual benefit of all would be the consideration of the cyberspace as a neutral ground or common heritage of humankind.

In this regard, as was suggested in this publication, there is an urgent need for States to establish a normative legal framework to develop a culture of responsibility as well as an ethics of fraternity and peaceful interactions in the context of cyberspace. But more desirable and to the mutual benefit of all would be the consideration of the cyberspace as a neutral ground or common heritage of humankind: a global common, preserved from tools designed to directly or indirectly harm people or to destroy national or individual assets. The cyberspace should become an instrument of cooperation to promote fraternity and mutual understanding between people and nations.

The cyberspace should become an instrument of cooperation to promote fraternity and mutual understanding between people and nations.

Conclusion

I would invite the reader to see the selection of texts that follow as an invitation to a conversation: "an eloquent expression of the Church's solidarity with and respectful affection for the human family, her dialogue with it about its challenges and problems!"[20] They articulate, through the lenses of the Church's faith and social doctrine, an emerging perspective and are intended to stimulate further reflection and responses. What is required now is that human beings search together for the values and choices that will promote the true wellbeing of humanity and foster peace and justice in our shared home. "In a pluralistic society, dialogue is the best way to realize what ought always to be affirmed and respected apart from any ephemeral consensus. Such dialogue needs to be enriched and illumined by clear thinking, rational arguments, a variety of perspectives and the contribution of different fields of knowledge and points of view. Nor can it exclude the conviction that it is possible to arrive at certain fundamental truths always to be upheld. Acknowledging the existence of certain enduring values, however demanding it may be to discern them, makes for a robust and solid social ethics. Once those fundamental values are acknowledged and adopted through dialogue and consensus, we realize that they rise above consensus; they transcend our concrete situations and remain non-negotiable. Our understanding of their meaning and scope can increase – and in that respect, consensus is a dynamic reality – but in themselves, they are held to be enduring by virtue of their inherent meaning."[21]

What is required now is that human beings search together for the values and choices that will promote the true wellbeing of humanity and foster peace and justice in our shared home.

Such dialogue needs to be enriched and illumined by clear thinking, rational arguments, a variety of perspectives and the contribution of different fields of knowledge and points of view.

Notes

1. Cf. *Gaudium et Spes*, 3
2. Cf. Pope Francis, *Message for the 53rd World Communication Day*.
3. Pope Francis, *Laudato Si'*, 102.
4. The current Covid-19 pandemic and the heightened use of cyberspace for virtual meetings and teleworking etc., has revealed that access to Internet is still a privilege of some, but not of all. Almost four billion of our brothers and sisters do not yet have access to Internet (Cf. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx).
5. Pope Francis, *Laudato Si'*, 105.
6. Idem.
7. Idem.
8. Pope Francis, *Laudato Si'*, 105.
9. https://www.un.org/en/sg-digital-cooperation-panel
10. Pope Francis, *Laudato Si'*, 136
11. Cf. https://standards.ieee.org/
12. Pope Francis, *Address to Pontifical Academy for Life, 2020*.

13. Cf. Jake Silber and James Manyika, "Tackling bias in artificial intelligence (and in humans), McKinsey Global Institute, 2019.

14. Pope Francis, *Laudato Si'*, 14

15. Pope Francis, *Laudato Si'*, 47.

16. Pope Francis, *Message for the World Communications Day: °Communication at the Service of an Authentic Culture of Encounter*, 2014.

17. Onora O'Neill, *A Question of Trust: Reith Lectures*, 2002 (Radio 4 - Reith Lectures 2002 - A Question Of Trust – BBC, available at: https://www.bbc.co.uk/radio4/reith2002).

18. Cf. Pope Benedict XVI, *Caritas in Veritate*, 1

19. Cf. Concluding statement from the Conference on *Robotics, AI and Humanity, Science, Ethics and Policy* organized jointly by the Pontifical Academy of Sciences (PAS) and the Pontifical Academy of Social Sciences (PASS), 16-17 May 2019, Casina Pio IV, Vatican City.

20. Cf. *Gaudium et Spes*, 3

21. Pope Francis, *Fratelli Tutti*, 211.

COLLECTION OF RECENT DOCUMENTS FROM THE CHURCH'S ENGAGEMENT ON CYBERSPACE

ENCYCLICAL LETTER LAUDATO SI'

POPE FRANCIS

24 May 2015

(Selected Excerpts)

102. Humanity has entered a new era in which our technical prowess has brought us to a crossroads. We are the beneficiaries of two centuries of enormous waves of change: steam engines, railways, the telegraph, electricity, automobiles, aeroplanes, chemical industries, modern medicine, information technology and, more recently, the digital revolution, robotics, biotechnologies and nanotechnologies. It is right to rejoice in these advances and to be excited by the immense possibilities which they continue to open up before us, for "science and technology are wonderful products of a God-given human creativity".[81] The modification of nature for useful purposes has distinguished the human family from the beginning; technology itself "expresses the inner tension that impels man gradually to overcome material limitations".[82] Technology has remedied countless evils which used to harm and limit human beings. How can we not feel gratitude and appreciation for this progress, especially in the fields of medicine, engineering and communications? How could we not acknowledge the work of many scientists and engineers who have provided alternatives to make development sustainable?

103. Technoscience, when well directed, can produce important means of improving the quality of human life, from useful domestic appliances to great transportation systems, bridges, buildings and public spaces. […]

104. Yet it must also be recognized that nuclear energy, biotechnology, information technology, knowledge of our DNA, and many other abilities which we have acquired, have given us tremendous power. More precisely, they have given those with the knowledge, and especially the economic resources to use them, an impressive dominance over the whole of humanity and the entire world. Never has humanity had such power over itself, yet nothing ensures that it will be used wisely, particularly when we consider how it is currently being used. […]

105. There is a tendency to believe that every increase in power means "an increase of 'progress' itself", an advance in "security, usefulness, welfare and vigour; …an assimilation of new values into the stream of culture",[83] as if reality, goodness and truth automatically flow from technological and economic power as such. The fact is that "contemporary man has not been trained to

** The numbering of the footnotes in the current collection corresponds to that which appears in the original documents.*

use power well",[84] because our immense technological development has not been accompanied by a development in human responsibility, values and conscience. Each age tends to have only a meagre awareness of its own limitations. It is possible that we do not grasp the gravity of the challenges now before us. "The risk is growing day by day that man will not use his power as he should"; in effect, "power is never considered in terms of the responsibility of choice which is inherent in freedom" since its "only norms are taken from alleged necessity, from either utility or security".[85] But human beings are not completely autonomous. Our freedom fades when it is handed over to the blind forces of the unconscious, of immediate needs, of self-interest, and of violence. In this sense, we stand naked and exposed in the face of our ever-increasing power, lacking the wherewithal to control it. We have certain superficial mechanisms, but we cannot claim to have a sound ethics, a culture and spirituality genuinely capable of setting limits and teaching clear-minded self-restraint.

106. The basic problem goes even deeper: it is the way that humanity has taken up technology and its development according to an undifferentiated and one-dimensional paradigm. This paradigm exalts the concept of a subject who, using logical and rational procedures, progressively approaches and gains control over an external object. This subject makes every effort to establish the scientific and experimental method, which in itself is already a technique of possession, mastery and transformation. It is as if the subject were to find itself in the presence of something formless, completely open to manipulation. […]

107. It can be said that many problems of today's world stem from the tendency, at times unconscious, to make the method and aims of science and technology an epistemological paradigm which shapes the lives of individuals and the workings of society. The effects of imposing this model on reality as a whole, human and social, are seen in the deterioration of the environment, but this is just one sign of a reductionism which affects every aspect of human and social life. We have to accept that technological products are not neutral, for they create a framework which ends up conditioning lifestyles and shaping social possibilities along the lines dictated by the interests of certain powerful groups. Decisions which may seem purely instrumental are in reality decisions about the kind of society we want to build.

108. The idea of promoting a different cultural paradigm and employing technology as a mere instrument is nowadays inconceivable. The technological paradigm has become so dominant that it would be difficult to do without its resources and even more difficult to utilize them without being dominated by their internal logic. It has become countercultural to

choose a lifestyle whose goals are even partly independent of technology, of its costs and its power to globalize and make us all the same. Technology tends to absorb everything into its ironclad logic, and those who are surrounded with technology "know full well that it moves forward in the final analysis neither for profit nor for the well-being of the human race", that "in the most radical sense of the term power is its motive – a lordship over all".[87] As a result, "man seizes hold of the naked elements of both nature and human nature". […]

110. The specialization which belongs to technology makes it difficult to see the larger picture. The fragmentation of knowledge proves helpful for concrete applications, and yet it often leads to a loss of appreciation for the whole, for the relationships between things, and for the broader horizon, which then becomes irrelevant. This very fact makes it hard to find adequate ways of solving the more complex problems of today's world, particularly those regarding the environment and the poor; these problems cannot be dealt with from a single perspective or from a single set of interests. A science which would offer solutions to the great issues would necessarily have to take into account the data generated by other fields of knowledge, including philosophy and social ethics; but this is a difficult habit to acquire today. Nor are there genuine ethical horizons to which one can appeal. Life gradually becomes a surrender to situations conditioned by technology, itself viewed as the principal key to the meaning of existence. In the concrete situation confronting us, there are a number of symptoms which point to what is wrong, such as environmental degradation, anxiety, a loss of the purpose of life and of community living. Once more we see that "realities are more important than ideas".[91] […]

112. Yet we can once more broaden our vision. We have the freedom needed to limit and direct technology; we can put it at the service of another type of progress, one which is healthier, more human, more social, more integral. […]

113. There is also the fact that people no longer seem to believe in a happy future; they no longer have blind trust in a better tomorrow based on the present state of the world and our technical abilities. There is a growing awareness that scientific and technological progress cannot be equated with the progress of humanity and history, a growing sense that the way to a better future lies elsewhere. This is not to reject the possibilities which technology continues to offer us. But humanity has changed profoundly, and the accumulation of constant novelties exalts a superficiality which pulls us in one direction. It becomes difficult to pause and recover depth in life. […]

177. Given the real potential for a misuse of human abilities, individual states can no longer ignore their responsibility for planning, coordination, oversight and enforcement within their respective borders. How can a society plan and protect its future amid constantly developing technological innovations? One authoritative source of oversight and coordination is the law, which lays down rules for admissible conduct in the light of the common good. The limits which a healthy, mature and sovereign society must impose are those related to foresight and security, regulatory norms, timely enforcement, the elimination of corruption, effective responses to undesired side-effects of production processes, and appropriate intervention where potential or uncertain risks are involved. […]

NOTES

81. JOHN PAUL II, *Address to Scientists and Representatives of the United Nations University*, Hiroshima (25 February 1981), 3: AAS 73 (1981), 422.

82. BENEDICT XVI, Encyclical Letter *Caritas in Veritate* (29 June 2009), 69: AAS 101 (2009), 702.

83. ROMANO GUARDINI, *Das Ende der Neuzeit*, 9th ed., Würzburg, 1965, 87 (English: *The End of the Modern World*, Wilmington, 1998, 82).

84. Ibid.

85. Ibid., 87-88 (*The End of the Modern World*, 83).

86. PONTIFICAL COUNCIL FOR JUSTICE AND PEACE, *Compendium of the Social Doctrine of the Church*, 462.

87. ROMANO GUARDINI, *Das Ende der Neuzeit*, 63-64 (*The End of the Modern World*, 56).

88. Ibid., 64 (*The End of the Modern World*, 56).

89. Cf. BENEDICT XVI, Encyclical Letter *Caritas in Veritate* (29 June 2009), 35: AAS 101 (2009), 671.

90. Ibid., 22: p. 657.

91. Apostolic Exhortation *Evangelii Gaudium* (24 November 2013), 231: AAS 105 (2013), 1114.

STATEMENT AT THE UNITED NATIONS SECURITY COUNCIL OPEN DEBATE ON PROTECTION OF CRITICAL INFRASTRUCTURE AGAINST TERRORIST ATTACKS

ARCHBISHOP BERNARDITO AUZA, PERMANENT OBSERVER OF THE HOLY SEE TO THE UNITED NATIONS IN NEW YORK

13 February 2017

(Selected Excerpts)

[…]

States should be urged to collaborate in this area at both the international and regional levels through the sharing of information and best practices, coordinated policies and joint border controls.

The world must act to prevent terrorists from having access to financial support by terror sponsors. The borderless nature of the terrorist groups perpetrating the destruction of critical infrastructure requires the international community to control cyber technologies that violent groups use to recruit new adherents, finance their activities and coordinate terror attacks.

[…]

Notes

1. Pope Francis. Visit to the Military Memorial of Redipuglia (Italy) on the occasion of the 100th anniversary of the outbreak of the First World War, 13 September 2014. Also Pope Francis, Homily on the Divine Mercy Sunday, Rome, 2015.

ADDRESS TO THE PARTICIPANTS IN THE CONGRESS ON "CHILD DIGNITY IN THE DIGITAL WORLD"

POPE FRANCIS

6 October 2017

(Selected Excerpts)

[…]

We are living in a new world that, when we were young, we could hardly have imagined. We define it by two simple words as a "digital world", but it is the fruit of extraordinary achievements of science and technology. In a few decades, it has changed the way we live and communicate. Even now, it is in some sense changing our very way of thinking and of being, and profoundly influencing the perception of our possibilities and our identity.

If, on the one hand, we are filled with real wonder and admiration at the new and impressive horizons opening up before us, on the other, we can sense a certain concern and even apprehension when we consider how quickly this development has taken place, the new and unforeseen problems it sets before us, and the negative consequences it entails. Those consequences are seldom willed, and yet are quite real. We rightly wonder if we are capable of guiding the processes we ourselves have set in motion, whether they might be escaping our grasp, and whether we are doing enough to keep them in check.

This is the great existential question facing humanity today, in light of a global crisis at once environmental, social, economic, political, moral and spiritual.

[…]

But there is also an urgent need, as part of the process of technological growth itself, for all those involved to acknowledge and address the ethical concerns that this growth raises, in all its breadth and its various consequences.

[…]

The net has opened a vast new forum for free expression and the exchange of ideas and information. This is certainly beneficial, but, as we have seen, it has also offered new means for engaging in heinous illicit activities, and, in the area with which we are concerned, for the abuse of minors and offences against their dignity, for the corruption of their minds and violence against their bodies. This has nothing to do with the exercise of freedom; it has to do with crimes that need to be fought with intelligence and determination,

through a broader cooperation among governments and law enforcement agencies on the global level, even as the net itself is now global.

[…]

MESSAGE TO THE EXECUTIVE CHAIRMAN OF THE "WORLD ECONOMIC FORUM" ON THE OCCASION OF THE ANNUAL GATHERING IN DAVOS-KLOSTERS

POPE FRANCIS

23-26 January 2018

(Selected Excerpts)

[…]

At the level of global governance, we are increasingly aware that there is a growing fragmentation between States and Institutions. New actors are emerging, as well as new economic competition and regional trade agreements. Even the most recent technologies are transforming economic models and the globalized world itself, which, conditioned by private interests and an ambition for profit at all costs, seem to favour further fragmentation and individualism, rather than to facilitate approaches that are more inclusive.

[…]

"Before the many barriers of injustice, of loneliness, of distrust and of suspicion which are still being elaborated in our day, the world of labour is called upon to take courageous steps in order that 'being and working together' is not merely a slogan but a programme for the present and the future" (Ibid.). Only through a firm resolve shared by all economic actors may we hope to give a new direction to the destiny of our world. So too artificial intelligence, robotics and other technological innovations must be so employed that they contribute to the service of humanity and to the protection of our common home, rather than to the contrary, as some assessments unfortunately foresee.

[…]

STATEMENT AT THE SECOND SESSION OF THE INTERGOVERNMENTAL GROUP OF EXPERTS ON E-COMMERCE AND THE DIGITAL ECONOMY

ARCHBISHOP IVAN JURKOVIČ, PERMANENT OBSERVER OF THE HOLY SEE TO THE UNITED NATIONS AND OTHER INTERNATIONAL ORGANIZATIONS IN GENEVA

18 April 2018

(Selected Excerpts)

[…]

The "digital divide", concerning education and access to the tools of the digital age in developing and least developed countries (LDCs), remains a challenge, despite better connectivity. Digital inclusiveness has an important social impact on the ability of a population to take advantage of the opportunities of the digital age; increasingly, what might be called "e-commerce inclusiveness" deserves the attention of policymakers.

[…]

For developing countries, digitalization in particularly important sectors is evolving at different speeds, with diverse implications for the enterprises concerned.

[…]

MESSAGE FOR THE 53RD WORLD COMMUNICATIONS DAY

POPE FRANCIS

24 January 2019

(Selected Excerpts)

Dear Brothers and Sisters,

Ever since the internet first became available, the Church has always sought to promote its use in the service of the encounter between persons, and of solidarity among all. With this Message I would like to invite you once again to reflect on the foundation and importance of our being-in-relation and to rediscover, in the vast array of challenges of the current communications context, the desire of the human person who does not want to be left isolated and alone.

THE METAPHORS OF THE NET AND COMMUNITY

Today's media environment is so pervasive as to be indistinguishable from the sphere of everyday life. The Net is a resource of our time. It is a source of knowledge and relationships that were once unthinkable. However, in terms of the profound transformations technology has brought to bear on the process of production, distribution and use of content, many experts also highlight the risks that threaten the search for, and sharing of, authentic information on a global scale. If the Internet represents an extraordinary possibility of access to knowledge, it is also true that it has proven to be one of the areas most exposed to disinformation and to the conscious and targeted distortion of facts and interpersonal relationships, which are often used to discredit.

We need to recognize how social networks, on the one hand, help us to better connect, rediscover, and assist one another, but on the other, lend themselves to the manipulation of personal data, aimed at obtaining political or economic advantages, without due respect for the person and his or her rights. Statistics show that among young people one in four is involved in episodes of cyberbullying.

In this complex scenario, it may be useful to reflect again on the metaphor of the net, which was the basis of the Internet to begin with, to rediscover its positive potential. The image of the net invites us to reflect on the multiplicity of lines and intersections that ensure its stability in the absence of a centre, a hierarchical structure, a form of vertical organization. The net works because all its elements share responsibility.

From an anthropological point of view, the metaphor of the net recalls another meaningful image: the community. A community is that much stronger if it is cohesive and supportive, if it is animated by feelings of trust, and pursues common objectives. The community as a network of solidarity requires mutual listening and dialogue, based on the responsible use of language.

[…]

This multiform and dangerous reality raises various questions of an ethical, social, juridical, political and economic nature, and challenges the Church as well. While governments seek legal ways to regulate the web and to protect the original vision of a free, open and secure network, we all have the possibility and the responsibility to promote its positive use.

ADDRESS TO PARTICIPANTS IN THE PLENARY ASSEMBLY OF THE PONTIFICAL ACADEMY FOR LIFE

POPE FRANCIS

25 February 2019

(Selected Excerpts)

[…]

However, today's evolution of technical capacity casts a dangerous spell: instead of delivering the tools that improve their care to human life, there is the risk of giving life to the logic of the devices that decide its value. This reversal is destined to produce nefarious outcomes: the machine is not limited to driving alone but ends up guiding man. Human reason is thus reduced to rationality alienated from effects, which cannot be considered worthy of mankind.

[…]

It is important to reiterate: "Artificial intelligence, robotics and other technological innovations must be so employed that they contribute to the service of humanity and to the protection of our common home, rather than to the contrary, as some assessments unfortunately foresee" (Message to the World Economic Forum in Davos, 12 January 2018). The inherent dignity of every human being must be firmly placed at the centre of our reflection and action. In this regard, it should be noted that the designation of "artificial intelligence", although certainly effective, may risk being misleading. The terms conceal the fact that – in spite of the useful fulfilment of servile tasks (this is the original meaning of the term "robot"), functional automatisms remain qualitatively distant from the human prerogatives of knowledge and action. And therefore they can become socially dangerous. Moreover, the risk of man being "technologized", rather than technology humanized, is already real: so-called "intelligent machines" are hastily attributed capacities that are properly human.

[…]

CONCLUDING STATEMENT FROM THE CONFERENCE ON ROBOTICS, ARTIFICIAL INTELLIGENCE AND HUMANITY, SCIENCE, ETHICS AND POLICY

PONTIFICAL ACADEMY OF SCIENCES AND PONTIFICAL ACADEMY OF SOCIAL SCIENCES

16-17 May 2019

(Selected Excerpts)

ISSUES AND AGENDA

[…]

5. Of growing concern are the risks for peace due to new forms of warfare (cyber-attacks, autonomous weapons), calling for new international security regulations.

6. Ethical and religious aspects of AI and robotics need clarification in order to guide potential needs for regulatory policies on applications and the future development of AI/robotics.

[…]

ADDRESS TO THE PARTICIPANTS IN THE SEMINAR "THE COMMON GOOD IN THE DIGITAL AGE"

POPE FRANCIS

27 September 2019

(Selected Excerpts)

[…]

If technological advancement became the cause of increasingly evident inequalities, it would not be true and real progress. If mankind's so-called technological progress were to become an enemy of the common good, this would lead to an unfortunate regression to a form of barbarism dictated by the law of the strongest. Dear friends, I thank you, therefore, because by your work you are engaged in efforts to promote civilization, whose goal includes the attenuation of economic, educational, technological, social and cultural inequalities.

You have laid a strong ethical foundation for the task of defending the dignity of every human person, convinced that the common good cannot be separated from the specific good of each individual. Your work will continue until no one remains the victim of a system, however advanced and efficient, that fails to value the intrinsic dignity and contribution of each person.

A better world is possible thanks to technological progress, if this is accompanied by an ethic inspired by a vision of the common good, an ethic of freedom, responsibility and fraternity, capable of fostering the full development of people in relation to others and to the whole of creation.

[…]

STATEMENT AT THE 74TH SESSION OF THE UNITED NATIONS GENERAL ASSEMBLY ON GALVANIZING MULTILATERAL EFFORTS FOR THE ERADICATION OF POVERTY, QUALITY EDUCATION, CLIMATE ACTION AND INCLUSION

CARDINAL PIETRO PAROLIN, SECRETARY OF STATE OF THE HOLY SEE

28 September 2019

(Selected Excerpts)

[…]

The proliferation of weapons is particularly alarming as it spurs and exacerbates violence, conflict and war. The Secretary-General's Report documents that armed groups are multiplying, worldwide military spending and arms competition are increasing, and the threat of the weaponization of artificial intelligence, cyberspace and outer space is growing.[4]

[…]

Notes

4. Report of the Secretary-General on the work of the Organization (A/74/1), paragraph 112.

STATEMENT AT THE 59TH SERIES OF MEETINGS OF THE WORLD INTELLECTUAL PROPERTY ORGANIZATION ASSEMBLIES

ARCHBISHOP IVAN JURKOVIČ, PERMANENT OBSERVER
OF THE HOLY SEE TO THE UNITED NATIONS AND OTHER
INTERNATIONAL ORGANIZATIONS IN GENEVA

1 October 2019

(Selected Excerpts)

[…]

If technological advancement is a cause of increasingly evident inequalities, then it should not be considered real progress. As recalled by Pope Francis "if mankind's so-called technological progress were to become an enemy of the common good, this would lead to an unfortunate regression to a form of barbarism dictated by the law of the strongest"1. The effort to develop "intelligent machines" must be continuously directed to the greater good, reducing the poverty gap and facing general needs for health, education, happiness and sustainability.

[…]

A better world is possible thanks to technological progress, but this must be accompanied by value inspired by a vision of the common good, an ethic of freedom, responsibility and fraternity, capable of fostering the full development of people in relation to others and to the whole of creation.

[…]

ADDRESS TO THE PARTICIPANTS IN THE CONGRESS ON "CHILD DIGNITY IN THE DIGITAL WORLD"

POPE FRANCIS

14 November 2019

(Selected Excerpts)

[…]

A greater awareness of the enormity and gravity of these phenomena is urgently required. Indeed, one feature of today's technological development is that it is always one step ahead of us, for frequently we first see its most attractive and positive aspects (which indeed are many), but only realize their negative effects once they are widespread and very hard to remedy. I would say this to you, who are scholars and researchers: you find yourselves before an essential challenge! Since these problems are vast and complex, a clear understanding of their nature and extent is needed. We cannot deceive ourselves into thinking that we can address these issues on the basis of shallow and superficial knowledge. Laying the foundations for greater protection of the dignity of minors should be one of the most noble aims of your scientific research.

[…]

A crucial aspect of the problem concerns the tension – which ultimately becomes a conflict – between the idea of the digital world as a realm of unlimited freedom of expression and communication, and the need for a responsible use of technologies and consequently a recognition of their limits.

The protection of complete freedom of expression is linked to the protection of privacy through increasingly sophisticated forms of message encryption, which would make any control extremely difficult, if not impossible.

[…]

Large companies are key players in the astonishing development of the digital world; they easily cut across national borders, are at the cutting edge of technological advances, and have accumulated enormous profits. It is now clear that they cannot consider themselves completely unaccountable vis-à-vis the services they provide for their customers.

[…]

In a world like ours, where boundaries between countries are continually blurred by the developments in digital technology, our efforts should emerge as a global movement associated with the deepest commitment of the human family and international institutions to protecting the dignity of minors and every human person. This demanding task sets before us new and challenging questions. How can we defend the dignity of persons, including minors, in this digital age, when the life and identity of an individual is inextricably linked to his or her online data, which new forms of power are constantly seeking to possess? How can we formulate shared principles and demands in the globalized digital world? These are challenging questions that call us to cooperate with all those working with patience and intelligence for this goal at the level of international relations and regulations.

[…]

ADDRESS TO THE PARTICIPANTS IN THE PLENARY ASSEMBLY OF THE PONTIFICAL ACADEMY FOR LIFE

PREPARED BY POPE FRANCIS, READ BY ARCHBISHOP VINCENZO PAGLIA, PRESIDENT OF THE PONTIFICAL ACADEMY FOR LIFE

28 February 2020

(Selected Excerpts)

[…]

The issues you have addressed in these days concern one of the most important changes affecting today's world. Indeed, we could say that the digital galaxy, and specifically artificial intelligence, is at the very heart of the epochal change we are experiencing. Digital innovation touches every aspect of our lives, both personal and social. It affects our way of understanding the world and ourselves. It is increasingly present in human activity and even in human decisions, and is thus altering the way we think and act. Decisions, even the most important decisions, as for example in the medical, economic or social fields, are now the result of human will and a series of algorithmic inputs. A personal act is now the point of convergence between an input that is truly human and an automatic calculus, with the result that it becomes increasingly complicated to understand its object, foresee its effects and define the contribution of each factor.

To be sure, humanity has already experienced profound upheavals in its history: for example, the introduction of the steam engine, or electricity, or the invention of printing which revolutionized the way we store and transmit information. At present, the convergence between different scientific and technological fields of knowledge is expanding and allows for interventions on phenomena of infinitesimal magnitude and planetary scope, to the point of blurring boundaries that hitherto were considered clearly distinguishable: for example, between inorganic and organic matter, between the real and the virtual, between stable identities and events in constant interconnection.

On the personal level, the digital age is changing our perception of space, of time and of the body. It is instilling a sense of unlimited possibilities, even as standardization is becoming more and more the main criterion of aggregation. It has become increasingly difficult to recognize and appreciate differences. On the socio-economic level, users are often reduced to "consumers", prey to private interests concentrated in the hands of a few. From digital traces scattered on the internet, algorithms now extract data that enable mental and relational habits to be controlled, for commercial

or political ends, frequently without our knowledge. This asymmetry, by which a select few know everything about us while we know nothing about them, dulls critical thought and the conscious exercise of freedom. Inequalities expand enormously; knowledge and wealth accumulate in a few hands with grave risks for democratic societies. Yet these dangers must not detract from the immense potential that new technologies offer. We find ourselves before a gift from God, a resource that can bear good fruits.

ANNEX TO THE PUBLIC CONSULTATION ON THE WHITE PAPER ON ARTIFICIAL INTELLIGENCE - A EUROPEAN APPROACH

COMMISSION OF THE BISHOPS' CONFERENCES OF THE EUROPEAN UNION (COMECE)

June 2020

(Selected Excerpts)

[…]

AI AND CYBER-SECURITY

The use of AI may not only bring innovative and effective tools enhancing security in a digital environment, but it may also open up new vulnerabilities. AI algorithms could be manipulated and, with the Internet of Things, lead to faster and more destructive attacks on critical infrastructures.

In the context of digital diplomacy, the misuse of AI can potentially have far-reaching consequences for the democratic order, for example, through an uncontrolled spread of disinformation or through external influences exercised by foreign state, economic or other non-state actors.

In this context, we encourage the EU, in particular, to:

- Define specific mandatory requirements for particularly risky AI technologies against cyber-threats affecting public and citizens' safety.
- Support capacity-building in view of strengthening the resilience of critical infrastructures, as well as of businesses and citizens against AI-induced security challenges.
- Scrutinise the role of private companies and of the actual beneficiaries of the effective final control regarding the collection and analysis of personal data.

ENCYCLICAL LETTER FRATELLI TUTTI

POPE FRANCIS

3 October 2020

(Selected Excerpts)

[…]

262. Rules by themselves will not suffice if we continue to think that the solution to current problems is deterrence through fear or the threat of nuclear, chemical or biological weapons. Indeed, "if we take into consideration the principal threats to peace and security with their many dimensions in this multipolar world of the twenty-first century as, for example, terrorism, asymmetrical conflicts, cybersecurity, environmental problems, poverty, not a few doubts arise regarding the inadequacy of nuclear deterrence as an effective response to such challenges. These concerns are even greater when we consider the catastrophic humanitarian and environmental consequences that would follow from any use of nuclear weapons, with devastating, indiscriminate and uncontainable effects, over time and space… We need also to ask ourselves how sustainable is a stability based on fear, when it actually increases fear and undermines relationships of trust between peoples. International peace and stability cannot be based on a false sense of security, on the threat of mutual destruction or total annihilation, or on simply maintaining a balance of power… In this context, the ultimate goal of the total elimination of nuclear weapons becomes both a challenge and a moral and humanitarian imperative… Growing interdependence and globalization mean that any response to the threat of nuclear weapons should be collective and concerted, based on mutual trust. This trust can be built only through dialogue that is truly directed to the common good and not to the protection of veiled or particular interests".[244] With the money spent on weapons and other military expenditures, let us establish a global fund[245] that can finally put an end to hunger and favour development in the most impoverished countries, so that their citizens will not resort to violent or illusory solutions, or have to leave their countries in order to seek a more dignified life.

Notes

244. Message to the United Nations Conference to Negotiate a Legally Binding Instrument to Prohibit Nuclear Weapons (23 March 2017): AAS 109 (2017), 394-396.

245. Cf. SAINT PAUL VI, Encyclical Letter Populorum Progressio (26 March 1967): AAS 59 (1967), 282.

ADDRESS TO THE MEMBERS OF THE DIPLOMATIC CORPS ACCREDITED TO THE HOLY SEE

POPE FRANCIS

8 February 2021

(Selected Excerpts)

[…]

The pandemic, which forced us to endure long months of isolation and often loneliness, has brought out the need of every individual for human relationships. I think before all else of those students who were unable to attend school or university regularly. "Attempts have been made everywhere to offer a rapid response through online educational platforms. These have brought to light a marked disparity in educational and technological opportunities, but they have also made us realize that, due to the lockdown and many other already existing needs, large numbers of children and adolescents have fallen behind in the natural process of schooling".[12] Furthermore, the increase in distance learning has also led to a greater dependence of children and adolescents on the internet and on virtual forms of communication in general, making them all the more vulnerable and overexposed to online criminal activities.

Notes

12. Video Message for the Meeting "Global Compact on Education. Together to Look Beyond" (15 October 2020).

STATEMENT AT THE HIGH-LEVEL SEGMENT OF THE CONFERENCE ON DISARMAMENT

ARCHBISHOP PAUL RICHARD GALLAGHER, SECRETARY FOR RELATIONS WITH STATES OF THE HOLY SEE

24 February 2021

(Selected Excerpts)

[…]

"While the importance of disarmament is particularly evident for nuclear, chemical and biological weapons, it applies just as strongly to the increased military competition in outer space, as well as in the fields of cyberspace and artificial intelligence"

[…]

STATEMENT AT THE FIRST COMMITTEE OF THE 76TH SESSION OF THE UNITED NATIONS GENERAL ASSEMBLY

ARCHBISHOP GABRIELE CACCIA, PERMANENT OBSERVER OF THE HOLY SEE TO THE UNITED NATIONS IN NEW YORK

18 October 2021

(Selected Excerpts)

[...]

CYBER SECURITY

Many Delegations have addressed the risks posed by the misuse of the ever-evolving information and communication technologies, in cyberspace and in daily life. Indeed, these risks need urgent attention, to preclude the further pursuit of means to disrupt commerce and communication. The development of information and communication technologies (ICTs) has brought with it the inevitable increase in global connectivity and in reliance on such technologies. Therefore, the "imperative of building and maintaining international peace, security, cooperation and trust in the ICT environment has never been so clear".[1] The final Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security expressed shared concern that "harmful ICT incidents are increasing in frequency and sophistication and are constantly evolving and diversifying. Increasing connectivity and reliance on ICTs without accompanying measures to ensure ICT security can bring unintended risks, making societies more vulnerable to malicious ICT activities. Despite the invaluable benefits of ICTs for humanity, their malicious use can have significant and far-reaching negative impacts." A cyber tool may not look like a gun or a bomb, but its malicious use can be even more destructive on civilians, as seen in attacks on critical infrastructure such as medical facilities, energy systems and water supplies.

There is even greater reason to ensure the security of technologies operating in cyberspace and to prevent interference with the command and control of weapon systems, especially nuclear weapons. Until such weapons can be eliminated, it is not only highly imprudent but deeply problematic to maintain systems in which an electronic intrusion into its controls might lead to the launch and detonation of a nuclear weapon. Thus, rules and norms negotiated in an intergovernmental forum to ensure the peace and

security of cyberspace are necessary. The Open-Ended Working Group, established for this purpose, is well suited to bring this about, and is, in and of itself, an important confidence-building measure.

[…]

NOTES

1. A/75/816.

CONCLUSIONS

CYBERSPACE: AN INSTRUMENT OF FRATERNITY? BETWEEN ETHICS AND INTERNATIONAL ACTION

VINCENZO BUONOMO
Professor Vincenzo Buonomo, Rector, Pontifical Lateran University

1.

When addressing the issue of cyberspace, progress, vulnerability, intervention measures, and the sharing of results are its most evident expressions. These expressions are no longer a theoretical possibility, but are an active reality in which we operate, at all times and by all means. What is most concerning now is that, what was initially experienced as an expression of freedom and relationship, has resulted in a field characterized by expansion without verification and possibility of control, limitless sharing of volumes of information, the fear for maintaining the integrity of one's identity, the risk of losing personal data, the primacy of technology over knowledge; the list goes on and on. Even more alarming are the continuous violations and the uncontrollable possibilities that ever-advancing technology and cyberspace activity is capable of bringing about. In this context, filled with innumerable uncertainties and void of clarity, we need an approach that attempts to identify criteria and prospects for building up an ethical boundary. Such an approach is not intended simply to prevent existing and developing threats but, above all, to inspire techniques to regulate behavior, including both individual and collective activity, and to inspire common practices or the protection of specific profiles (intellectual property, processes and new acquisitions, for example).

Such an approach is not intended simply to prevent existing and developing threats but, above all, to inspire techniques to regulate behavior, including both individual and collective activity, and to inspire common practices or the protection of specific profiles.

This problem does not simply concern States; rather it directly and primarily increases the capacities at the disposal of companies, individuals, and governmental bodies, based on the use of these new systems. This is the case even when such systems are purported to be a means of gathering consensus or when, based on the result of research and studies, they demonstrate their effectiveness. Therefore, while acknowledging the advantages and the progress attained through the development of artificial intelligence, we can no longer ignore the extent to which cyberspace has become today a *commons* (agora) in which "power" is manifested, possibly linked to the use of force or at least aimed at affirming the existence of particular interests, including selfish ones. Such a perspective risks (and indeed succeeds!) to obliviate the fact that the fruit of human thought,

efforts and intelligence contributes essentially to provide continuity to the plan of creation. In reality, this human element stands necessarily as a common denominator, placed at the service and benefit of each and all.

A systematic study shows that cyberspace is a structured and specialized field which imposes on decision-makers, in any field, a conceptual strategy capable of discerning the needs of the global order so as to face the difficulties that affect all processes, both internal and international, in the name of the principle "what is not forbidden is allowed". Therefore, it is not enough to evaluate cyberspace through criteria that can determine crises or inflict repercussions on the orderly life of our societies, but it is also necessary to indicate the positive effects and spaces that can foster effective cooperation and integral development. In essence, it is necessary to foster a full recognition of the dignity of persons, communities and peoples. Similarly, it is not enough to quantify the positive effects of the new opportunities offered by cyberspace and to identify the extent and positive usefulness of their implementation, while forgetting the structural deficiencies that such opportunities pose, considering an ethical dimension and a moral evaluation only as an afterthought. We are faced with questions and challenges that "cannot be resolved by piecemeal solutions or quick fixes. Much needs to change, through fundamental reform and major renewal. Only a healthy politics, involving the most diverse sectors and skills, is capable of overseeing this process"[1], as the social magisterium of the Catholic Church has affirmed through an analysis inspired by that healthy realism capable of identifying concrete situations, evaluating them, and then offering indicators for the actions of individuals and communities.

Therefore, it is not enough to evaluate cyberspace through criteria that can determine crises or inflict repercussions on the orderly life of our societies, but it is also necessary to indicate the positive effects and spaces that can foster effective cooperation and integral development.

The understanding and the consequent use of cyberspace impose the need to intercept reality from when it emerges. We are at a crossroads: we can either accept fear, discouragement, and an objective near impotence in the face of an interconnected and complex system, or we can discover the desire to contribute to modern advancements, as protagonists who seek to bring attention to that ethical component so often invoked, but too often ignored. The ability to analyze, therefore, imposes a clear choice aimed at determining the ways in which destabilizing situations can be transformed into possibilities and objectives can make up for shortcomings, reduce risks, and bridge the widening gaps.

Can the cyberspace sphere be a vehicle capable of generating concrete acts of fraternity?

We are faced, then, with a question: can the cyberspace sphere be a vehicle capable of generating concrete acts of fraternity? A first answer lies in understanding fraternity as a concrete instrument of life in common, as a source of that common good of all and of everyone. One often speaks about the common good, and it is easy to desire its implementation. Nonetheless, such sentiments are often reduced to a mere aspiration.

2.

It is a well-known fact that cyberspace has altered the way of communicating and, indeed, the way of living for the entire human family. We must not forget, however, that the cyber divide that is experienced on a daily basis is just as certain, at least in comparison with previous situations. It is certainly not the first time that innovation has changed the paradigm of ways of thinking, operating, and evaluating, even to the point of modifying lifestyles. But in this case, to the divide between before and after, a new and very significant element is added: while for centuries, territories were defined by clear boundaries within which authorities exercised their power, today there is a significant difficulty in concretely identifying these territories laid down as "cyber spaces".

What follows, then, is the challenge to identify the specific political and institutional processes that correspond to novel realities introduced by cyberspace. Indeed, experience tells us that such processes are now determined, in a direct or indirect way, by the emergence and progress of cyberspace. Moreover, the verification of the negative effects of the activities produced through technology and cyberspace have become crucial for our understanding and action. After all, there are many crises on the global level that have originated from what experts identify as cyberconflict, in its various forms of attack, data theft, aggression and even war.

Evidently, it is no longer possible to consider cyberspace as mere technical data or, in any case, to qualify it as an environment in which one operates to design processes, even if not always effective, by taking advantage of new tools, often problem-solving tools. Similarly, those perspectives that would link cyberspace to the transmission and exchange of information remain limited. This is even more the case when cyberspace is reduced to its "practical" aspect and effect: to an immediate circulation (in zero time) of news and data on real events, or which aims at building imaginary and often misleading scenarios due to inaccuracies or even willful unreliability.

Evidently, it is no longer possible to consider cyberspace as mere technical data or, in any case, to qualify it as an environment in which one operates to design processes, even if not always effective, by taking advantage of new tools.

We are aware that for our societies, information is no longer a fact, but a right and a manifestation of freedom. For this reason, we tend to consider any protective instrument or measure, which enshrines the use and/or the access to cyberspace as a fundamental right, in a positive light. This is true even if we perceive or recognize the resulting threats and dangers to the ordinary course of social relations, the functioning of statehood institutions and wider international cooperation implemented by the multilateral system.

At this point, the elements we have at our disposal confirm that the cyberspace sphere is something capable of truly compromising not only data and situations, but also risks the broader stability which constitutes the necessary foundation for fraternal relations between people and

communities, as well as relations of peace and security in international relations.

Faced with this complexity, many questions arise regarding which spaces to grant, where to intervene in order to control cyberspace, and how we can incorporate fraternity. A preliminary response resides in the aspiration to include, in every action, the rightful "recognition of certain incontestable natural ethical limits"[2]. Thus, we are not interpreting an ideal or ideological need, nor a political line. Rather, we are recognizing the desire of all, the willingness of many, and the opposition of a few. Starting from such an approach, far from adopting assertive tones or the desire to unilaterally impose authority, fraternity makes it possible to construct a specific approach and methodology that does not simply evaluate cyberspace in the light of Church doctrine, but rather indicates possible ways and spaces in which the Christian vision and message can find a place in this "new sphere" and make its contribution. This initiative requires the use and, in certain cases, the interpretation of language that is proper to the technical dimension, with the conviction that these efforts will bolster that same technical dimension.

Starting from such an approach, far from adopting assertive tones or the desire to unilaterally impose authority, fraternity makes it possible to construct a specific approach and methodology that does not simply evaluate cyberspace in the light of Church doctrine, but rather indicates possible ways and spaces in which the Christian vision and message can find a place in this "new sphere" and make its contribution.

Furthermore, access to and use of cyberspace has modified strategies and modalities of communication, which then require recourse and margins of control to avoid its instrumentalized or improper use. These aspects have changed the traditional distinctions between public and private, between information and communication, and have even modified relations between States, their ability to react, and the way they respond to threats or regulatory gaps.

3.

This analysis shows that cyberspace is a new territory and a virtual sovereign space, within which relationships are woven, bonds and obligations are established, and policies and strategies of action are outlined. It is not an ephemeral space since in it there are increasingly widespread intrusions as well as real acts of aggression that make prevention difficult.

Rather than being oriented to achieve the major objectives of security, development, respect for human rights, and above all the full self-determination of peoples, cyber capacity building has now emerged as a force capable of limiting actions so as to ensure that justice which is "properly sought solely out of love of justice itself, out of respect for the victims, as a means of preventing new crimes and protecting the common good"[3]. Hence, there is a need to utilize cyber capacity as a catalyst for creating spaces of fraternity, that is, relationships of solidarity which are fair and respectful of the substantial equality of all people, communities, and populations.

Understood in this fashion, the capacity to operate in cyberspace would be firmly rooted upon a concrete foundation with a clear field of activity, capable of preventing the development of mechanisms that currently fall between the cracks of every preventative system in place and that are aimed at limiting or undermining public subjects, companies, or individuals. Moreover, it will be able to respond to the need for regulatory measures that, while perhaps difficult to implement within the internal legislation of individual countries, could nonetheless by realized on the multilateral level, to respond to the indispensable need for a shared approach and implementation. This is necessary not only to protect traditional borders or territories, but also to provide the stability that cyberspace and the activities that take place within it require.

In this way, the social doctrine of the Church is called to confront a challenge that has emerged in contemporary societies. To respond adequately to this challenge requires availability, competence, and a methodology that is capable of teaching and inspiring fraternity. By building bridges of relationships, the Church can offer its expertise, not by standing in judgment of society but, rather, by uniting people, facts and processes: "Rather than experts in dire predictions, dour judges bent on rooting out every threat and deviation, we should appear as joyful messengers of challenging proposals, guardians of the goodness and beauty which shine forth in a life of fidelity to the Gospel"[4]. This initiative is fully consistent and in continuity with the Church's mission, to proclaim "the Good News to all creatures" (Mk 15:16). Today, this mission cannot fail to take advantage of the opportunities offered by cyberspace, appreciating its positive aspects and aware of its limits.

To respond adequately to this challenge requires availability, competence, and a methodology that is capable of teaching and inspiring fraternity. By building bridges of relationships, the Church can offer its expertise, not by standing in judgment of society but, rather, by uniting people, facts and processes.

Notes

1. Francis, Encyclical *Fratelli Tutti*, 3 October 2020, 179, text available at https://www.vatican.va/content/francesco/en/encyclicals/documents/papa-francesco_20201003_enciclica-fratelli-tutti.html (accessed 06/29/2021).

2. Francis, *Address to the UN General Assembly*, 25 September 2015, text available at https://www.vatican.va/content/francesco/en/speeches/2015/september/documents/papa-francesco_20150925_onu-visita.html (accessed 06/29/2021).

3. *Fratelli Tutti*, 252.

4. Francis, Apostolic Exhortation *Evangelii Gaudium*, 23 November 2013, 168, text available at https://www.vatican.va/content/francesco/en/apost_exhortations/documents/papa-francesco_esortazione-ap_20131124_evangelii-gaudium.html (accessed 06/29/2021).

Imprimé en France par IOF Imprimerie du Marais

Dépôt légal décembre 2021

ISBN: 978-2-8399-3461-9