



中国传媒大学
COMMUNICATION UNIVERSITY OF CHINA



Institute for a Community
with Shared Future
人类命运共同体研究院



Global Cooperation or Digital Hegemony? The Role of Technology and Cybersecurity Under GSI



By Dr. Adeel Irfan, a Participant of ICSF-UoS
Fellowship Program 2025-26 at University of
Sargodha

Published on 12th January 2026

The discourse of world security has quietly been shifted to the digital aspect in an age where power is measured in technologies as opposed to missiles. It has happened that we have reached a point where a single cyberattack can bring down hospitals, backdoor algorithms can interfere with elections, and information is the most valuable strategic asset. However, with this radical change, the world is yet to have a collective national perception of how to govern its digital future. The outcome is disintegration, distrust, and the growing competition of digital supremacy. It is in this ambiguity that the Global Security Initiative (GSI) of China is introduced as one of such proposals to redefine the way nations are considering technology, cybersecurity and the principles of online interaction. Although the GSI can be perceived in the perspective of geopolitics, it should be discussed more carefully. It in a sense represents what the Global South has been insisting it wants over the years, a more inclusive, equitable and respectful approach to the digital governance one that upholds sovereignty. And whether the world likes them or not, such ideas can no longer be disregarded in the debate on digital hegemony.



The Problem No One Can Ignore

Admittedly, the world is in the digital power game. United States and China take control of the tech ecosystems of the world, cloud technology, AI development, or even



semiconductor manufacturing supply chains. Europe struggles to establish its own rules. In the meantime, majority of the developing states remain subjected, vulnerable and even invisible in the international rule-making. Such disintegration is hazardous. The threats in cybersecurity are increasing at a rate that surpasses the response by the institutions. Hacking sponsored by the state, fake information created by AI, and cyber-spying are not the exception but common aspects of the international politics. The lack of international norms is not a mere technical but a global security crisis ad gradia. The existing model is not functioning. The world has a patchwork of irreconcilable visions that include, but are not limited to: an American one, where private technological giants dominate the world, a European one, where regulation and rights take center stage, and a Chinese one, where cyber sovereignty and state control are prioritized. However, nobody has managed to construct a really collaborative structure. And as long as this does not occur, digital insecurity will be the defining aspect of our era.

What the GSI Gets Right

Regardless of whether one is in support of the political system in China or not, the GSI makes an important observation: there can never be digital security as a result of domination. When a few corporations or one nation can dominate global data flows, cloud systems or AI systems, distrust is unavoidable. The concentration of digital power on a small number of actors public or private has led to the development of a kind of digital hegemony which challenges the sovereignty and generates geopolitical tension. The GSI questions this reasoning by emphasizing on indivisible security: the notion that no nation



can be safe when others are not safe. This might appear as a diplomatic rhetoric but in reality, this is a practical base of digital governance. Threats related to cyber do not have boundaries. Viruses propagate all over the world in a few seconds. The perception of the user is influenced by AI systems that have been trained in a different country thousands of miles apart. In this kind of a system of interconnection, striving towards absolute superiority is not only impractical, but also disruptive. Besides, the focus of the GSI on cyber sovereignty is very powerful in the Global South. The nations in Asia, Africa and Latin America are sick and tired of being digitally reliant on Western resources which harvest the information without any responsibility. They desire values of infrastructure ownership, local data control, and equal access to the development of technology. The GSI is a place that allows such discussions to occur.

Where the GSI Raises Questions

But the GSI raises alarming questions, the ones that the world cannot do away with. I would also like to assume that its sovereignty-first policy can empower developing nations but it can also be hazardous to permit digital authoritarianism unless it is supplemented with strong transparency and accountability. The opponents are worried that the model will sanction surveillance operations or limit the digital freedoms of weak democracies. These are issues that should be considered. Geopolitical realism is another problem. Will the GSI actually





facilitate international collaboration as US-China competition is taking off? Is it possible to have a Chinese-led structure that has widespread legitimacy without the establishment of confidence, an increase of transparency in standards, and a distinction between economic aspirations and security pledges? The lack of these elements will leave scepticism.

A Middle Path Is Possible and Necessary

Nevertheless, the GSI would be a tactical error to turn the back on the criticisms. The world has become so globalized that it cannot be regulated by a single bloc or worldview. The world does not require rigid ideological positions but pluralism; the existence of multiple governance philosophies that have the opportunity to compromise and mutually enrich each other. The GSI has a potential to be a platform of precisely that, as long as three conditions are met.

- To start with, China has to adopt much more transparency concerning its cyber-partnerships, infrastructural projects, and models of AI governance. Trust does not develop without openness.
- Second, developing countries should stop perceiving the GSI as a ready-made template but as a chance to negotiate improved digital conditions, such as the need to train more, transfer more technology, and build more local capacities.
- Third, international institutions have to develop. The UN, regional organisations, and cyber diplomacy forums should find a way of establishing inclusive arrangements in which the Global South does not remain a passive beneficiary but



is a rule-maker. The cyberspace is too significant to be controlled by a few influential states.

The Future Depends on Cooperation, Not Control

Digital hegemony does not simply come down to a debate over technology; it is who dictates the 21st century. The world is at a crossroads. One of these directions results in a digital Cold War, disaggregated networks, rival AI ecosystems, and even more aggressive cyber wars. The



alternative route is to a future through negotiation in which the digital power is even out through mutual norms and global collaboration. The GSI is not an ideal solution. It is a discussion the world badly needs. When it comes to the battle of digital order, the rejection of other visions is more harmful than their discussion. As long as the globe is concerned with the issue of security, whether in the digital age or not, it must be founded on cooperation, mutual respect, and readiness to reconsider the pillars of technological power.