Digital Economy: Angel or demon?

Jacques Fontanel

Digital Economy: Angel or demon?

Pax Economica

Jacques Fontanel

Conference, December,12, 2017

Université Grenoble-Alpes, France

Summary : The information war is already engaged. First of all, it is obvious that the control of information is crucial for the management of political societies and the enterprises decisions. Then, the Internet revolution led to two major changes in our perception of reality; the availability of a large the amount of information is very useful but it is distributed between many actors. Finally, these systems seem to be fragile and could be hit and looted. Information is power, which is able to modify the behaviours of States or enterprises.

Ransomware, cyber-attack, digital economy, State power

The digital economy, whose definition is not yet clearly codified, includes all economic and social activities that are managed by platforms, i.e. the Internet, remote mobile devices and the necessary sensors equipment or investments. It integrates new information and communication technologies (NICT) as well as the electronic and digital economy, and it is essential in the implementation of the "new economy". It takes a considerable place in the national production of the most developed countries, it brings its techniques and its dynamism at the same time in the investment of the materials of connection and in the diffusion the whole productive systems processes.

Interest

It is a fast growing sector, considered as very efficient in the production of goods, services and knowledge; it has become a strategic factor of the economic growth, because it is an effective fertilizer for the development of the shares of domestic and international markets. Today, via Internet, it dematerialises physical distances to develop and share productive concepts and ideas, leading to the birth of new entrepreneurs and markets.

However, the heart of the digital economy lies in the manufacturing of hardware and components, software and IT services and telecommunications. First of all, the digital sector requires appropriate, specialized, constantly moving infrastructures, with an exceptional potential for innovation. It is a sector that is largely dominated by a few operators, under the leadership of the United States, but with increasing influences from South Korea and China. These productions open up many new or renewed activities concerning e-commerce, online professional or commercial services, video games or the diffusion of sounds of any kind. Most of these activities did not exist in this form before the implementation of appropriate software, but also they compete with strong commercial systems, sometimes to the detriment of the activity of the latter, or through change of the consumption paradigm, either by transforming the behaviour of potential buyers. Finally, all other sectors are concerned by the services produced by the digital economy, particularly in the banking, distribution, transport or health sectors.

The implementation of the tools implies an increase of the private and public investment concerning materials, telecommunications, software, process of production or organizational innovation. But it also leads to an improvement of the information available to employees, which favours an increase in productivity in all peripheral sectors of the national economy. This results in time saving, improved trade and more efficient management of economic and administrative entities. Overall factor productivity is pushed upward in both growth areas of the digital economy. With the dematerialization of distances, it eliminates barriers to entry in certain markets and creates new opportunities for companies. A humanoid robot costs an average of 60,000 dollars, he does not claim any salary, vacation, reform of the Labour Code, or right to strike. In other words, the investment is quickly amortized.

The rise of the digital economy is leading to a new industrial revolution in all spheres of economic life and society. It structurally modifies the behaviour of the consumers, it rationalizes the productive and exchange phases of the company and it deeply transforms the organizations of the companies and the public institutions. However, an ever more digital economy, where trades and skills are becoming increasingly complex, multi-skilled profiles may stagnate or even decrease.

However, as a hammer is used as a tool or arm, digital economy is dangerous without control and verifications. Because the digital economy can only work on the basis of confidence in the hardware, the quality of the information produced and the power and reliability of telecommunications at the right time must be controlled.

Dangers of digital economy

The main problem of digital industry and services is the international, national and personal problem of security. Military protection with mass destruction arms is not adapted to the virulence of cyber-attack (Coulomb & Fontanel, 2006; Fontanel, 2010; Fontanel & Corvaisier-Drouart, 2014). Digital economy infiltrates all economic activities, it reduce the competitiveness of poor countries, it is very open to financial speculation, it encourages cybercrime, it produces false information and it develops political strategic and economic cyber attacks that are difficult to identify. Companies are called to the utmost vigilance in the operation of phisting operations. In France alone, during the month of December 2017, more than 17 million fraudulent attempts at phistings have been identified. Personal information, passwords are discovered and misused. In 2016, the bank of Bangladesh was the victim of a cyber attack, she lost $ 100 million a holiday salt. Ransomware (NoPetya in Ukraine) become scourges that are difficult to identify (Sullivan & Kamensky, 2017 ; Guedez, 2017).

The vast cyberattack caused by the "Petrwrap" (Petya) ransomware strikes dozens of countries, including France, where several companies have been affected, it spreads around the world. A flagrancy investigation was opened for "fraudulent access and retention in automated data processing systems", "obstruction of the operation" of these systems, "extortion and attempted extortion". The British advertising giant WPP, Saint-Gobain, Auchan and SNCF were directly affected. The eventual deviations are difficult to evaluate. Economic and politician world currently experiences an industrialized and automated attack that is based on a very intelligent network analysis to detect existing weaknesses The Wannacry virus in May 2017 caused also major damages, for now contained officially. IT security researchers said that they had discovered a potential link between North Korea and the global cyber-attack that has hit tens of thousands of businesses and governments around the world. Neel Nehta, computer scientist at Google, has put online computer codes showing some similarities between the "Wannacry" virus, which affected 300,000 computers in 150 countries, and another series of piracy attributed to North Korea. Some information and procedure re developed by Sentryo (2017) in order to fight against this virus.

Once implanted on the machines, the cyber-attack forces the restart after a few minutes (between 10 minutes and 1 hour). It encrypts the files in the computer's memory. About sixty types of files are targeted. The ransom-ware caused a kind of panic. Petya attempts otherwise to spread through an internal Windows tool (WMIC) and PsExec remote management tool, using stolen identifiers on the post. The massive waves of this massive wave of cyber-attacks spread to several European and American multinational firms after striking major companies and government structures in Ukraine and Russia. The pharmaceutical company Merck became the first known victim in the United States, its computer system having been "compromised". The virus is spreading around the world, a large number of countries are affected. Ukraine is the most affected country before Russia and, to a lesser extent, Poland and Italy. A message appears on the screen and asks to make a payment of 300 dollars in bitcoins, and to send a proof of the payment by email, in order to obtain a decryption key to find his files intact. We are talking about ransomware (Calyptic Security, 2017).

Because the digital economy can only work on the basis of confidence in the hardware, the quality of the information given and the power and reliability of telecommunications at the right time. State services seek to locate and neutralize these attacks in order to further improve the security of public services and to encourage businesses to do the same. Today, no track comes out. The motivation of ransomware is usually pecuniary. Cyber-security becomes one of the biggest priorities for businesses and governments, as practically all of economic and social life migrate their main internal information to data centres and the cloud. State services seek to locate and neutralize these attacks in order to further improve the security of public services and to encourage businesses to do the same. It becomes useful to create a form of new private-public collaboration, because the governments do not have the skills to solve this problem. The faith in tech-powered productivity growth is clearly challenged, with some fears that are not completely justified, such as the fight against robot.

The information war is already engaged, everywhere, even in Cyberspace (Betz & Stevens, 2017). First of all, it is obvious that the control of information is crucial for the management of political societies and the enterprises decisions. Then, the Internet revolution led to two major changes in our perception of reality; the availability of a large the amount of information is very useful but it is scattered between many actors. Finally, these systems seem to be fragile and could be hit and looted. Information is power, which is able to modify the behaviours of Stets or enterprises. It creates, may be artificially and wrongfully, a soft power that has the ability to attract, to seduce and to influence the main decisions of the national or international actors.

Moreover, cyber-war is a new instrument for the expression of the state’s power and the economic war.

Bibliography

Betz,D.J., Stevens, T. (2017), Cyberspace and the State. Toward a Strategy for Cyber-power, IISS, Taylor and Francis,

Calyptic Security (2017), Biggest Cyber Attacks 2017 : How they happened ? https://www.calyptix.com/top-threats/biggest-cyber-attacks-2017-happened/

Coulomb, F. Fontanel, J. (2006), Mondialisation, guerre économique et souveraineté nationale, in La question politique en économie internationale (Ed. Berthaud & Kebabdjian), La Découverte, Paris.

Fontanel, J. (2010), Economie politique de la sécurité internationale, La librairie des Humanités, L'Harmattan, Paris.

Fontanel, J. , Corvaisier-Crouart, B. (2014) For a general concept of economic and human security, in « The Evolving Boundaries of Defence : An Assessment of Recent Shifts in Defence Activities, Emerald, Vol. 23.

Guedez, A. (2017), (2017), Cyber Attacks 2017 : What were their impacts, and what to expect in cybersecurity for 2018, November, 28, Gb Advisors, https://www.gb-advisors.com/cyber-attacks-2017/

Sentryo (2017), Conseils pratiques pour lutter contre le ransomware Wannacry, https://www.sentryo.net/fr/conseils-pratiques-ransomware-wannacry/

Sullivan, J.E., Kamensky, D. (2017), How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid, The Electricity Journal, Vol. 30 ? Issue 3, 2017. April.