P. Haletskiy, Student
M. Semenuk, research adviser
T. Zhibritska, language adviser
Berdichev College of Industry, Economics and Law

NETWORK SOVEREIGNTY

The aim of this study was to tell about actual topic nowadays – network sovereignty. Because now the Internet is everywhere and, in my mind, this question should be considered at the legislative level.

Network sovereignty is the effort of a state, to create boundaries on a network and then exercise a control, often in the form of law enforcement over such boundaries.

Most of the states invoke sole power over their physical territorial boundaries, state sovereignty, such governing bodies also invoke sole power within the network boundaries they set and claim network sovereignty. In the context of the Internet, the intention is to govern the web and control it within the borders of the state. Often, that is witnessed as states seeking to control all information flowing into and within their borders.

The concept stems from questions of how states can maintain law over an entity such like the Internet, whose infrastructure exists in real space, but its entity itself exists in the intangible cyberspace. Some Internet Scholars, such as Joel R. Reidenberg, argue, "Networks have key attributes of sovereignty: participant/citizens via service provider membership agreements, 'constitutional' rights through contractual terms of service, and police powers through taxation (fees) and system operator sanctions." [1] Indeed, many countries have pushed to ensure the protection of their citizens' privacy and of internal business longevity by data protection and information privacy legislation (for example the EU's Data Protection Directive, and at Ukraine Council of national security & defense of Ukraine decision from April 28, 2017 “On approval of the Rules for the implementation of activities in the field of telecommunications”

Networks are challenging places for states to extend their sovereign control. In her book Sociology in the Age of the Internet, communications professor Allison Cavanagh argues that state sovereignty has been drastically decreased by networks. [2]

Many governments are trying to exert some form of control over the Internet. Some examples include the SOPA-PIPA debates in the United States, the Golden Shield Project in China, and by decree of the President of Ukraine Petro Poroshenko No. 133/2017 of May 15, 2017 on the enforcement of the NSDC decision of April 28, 2017 “On the application of personal special economic and other restrictive measures (sanctions)” The peculiarity of the new sanctions was the requirement to block Internet service providers from accessing web-resources of VKontakte, Odnoklassniki, "Mail.ru", "Yandex", "Kaspersky Lab", "Dr.Web", the official distributor of "1C" on the territory of Ukraine.

On the other side, many experts believe that the government has no right to be on the Internet. As Law Professor David Post at the University of Georgetown argued, "'[States] are mapping statehood onto a domain that doesn't recognize physical boundaries,'" at least in the context on the Internet. He went on to say, "'When 150 jurisdictions apply their law, it's a conflict-of-law nightmare. [3] Some oponents of the Internet, such as John Perry Barlow, argued that the current form of the Internet is ungovernable and should remain as open as possible. [4] Network Sovereignty can affect state security, law enforcement on the Internet, фnd the ways that private citizens use the Internet, as many people attempt to circumvent the protections and legal devices, placed by many governments on the Internet, by using tools such as VPNs.

Virtual Private Networks (VPNs) are a significant tool to allow private citizens to get around network sovereignty and any restrictions their government may place on their access to the Internet. VPNs allow a computer to route its Internet connection from one location to another. For example one would connect from a connection at point A to a connection at point B, and to others, it would appear that they are accessing the Internet from point B even if they are in point A. For example, in China, VPNs are used to access otherwise-blocked content. Also for the example of website «Vkontakte» stating that with VPN, "smut that's banned in the Ukraine can wind its way into Ukrainian homes through electrical impulses in, say, Amsterdam. In that example, by using VPNs, an Internet user in Ukraine could access banned material that is hosted in Amsterdam by accessing through a server, hosted in Amsterdam, to make it appear that the user is in Amsterdam, based on the IP address. Therefore, citizens have a way around network sovereignty, simply by accessing a different server through a VPN. That greatly limits how governments can enforce network sovereignty and protect their cyberspace borders. Essentially, there is no way that a government could prevent every citizen from accessing banned content by means such as VPNs.

Summarizing the above, network sovereignty has implications for state security, Internet governance, and the users of the Internet's national and international networks and state must regulate this issue.

REFERENCES

1. Reidenberg, Joel R. (1996). "Governing Networks and Rule-Making in Cyberspace". Emory Law Journal.p. 45: 928.

2. Cavanagh, Allison (2007-04-01). Sociology in the Age of Internet. McGraw-Hill International. p. 41.

3. Yang, Catherine (June 14, 1997). "Law Creeps Onto the Lawless Internet". Business Week. Retrieved 28 January 2014.

4. Barlow, John Perry. "A Declaration of the Independence of Cyberspace". Electronic Frontier Foundation. Archived from the original on 23 October 2013. Retrieved 28 January 2014.

5. Council of national security & defense of Ukraine decision from April 28, 2017 “On approval of the rules for the implementation of activities in the field of telecommunications”

6. Council of national security & defense of Ukraine decision as of June 21, 2018 “On the application of personal special economic and other restrictive measures (sanctions)”