New Threats to Economic Security in the Segment of "Deepweb" and "Darknet" Networks

Karpunina E.K.[1], Yurina E.A.[1], Sergeev D.R.[1]

[1]*Institut of Economics, management and service, Tambov State University named after G.R. Derzhavin, Internationalnaya str., 33, Tambov, Russia*

Keywords: economic security, digital economy, DeepWeb, DarkNet, cryptocurrency, information security.

Abstract: Due to the high speed of modern transformations of the economic system, caused by the fact that information and digital technologies had appeared in all spheres of society, as well as by the widespread penetration of the Internet, the economic conditions and interaction mechanisms of economic entities started to change. Virtual technologies of promoting goods and services, the development of various Internet services for interaction between business entities and the population, are becoming predominant. These technologies provide, on the one hand, convenience and speed of data transfer, and, on the other hand, create new, still unexplored threats to economic security and integrity of the state. In this regard, the need to find adequate tools and methods to ensure the economic security of the countries of the world is of particular relevance. The purpose of the scientific article is to study the concepts of "DeepWeb" and "DarkNet" as new specific threats to the economic security of the state through the disclosure of their content, mechanisms of influence and the infliction of economic damage to the national economy. The authors systematized effective tools for leveling threats to economic security from the actions of the DeepWeb and DarkNet networks available in foreign practice, and also determined the directions of the state's activities applicable in the Russian context. The author's developments and recommendations can be applied as a scientific base in building a system to ensure the economic security of the state and the dynamic development of the national economies of the countries of the world.

1 Introduction

For any state, the issue of paramount importance is to ensure its own security, both its national and individual components - economic and informational ones. Nowadays, the phenomenon of close intertwining of these concepts arises in connection with the coming of the all-consuming Internet to our professional and personal life.

The so-called “digital planet” (the term was introduced by the creators of the Digital Evolution Index rating by Bhaskar Chakravorty, Christopher Tunnard Ravi, Shankar Chaturvedi [1], that is, the replacement of physical interactions (in communication, interaction at the political and social level, trade, economy, media and entertainment) by digital interactions created the prerequisites, on the one hand, for increasing the openness of economic and public relations, and on the other hand, for the emergence of new, not yet studied, threats to the information and economic security of economic entities at various levels.

Today, legitimate information transformative technologies (for example, according to the results of a pilot satisfaction rating with urban digital services "Penetration of financial and technological services in megacities of Russia and in the world", conducted by EY company in 2017, China became the leader with 69% penetration, India was on the second place with 52%, Russia took the third place with 43%, Great Britain was on the fourth place with 42%) and innovative business models are actively supported and developed by management information tools, but the Internet already known to all consists not only of social networks, news portals, forums and video hosting sites. The Internet is a complex and multi-level system, which includes a huge number of sites and networks with closed access and secret information which ordinary users are not aware about. The combination of these sites and networks is commonly referred to as the terms "DeepWeb" ("deep web") and "DarkNet" ("black Internet").

Due to the secrecy of information about such networks, there is an underestimation of their negative impact on the life processes of society and, accordingly, damage to their functioning by national economies, which makes it extremely important to study their specifics and develop effective mechanisms for their leveling.

2 Materials and Methods

The basis of this scientific work is the research of Russian and foreign scientists on the problems of ensuring economic security (A. Westing, P. Desuz, V. Cable, E. Laszlo, A. Maslow, X. Moll, T. Watkins, and others.), as well as issues of digitalization of economic activities and the formation of the global information space (D. Bell, C. Lidbitera, P. Drucker, I. Barron, C. Evans, S.D. Bodrunov, V.G. Varnavsky, P. V. Gulyaev , A.A. Dagayev, A.M. Druzhinin and others).

D. Bartlett, E. Altovsky, C. M. Francisco, D. R. Little made an attempt to describe the essence of the "Deep Web" and "DarkNet" closed access networks, but their research mostly had an information component, rather than an economic one.

Thus, despite some attempts to study the new threats to economic security from the digital transformation of public relations and economic activity, there is currently no comprehensive toolkit for their leveling.

Information base of the research consists of statistical and analytical materials of international databases and consulting agencies Boston Consulting Group, Oxford Economics, reports of the World Intellectual Property Organization (WIPO) of the UN, Federal State Statistics Service, reporting and analytical information of the Ministry of Economic Development of the Russian Federation, materials of scientific conferences, periodicals, scientific monographs.

3 Results and Discussion.

The modern understanding of security is associated with the state of security of the vital interests of society, the state, the individual, and trends in its development under the influence of internal and external threats.

Attempts of scientific interpretation of the category "economic security" make it possible to link it with the reflection of the qualitative characteristics of the economic system, including its ability to provide normal living conditions for individuals, business entities, the entire national economy of the country, sustainable development resources and coordinated implementation of the economic interests of various actors.

Economic security is inextricably linked with the concept of "threat", when the latter is a threat, not a fact of damage, and there is an objective possibility to quantify a threat as a change in the mathematical expectation of the magnitude of damage.

At the same time, there are a huge number of types of threats to economic security [2]: from external (political and economic instability, exacerbation of global environmental problems, unpredictable reaction of trading partners) and internal (on the part of the economic system itself), purposefully created by other actors and emerging spontaneously to partially neutralized and uncontrollable management. At the same time, the greatest practical application today is the classification of threats to economic security by the sphere of their occurrence.

So, from these positions there can be threats of a financial, informational nature, threats to the management system and development prospects, etc.

The existing infinity of the Internet space and Internet technologies, which determines the environment for carrying out economic activity, creates conditions not only for more competition in the market, but also for the emergence of new threats to the economic security of economic systems.

A segment of the Internet with a high degree of anonymity, called DarkNet is becoming one of these threats to the economic security of the national economy. It is impossible to connect to this network segment using standard web browsers for surfing the network.

DarkNet networks use non-standard protocols for data exchange. All communication in this network is anonymous and the IP addresses of devices that connect to this network are not publicly available. This degree of anonymity allows users to communicate and make purchases without fear of interference from public security services.

DarkNet can be used in the following cases: if the user is afraid of disclosing secrets of his/her private life; if the user is afraid of being subjected to political repression; if the user wishes to secretly commit a crime in the field of information technology; if the user is required to transfer data that is protected by copyright; if the user wishes to purchase illegal goods (weapons, drugs, fake passports, counterfeit banknotes, etc.)

D. Bartlett writes that "for someone DarkNet is an encrypted world of hidden Tor services, in which it is impossible to calculate users. For someone, these are sites that are not indexed by ordinary search engines: the mysterious jungles of password-protected web resources, unrelated pages and hidden content that is accessible only for certain users. For others, this is just a general concept, which means all that abyss of shocking, frightening and provocative corners of the Internet, where imaginary criminals and villains of all stripes and calibers live"[3]. Indeed, the DarkNet networks, like the open Internet networks, consist of sites, forums and marketplaces. But it is worth noting that working with them seems possible using only special software.

E. Altovsky claims that for solving this task "numerous anonymous access systems will help, which will allow not only to hide the ultimate goal of "traveling"on the Internet from" intermediaries ", but also make sure that the sites they visit will not know who visited them . The easiest way to access sites anonymously is to use an anonymizer located in one of the countries of the free world [4].

Today, one of the most popular software tools for ensuring anonymity on the web is Tor's web browser, which can hide IP addresses of users. Using the Tor web browser data transfer is carried out in such a way that information from the user to the destination computer in the chain is transmitted in an encrypted way. Intermediate computers between the user and the first computer in the chain have information only about the information sender. When information is exchanged between the last computer and the site, information is available only about its recipient, access to the information can only be obtained if the transmission did not use encryption. Thus, the final site has no data about the current sender of information (Figure 1).

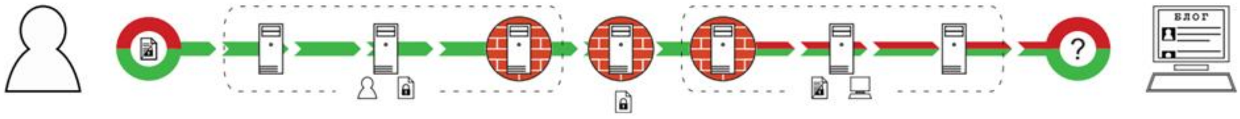

Figure 1: Connection to the site through Tor – chain.

In the DarkNet networks, platforms for selling arms, drugs and other illegal goods and services have been created, they are also used to sell hacked accounts, stolen information, hacked credit cards. Here you can have access to the data that is a trade secret of major corporations and is stolen from corporate servers for reasons of flaws and gaps in information security systems. All this fully meets the criteria for identifying a "threat to economic security". Conditionally, "DarkNet" can be divided into several levels. It is not enough to have specialized soft ware to move through the levels of the deep network. Data for transition to deeper levels is encrypted in pictures, audio files and texts of more available levels. The net installers call the visible network level D. The next level is level C, which allows access to the DeepWeb network. The resource directory of level C is the hidden Wikipedia "HiddenWikki", which is a directory of links to sites that do not open at level D.

All these resources are not on the usual Internet domains (.com, .ru, etc.), but use the pseudo.*onion* domain. Links to these sites are also different from the usual ones for the ordinary user and do not reflect the essence of the site, but consist of a chaotic character set. For additional security, access to the site is carried out either after registration, or after entering an invite-password, which is posted on specialized forums, or received from the user of this resource, with appropriate permissions.

The DeepWeb platform has contributed to the attractiveness of the «bitcoin» cryptocurrency, since transactions using cryptocurrency give the user relative anonymity when making a purchase of an illegal product. This currency has become widely known, and therefore, uncontrolled transactions in these networks have become a serious threat to the economic security of many states.

Thus, taking into account all of the above, it should be noted that "DarkNet" networks represent a real threat to the economic security of the state, since their presence and, especially, rapid development creates prerequisites for the growth of the market of prohibited goods (which it demonstrates in a given period of time), which, in turn, undermines the economic stability of the national economy of any country. This necessitates the formation of a system of measures on the part of the state, aimed at leveling the negative manifestations of this segment of the global Internet.

4 Conclusions.

To solve this problem, let us pay our research attention to the practice of preventing this threat to economic security by the developed countries of the world.

Currently, there are several methods for solving the problem in Europe and America:

- the use of machine algorithms to search for manifestations of criminal activity (hidden operations on controlled purchases and well-planned observation);

- obtaining information from open websites (which is associated with criminal activity in the process of searching for potential customers in public networks). An example is the capture of Reddit forum users (a social news site where registered users can post links to any information they like on the Internet). Five users of this forum were detained after the administration of the *Reddit* website had given the police their contact details. The reason for the suspicions was their activity in the Darknet markets forum thread, where they discussed the purchase and sale of prohibited goods;

- mail blocking;

- the use of large amounts of data, for example, specialists of DCU (Microsoft's anti-high-tech crime analytical unit Digital Crimes Unit) have managed to quickly match hundreds of illegal sites to twelve bank accounts ;

- tracking cash flows (including the purchase and sale of digital currency) and cooperation with banks. Thus, one of the most effective solutions for controlling illicit trafficking of "bitcoin"is the Eliptic system, which cooperates with financial institutions and law enforcement agencies;

- use of modified software versions. For example, to disclose illegal forums, the FBI service uses portal vulnerabilities by implementing its own code, which sends the IP addresses of intruders to law enforcement agencies.

Russia is characterized by the practice of using a system of prohibitions and blocking websites. However, it also gives certain results: in the case of blocking a website of a company or a media resource, about 90% of users lose interest in it, because they do not have the need to search for a way to access a blocked website.

In our opinion, the leveling of threats emanating from the deep segment of the Internet is possible due to the creation of an economic-legal field and the formation of a system for protecting the interests of the population by the state. It is also necessary to optimize the mechanisms of involving those representatives of civil society in the work, who can contribute to the creation of preventive bases for ensuring the economic security of the state, as well as the security of the population and the national security of the state as a whole. If the "blocking" policy continues to be implemented, it may lead to the emergence of new and strengthening of the old threats to the economic security of society and the state.

The creation of barriers to prevent illegal actions on the Internet and the "DarkNet" and "DeepWeb" segments is possible only with the coordinated work of competent information, anti-terrorism and anti-extremist structures of all the states of the world. Optimization and development of such a process will be facilitated by international cooperation on issues of economic and information security.

References

[1] http://www.eoy.dk/

[2] Musatayeva M. O. Sources, types and threats to economic security, the creation of economic security services // Scientific-methodical electronic journal "Concept". - 2015. - V. 23. - P. 26–30. - URL: http://e-koncept.ru/2015/95250.htm.

[3] Bartlett D. "Underground Internet. The Dark Side of the World Wide Web"[Text] / D.Bartlett - electronic edition / https://www.ozon.ru/context/detail/id/139110842/

[4] Altovsky E."Handbookfor a cyber-dissident " [Text] / E. Altovsky - electronic edition / https://www.ifap.ru/library/book534.pdf