Asesorías y Tutorías para la Investigación Científica en la Educación Puig-Salabarría S.C.
José María Pino Suárez 400-2 esq a Lerdo de Tejada. Toluca, Estado de México. 7223898475
RFC: ATI120618V12

Revista Dilemas Contemporáneos: Educación, Política y Valores.
http://www.dilemascontemporaneoseducacionpoliticayvalores.com/
Año: VI Número: Edición Especial Artículo no.:91 Período: Marzo, 2019.

TÍTULO: Objetivos y desafíos de garantizar la seguridad económica y de la información en la economía digital.

AUTORES:

1. Evgeniy A. Voronin.

2. Igor V. Yushin.

RESUMEN: Al restringir el acceso a la información a través de medidas mal concebidas para aumentar su seguridad, retrasamos el crecimiento económico y al mismo tiempo relajamos la probabilidad de riesgos y pérdidas económicas. En consecuencia, solo una combinación equilibrada de seguridad económica con ciberseguridad puede garantizar el desarrollo económico sostenible de la sociedad en el entorno digital. Cualquier solución del problema usaría nuevas tecnologías de inteligencia artificial y aprendizaje automático. La I + D posterior debe proporcionar métodos y algoritmos matemáticos para evaluar y predecir la información y la seguridad económica, teniendo en cuenta su interacción inherente y las agendas conflictivas.

PALABRAS CLAVES: economía digital, seguridad, seguridad de la información, seguridad económica, blockchain.

TITLE: Objectives and challenges of ensuring economic and information security in the digital economy.

AUTHORS:

1. Evgeniy A. Voronin.

2. Igor V. Yushin.

ABSTRACT: Restricting access to information through ill-conceived measures to increase its security, we slow down economic growth while relaxing them we increase the likelihood of economic risks and losses. Consequently, only a balanced combination of economic security with cybersecurity can ensure the sustainable economic development of society in the digital environment. Any solution of the problem would use new technologies of artificial intelligence and machine learning. Ensuing R&D should render mathematical methods and algorithms for assessing and predicting information and economic security, taking into account their inherent interplay and conflicting agendas.

KEY WORDS: digital economy, security, information security, economic security, blockchain.

INTRODUCTION.

The world economic system has entered the 4th stage of its development. The characteristic feature of the latter is the rapid growth of its digital component (Schwab, Klaus. 2016).

According to the World Bank, the total value of electronic goods and services in 2017 exceeded 4.1 trillion. USD (5.5% of global GDP), and by 2035, according to some analysts; this value will at least quadruple.

Changes that go with the formation of the “digital economy” should not however be reduced to just quantitative indicators. “Digital revolution” is breaking down the very foundations of the customary socio-economic paradigm by radically transforming at one fell swoop production sphere, social relations, business practices and finally the system of government.

The explosive development of advanced information and communication technologies: quantum, DNA and other molecular processors, tools for analyzing ultra-large data arrays, elements and

precursors of artificial intelligence and fully automated control systems based on it — all these developments open up dazzling prospects for economic growth at the same time very much leveling ground for development of individual states through diluting imbalances accumulated since the inception of the Industrial era.

Accordingly positive expectations that the very concept of digital economy tend to foment more and more often serve as a basis for the development strategies not only of individual countries — often without any connection with the real possibilities of their economic capabilities — but entire regional blocs, as well as supranational power structures. By the same token the fact that tectonic shifts in the order of things brought about by developments like “digital revolution” tend to engender risks proportioned to scale is blurred over in every way possible – mostly by reducing implied problematics to trivia.

DEVELOPMENT.

Methods.

Russia in this regard only follows suit. In the state program “Digital Economy of the Russian Federation” enacted by the Russian government on July 28, 2017 , the digital economy is viewed as a set of purely technological solutions aimed at increasing competitiveness of the national economic complex — more of its’ external upgrade. Accordingly of all the threats to national security relevant to the subject of total digitalization the authors of the program pay attention only to theft or loss of personal data of citizens as well as failures in cloud-storage of large data arrays.

All the aforementioned bears witness to very serious gaps in the theoretical understanding of the phenomenon of the digital economy as a whole and especially those subtle not always linear interdependences of threats and advantages that the digitization of the world economy generates.

In order to grasp the internal logic of the digital environment one first need to take notice of the fact the latter phenomenon is but an element – most prominent to be sure – of much broader one – the so called information society. The typifying feature of the latter is that information and knowledge as its most sublime manifestation – becomes the major source of economic value (Bell, 1967). A characteristic property of knowledge as a commodity is that in contrast to material goods it is infinitely divisible. In other words the possessor of knowledge while passing it on to another does not lose this knowledge himself. Thus economic circulation of information boils down ultimately to securing the monopoly right to extract commercial profit from one or another intangible asset. This circumstance in turn affects most significantly the understanding of the role of the digital economy plays in the system of ensuring national and economic security — depending on whether business complex of the nation in question is highly saturated with intellectual capital or rather in itself is more a source of intellectual rent than its recipient. In the first instance the emphasis is naturally on regulating cyberspace and developing tools that restrict one way or another the free flow of information while in the second priority is given to maintaining a certain degree of freedom in the digital economy — as a means of correcting imbalances in the global distribution intellectual capital. Theoretically speaking the second approach based on deregulation of the information sphere and revision of intellectual property as an institution (e. g. along the lines of servitude in the law of real property) is more in keeping with the national interests of Russia.

In reality; however,r due to the combination of both market and non-market incentives it has no option but to follow the “mainstream” policy – the one based exclusively on the agenda of the major beneficiaries in rental opportunities of the digital economy – gradually limiting both cross-border and internal circulation of electronic information.

An appearance of rationality to such a practice is habitually rendered by the following considerations (Meltzer and Lovelock. 2018): that tightening control over the digital environment provides:

1) Higher security of confidential information and better privacy for citizens.

2) Swifter response on the part of law enforcement.

3) Higher level of national security in general.

4) Higher rate of economic growth and better competitiveness of the national economy complex.

5) Equal opportunities for all participants in the economic turnover.

On a closer look; however, all these arguments prove to be extremely controversial and largely conflicting; for example, an increase in "transparency" of data flows for the law enforcement hardly agrees with prioritizing personal data protection. Saying this, we don't appeal to some abstract starry-eyed considerations — not even to the sad reality that law enforcement agencies are often leak large amounts of personal data themselves. The fact is that increase in investigative activities by means of global network — or more to the point public awareness of these activities — stimulates greatly mass demand for anonymizing technology and solutions. This, in turn, feeds cyber-activism – both financially and socially – that is the very "hacker" environment from which confidential information is supposed to be protected.

As for the positive effect that Internet over-regulation supposedly elicits on the state of national security its very existence remains highly debatable. Measures required for the long-term storage of Internet content as well as for ensuring control over traffic exchange points create an excessive financial burden on Internet providers and ultimately on subscribers. This, in turn, reduces the effective demand for digital goods and services. Thus recession is introduced into the very sector of the economy that is most capable of damping dissipative moods in society — by providing jobs and livelihood to their main carriers, the so-called precariat, especially its "white-collar-aspiring" segment.

On the other hand, all the experience build up so far by firms specializing in cybersecurity unanimously points to the fact that the most sophisticated tools for filtering Internet traffic are able to provide protection only against relatively stereotyped threats while remaining ultimately powerless when confronted with crowd-sourcing effect of global "hacker" community.

Excessive confidence in purely technological solutions in the field of control over the digital environment on the part of law enforcement agencies seems doubly flawed. The fact is that the hardware and software base of such activities is extremely expensive and due to considerations of a purely budgetary nature cannot be quickly and radically updated. Meanwhile the period of technological changeability in the field of IT technologies — the products of which, in fact, constitute the subject of state monitoring of cyberspace — currently do not exceed one year (on average, 7–8 months). In other words, even the state-of-the-art filtration monitoring equipment would inevitably become somewhat outdated while still being installed and mastered by its operators with the number of vulnerabilities and dead zones growing exponentially ever since.

The level of threats "visible" to this kind of technology would constantly decrease while imbuing its operating law enforcement officers with false sense of complete control over the situation. Yet at the same time harmful activities in the network could be carried out at the catastrophic pace. The latter scenario is especially likely to unfold if the monitoring soft- and hardware is at least in part built on an imported element base. Perils of overdependence on foreign-built equipment are more than eloquently demonstrated by the events of the so-called “Arab Spring”. Tunisia, Egypt and Libya were by the time known for the very tight control of their respective Internet segments. Yet when the civil unrest emerged equipment to control data flow in all three countries suddenly failed — although hadn’t ever before given any reason to question its reliability.

However, even in a purely hypothetical situation of establishing effective control over the national digital environment, one can hardly expect positive consequences for national security. Criminal

elements would sooner or later realize the risks of operating in the “intranet mode” and take their operations completely off-line — which in turn would lead to a multiple increase in costs of detective and investigative activities along with a sharp decrease in their effectiveness. On the other hand, the digital economy would lose powerful stimulus for growth generated by massive demand for means of ensuring the confidentiality of information. Moreover the experience of the largest actors of the digital economy shows: the popularity (attendance) of network platforms is growing in inverse proportion to their degree of regulation.

All of the abovementioned makes one doubt the validity of the argument that a high degree of control over the digital environment can somehow contribute to economic growth and increase the competitiveness of the national economy complex.

Due to the intangible nature of goods and services generated by digital economy, it can only be innovative. Strengthening control over digital environment would mean full enforcement of intellectual property right interpreted very much along the lines of jus in re propria. This will inevitably create a powerful inhibitor for any meaningful innovative activities in the catching-up economies thus rendering futile whatever hope they may harbor to achieve competitiveness in the digital sphere.

As for ensuring level ground for all participants in economic turnover (by means of tighter control over cyberspace) this task controversial in itself can hardly be considered a priority for countries like Russia. It is controversial because the alleged “equality” reduces to the uniformity of the nominal rights of economic entities but often ignores the incomparable opportunities to exercise and protect these rights – i. e. the difference in available financial resources and other assets. From the point of view of Russian interests such problems should be considered secondary because “equality of opportunities” in the market of digital goods and services will in practice ensure and perpetuate the

dominant position of the largest foreign players – instead of a break so much needed by the domestic digital economy.

Until recently a kind of panacea against all the threats and challenges described above was sought in proliferation of the so-called replicated distributed database technology (RDD, blockchain). The latter was expected to provide a form of electronic transactions with an extremely high degree of security while virtually no interference on the part of state. As of now however the experience acquired so far in using the said technology as cryptocurrency has revealed the following critical vulnerabilities:

1) blockchain does not guarantee information from being stolen or fraudulently appropriated.

2) it does not allow to accurately determine the subject of unauthorized access to protected information (Dobkina, 2018).

3) products based on blockchain technology can be forged (Cimpanu, Catalin: 2018).

All of this casts serious doubt on the validity of the purported blockchain technology characteristics. In particular it makes one wonder whether the blocks arranged in a single chain really contain complete information about all operations ever performed on them?

The reputation of the RDD has been significantly undermined by the now-familiar “anomalies” in the activities of the largest cryptocurrency exchanges (DCE). It is known that the majority of altcoins, that in the aggregate provide 31% of trading volume in 1600 DCE’s, have virtually no liquidity (Haig, 2018). Moreover, according to a study conducted in 2018 by the Blockchain Transparency Institute (BTI) the major cryptocurrency trading platforms systematically overestimate their own trading volumes — as much as hundreds and thousands of times — in order to attract new customers. By the same token their average daily values are exaggerated by an average of two-thirds or 6 billion USD. The Upbit platform, one of the ten largest DCE’s, overestimates its own daily turnover by factor of 11. The smaller sites — yet still ranked in the top-100 — act more boldly: Bibox “improves” its daily trading volumes by factor 85, Bit-Z — 469 times, ZB — 391 times, LBank — 4,400 times, BCEX

— 22,000 (!) times. Keeping all this in mind one can't help but wonder whether blockchain is truly the best way to ensure security of the digital economy? Or is it more of a threat to the latter?

All of the above-mentioned vulnerabilities associated with the digital economy are essentially marginal in nature — in the sense that they can be easily overcome by a relatively minor policy adjustment and the use of proven technological solutions. The key threat to economic security is rooted in the very nature of the phenomenon in question. The elemental base of the digital economy pertains to the "core" of the 5 technological paradigm which is currently emerging from the phase of rapid growth, entering state of "maturity". The latter is characterized by a sharp decline in return on investment in the dominant production sectors and as a result by the flight of capital from the real sector of the economy into circulation. All this creates ideal conditions for the formation of "financial bubbles", and a number of specific characteristics of the digital economy contribute to the conservation and even institutionalization of the situation. So we have to refer to the already mentioned obligatorily-innovative nature of the digital economy and all it entails.

In the maturity phase of the technological paradigm the principle of "creative destruction" which motivates any innovative development is subject to a sort of inversion (so-called "disruptive destruction") (Christensen, Leslie, 1997): basic and radical innovations lose commercial viability, while improving innovations become more and more marginal in nature until they become purely fictitious, "imputed".

Under normal conditions, this process is unlikely to last for long. As soon as the next stock market crash established true value of accumulated toxic assets cash flow would have no choice but to channel into new technological paradigm production. The digital economy however is uniquely capable to proliferate almost indefinitely its potentially toxic assets. First of all, due to almost total digitization of stock exchange and the financial sector in general the very process of reorganizing battered financial market creates a powerful incentive for inflating new financial bubbles – a

development well-illustrated by the very emergence of blockchain-based cryptocurrency market. Secondly one should keep in mind the suggestive power of "virtual reality" effect. Available audio-visual solutions are sufficient to visualize literally any kind of technology creating an image of it more graphic and "realistic" in the eyes of a layman than life itself so to say. This in turn can make look solid and viable almost any R&D or venture project – no matter how outlandish in essence – thus conjuring an illusion of dizzying prospects for the development without any meaningful changes in technological base. The synergy of these two circumstances can provides the digital economy with the appearance of positive dynamics all but indefinitely.

As a result, financial capital is in no hurry to leave the speculative sector thus significantly curbing investment opportunities for the development of core technologies of the new technological paradigm while creating an ideal environment for the "economy of financial bubbles" to take on a self-perpetuating character.

Results.

The effect of the "phantom growth" generated by digital sector escaped macroeconomic statistics until the group of researchers from MIT led by Eric Brynjolfsson managed to quantify the influence of consumer rent from digital goods and services distributed free of charge on GDP growth. Their calculations were based on the following formula:

$$GDP_{\Delta} = I^{FQ}+(\gamma p_0{}^{0*} - p_0{}^1)q_0{}^1/(\gamma p^0 \cdot q^0(1+I^{FP}))+(2\gamma w^0 \cdot (z^1 - z^0)+(w^1 - \gamma w^0)\cdot(z^1 - z^0)+2\gamma w_0{}^1 z_0{}^1)/(\gamma p^0 \cdot q^0(1+I^{FP}))+(\gamma w_0{}^0 * - w_0{}^1)z_0{}^1/(\gamma p^0 \cdot q^0(1+ I^{FP}))$$

where:

GDP_{Δ} – GDP growth

I^{FP} – Fisher index for GDP deflator

I^{FQ} – Fisher index for GDP

γ = 1 + increase in consumer price index

p – price of goods / services

q – quantity of goods / services

w – price vector marginal estimate

z – consumer rent

superscript denotes period (0 – beginning, 1 – end)

0 in the subscript denotes new goods / services

When applied to the key actors of the digital economy, the formula showed that consumer rent alone from the free services of the Facebook network "increased" the US GDP growth in 2017 from 2.06% to 2.17% (i.e. by 5.3%), and along with eight others the largest commercial digital platforms (Alibaba, Airbnb, Instagram, LinkedIn, Skype, Snapchat, Twitter, Uber) — up to 2.54% (or almost a quarter). All this allows to make an approximate assessment of the speculative potential of the digital sector of the economy.

As for the formula developed by E. Brynjolfsson and his colleagues it would be expedient to use it to determine the critical relationships between real and speculative macroeconomic dynamics — first of all when the latter begins to act as an inhibitor for the first. The obtained values can be further used in special automatic devices for monitoring electronic exchange trading that can limit operations with assets that are obviously of a "toxic" nature and perhaps those showing excessively positive dynamics indicative of a new financial bubble being inflated.

Discussion.

All of the abovementioned allows us to state with a fair degree of confidence that the priorities for developing and strengthening security of the digital economy are not universal varying significantly from country to country and depending on the state and level of development of the national economy complex, degree of its saturation with intellectual capital, place in the global distribution of intellectual rent, etc.

In case of Russia, as a catching-up economy, an agenda promoted in the sphere of digital security by USA and other and technologically-advanced countries is obviously not in keeping with its national interest – moreover the agenda directly contradicts the latter. Enhancing security of the digital economy by tightening state control over the data flow would ultimately prove detrimental to the interests of the national economy complex as a whole. The development and improvement of the competitiveness of the digital economy should be carried out primarily by means of crowdsourcing efforts of the mass Internet audience making competent use of a synergy of its combined creative potential and consumer instincts. Excessive relying on purely technological tools of controlling the digital environment — especially in technologically underdeveloped countries — will prove in the long term more of a threat to national security than whatever it is intended to combat. All of this fully applies to the blockchain technology which in its present form requires substantial revision and lengthy captious testing. Yet even in the unlikely eventuality of all abovementioned conditions to be met state participation in providing security and competitiveness of the digital sector should primarily focus on making sure that its development does not divert excessive investment resources slowing down thereby the development of other sectors of the S&T complex — especially those components of the latter that form the core of the new technological paradigm.

The aforementioned reflects major objectives and challenges of ensuring digital security as well as appropriate solutions at the macroeconomic level. At the microeconomic level the situation is somewhat different. Down there actors have no choice but to solve their problems of ensuring information and economic security no matter what's the situation high above. Which in turn begs an analysis of economic threats including forecast of their consequences, development of measures to counter them (Skabtsov, 2018) and general answers to what is to be done in conditions of considerable market volatility, high rate of change in its state, technical and scientific progress.

To make an adequate decision, it is necessary to take into account a large number of external and internal factors, to process large amounts of information and to employ innovative, sometimes heuristic decision-making algorithms (Biryukov, 2017). Unfortunately, an expert and even a group of experts cannot cope with these tasks, so it is necessary to involve the technologies of artificial intelligence, machine learning and data-mining. All this boils down to the task of developing and selecting the appropriate data-processing and analytical tools and systems. It should be noted that systems of this type should solve the problems of information security in terms of countering false information or its partial distortion which cybersecurity systems cannot solve.

The most important component of information security is the cybersecurity. It would seem that the market of information technologies offers a large enough number of various protective solutions: antivirus apps, firewalls, etc. However in many cases they themselves are sources of cyber-threat due to “bookmarks”, “black moves” and other hacking methods (Erikson, 2010). To make things worse due to the high rates of development of microelectronics and information technology any of these solutions in particular is soon rendered if not completely obsolete then definitely not up for the task. In this regard the problem of ensuring cybersecurity boils down to the following objectives: the development of technological tools of protection, a comparative assessment of their effectiveness, intellectual monitoring of the digital information space with the focus on analysis of cyber-attacks, their types and likelihood (Beyer, et al. 2018).

CONCLUSIONS.

There are some conclusions as the following:

1. At the macroeconomic level, solutions intended to ensure informational and economic security don’t necessarily complement each other and the so their harmonization requires further research in both social and economic sphere.

2. The objectives of ensuring economic and information security at the state level are deeply interconnected and can be solved by establishing macroeconomic balance through political, legislative and macroeconomic means.

3. To ensure information and economic security at the microeconomic level, it is necessary to apply information and analytical systems based on machine learning technologies and data-mining.

4. Continuous monitoring of the digital information space for the study and prediction of cyber-attacks is a necessary condition for creating an effective information security system.

BIBLIOGRAPHIC REFERENCES.

1. Bell, D. (1967). Notes on the Post-Industrial Society. – The Public Interest, 1967, № 7, p. 102.
2. Beyer, B. Jones, C. Petoff, J. Murphy, N. (2018). Site Reliability Engineering. Reliability and security in Google. - SPb .: Peter, 2018. - 592 p.: - (“O'Reilly's Bestsellers” series).
3. Biryukov, A.A. (2017). Information security: protection and attack. - 2nd ed. Revised and enlarged. - M .: DMK Press, 2017. - 434 p.
4. Christensen C. M., Leslie D. (1997). The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail, 1997.
5. Cimpanu, G. Catalin, B. (2018). Hacker Makes Over $18 Million in Double-Spend Attack on Bitcoin Gold Network // BleepingComputer, May 24 2018 (publication is available via link: https://www.bleepingcomputer.com/news/security/hacker-makes-over-18-million-in-double-spend-attack-on-bitcoin-gold-network/)
6. Dobkina L. (2018). The five largest thefts of cryptocurrency // IHODL. 16.01.2018 (publication is available via link: https://ru.ihodl.com/analytics/2018-01-16/5-krupnejshih-krazh-kriptovalyut/)
7. Erikson, J. (2010). The art of exploit. 2nd edition. - Per. from English. - SPb .: Symbol Plus. 2010. - 512 p.

8. Haig, S. (2018). Pairings of 6 Cryptocurrencies Comprises 69% of Total Crypto Volume // BitcoinNews. 25/06/2018 (publication is available via link: https://news.bitcoin.com/pairings-6-cryptocurrencies-comprises-69-totalcrypto-volme/?utm_source=OneSignal%20Push&utm_medium=notification&utm_campaign=Push%20Notification)

9. Meltzer, P., Lovelock, P. (2018). Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia // Global Economy & Development, March 2018. P 13.

10. Schwab, A. Klaus. G. (2016). The Fourth Industrial Revolution. World Economic Forum. – Cologny/Geneva, 2016. (publication is available via link: https://luminariaz.files.wordpress.com/2017/11/the-fourth-industrial-revolution-2016-21.pdf

11. Skabtsov, N. (2018). Security Audit Information Systems. – SPb.: Piter. 2018. – 271p. (Series "Library programmer").

DATA OF THE AUTHORS.

1. Evgeniy A. Voronin. Doctor (tech.), Professor, Leading Researcher of FRC «Computer science and management» of RAS, Moscow, Russian Federation. E-mail: e.voronin1@gmail.com

2. Igor V. Yushin. Ph.D., Assistant Professor at RANEPA, Moscow, Russian Federation. E-mail: yushin-iv@ranepa.ru

RECIBIDO: 7 de febrero del 2019. **APROBADO**: 21 de febrero del 2019.