

GLOBAL DIGITALIZATION TRENDS AND INTERNATIONAL INFORMATION SECURITY

Control over personal data and big data turnover can allow states to monitor economic, political, and social spheres of other states in almost real-time and to adjust their strategies accordingly.

Vitali Romanovski

PhD Researcher, Belarusian State University, Minsk, Belarus

Digitalization is a key factor driving progress. It has a huge impact on technological development, human consciousness, social dynamics, and societal development. As such, the global digital revolution is transforming global politics. Digital technologies are becoming a key strategic tool for economic development and military superiority. The development of digital platforms to manage digitalization has already become a matter of national security. In turn, the development strategy in the global digital environment is one of the determining factors of sustainable economic growth and state security. In other words, digital technological sovereignty is becoming a factor in ensuring state sovereignty.

The features of today's digitalization processes, including the development of neural network algorithms, the emergence of the phenomenon of hybrid digital subjectivity and the growing influence of transnational digital corporations on communications in the digital space create the need for effective state policy in order to ensure the security of the individual, society and the state.

Today, the importance of the security of critical information infrastructure increases. Cyberattacks and systemic failures in its networks can lead to unpredictable consequences in the social, energy, and industrial spheres of a state or an entire region. For that, creating autonomous cybersecurity solutions for critical information infrastructure becomes a natural and justified endeavor.

Control over personal data and big data turnover can allow states to monitor economic, political, and social spheres of other states in almost real-time and to adjust their strategies accordingly. Obviously, in order to create an information security system adequate for the current realities, state entities need to take into account the dynamics and vectors of global trends in digital development and regulatory policies. This article suggests a few perspectives in this regard.

Digital Dimension of International Politics

A number of features characterize today's international relations. Firstly, the balance of power in the world that arose after the collapse of the USSR is shifting and conflicts increasingly dominate the international domain. The geopolitical struggle between the world's leading states is becoming more intense. Another problem is the lack of moral and legal awareness. To ensure their national interests, states are moving away from the international legal norms enshrined in the UN Charter. The power of force replaces the power of law. Moreover, the cultural and ethnic factors are becoming more salient in international politics. The demand for self-identification and a novel framework of values is growing. In this context, regionalization is becoming a global trend. Also, scientific and technological innovations are transforming the social environment. The level of development in technology, science, and education determines the role and place of the state.



As the world moves towards a multipolar order, new forms of international conflicts emerge. Digital technologies exacerbate the existing contradictions between the states in economic, political, and military spheres. The digital domain has become a new field of competition.

In the foreseeable future, states will live in conditions of evolving cyber and cognitive threats. Weaponization of the cyberspace is gaining momentum. Many states are actively developing offensive information capabilities. Information processing and transmission technologies are being weaponized to impact both military and civilian systems of the enemy in order to weaken their economy and reduce their armed forces' combat readiness. It is obvious, however, that attempts to turn the information sphere into an arena of interstate confrontation increase the threat of a direct military clash with unpredictable consequences for all parties.

Digitalization is and will remain a key locomotive in global economic and social development. UN programs related to global digitalization are relevant. The demand to develop appropriate infrastructure and data processing technologies – artificial intelligence and quantum technologies – is growing. Nevertheless, the scientific and technological component of development becomes a contributing factor to ensure state sovereignty and compete with the other states in the international arena. The new competition involves new tools and forms of influence and confrontation. Of particular importance is the control over data markets, the activities of global and regional digital corporations, and the formation of interstate techno-economic blocks.

Data

In digital geopolitics and geo-economics, access to primary data is of fundamental importance. The technological strength of modern states can be measured by the volume of the databases and the quality data processing infrastructure that they possess. Control of data markets means the acquisition of asymmetric economic and military-political advantages.

In turn, the progressive and adaptive change in digitalization strategies, the development of digital infrastructure, and the increasing importance of uninterrupted cross-border data flows lead to new risks. Among them is a 'data divide' phenomenon. The competitive advantage of a state is the very ability to control data in order to solve economic development problems and prevent the other party from doing the same. In view of tectonic shifts in the current world order, the "data gap" carries political and economic risks and becomes an integral part of international information security.

Today, the importance of the security of critical information infrastructure increases. Cyberattacks and systemic failures in its networks can lead to unpredictable consequences in the social, energy, and industrial spheres of a state or an entire region.

Techno-Economic Blocks

The prospect of the development of interstate techno-economic blocks and regional digital platforms is becoming one of the defining characteristics of the current stage of global digitalization. Their advantage is the potential for greater compliance with the socio-cultural code and the needs of society in a particular region. The relationship between the blocks will likely be determined by the geopolitical context and the possibility of interfacing state and regional digital platforms of one block with the corresponding platforms of another. Given the high dynamics of these processes, their timely regulatory support, especially in the international legal aspect, is of particular relevance.

The most important trend associated with the formation of techno-economic blocks is the process of the emergence of techno-economic regimes. They are created through the development and use of technologies, technical standards, legal regulations, and investment activities. De facto, these regimes are zones of influence and are seen as a factor in ensuring technological sovereignty.

Obviously, independent technological solutions and technical standards become a factor in ensuring security in the military, economic, information, and social spheres. In addition, in conditions when a one-time transition to domestic technologies is unlikely, the regulation of the information security sphere becomes particularly relevant.

The noted ‘islandization’ of information relations, i.e. the process of creating closed information systems and digital platforms, exacerbates the problem of ensuring the security of critical infrastructures. Obviously, there are infrastructure facilities whose security is transnational and must be ensured under international standards. The issue of critical energy infrastructure, for example, nuclear power plants, is especially important.

Big Tech

States are and in the foreseeable future will remain key actors in international relations. However, they have to reckon with the interests of the business community in the scientific and technological sphere. The speed of techno-economic platform formation and interstate

States are and in the foreseeable future will remain key actors in international relations. However, they have to reckon with the interests of the business community in the scientific and technological sphere.

interaction within them are determined by the competition between digital platforms and the states themselves over control of data flows and digital services. At the moment, multinationals are in a better position, and the efforts of regional states to create digital solutions independent of techno-giants are insufficient. The lack of significant financial infusions and political will to develop national digital products makes it more likely that the digital dictatorship of tech corporations will strengthen. For this reason, regional alliances are becoming especially important for small and medium-sized countries, for which it is not possible to ensure absolute techno-information sovereignty in the short and medium term. The possibility of regional information ecosystems with their own standards goes up when national states are stronger. However, even though small and medium-sized countries may have less digital, scientific, technological, and financial potential compared to larger countries, they can still develop their own Big Tech companies and use niche leadership strategies for growth.

State and Society

The state and society are increasingly aware of the risks related to ICT development. States see digital development issues through the national security prism. For society, however, the speed of changes in legislation and the displacement of red lines in the legal field is unusual. Nevertheless, both of them should be on board when building digital ecosystems and security systems.

The boundaries of legitimate behavior have shifted. Freedom of speech and information access are being replaced by a narrowing of permissible discourse. Sociocultural responsibility dominates legal responsibility, subjects of legal relations are deprived of the right to defense. Technological solutions and public opinion administration become regulators themselves. Society is just beginning to adapt to the changes that are taking place, mostly with the “deaf defense” or “silence” strategies. It’s vital to comprehend how state-citizen, state-state, state-business, and citizen-business interact and adjust the state’s strategic communications accordingly.

International Law

The high rates of global digitalization, the development of artificial intelligence, quantum communications, and the transformation of the social dimension of world politics emphasize the need for legal efforts to ensure international information security. Today, however, the law does not have time to adapt to the ‘islandization’ of information relations. Where legal norms are not applicable, standards and rules appear. It is obvious that in the absence of restraining international legal norms, digital aggression and weaponization of cyberspace will become prevalent.



National legal systems require further development. Particular attention should be paid to the general theory of information law in order to provide a scientific ground for public law policy and ensure national security in the information sphere. Defining the legal nature of international information law is also an urgent scientific task.

The international legal regulation of the information sphere should not be restricted to current issues alone, as these are heavily influenced by geopolitical and geo-economic dynamics. The pace of global digitalization and the current geopolitical and geo-economic situation makes it possible to assume that in the medium and long term, the development vector of the emerging international information security system will be aimed at regional transformations caused by the intensification of the policies of national states to ensure their information and technological sovereignty. It is becoming obvious that non-governmental structures, academia, the business community, states, and intergovernmental organizations should pay special attention to this issue, and direct their efforts towards developing new rules for information relations in the context of regionalization.

Conclusion

Developments in digital technologies lead to conceptual and regulatory shifts that exacerbate the old

Developments in digital technologies lead to conceptual and regulatory shifts that exacerbate the old dilemmas of international relations.

dilemmas of international relations. Indeed, excessive digital regionalization and technological wars could impede the evolution of the digital sphere, which exists due to open innovation, global markets, and the universality of standards and norms. The existence of different conceptual approaches to the creation of technoeconomic regions and regimes does not negate the possibility of their synergy for a future global technological breakthrough. Even in regions with heightened military and economic tensions, it's crucial to establish constructive communication between technoeconomic blocks to ensure this synergy.

In the short and medium term, it will probably not be possible to create universal binding norms or a global legal platform regulating the activities of states in the digital domain. As national states step up their attempts to maintain information sovereignty, it has become essential to shape the legal framework to ensure information security at the regional level, develop relevant approaches within regional associations, and propose their best practices at the global level.