PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NO. 4 (1700), 8 JANUARY 2021 © PISM

BULLETIN

The Clean Network Initiative as an Element of the U.S.-China Competition

Andrzej Dąbrowski

Fearing China's global dominance in the field of information and communications technology (ICT), including high-capacity 5G telecommunications networks, and the country's access to new markets, in August 2020 the U.S. launched the Clean Network Initiative (CN). The coalition of states, institutions, and companies participating in it aims to prevent Chinese ICT from dominating the economies of America's allies. The U.S. may determine the future level of cooperation with allies on the degree of saturation of their economies and infrastructure with Chinese technologies.

As part of tightening customs and trade policy towards China, the U.S. began preventing companies from that country from further strengthening their positions on the American ICT market. The main intention is to prevent Chinese entities from becoming the basic supplier of 5G technology, which allow data transmission at speeds several times higher than the currently used 4G (LTE+) networks, which will translate into the development of new industries and products, stimulating economic growth. In this way, the U.S. wants to protect itself against the potential for undesirable influence from China on this element of American critical infrastructure. In 2019, the Trump administration included Huawei on a list of entities banned from receiving exported electronic components from the U.S. and prohibited the construction of 5G networks using the company's equipment. In June 2020 the Federal Communications Commission (FCC) placed Chinese ZTE and Huawei on its "threat list" of entities. The FCC justified the decision by referring to the ties of both companies to the Chinese Communist Party and the obligation under Chinese law for their cooperation with Chinese secret services. As a result, companies building 5G networks in the U.S. will not be allowed to use federal funds for the purchase of equipment from these manufacturers.

The administration's actions received cross-party support in Congress. In mid-November 2020. The House of Representatives passed the Telecommunications Act, which offers $750 million to help finance 5G infrastructure in the U.S. The House also discussed the draft Transatlantic Telecommunications Security Act, which is to provide financial support for the construction of the 5G network in Three Seas Initiative (TSI) countries.

Excluding Chinese 5G. In August 2020, Secretary of State Mike Pompeo announced the Clean Network initiative. It extends the concept of the Clean Path programme, which was designed to seal the ICT infrastructure of U.S. diplomatic missions. Ultimately, CN comprised six cross-cutting areas of ICT and data protection. The initiative is in the form of political declarations by individual countries and companies that have joined it. So far, declarations of compliance with the principles of CN have been expressed by the governments of Albania, Brazil, Bulgaria, Czechia, Estonia, India, Israel, Japan, Poland, Slovakia, and others. The companies willing to implement CN include the largest ICT providers from the U.S., Canada, the EU, and East Asian countries, including Orange, T-Mobile, and the SoftBank Group. Despite the lack of a clear declaration on CN, the UK government has announced that it will ban Huawei solutions in creating British 5G networks and get rid of the company's existing installations by 2027. France made a similar decision. The U.S. State Department has not released plans to formalise cooperation with CN participants in the form of regular meetings or institutionalisation.

The Chinese Road to Secure 5G. In response to the interest in CN and fear of losing prospective markets, the Chinese Ministry of Foreign Affairs announced its own concept for

cooperation on 5G security. The Global Initiative on Data Security (GIDS) is a collection of declarations by the Chinese government concerning, among others, the security of data storage and processing and maintenance of supply chains of ICT components. Like CN, GIDS is open to any country and company interested in cooperating and complying with these standards. The GIDS proposals reflect accusations made by the Trump administration against Chinese ICT companies and Chinese government and of theft of intellectual property from American companies and research centres. In its messaging, China points to the U.S. as a country that is afraid of competition and is targeting the interests of Chinese companies through political pressure.

The political nature of the GIDS declaration serves primarily to show China as a country promoting security and the market-oriented nature of ICT investments. The Chinese government aims to involve as many countries as possible to support the initiative. Chairman Xi Jinping addressed the G20 leaders at the last summit of the group and promoted the initiative at the meeting of the Shanghai Cooperation Organisation, where China plays a dominant economic and political role. So far, interest in participation in GIDS has been signalled by Kazakhstan, Laos, Pakistan, Syria, and Russia—countries already associated with the Digital Silk Road concept.

U.S. Cooperation with Allies. For CN to succeed, the key will be to create the largest possible group of countries and companies willing to secure their existing and future infrastructure without undesirable Chinese tech. The U.S. also wants to deepen international cooperation with organisations in which it plays a leading role or with which it is strongly linked economically and politically (mainly NATO and the European Union).

In 2019, the EU decided to create its own recommendations for 5G networks. The risk report published by the European Commission (October 2019) and the proposed instruments (i.e., toolbox) to guarantee the security of 5G infrastructure in the EU (January 2020) do not directly point to China as a threat. However, they present the challenges posed by, for example, the dependence of the 5G market on a single supplier or resulting from possible political influence of a company's state of origin as undesirable. The documents emphasise that 5G software should not contain deliberate vulnerabilities that would allow it to be successfully attacked (data theft). The U.S. perceives the EU's "toolbox" as complementary to the CN concept, despite the lack of direct reference in the Union's document to the role of China. The biggest problem from the American perspective may be the attitude of Germany, which, being the main market for telecommunications services in the EU, has long avoided blocking Chinese 5G companies. Only at the end of September 2020 did Angela Merkel's government signal the possibility of blocking Huawei after initially deciding to allow this company to implement some 5G projects. The decision was dictated by Huawei's involvement in the German market to date and the need to possibly finance the replacement of the existing infrastructure.

Conclusions. The administration of President Joe Biden will continue its efforts to secure 5G infrastructure in the U.S. from Chinese influence and will uphold this policy towards allies to block China's access to their ICT market while also investing in deepening international cooperation in this field.

The U.S. actions stem not only from security concerns but also from American economic interests. The increasing domination of highly developed markets by cheap Chinese ICT has already started undermining the competitiveness of American companies in this industry.

It is in Poland's interest to actively participate in the European and transatlantic debate on the security of 5G networks and other ICT. The country should argue for maintaining the highest security standards of 5G infrastructure, formulated with clear criteria and calculating not only the economic rationale but, above all, emphasising protection against unwanted interference by third countries and entities they can control. An important element when choosing 5G technology providers should be diversification, which will make it more difficult for one entity to exert pressure on Poland through a monopoly or single manufacturer. It will be beneficial for Poland to take into account EU recommendations on counteracting the monopolisation of critical services in planning the development of 5G infrastructure.

It is the interest of all TSI countries to coordinate their activities in 5G standards implementation and use U.S. support in building secure infrastructure. For this purpose, TSI may use the Central European Digitisation Council proposal discussed at the forum's last summit as a tool for consultation and exchange of good practices.

Table 1. Areas of Activity under the Clean Network Initiative

Programme Pillar	**Stated Goal**	**Subject (Affected Entities)**
Clean Carrier	"to ensure that People's Republic of China (PRC) carriers are not connected with U.S. telecommunications networks"	PRC carriers; U.S. telcos
Clean Apps	"to prevent untrusted PRC smartphone manufacturers from pre-installing—or otherwise making available for download—trusted apps on their apps store.	PRC smartphone manufacturers, U.S. app providers
Clean Store	"to remove untrusted applications from U.S. mobile app stores"	PRC app providers; U.S mobile app stores
Clean Cloud	"to prevent U.S. citizens' most sensitive personal information and [U.S.] businesses' most valuable intellectual property" from being compromised	examples of specific companies named: Alibaba, Baidu, China Mobile, China Telecom, Tencent
Clean Cable	"to ensure the undersea cables connecting [the U.S.] to the global internet are not subverted for intelligence gathering"	Huawei Marine
Clean Path	to ensure "an end-to-end communication path that does not use any transmission, control, computing, or storage equipment from untrusted IT vendors" for the U.S. diplomatic facilities	Huawei, ZTE