**PRZEMYSŁAW BAKOWSKI**

# OPEN SOURCE CODE – „BETWEEN WEST & EAST"

**STRESZCZENIE**

Technologie numeryczne są zbudowane na bazie sprzętu i oprogramowania, i jako takie są motorem drugiej rewolucji przemysłowej. Ponad 12% światowego dochodu generują technologie informacyjne. Jednakże gospodarki większości krajów europejskich są za słabe żeby konkurować z globalnymi firmami softwarowymi i producentami sprzętu numerycznego. Niektóre z tych firm są pod pośrednią kontrolą innych państw. W tym kontekście podkreśla się konieczność budowy oprogramowania krajowego opartego na open source software. Krajowe oprogramowanie systemowe, programy ochrony i oprogramowanie profesjonalne wydają się być jedynym środkiem uniknięcia uwarunkowań ekonomicznych i potencjalnych zagrożeń pochodzących z zewnątrz kraju.

**ABSTRACT**

The digital technologies based on digital hardware and software are driving the second industrial revolution; more than 12% of Gross World Product are related to IT. The economy of most European countries is too small to compete with global software companies and digital hardware producers, some of them being under the indirect control of sovereign powers. In this context we underline the necessity of building national software competences in open software components and systems. Nationally developed and controlled operating systems, security software and professional software seem to be the only way to escape the economic constraints and potential security threats from external actors.

## INTRODUCTION

The exponential growth of digital technologies and products including hardware and software is transforming the global economy and the way we live [6]. Historically, the development and production of digital hardware and software was under the control of western companies.

This is no more true.

The most important software is still developed by western companies, like Microsoft, Google or Oracle, but a great part of their activities has been moved to India and China. The development and the production of digital hardware is done mainly in Asian countries. Taiwan has the largest silicon foundries (TSCM) [15], the design of circuits is done in Japan, India, and South Korea, the manufacturing of devices and systems has been moved to mainland China by companies like Foxconn [18].

In this context, most European countries are just passive consumers trapped between the US as a provider of software, and Greater China (Taiwan and mainland China) as producer of digital hardware. In Europe, almost all of the technologies driving the improvements in the industries and services are coming from outside and are economically controlled by the US and China.

This has a major impact on the economy and the security.

There is no easy way to escape from this two-sided dependency. A partial solution to this problem may be provided through the vigorous development and mandatory use of open source software mainly founded by national authorities.

Some examples of such undertakings can be already seen in France and Germany.

## THE RISE OF DIGITAL TECHNOLOGIES

### Hardware

More and more complex software systems and applications can be run thanks to the exponential increase of the number of transistors integrated in processing units and the progressive

rise of frequency. The number of transistors in modern processors is close to one billion with the operating frequency of several GHz.

Modern operating systems contain millions of code-lines. They may control multiprocessing units with several levels of computing modes. Most operating systems have their roots in the Unix system developed in the early 1970s by AT&T.

There are two important processing platforms (processor families): the Intel family and the ARM family.

Intel processors were initially designed in the USA. Nowadays, this is done both in the US and in Bangalore (India), where Intel employs several thousands of engineers and massively recruits new candidates. The production of Intel processors is largely off-shored to Greater China (Taipei, Dalian) [7].

The initial design of the generic architecture of the ARM processor architecture is still done in the United Kingdom. ARM company is purely fabless, i.e. it does not produce any processor. All architectural extensions (Samsung, nVidia, Marvel) and all the production of ARM-based processors is done in Taiwan by TSCM [15], in mainland China by SMIC [24], and in South Korea by Samsung [16].

It is worth noting that over 80% of the global production of integrated circuits is done in the foundries of Greater China [17].

**Digital devices and systems**

Since the early 1960s the production of electronic equipment has been captured by Japan. This trend continued in 1970s and 1980s in Taiwan and South Korea and more recently in mainland China.

Nowadays, Chinese companies like Foxconn (more than 1.3 million employees in 2011) [18] produce all kinds of most advanced digital devices including iPad2, DELL computers, PlayStation, and many others. Therefore, the Chinese engineers, who leave Foxconn after 3 years of work in average, have the knowledge of the internal designs of most advanced devices. Foxconn financial power and over-critical economic size allows it to capture the production of almost all modern digital devices. It also buys competitors' businesses and through *reverse off-shoring* expands its manufacturing and commercial facilities in the USA and Europe [e.g. in December 2009, Foxconn bought DELL factory in Lodz (Poland) and reduced the number of employees from 3200 to 1600].

Another example is Lenovo, a Chinese company designing and producing personal computers. Lenovo computers are installed in the offices and factories all over the world. The huge size of the Chinese market and the financial incentives from the Chinese government provides Lenovo with exceptional advantages over traditional PC producers like DELL or HP (which also produce in China).

It is worth noting that since 2010 the most powerful super-computers, such as *Tianhe-1A* have been designed and manufactured in China [13]. Tianhe-1A is still based on Intel/AMD processors; this however, may soon change with the advent of purely Chinese designed Godson-3 (architecture) and Loongson – 3 processors compatible with MIPS and x86 architectures [14].

**Telecommunications**

Digital communication systems interconnect processing devices. Telecommunications systems are built from digital links and communication nodes. The nodes themselves are sophisticated processing systems driven by complex software including operating systems and Internet protocols. Terminal links (a.k.a. last mile links) are more and more often wireless (WiFi, 3G, 4G links). The terminal devices are computers or smart-phones controlled by specific operating systems.

Traditionally, the design of the Internet routers and switches was done in the USA. Since the early 1990s the production of telecommunications equipment including routers/switches (e.g. CISCO) and of terminal equipment (Nokia, Motorola, Philips) has been moved to China. At the same

time, the original Chinese companies, such as Huawei or ZTE, have started the design and production of telecommunications equipment for local and international markets.

Nowadays, these Chinese companies propose the complete equipment for the most advanced telecommunications infrastructures, including routers and wired or wireless communication links based on the most recent standards, FTTH, LTE, WiMAX etc.

Western designers/producers (CISCO, Ericsson, Lucent-Alcatel) of telecommunications equipment face formidable competitors proposing equivalent and compatible equipment at much lower prices. For companies like Huawei and ZTE, design and production is cheap due to lower salaries and the financial help from the Chinese government.

Huawei and ZTE are opening R&D centers in Europe and the USA. These centers have several objectives. The first is to attract the local researchers and engineers and absorb the local knowledge and technology. The second is to influence the development and control of new technological standards, LTE for example. The third is to train future managers to tailor and sell the company products according to the needs of local operators [8],[25].

**Software**

Software is the essential functional layer of all digital devices containing programmable components. These devices include all kinds of computers from personal to supercomputers, communication nodes, and wireless terminals such as smart-phones.

All these devices work under the control of operating systems. The applications include internet services, data-bases, multimedia middle-ware, and many other software components.

Professional software includes Enterprise Resource Planning (ERP) systems, Financial Services systems, Fast Trading systems, CAD systems, and many others. Control software drives and regulates production machinery and facilities, energy plants and energy network, aerial traffic, and many others.Almost all kinds of human activity is facilitated or controlled by software systems.

The growth of the accumulated and transmitted data, and that of programs, is exponential; on average the size of data and programs doubles every year.

The production of the software seems to remain under the control of western companies; however a great part of software development and coding is transferred to Asian countries like India and China. All large software companies have their offices in Bangalore or Delhi, but progressively the volume of software development in China exceeds that of India [1].

It is worth noting that the largest Indian software companies, such as Infosys or Tata Services, have started to transfer their activities to China [19].

Infosys (over 130 000 employees – mainly software engineers) and several other Indian companies have captured a great part of the software development and information services from western companies. They have even started to implant their activities in other countries (*reverse off-shoring*) including the USA and Europe (e.g. Lodz (Poland), about 1000 employees) [20].

In China, the market of Internet software related to media and business is strictly controlled. In this domain, even the most prominent western companies like Google or Amazon have no chance of establishing their business [10].

**Hardware and Software – Security Aspects**

The growing dependence on IT technologies implies facing different kinds of security threats. Both hardware and software may be modified or augmented to include the functions that may stop (kill) the operation of the equipment, or install the back-doors allowing the transmission of the data to the interested recipients [9].

The electronic components embedded in digital systems, such as computers or routers, may be triggered remotely to operate as kill switches or back-door functions by disallowing encryption logic.

Operating systems often contain back-door functions allowing the extraction of data from the host computer/device. The activities of hidden mal-ware (malevolent software) embedded in hardware and operating systems are extremely difficult to detect. That is why the Chinese govern-

ment obliged Microsoft to open the source code of Windows in order to analyze and control all backdoor operations integrated in this operating system [27] [9]. No other country or private company has the compelling means (i.e. the size of Chinese market) to enforce such a disclosure.

On the other hand, given the majority of components produced and, in many cases, designed in Great China, the companies controlled by the Chinese authorities are able to provide the modified components in the equipment sold to American and European institutions, including the defence departments.

Even the most efficient anti-virus software is not able to operate at the level of hardware or of operating systems. The role of an anti-virus program is essentially limited to the detection of viruses, worms, Trojan horses at application level. Much of the anti-virus software is provided by Russian, Indian or Chinese companies. For example, the Kaspersky anti-virus programs are developed in Russia. The founder of Kaspersky company, Eugene Kaspersky, was initially working for the laboratories sponsored by the Russian security services (KGB).

Another example is the Norton anti-virus suite produced by Symantec which was bought by Huawei. Today Huawei-Symantec has expanded its activities over all the continents [22]. Currently the CEO of Huawei-Symantec is Ren Zhengfei who is also president of Huawei, the biggest producer of telecommunications equipment, and he is a former high ranking intelligence officer of PLA (People's Liberation Army)[12]. This certainly explains why the recent bid from Huawei to acquire 3Com (3Com manufactures networking equipment and anti-hacking computer software for the military) has been blocked by the US security department [23].

**Open source software – national economy and security**

In many cases, Windows operating system and some other applications are sold for almost nothing (even the illegal download and installation is tolerated) in order to create locked-in dependence. Once the user is accustomed to the functionalities of the software there is no easy way to dispense with it. The *switching costs* may be simply higher than the cost of acquisition of the new version of the originally installed software [5].

From this point, the use of the same software (always the next generation with incremental changes) makes the user the prisoner of his/her own habits. He/she is ready to pay in order to continue working and using the data without changes of functions and formats. The same locked-in mechanism is applied to the professional applications like ERP systems and security software. There are two reasons to lock-in users, the first is a long-term profitability reason, the second is *strategic*. It aims at the control of the user's equipment through the hidden control functions integrated in the software that can be triggered without the user's knowledge.

Such a situation is highly inconvenient and sometimes may be damaging to the national interests of the countries that have neither indigenous hardware nor software. In this context, for a middle-sized European country, it is vital to develop and tailor the open-source operating systems, the protection/security software and the critical management systems. Designing specific hardware and its implementation seems to be out of reach for most European countries. A complete design and the production facilities for complex integrated circuits would require the investments of several billions of dollars.

The use of locally supplied software, based on open source solutions, should become mandatory for national institutions (power supply installations, telecommunications systems, financial institutions, and education) in order to guarantee better economic development and higher security.

**Open source operating systems**

In Europe, the development of open source software has a long tradition especially in the domain of OS and ERP systems [21]. The LINUX system initially developed by Finnish scientist – Linus Torvalds [28], has been developed in France (distribution Mandriva) and in Germany (distribution SUZE). The distributions of these operating systems offer full scale services for server and client installations.

The French administration is required to use the French version of Linux instead of Windows; this is motivated by both, economic reasons (no need of licence) and security reasons (protection of French *Gendarmerie* and Defence).

The same is true for the German Ministry of Interior.

**Open source ERP systems**

The availability of open source professional software like ERP allows institutions such as industrial establishments and offices, to free themselves from commercial solutions and locked-in effect. For example, OpenERP is a Belgian product that offers a vast choice of open source modules to deal with different kinds of activities, and retail and management processes ([21].

**Open source security software**

Nowadays, there are many open source security programs [27]. Most of them provide the essential anti-virus functions if run on Linux. However, many wide-spread and powerful tools are available only as closed software (compiled software). The development and the distribution of such closed security tools,(e.g. Norton from Semantec-Huawei or Kaspersky suite), may serve the interests of the companies making these tools.

All the above mentioned reasons are enough to take into consideration the development and implementation of open source solutions at national level. But more important is the initiating of competence related to the understanding and design of modern software based on open source components. In the long term only the countries and their governments that understand the need of training and education in the domain of open source will survive.

**CONCLUSION**

The globalization of the development and production of software and hardware systems by huge corporations makes European countries highly dependent. This dependence is essentially economic because, in order to continue their activities, the local companies and institutions must purchase externally produced software and hardware equipment.

From a security point of view, the same institutions are exposed to the externally controlled functions integrated in this equipment.

A partial solution to these problems may be the mandatory introduction of open source software into the vital industries and institutions. This, however, must be complemented by high competence and nationally subsidized training in open source software analysis, design and reuse.

**REFERENCES**

[1] Eltschinger C., *Source Code China – The New Global Hub of IT Outsourcing*, Wiley, 2007
[2] Harwit E., *China's Telecommunications Revolution*, Oxford University Press, 2009
[3] *U.S.-China Economic and Security Review Commission Staff Report*, January 2011
[4] Jain B., *Huawei Part of Chinese Spy Network*, „Economic Times", May 7, 2010
[5] Shapiro C., Varian R., *Information Rules*, Harward Business School Press, 1999
[6] Cortada J., *The Digital Hand: How Computers Changed the Work of American Manufacturing, Transportation, and Retail Industries*, Oxford University Press, 2004
[7] Tan W. T., *Embedded Intel China – The Inside Story*, Marshall Cavendish, 2010
[8] Cohen P., Richard L., *Le Vampire du Milieu*, Fayard, 2010
[9] Clarke R., Knake R., *Cyber War*, Harper Collins, 2010
[10] So S., Westland J. C., *Red Wired*, Marshall Cavendish, 2010
[11] Lerner J., Schankerman M., *The Commingled Code – Open Source and Economic Development*, The MIT Press, 2010
[12] McGregor R., *The Party: The Secret World of China's Communist Rulers*, Harper Collins, 2010
[13] Prickett Morgan T., *China takes HPC heavyweight title*, „The Register", October 2010
[14] Hu W., Wang J., Gao X., Chen Y., *Micro-architecture of Godson-3 Multi-Core Processor*, Hotchips Conference, San Francisco, 2008
[15] *TSCM may beat Intel with world's first 3D chips*, „PCWorld", June 2011
[16] *20nm ARM Chips this year form Samsung, 20nm ARM Chips this year form Samsung*, „Xbitlabs", February 2011
[17] *Greater China IC foundry industry overview*, „Digitimes", January 2011
[18] Anthony S., *The man behind Foxconn, the largest and most powerful exporter in the world*, „Businessweek", September 2010
[19] *Infosys to start new campus in Shanghai*, BPOWatch, May 2011
[20] *Infosys BPO Poland selects a new Skanska building in Lodz*, BizPoland.pl, June 2011
[21] Pinckaers F., Gardiner G., *OpenERP for Retail and Industrial Management*, Tiny Sprl, 2009
[22] *Huawei Symantec opens in South Africa*, „Hi-Tech Security Solutions", April 2011
[23] *Huawei 3Com total failure, Bain Capital withdrawal*, „Itnews", December 2010
[24] *ARM signs foundry deal with SMIC in China*, „ElectronicsWeekly", October 2010
[25] *Aero2 (Poland) Awards TDD LTE Contract to Huawei*, „LTEWorld", November 2010
[26] *China Gets A Peek At Microsoft Source Code*, „InfromationWeek", June 2010
[27] *50 Open Source Tools To Replace Popular Security Software*", „ITManagement", May 2010