Cyberstability Paper Series

New Conditions and Constellations in Cyber

Is There Space for a Digital Non-Aligned Movement?

Latha Reddy
Co-Chair of the Global Commission on the Stability of Cyberspace,
Former Deputy National Security Advisor of India

Anoushka Soni
National University of Juridical Sciences, Kolkata

September 2021

Cyberstability Paper Series
New Conditions and Constellations in Cyber

Is There Space for a Digital Non-Aligned Movement?

Latha Reddy | Co-Chair of the Global Commission on the Stability of Cyberspace, Former Deputy National Security Advisor of India

Anoushka Soni | National University of Juridical Sciences, Kolkata

September 2021

In an increasingly interconnected world, the discourse surrounding international norm settings in cyberspace has taken center stage. Digital rivalries between major world powers, particularly the United States and China, have necessitated a reevaluation of geopolitical affiliations by a number of historically neutral or non-aligned nations, such as India, Brazil, and others, when these countries take into consideration their national economic and security concerns. It is evident that, in this situation of increasingly great power polarity, many countries are seeking the creation of an alternative political space that allows them to exercise strategic autonomy. The formation of the Non-Aligned Movement in 1961 was a product of similar desires, and the same incentive now exists that demands a relook at traditional notions of non-alignment, as well as the emergence of new conceptualizations of non-alignment for a digital age.

Firstly, this paper addresses the increasingly heated debate on digital issues, and the various geopolitical, economic and security concerns that have arisen out of them, with a focus on 5G implementation as a case study. It also analyzes the traditionalist notion of the Non-Aligned Movement ("NAM")—its concerns, advocacy efforts, and the space it occupies within this digital age. Secondly, the paper engages with the notion of Europe as the new face of non-alignment, and details the

Latha Reddy is Co-Chair of the Global Commission on the Stability of Cyberspace. She is the former Deputy National Security Adviser of India, where she was responsible for cybersecurity and other critical internal and external security issues. Previously she also served as a Commissioner on the Global Commission on Internet Governance.

Anoushka Soni is a final year law student at the National University of Juridical Sciences, Kolkata. She has an avid interest in technology as well as international law, and was the Associate Director of the Society for International Law and Policy at NUJS.

individual and divergent concerns plaguing leading European nations. It also proposes a model for European integration on the 5G issue, through regional collaboration, flexibility, and identification of common ground. Finally, the paper attempts to bring together the traditional ideas of non-alignment with the emerging ones, and proposes a joint 5G Initiative requiring involvement of leaders in the European Union ("EU") as well as NAM, to usher in a new era of digital non-alignment.

The formation of the Non-Aligned Movement itself came from the desire to exercise greater collective bargaining power against existing "superpowers," while remaining detached from the conflict. The members of NAM concerned themselves with ensuring that they were not left as mere spectators in paramount issues of global importance, such as the nuclear arms race. They first came together to demand that a seat at the nuclear policy-making table could not be restricted solely to those states that were the reason for, or part of, the problem, and that being a potential victim of the use of nuclear weapons was a sufficient stake in the issue. Given that technology was a crucial factor in the clash between the United States and the Soviet Union during the first Cold War, it is unsurprising that the current conflict between the United States and China is being termed as the "next Cold War" and is similarly entrenched within emerging digital technology issues.[1]

A major issue of global concern that finds itself center stage at present is the deployment of fifth generation cellular networks, or 5G, and therefore is the primary focus of this analysis. Although the 5G debate may be seen as newly emerging, its foundations were laid down years ago, when, in 2012, the US House Intelligence Committee released an "Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE."[2] The Investigative Report primarily raised concerns on the surveillance capabilities of these companies, and the national security threat to the US that letting them set up on American soil would pose. This escalated in 2020, when the Federal Communications Commission ("FCC") formally designated Huawei and ZTE as "national security threats" on account of accusations of their affiliations with the Chinese government, and of their harvesting data of US citizens.[3]

The strengths in Chinese 5G technology lie primarily in the higher quality and its lower cost as compared to the technology offered by its European competitors.[4] However, concerns over Chinese technology have never been about quality considerations, but rather suspicion over surveillance and security issues, and the increasing supremacy accorded to these concerns over economic considerations has led to a cascading effect across the world economy. This is only exacerbated through Chinese surveillance laws, which mandate cooperation with the government upon request,[5] as well as the existing affiliation that exists between large Chinese companies and the ruling Communist Party.[6] The blocking of Huawei and ZTE by the US have been accompanied by restrictions on chip-making equipment, leading to losses amounting to billions of dollars in profits for the semiconductor industry.[7] The consequences of these measures within the US are not restricted to monetary losses only, but go beyond them into constricting the amount the semiconductor companies can spend on research and development into improving their own technology.[8] Simultaneously, the Chinese semiconductor industry remains underdeveloped and reliant on foreign—mostly US—chip providers, or European manufacturers of semiconductor fabrication machinery, and therefore the ban had an impact on Chinese semiconduction production as well. Therefore, the trade war on semiconductors could lead to the unintended effect of a decline in the quality of cutting-edge technology within the US, while simultaneously hampering China from building expertise in specialist chips. The conflict will also manifest itself in developing nations, specifically those in Eastern Europe and Africa, where Chinese equipment, due to its substantially lower cost, forms the bulk of the basis of Internet access in the region.[9] While the US may be able to afford the economic consequences of banning Chinese companies, taking this hardline stance without

providing its developing friends and allies with an alternative may end with the world divided not only on political lines, but with a redrawing of those lines out of economic necessity, and with states prioritizing the responsibility they have to their own people.

The pervasive nature of this dispute cannot be constrained bilaterally to one between the US and China. It is part of a wider supply chain security issue, given the opposing interests and alliances at stake, and could lead to the burgeoning of a "Cold War 2.0," which is to be fought not on moralistic and ideological grounds, but instead on technological lines through trade battles and economic coercion.[10] Countries such as the United Kingdom ("UK"), which had initially allowed Huawei's participation in its 5G infrastructure, have reversed their decision on security grounds.[11] Countries in the Gulf, such as Saudi Arabia, Bahrain, and Qatar, etc.,[12] as well as Asian powers such as India,[13] have also been forced by their various specific geopolitical concerns, weighed against economic interests as well as foreign pressure, to enter into the 5G debate.

To mitigate the impact of this conflict, NAM must once again come together to ensure the free flow of technology and data, while simultaneously guaranteeing protection to the sovereign interests of nations. There must be an active attempt to achieve digital non-alignment, which requires economic investments and political strategy decisions to be made in such a way so as to avoid dependence on digital products from either the US or China.[14] The members of NAM are uniquely placed in this regard, since their individual geopolitical and economic considerations often compel them toward non-alignment as a political philosophy. To achieve their objectives, NAM has made submissions to various multilateral forums such as the Open-ended Working Group ("OEWG") as established by the UN General Assembly.

NAM must once again come together to ensure the free flow of technology and data, while simultaneously guaranteeing protection to the sovereign interests of nations.

The primary concerns on international cybersecurity iterated by NAM are first, that cyberspace will become a "theatre of military operations" through the development of cyber-offensive capabilities and the malicious use of ICTs, which will adversely impact the integrity and security of state infrastructure.[15] Second, there is the possibility of the adoption of unilateral measures beyond the ambit of the Charter of the United Nations and international law, which must be avoided so as not to impede the economic and social development of affected countries. Third, there is the concern that the development of an international legal framework would not be consensus-based but "top down" by a very small, self-appointed group, and therefore NAM has advocated for a framework within the UN with "active and equal" participation of all states. This must be accompanied by a multilateral inclusive institutional platform solely dedicated to international cooperation on safeguarding the peaceful uses of ICTs. Their final concern is that the digital divide between connected and less connected nations will continue to impact them adversely, leading to NAM recommendation that the digital divide be transformed into digital opportunities, for inclusive and non-discriminatory access to knowledge, and extension of support to developing countries in capacity building.

The final report by the OEWG addresses most of the concerns put forth by NAM, barring the recommendation that the legal framework must be accompanied by a "multilateral inclusive institutional platform dedicated to international cooperation on safeguarding the peaceful use of ICTs."[16] The NAM statement, though ambiguous, may be seen as seeking the establishment of a permanent forum within the UN, which is multilateral, inclusive and institutionally dedicated to international cooperation in ICTs. However, the OEWG report reiterates the OEWG itself as a "democratic, transparent, and inclusive platform" as well as the initiator of regular institutional dialogue on the

developments in ICTs in the context of international security. There exists a visible contrast between NAM's constant emphasis on multilateralism,[17] which is theoretically defined as the coordinated diplomatic interaction of three or more states in international politics, often accompanied by a commitment to certain core values,[18] and the OEWG's insistence on restricting "multilateral" only to the level of dialogue that must be achieved. Further, in a sphere where discourse is increasingly divided, the fear of resort to unilateralism and unilateral solutions is pervasive, and that is why NAM views multilateralism as the only sustainable method of addressing these security concerns.

The enhanced focus on the security implications of 5G, and the pervasive presence of national security concerns in 5G decisions taken by countries such as India, the UK, and the US, etc., evince that this issue has become entrenched within a sphere that has traditionally been governmental prerogative. National security issues are at the forefront of what states consider primarily governmental decisions, which may justify the necessarily multilateral leaning of the 5G debate in recent times. Effective multistakeholder involvement in 5G would, therefore, be limited to non-critical spheres such as infrastructure development and capacity building, and a governmental prioritization of national security concerns may overshadow these. Further, existing multilateral forums, such as the International Telecommunications Union ("ITU"), that are working on telecommunications and could contribute to the 5G debate by inclusion of their existing stakeholder groups, have so far directed their focus toward a technical analysis of the costs and vulnerabilities of the 5G network, rather than transforming themselves into a forum for engagement on the broader discourse around 5G.[19] This change of focus is perhaps linked to the existing ITU Secretary-General Zhao Houlin being a Chinese national, and China being the fifth-largest contributor to the ITU's budget as well, which has allowed it to play a central role in international standard setting.[20]

However, a leaning toward multilateralism need not mean the exclusion of the multistakeholder model, as evinced by the nonstate consultation process around the first UN OEWG,[21] or the accessibility of the Group of Governmental Experts on Lethal Autonomous Weapon Systems ("GGE LAWS") to non-state actor participation. The GGE LAWS, for instance, a primarily inter-governmental forum, contains representatives of non-governmental organizations, various law schools, universities, and research institutes who also actively participate and contribute, despite LAWS ostensibly being an issue of national security.[22] Therefore, the multilateral approach adopted by the GGE on LAWS is not independent of stakeholder input, to ensure transparency and accountability in the process. Similarly, primarily multistakeholder models, such as the Internet Governance Forum ("IGF"), have proposed extensions such as the IGF Plus, which is intended to provided additional multistakeholder and also multilateral legitimacy.[23] These proposals recognize the importance of multilateral input in addressing shortcomings of the multistakeholder model, such as lack of actionable outcomes due to limited government participation, especially from small and developing countries.

Simultaneously, while NAM members often attempt to maintain neutrality to access these multistakeholder frameworks, they are compelled by their own competing economic and security interests to take a stance on such issues. For instance, the Indian position on 5G was reflective of a desire to balance these interests, which devolved into an increasingly clear exclusion of China from the Indian market. Though India initially permitted all applicants to participate in 5G trials,[24] a security review was later mandated with an emphasis on Chinese companies specifically,[25] and the border skirmish in the Galwan valley led to a ban on 260 Chinese smart phone apps on national security grounds.[26] Subsequently, the Department of Telecommunications of India permitted the conduction of trials for the usage and application of 5G technology by telecom service providers, including Ericsson, Nokia, Samsung, and C-DOT, with a notable absence of Chinese equipment

manufacturers.[27] India's position, with it being a founding and influential member of NAM, may influence other members of NAM to clarify their strategic orientations, and to abandon neutrality in favor of crucial national interests.

In other spheres of international debate where NAM has exercised influence, their statements carry weight because the interests of all their members align, such as in the case of LAWS under the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects ("CCW"). The statement made by NAM before the GGE concretely calls for a legally binding international instrument that has provisions both for the prohibition and regulation of LAWS.[28] Through extensive lobbying, especially with states that are concerned about the increasingly asymmetric nature of warfare and reflecting such concerns in their statements, NAM was able to achieve consensus building on a polarized issue, and exert their influence on a global stage. In the case of LAWS, members of NAM are similarly situated, since most developing nations have not achieved the technological advancement necessary to develop their own fully autonomous weapons systems. However, unlike LAWS, the individualistic national security nature of the 5G debate presents a diverging set of state-specific issues when compared to the global ethical and security concerns of asymmetric warfare that LAWS raises.[29] Therefore, similar consensus building across all emerging technologies will mean achieving the unlikely goal of setting aside these individual security concerns in favor of collective interests.

With the positions of the members of NAM and their alliances in the Digital Cold War remaining uncertain, it remains to be seen whether Europe can provide a middle ground among the technological protectionism and trade clashes escalating globally. The absence of a unified position within Europe on the 5G issue is indicative of a larger divide in the European system itself. The 5G debate was most politicized within the United Kingdom, where access was initially granted to Huawei; however, following the sanctions imposed on Huawei by Washington, UK mobile providers were subsequently, first, banned from buying new Huawei 5G equipment and, second, mandated to remove any existing equipment by 2027.[30] The economic infeasibility of such decisions is highlighted by the UK Digital Secretary, who estimated the cost of this move to be two billion pounds, coupled with two to three years of delay in the 5G rollout.[31]

It remains to be seen whether Europe can provide a middle ground among the technological protectionism and trade clashes escalating globally.

The UK is one of the staunchest allies of the United States, and therefore, the political necessity demanding the UK's position in this conflict is understandable. However, Germany, another US ally, has also been internally divided on the 5G issue, taking a position of "strategic equidistance," which is reflected both in its legal and policy approaches to the 5G issue; not wishing to impact mutually beneficial trade relations with China. For instance, on the legal front, Germany's new amendments to the Information Technology Security Act contain what is popularly known as the "Huawei clause,"[32] which, interestingly, provides for a two-part assessment mechanism, consisting of a technical evaluation accompanied by a declaration that the components purchased cannot be used for sabotage or espionage.[33] While ostensibly a neutral measure, the law is qualified by the requirement that vendor safety provisions, through the exclusion of vendors, are only triggered if all authorities involved unanimously wish to ban a vendor, which, given the wide ranging and controversial nature of this debate, is an unlikely occurrence. Accompanied by a lack of specific exclusion of any one vendor, notably Huawei, the increased legal hurdles in banning vendors are an attempt to walk a fine line between pressure from the US and the protection of its own economic interests.[34]

Germany's position on 5G and the primacy it accorded to economic considerations over external pressure is likely to be followed by other members of the EU, and similar measures were adopted by France and Italy, while softer stances were taken by Hungary, Spain, and Slovakia, etc.[35] The Italian government, similar to the German approach, has retained the power to veto any deals for the supply of 5G which it views as a threat to its national security. This power has, in fact, been exercised in the case of Huawei, where their deal with Fastweb was prohibited due to the processing of highly sensitive data involved. However, Vodafone (UK) recently secured approval to use Huawei equipment, illustrating that there is no clear targeting of Chinese manufacturers under the law.[36] France has taken another divergent approach, by adopting a phase-out process, and prohibiting renewal of licenses for Huawei equipment—thereby ensuring that within three to eight years the country is not reliant on the same.[37]

Hungary however, remains open to cooperating with China on economic and technological issues, and Huawei has been allowed to open a new research and development center in Budapest, which is largely seen as favoring Hungary's strategic and economic interests.[38] Further, barring restrictions at the broader, multilateral level of the EU, Hungary has no incentive to incur the kind of costs that removal of Chinese companies from within its economy would require, when they have already begun working together in key areas such as public institutions, emergency services, educational and health institutions, and public, state-owned companies.[39] Similarly, Spain has adopted a "neutral and independent" approach, refusing to de facto ban any supplier outright, and instead adopting a risk assessment mechanism to allow or ban mobile companies from partaking in the 5G rollout.[40] Poland and Romania have further signed bilateral deals with the United States to permit only "trusted" suppliers of 5G networks, a move that has been challenged by Huawei as violative of EU law.[41]

The varying political, security, and economic considerations that accompany the 5G debate have led to an absence of an extreme stance, notably a ban, being taken by Brussels. The report issued by the EU on coordinated risk assessment on cybersecurity in 5G networks identifies a key risk in the implementation of 5G as an increased and major dependance on a single supplier, which could lead to supply interruptions.[42] Further, the report identifies that dependence on suppliers presenting a "high degree of risk" increases the impact of vulnerabilities and their exploitation by third party malicious actors. EU as a whole seems to be adopting a flexible approach, allowing its members to determine what part Chinese companies can play in their 5G networks.[43] The EU endorses individual risk assessment mechanisms, which demand evaluation of vendors on technical competency as well as national security concerns. The potential for consensus building lies in flexibility, as well as in risk assessments which could also include mandatory signing of "no-spy" agreements with high-risk vendors, such as the one Huawei was willing to sign with governments including the UK.[44] The EU is considering a collective risk assessment model, whereby vendors would be declared as high risk at a regional level, and would be subject to security enhancement obligations, allowing the EU to achieve their objective of cooperation on cybersecurity.[45] Further, since the primary competitors to Chinese 5G developers are companies founded within Europe, such as Vodafone, Ericsson, and Nokia, etc., a regional funding model to provide alternatives to Chinese equipment may be considered.[46] These proposed alternatives could form an integral part of European digital policy to ensure that technological sovereignty, which is European autonomy in the digital sector, is a realizable aim.

Traditionally, the European governance model focuses on establishment of multistakeholder efforts,[47] giving non-state actors authority in policy processes at a global scale. However, consensus building surrounding 5G and other cybersecurity issues requires a renewed focus into multilateral-

ism to ensure broader global cooperation. The EU has adopted the multistakeholder model in their other region-wide initiatives, such as the General Data Protection Regulation ("GDPR"), where the European Commission, an inter-governmental body, established a multistakeholder expert group under its aegis to assist the identification of challenges in GDPR application from different stakeholder perspectives.[48] The European experience during and after both World Wars necessitated protection for privacy and personal information, which then evolved into fundamental rights in the EU.[49] In the US, however, privacy rights are balanced with commercial interests of other entities, and data privacy occasionally finds itself fundamentally opposed to the absolutist protection given to free speech within the US.[50] China has taken a third approach to data protection through a patchwork of legal instruments and non-binding rules, which has brought it closer to global standards.[51] In the sphere of data protection, the GDPR stands out as the instrument that places privacy at its forefront, not only within the EU, but it also requires data transfers from countries outside the EU to comply with these stringent norms. While concerns have been raised over the economic feasibility of these for smaller businesses, the EU has largely emerged as an alternative to the minimalist and state-centered data protection models of US and China, to set its own global standards. The level of protection under the GDPR was upheld only through the creation of various bilateral and plurilateral instruments mandating GDPR or other similar protection as the minimum standard. Therefore, while multistakeholderism played a crucial role in the conceptualization and implementation of the GDPR at an EU-wide level, multilateralism helped translate the GDPR into the global baseline for data protection. As a result, through increased cooperation at the regional level, continuous dialogue and knowledge sharing, Europe could be uniquely placed to lead the way in consensus building at a global level—its desire for strategic autonomy and appreciation of European interests giving it a central NAM-like role.[52]

A review of the position taken by NAM, along with the comprehensive analysis on the European dilemma, raises the question of a potential alliance for the future of digital non-alignment. The conceptualization of non-alignment has historically been linked to neutrality. However, neutrality is not a static concept, and the ability of a state to remain neutral depends on each state's prevailing individual political, geostrategic, economic, and social conditions. The primacy given to ideology during the first Cold War no longer exists today, and countries prefer to prioritize their economic and security interests. Viewing technological issues through political lenses, such as is being done by the US in their outright ban on Chinese equipment, is a myopic vision that the US expects its allies to unconditionally adopt. Unsurprisingly, countries in the EU and within NAM do not see this issue in such distinct black and white terms, and wish to segregate their economic dealings with China from their political ramifications.

The 5G debate is only the beginning of a world divided along technological lines, with the US and China primarily facilitating this divide.

The 5G debate is only the beginning of a world divided along technological lines, with the US and China primarily facilitating this divide. The digital era brings with it new challenges and concerns that plague countries today, and, in a digitally globalized world, the solutions to these problems necessitate global cooperation. Some of the key considerations that the UN Roadmap for Digital Cooperation highlights are the requirement for an inclusive digital economy and society, human and institutional capacity building, digital human rights, digital trust and security, and global digital cooperation.[53] An absence of one of the above may impact the others, such as in the 5G debate, where the absence of digital trust and security due to use of what is perceived to be potentially malicious technology, directly and adversely hinders global digital cooperation in other areas.

The solutions to these concerns highlighted by the UN Roadmap require global cooperation initiatives, bringing together diverse approaches to governance frameworks, thereby incorporating both NAM's focus on multilateralism, and the EU focus on multistakeholderism, to create platforms such as a joint EU-NAM 5G Initiative. 5G is an issue in which EU and NAM are uniquely placed, with their economic considerations requiring the creation of a non-aligned alternative to the US-China binary. The joint 5G Initiative could pave the way for EU-NAM cooperation on other digital issues of global concern, especially where there exists a similar convergence of positions due to prioritization of economic concerns, absence of existing, sufficiently competitive alternatives for self-reliance, and a desire to exercise collective influence to de-escalate global repercussions of trade conflicts. There will necessarily exist areas within cybersecurity where such cooperation may be unable to be achieved, such as data protection, where Europe's advanced technological infrastructure, coupled with regional cultural influences, allows it to place privacy on the highest pedestal—something which the primarily developing countries that compose NAM are unable to do.[54] However, the proposed initiative remains crucial for opening a dialogue of digital cooperation focused on non-alignment between two regional groups that have not exercised formal opportunities for collaboration in the past. It could also be a steppingstone to the creation of a multilateral inclusive institutional platform as NAM has called for,[55] with a more even distribution of power within it. Such an initiative could be set up jointly by NAM and the EU, with one influential country from each grouping being given joint leadership. For instance, an EU-NAM initiative led by Germany and India would ensure that countries that are seen as key players within their respective regions are provided a platform to lead collaboration on a global scale. Given that the India–EU summit has already begun discussions on collaboration in the field of 5G,[56] and India's upcoming presidency of the G20,[57] India's leadership role here will facilitate coordination not only with NAM but also with the EU. This initiative must be subsequently promoted and encouraged at meetings within the EU, as well as at preparatory and official summit meetings of the NAM Contact Group. After achieving sufficient interest generation, preparatory dialogue for various administrative aspects of the Initiative may begin, which would include discussions on the Secretariat, funding, and cooperative frameworks, etc.

The crux of the initiative should be its approach toward 5G technologies—especially given the divergent positions of various states that would be party to this initiative. Most developing countries within the 5G debate are primarily concerned with avoiding technological asymmetry and do not wish to be left behind in the 5G race, nor deprived of its infrastructural benefits that would improve crucial areas such as health, education, and defense, etc.[58] However, these desires are sometimes overshadowed by the national security concerns at stake, which have been at the heart of the debate surrounding 5G. Therefore, the initiative must adopt a flexible yet cohesive framework, taking inspiration from initiatives for regional cooperation adopted within the EU. Ideas such as collective risk assessment models, flexibility—with a margin of appreciation given to each member state to the extent to which high risk vendors shall be used, subject to certain additional safeguards such as "no-spy" agreements, entity-level identification of high-risk vendors, an emphasis on the phasing out of high-risk vendors by 2030, etc., would ensure that there is a degree of interoperability achieved within the initiative while still accounting for individualistic national concerns.

Simultaneously, while high-risk vendors, traditionally considered to be Huawei and ZTE due to pervasive domestic law requirements in China,[59] are being phased out of the backbone of national networks, alternatives to these high-quality and low-cost technologies must also be considered to ensure that developing countries are not left without access to 5G. The funding model adopted by the EU-NAM initiative could be used to create a 5G Implementation Initiative under the aegis of the broader initiative, where regional players from the EU and NAM member states can come to-

gether to collectively develop alternatives to Chinese technologies. These would require existing market players within the EU to collaborate with companies working on 5G within other states who are party to the initiative to collaboratively develop these viable and cost-effective alternatives. The initiative must ensure that it creates space for those countries that wish to rely on Chinese 5G technology, through imposing greater compliance obligations, while also providing alternatives to other countries moving away from Chinese technology on security grounds.

The Initiative may also lead the way in ensuring global adoption of proposals such as a Digital Stability Board, modeled around the Financial Stability Board, which could play a crucial role in regulation, best practices, and standard setting.[60] The Digital Stability Board, as visualized by the Centre for International Governance Innovation, is seen as an intergovernmental body, working with various stakeholders on the coordination and development of standards on an inclusive list of digital concerns.[61] The current centrality of 5G implies that the Board could play a role in norm setting in the sphere, and also pave the way for the development of norms around 6G. Since one of the proposals in this regard is for the Board to oversee personal information as data trusts,[62] which is being incorporated into the domestic law of countries such as India,[63] the Initiative would be uniquely placed to craft multilateral consensus on this. Given China's large investments in Europe, and its efforts toward European partnerships,[64] the Initiative could also pave the way for a multilateral dialogue with China. This would allow the initiative to truly achieve non-alignment in the digital sphere.

The Initiative may also lead the way in ensuring global adoption of proposals such as a Digital Stability Board, modeled around the Financial Stability Board, which could play a crucial role in regulation, best practices, and standard setting.

Despite evident ideological and political divides between certain members of the EU and NAM, including on issues that form a core part of digital cooperation, they are at least temporarily bound by the mutual desire to remain independent in a primarily bilateral conflict, with the world caught in its crosshairs. Therefore, a digital future led jointly and equally by the EU and NAM through this initiative could provide an attractive model of non-alignment for a large number of countries in Africa, Asia, and South America, who find themselves torn between either end of this debate, and assist them in achieving a balance in an increasingly polarized world. Digital non-alignment must be secured by leaders of the EU and NAM, since the fate of the digital era and the de-escalation of a Digital Cold War rests on this unlikely, yet mutually beneficial, potential alliance for the future.

Endnotes

1 Yang Yao, "The New Cold War: America's new approach to Sino-American relations," China International Strategy Review 3, 20–33 (2021), https://link.springer.com/article/10.1007/s42533-021-00071-1; Dealbook, "Inside the New Tech Cold War," October 1, 2020, https://www.nytimes.com/2020/10/01/business/dealbook/tech-cold-war-us-china.html.

2 Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, H.R. Rep. (2012)

3 Aashish Aryan, "US says Huawei, ZTE are 'national security threats': How will this impact India?," The Indian Express, July 1, 2020, https://indianexpress.com/article/explained/us-fcc-huawei-zte-national-security-threats-6484631/.

4 Robert Clark, "China aims to drive down 5G power cost," Light Reading, March 11, 2020, https://www.lightreading.com/asia/china-aims-to-drive-down-5g-power-cost/d/d-id/765140; Chen Qingqing and Shen Weiduo, "Political factors aside, Ericsson can't compete with Huawei: analysts," Global Times, May 12, 2021, https://www.globaltimes.cn/page/202105/1223316.shtml.

5 Robin Emmott, "China's intelligence law looms over EU 5G safeguards: official," Reuters, July 19, 2019, https://www.reuters.com/article/us-eu-huawei-tech-idUSKCN1UE18I.

6 Gautam Chikermane, "No Huawei in 5G is a start, No China in critical infrastructure should be next," Observer Research Foundation, May 5, 2021, https://www.orfonline.org/expert-speak/no-huawei-in-5g-is-a-start-no-china-in-critical-infrastructure-should-be-next/.

7 Stu Woo, "The US vs China: The high cost of the technology cold war," Mint, October 23, 2020, https://www.livemint.com/news/world/the-us-vs-china-the-high-cost-of-the-technology-cold-war-11603441980369.html.

8 Chad P. Bown, "How Trump's export curbs on semiconductors and equipment hurt the US technology sector," Peterson Institute for International Economics, September 28, 2020, https://www.piie.com/blogs/trade-and-investment-policy-watch/how-trumps-export-curbs-semiconductors-and-equipment-hurt-us.

9 Stu Woo, "The U.S. vs. China: The High Cost of the Technology Cold War," The Wall Street Journal, October 22, 2020, https://www.wsj.com/articles/the-u-s-vs-china-the-high-cost-of-the-technology-cold-war-11603397438.

10 Marc Champion, "How U.S.-China Tech Rivalry Looks Like a Digital Cold War," Bloomberg, December 12, 2019, https://www.bloomberg.com/quicktake/how-u-s-china-tech-rivalry-looks-like-a-digital-cold-war; Enda Curran, "Paulson Warns of 'Economic Iron Curtain' Between US, China," Bloomberg, November 6, 2018, https://www.bloomberg.com/news/articles/2018-11-07/paulson-warns-of-economic-iron-curtain-between-u-s-china.

11 Bloomberg, "UK told Huawei that US pressure contributed to ban: Observer," The Indian Express, July 19, 2020, https://indianexpress.com/article/technology/tech-news-technology/uk-government-us-pressure-huawei-ban-5g-observer-6513037/; Jonathan Shieber, "UK government reverses course on Huawei's involvement in 5G networks," May 24, 2020, https://techcrunch.com/2020/05/23/uk-government-reverses-course-on-huaweis-involvement-in-5g-networks/.

12 Mohammed Soliman, "The GCC, US-China tech war, and the next 5G storm," Middle East Institute, September 1, 2020, https://www.mei.edu/publications/gcc-us-china-tech-war-and-next-5g-storm.

13 Harsh V. Pant and Aarshi Tirkey, "India Draws a Line in the 5G Sand," Observer Research Foundation, May 19, 2021, https://www.orfonline.org/research/india-draws-a-line-in-the-5g-sand/.

14 Parminder Jeet Singh, "India should aim for a digital non-alignment," Hindustan Times, July 2, 2019, https://www.hindustantimes.com/analysis/india-should-aim-for-a-digital-non-align-

ment/story-ViT3PTiuo5j6dKUvt94YpO.html.

15 NAM Statement, "OEWG on developments in the field of information and telecommunications in the context of international security," Informal Virtual Meeting, February 18–22, 2021, https://front.un-arm.org/wp-content/uploads/2021/02/NAM-Statement-Informal-Consultation-OEWG-on-ICT.pdf.

16 UN General Assembly, Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report, A/AC.290/2021/CRP.2, (March 10, 2021), https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

17 NAM Working Paper for the Second Substantive Session of the Open-ended Working Group on developments in the Field of Information and Telecommunications in the Context of International Security (OEWG), Remarks on the Pre-Draft Circulated by the OEWG Chair, https://front.un-arm.org/wp-content/uploads/2020/04/nam-wp-to-the-oewg-final.pdf.

18 Hanns W. Maull, "Multilateralism: Variants, Potential, Constraints and Conditions for Success," Stiftung Wissenschaft and Politik, March, 2020, https://www.swp-berlin.org/publications/products/comments/2020C09_multilateralism.pdf.

19 "5G—Fifth generation of mobile technologies," International Telecommunications Union, December 2019, https://www.itu.int/en/mediacentre/backgrounders/Pages/5G-fifth-generation-of-mobile-technologies.aspx.

20 Hideaki Ryugen and Hiroyuki Akiyama, "China leads the way on global standards for 5G and beyond," Financial Times, August 5, 2020, https://www.ft.com/content/858d81bd-c42c-404d-b30d-0be32a097f1c.

21 "Outcome Report of the Informal Multistakeholder Consultation on OEWG Zero Draft Report," February 25, 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Outcome-Report-of-the-Informal-Multistakeholder-Consultation-on-OEWG-zero-draft.pdf; "Open-ended Working Group," United Nations Office for Disarmament Affairs, https://www.un.org/disarmament/open-ended-working-group/.

22 Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons System, "Report of the 2019 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapon System," CCW/GGE.1/2019/3, (September 25, 2019), https://documents.unoda.org/wp-content/uploads/2020/09/CCW_GGE.1_2019_3_E.pdf.

23 "Report of the UN Secretary General's High-level Panel on Digital Cooperation," Internet Governance Forum, https://www.intgovforum.org/multilingual/content/report-of-the-un-secretary-general%E2%80%99s-%E2%80%8Ehigh-level-panel-on-digital-cooperation.

24 Ministry of Communications, "Telecom Department gives go-ahead for 5G Technology and Spectrum Trials," news release, May 4, 2021, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1715927.

25 Ministry of Communications, "5G field trials," news release, June 26, 2019, http://loksabhaph.nic.in/Questions/QResult15.aspx?qref=628&lsno=17.

26 India TV Tech Desk, "Complete list of 267 Chinese apps banned in India: PUBG Mobile, TikTok, AliExpress and more," India TV, November 24, 2020, https://www.indiatvnews.com/technology/news-list-of-all-chinese-apps-banned-in-india-2020-667131.

27 Lalit K Jha, "India's decision to allow 5G trials without Chinese companies is sovereign: US," Mint, May 12, 2021, https://www.livemint.com/news/india/indias-decision-to-allow-5g-trials-without-chinese-companies-is-sovereign-us-11620776922441.html.

28 Government of Venezuela, "General Principles on Lethal Autonomous Weapons Systems," Working Paper submitted on behalf of the Non-Aligned Movement (NAM) and other states parties to the Convention on Conventional Weapons Group of Governmental Experts on lethal

autonomous weapons systems, March 28, 2018, https://www.unog.ch/80256EDD006B8954/(httpAssets)/E9BBB3F7ACBE8790C125825F004AA329/$file/CCW_GGE_1_2018_WP.1.pdf.

29 "Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects," International Committee of the Red Cross, November 2014, https://www.icrc.org/en/document/report-icrc-meeting-autonomous-weapon-systems-26-28-march-2014.

30 Leo Kelion, "Huawei 5G kit must be removed from UK by 2027," BBC News, July 14, 2020, https://www.bbc.com/news/technology-53403793.

31 Annabelle Timsit, "The UK will ban Huawei from its 5G network earlier than expected," Quartz, November 27, 2020, https://qz.com/1938635/uk-huawei-ban-could-be-implemented-earlier-than-planned/.

32 Stefan Krempl, "IT Security Act 2.0: "Middle finger in the face of civil society"," heise online, October 12, 2020, https://www.heise.de/news/IT-Sicherheitsgesetz-2-0-Mittelfinger-ins-Gesicht-der-Zivilgesellschaft-4986032.html.

33 Beryl Thomas, "What Germany's new cyber security law means for Huawei, Europe, and NATO," European Council on Foreign Relations, February 5, 2021, https://ecfr.eu/article/what-germanys-new-cyber-security-law-means-for-huawei-europe-and-nato/.

34 Matthew Karnitschnig, "How Germany opened the door to China – and threw away the key," Politico, September 10, 2020, https://www.politico.eu/article/germany-china-economy-business-technology-industry-trade-security/.

35 Yang Kunyi, "Slovakia believes Huawei can demonstrate transparency: Deputy prime minister," Global Times, November 12, 2019, https://www.globaltimes.cn/content/1169827.shtml.

36 Elvira Pollina and Giuseppe Fonte, "Italy gives Vodafone 5G deal with Huawei conditional approval – sources," Reuters, May 31, 2020, https://www.reuters.com/technology/italy-gives-vodafone-5g-deal-with-huawei-conditional-approval-sources-2021-05-31/.

37 Mathieu Rosemain and Gwénaëlle Barzic, "Exclusive: French limits on Huawei 5G equipment amount to de facto ban by 2028," Reuters, July 22, 2020, https://www.reuters.com/article/us-france-huawei-5g-security-exclusive-idUSKCN24N26R.

38 Pawel Paszak, "Huawei in Poland and Hungary. Could it be a part of 5G?," Warsaw Institute, November 30, 2020, https://warsawinstitute.org/huawei-poland-hungary-part-5g/.

39 Reuters Staff, "Hungarian minister opens door to Huawei for 5G network rollout," Reuters, November 5, 2019, https://www.reuters.com/article/us-hungary-telecoms-huawei-idUSKBN1XF12U.

40 Fernando Heller, "Spanish government to prepare a list of 'safe' 5G mobile providers," Euractiv, December 16, 2020, https://www.euractiv.com/section/5g/news/spanish-government-to-prepare-a-list-of-safe-5g-mobile-providers/.

41 Laurens Cerulus, "Huawei challenges legality of 5G bans in Poland, Romania," Politico, November 2, 2020, https://www.politico.eu/article/huawei-hints-at-legal-action-against-5g-bans-in-poland-romania/.

42 EU coordinated risk assessment of the cybersecurity of 5G networks, October 9, 2019, (NIS Cooperation Group); European Commission and the Finnish Presidency of the Council of the EU, "Member States publish a report on EU coordinated risk assessment of 5G networks security," press release, October 9, 2019, https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6049.

43 Douglas Busvine, "Europe telecoms lobby group 'denounces' bans on Chinese vendors," Reuters, October 16, 2020, https://www.reuters.com/article/us-huawei-europe/europe-telecoms-lobby-group-denounces-bans-on-chinese-vendors-idUSKBN2711I7.

44 Paul Sandle, "Huawei willing to sign 'no-spy' pacts with governments: chairman," Reuters, May 14, 2019, https://www.reuters.com/article/us-huawei-security-britain-chairman/huawei-willing-to-sign-no-spy-agreements-with-governments-chairman-idUSKCN1SK1HL.

45 European Commission, "New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient," Press Release, December 16, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391.

46 European 5G Observatory, "Recovery and Resilience Facility (RRF): 130 billion EUR," https://5gobservatory.eu/public-initiatives/public-funding-of-5g-deployment/.

47 "Joint comments from the EU and its Member States on the initial 'pre-draft' report of the Open-Ended Working Group on developments in the field of Information and Telecommunication in the context of international security," https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/UNGGE/Joint+Comments+from+the+EU+and+its+Member+States+on+the+Initial+%E2%80%98Pre-Draft%E2%80%99+Report+of+the+Open-Ended+Working+Group+on+Developments+in+the+Field+of+Information+and+Telecommunications+in+the+Context+of+International+Security.pdf.

48 Register of Commission Expert Groups and Other Similar Entities, "Multistakeholder expert group to support the application of Regulation (EU) 2016/679 (E03537)," 2017, https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3537.

49 Charter of Fundamental Rights of the European Union, Dec.7, 2000, 2012/C 326/02, Art. 8.

50 U.S. Const. amend. I; Stephen Cobb, "Data privacy and data protection: US law and legislation," ESET White Paper, April 2016, https://www.researchgate.net/publication/309456653_Data_privacy_and_data_protection_US_law_and_legislation.

51 Emmanuel Pernot-Leplay, "China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?", Penn State Journal of Law & International Affairs, 8, No. 1, (March 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3542820&__cf_chl_captcha_tk__=pmd_JcuRohxlGPngli9RYNCUw_Xd2GOGz7.wJUdDfKryp7c-1630170613-0-gqNtZGzNAuWjcnBszQw9.

52 Amandeep Gill, "Europe is the new NAM," Observer Research Foundation, January 16, 2021, https://www.orfonline.org/expert-speak/europe-is-the-new-nam/.

53 United Nations, Report of the Secretary General: Roadmap for Digital Cooperation, June 2020 https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf.

54 Bhaskar Chakravorti, "Why the Rest of the World Can't Free Ride on Europe's GDPR Rules," Harvard Business Review, April 30, 2018, https://hbr.org/2018/04/why-the-rest-of-world-cant-free-ride-on-europes-gdpr-rules; Prashant Reddy T., "Should There be a 'Developing Country' Template For Data Protection Legislation?," The Wire, May 17, 2018, https://thewire.in/tech/should-there-be-a-developing-country-template-for-data-protection-legislation; Rahul Matthan, "India need not adopt the onerous European General Data Protection Regulation," Mint, April 4, 2018, https://www.livemint.com/Opinion/xBXHfSpoq4sc71YH3XbsdL/India-need-not-adopt-the-onerous-European-GDPR.html.

55 NAM Statement, "OEWG on developments in the field of information and telecommunications in the context of international security," Informal Virtual Meeting, February 18–22, 2021, https://front.un-arm.org/wp-content/uploads/2021/02/NAM-Statement-Informal-Consultation-OEWG-on-ICT.pdf.

56 Archana Chaudhary, "EU official looks to align with India to protect democracy," Economic Times, April 19, 2021, https://economictimes.indiatimes.com/industry/telecom/telecom-news/eu-official-looks-to-align-with-india-on-5g-to-protect-democracy/articleshow/82145426.cms?-from=mdr.

57 Mohit Chowdhry, "A digital agenda for India's G20 presidency," Observer Research Foundation, June 1, 2020, https://www.orfonline.org/expert-speak/a-digital-agenda-for-indi-

as-g20-presidency/.

58 Kadri Kaska, Henrik Backvard and Tomáš Minárik, "Huawei, 5G and China as a Security Threat," NATO Cooperative Cyber Defence Centre of Excellence, 2019, https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf.

59 Samuel Stolton, "Huawei admit Chinese law obliges companies to work with government, under conditions," Euractiv, April 11, 2019, https://www.euractiv.com/section/cybersecurity/news/huawei-admit-chinese-law-obliges-companies-to-work-with-government/.

60 Rohinton P. Medhore, "A Post-COVID-19 Digital Bretton Woods," Centre for International Governance Innovation, April 19, 2020, https://www.cigionline.org/articles/post-covid-19-digital-bretton-woods/.

61 Robert Fay, "Digital Platforms Require a Global Governance Framework," Centre for International Governance Innovation, October 28, 2019, https://www.cigionline.org/articles/digital-platforms-require-global-governance-framework/; Daniel Garcia-Macia and Rishi Goyal, "Decoupling in the Digital Era," International Monetary Fund, 2021, https://www.imf.org/external/pubs/ft/fandd/2021/03/international-cooperation-and-the-digital-economy-garcia.htm.

62 Rohinton P Medhora, "We need a new era of international data diplomacy," Financial Times, January 18, 2021, https://www.ft.com/content/66f1ff42-fe49-4376-aafb-3943a9f-04a1c?shareType=nongift.

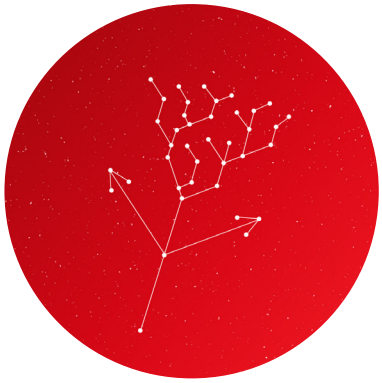
63 Trishi Jindal and Aniruddh Nigam, "Data Stewardship for Non-Personal Data in India," Vidhi Centre for Legal Policy, November 20, 2020, https://vidhilegalpolicy.in/research/data-stewardship-for-non-personal-data-in-india/.

64 Isabel Gacho Carmona, "The European Union before China's rise as a tech power: the 5G case," Instituto Espanol de Estudios Estrategicos, March 19, 2020, http://www.ieee.es/Galerias/fichero/docs_opinion/2020/DIEEEO23_2020ISAGAC_5G-ENG.pdf.

About the Authors

Latha Reddy is Co-Chair of the Global Commission on the Stability of Cyberspace. She served in the Indian Foreign Service from 1975-2011 and was appointed as India's Deputy National Security Adviser from 2011-2013 where she was responsible for cybersecurity and other critical internal and external security issues. She has extensive experience in foreign policy, and in bilateral, regional and multilateral negotiations. In addition, she has expertise on security and strategic issues and has worked on strategic technology policies, particularly on cyber issues relating to cyber security policy, international cyber cooperation and Internet governance. She served as a Commissioner on the Global Commission on Internet Governance and is involved with several organizations and think-tanks, both globally and in India. She is currently, among other positions, serving as a Distinguished Fellow in the EastWest Institute in the US and the Observer Research Foundation in India.

Anoushka Soni is a final year law student at the National University of Juridical Sciences, Kolkata. Anoushka has an avid interest in technology as well as international law, having been the Associate Director of the Society for International Law and Policy at NUJS. She has previously authored papers on Autonomous Weapon Systems at the Centre for Internet and Society, Bangalore and has additionally collaborated with the Association for Progressive Communications on their Internet Rules: Unboxing Digital Laws in South Asia workshop in 2020, as well as their Advocacy International: Advancing the Digital Rights Agenda for Asia, in 2021. Anoushka shall be joining a premier Indian law firm, Cyril Amarchand Mangaldas in their technology, media and telecommunications practice in 2022.



About the Cyberstability Paper Series

Since the release of the final report of the Global Commission on the Stability of Cyberspace in November 2019, the concept of cyberstability has continued to evolve. A number of new 'conditions' are emerging: new agreements on norms, capacity building and other stability measures have been proposed and solidified within the United Nations and elsewhere, and stakeholders are exploring ways to increase stability and minimize the risk of conflict in cyberspace through technical fixes or governance structures. The constellations of initiatives involved in working towards cyberstability is expanding, underlining the need to connect the traditional state-led dialogues with those of the Internet communities from civil society and industry. Gaps continue to close, between the global north and south, between technology and policy, but also the stability in and the stability of cyberspace.

The first Cyberstability Paper Series explores these "New Conditions and Constellations in Cyber" by collecting twelve papers from leading experts, each providing a glance into past or future challenges and contributions to cyberstability. The papers are released on a rolling basis from July until December 2021, culminating in an edited volume. All papers will be available for open access, and a limited number of printed hardback copies are available.

Published by

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

The Hague Centre
for Strategic Studies