PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

BULLETIN

No. 75 (1015), 4 August 2017 © PISM

China's Internet Policy

Marcin Przychodniak

China treats the internet as an arena for global competition. It believes that EU and U.S. support for unrestricted access to information on the global level endangers the stability of its political regime. China has strengthened control over internet usage within its borders to restrict information flow. It also uses the economic expansion of Chinese IT companies abroad to make its position on cyberspace stronger and its draft International Code of Conduct for Information Security is contradictory to the EU and U.S. concepts. China's actions require EU resistance to defend global open internet and economic freedom.

An October 2016 agreement between the U.S. Treasury and ICANN on management of the internet has ended and was not extended. When the U.S. ended supervision of the internet, the need for the international community to develop new administration procedures for it were clear. Meanwhile, there has been an ongoing debate within the UN on the jurisdiction of existing international law as it pertains to the internet.[1] This debate is also connected to cybersecurity issues, not only concerning protection from attacks but also, for example, the limits of retaliatory actions.[2] China is actively participating in all these debates.

China's Main Goals in Cyberspace. China has the most internet users in the world (about 730 million). Its cyberspace policy aims to achieve two main goals: internal, that is, to control the flow of information to protect the stability of the regime, and external, to meet economic targets.

In 2014, the Communist Party of China (CPC) established the Central Leading Group for Internet Security and Informatisation (LGISI). Leading groups play an important part in the policy-forming process and their importance has increased under Xi Jinping. He heads the group and his deputies are other CPC Politburo Standing Committee members: Prime Minister Li Keqiang and Liu Yunshan (who is head of the Central Leading Group for Propaganda and Ideological Work). LGISI decisions are implemented by the Cyberspace Administration of China, also created in 2014. Its main work includes the so-called Great Firewall, a system designed to block access to specific information and certain foreign websites, blocking virtual private networks (VPN), which allow users to get around the Great Firewall, information control bureaus, which delete undesirable posts on social media, and legislative initiatives, such as the obligation on internet firms operating in China to keep data in the country and restrictions on opening news platforms.

Simultaneously, China actively supports Chinese IT companies in trade and investment expansion matters, such as in Central Europe, Central Asia, Southeast Asia, and Africa. Mainly because of government support—closure of the Chinese market to foreign competitors and domestic financial assistance—companies like Alibaba, Huawei, and Lenovo have achieved global brand status. These companies are strongly involved in China's flagship Belt and Road Initiative (BRI), wherein one of its priorities is

[1] R. Tarnogórski, "The International Regulation and Governance of the Internet," *PISM Bulletin*, no. 73 (406), 25 July 2012.

[2] R. Tarnogórski, "Time for an International Law on Cyber Conflicts," *PISM Bulletin*, no. 32 (485), 26 March 2013.

telecommunications. In Central Europe, regional offices of Huawei (Warsaw) and ZTE (Budapest) have been established. Huawei, besides involvement in the construction of internet infrastructure for Polish mobile companies, is also second in terms of shares of the Polish smartphone market. The 2016 Chinese Ministry of Industry and Information Technology strategy set up a target of investing over $170 billion in the construction and modernisation of telecommunications networks in Africa over the following two years. Huawei and ZTE together have established training facilities in nine African countries and built net infrastructure in 20 more. Chinese e-commerce companies (e.g., Alibaba, JD.com) are building 20 warehouses in countries involved in the BRI, such as Indonesia, and Alibaba has created a special "digital free-trade zone" in Malaysia.

China also seeks to settle relations with other countries over cybersecurity issues. It wants to reduce its image of a state supporting industrial and intellectual property (IIP) theft on the internet. In 2015, China signed an IIP agreement with the U.S. in which both sides renounced such practices. That alone has not eliminated such theft originating from China but it has significantly decreased. Similar agreements were also signed with the UK and Canada. Worth noting is a deal with Russia, signed in 2015, that includes a "non-aggression in cyberspace" clause, although with rather more political than practical effect. China is constantly aware of the Russian cybersecurity threat, and a report by Chinese company Qihoo 360 from 2017 identifies Russian hacking groups as actively operating in China.

China's Position on Internet Management. Chinese authorities emphasise they will never accept a situation in which the internet abides by earlier regulations imposed by the U.S., which essentially founded it in the 1960s. China frequently points out that 10 of the 13 main DNS servers, which keep the internet in working order, are located in the United States. Since the U.S.-ICANN deal expired, China has worked to strengthen the role of developing states in the ICANN structure.

China strongly promotes a "sovereignty" concept of internet control. According to it, states may control both information flow and the network management model within their borders. This is contrary to the EU position of keeping the internet as an open platform for all stakeholders, which coincided with the U.S. stance. The U.S. position is no longer as clear. In May 2017, President Donald Trump signed an executive order on cybersecurity that in initial drafts contained passages supporting agreements with a multi-stakeholder approach to internet management but which were deleted from the final order.

Within the international debate about internet management, and contrary to the U.S. and EU positions, China underlines that existing international law is not applicable to internet management and a new code is needed. In 2015, China, backed by Shanghai Cooperation Organisation, reported to the UN with an upgraded draft of its International Code of Conduct of Information Security. The draft suggests regulations that strengthen the state's role in internet management, but its controversial nature of that part delayed further discussion. In China's perspective, the UN is the appropriate forum to create new cyberspace regulations. That is why China did not join the Council of Europe's 2001 convention on cybersecurity, describing it as too European-oriented and not taking into consideration the aspect of state sovereignty. China actively participated in the work of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) organised within United Nations. GGE was meant to evaluate whether and how international law applies to the internet, but it failed to reach a compromise. One of the reasons was China's position (along with that of Russia, Belarus, Malaysia, and others) on the rejection of self-defence (Article 51 in UN Charter) to cyberattack.

Conclusions. China will not abandon its "sovereignty concept" as it pertains to the internet because information control is crucial to the stability of the regime and because it also provides the country with an opportunity to present itself as a leader among states opposing the current solutions. Strengthening the state's position in internet governance as suggested by China could result in a reduction of global information flow and internet technology development. It is necessary the EU maintain its objections to initiatives like China's in international forums, especially in the context of the changes in the U.S. position.

In Poland and other Central European countries, cooperation with Chinese IT companies is connected to notable profits, especially in the infrastructure of Polish telecommunications companies. A cautious approach should be established towards political initiatives on cyberspace issues oriented to the "sovereignty" concept. The debate on legal regulation of the internet will continue in the UN and will remain important in 2018 when Poland becomes a non-permanent member of the Security Council. It is in Poland's best interest to support the open model of global internet management because it also favours the new technologies sector and internet business development, important parts of its economy.