Analysis

Document

20/2016 March 23, 2017

[Visit Website](#) [Receive Newsletter](#)

David Ramírez Morán

Strategy and reliance on information technologies

This document has been translated by a Translation and Interpreting Degree student doing work experience, LAURA REVUELTA GUERRERO, under the auspices of the Collaboration Agreement between the Universidad Pontificia Comillas, Madrid, and the Spanish Institute of Strategic Studies.

Strategy and reliance on information technologies

Abstract:

The defence-oriented information technology market is undergoing the same particular changes that trade is experiencing with other weapon systems. Both trade and diplomatic practices related to the sensitive system recruitment are emerging among the agents involved. Doubts regarding the reliability of such systems, together with a lack of flexibility concerning locked-in solutions to the changing environment, and the buyer's interests are giving rise to new initiatives in order to protect and secure information.

Keywords:

Reliance, information and communication technologies (ICT), strategy, sovereignty, industry.

Introduction

Today’s society has turned ICT into essential tools for the development of almost any activity. Public administrations, ministries of defence, and their respective armed forces cannot escape this reality either but must accept instead that they are a part of the group of users dependent on these services. At the same time, public institutions play a key role by providing some of these services related to the Information Society since they have facilities of their own. Hence they play a dual-role as customers and suppliers of the information services.

The platforms of the Armed Forces keep expanding their number of IT systems to maintain a proper functioning. Current combat aircrafts, warships, and land vehicles incorporate several computers that take over tasks such as the engine management, the communications between the staff, or the functioning of the different combat systems integrated in the platform. Moreover, since there is a greater integration of these systems, it is necessary to have intercommunication systems between all these elements. It can therefore be said that those platforms rely on an IT infrastructure that ensure their functionality and communications.

If infrastructures were regarded as an essential capability to fulfil the needs of the Armed Forces, it would then be necessary to establish a procurement policy to fulfil the required standards of costs, benefits, and reliability, while securing standards of supply security, technology access, and other restrictions linked to geopolitics and geoestrategy. This article focuses mainly on these restrictions, which will be discussed after a brief description of the different concepts that are going to me mentioned throughout the article.

Infrastructures as commodities

Infrastructure is made from hardware —the physical components of computers and telecommunications, including the electronic circuitry— and software —the various kinds of programs and instructions that are transformed into services when operated through the hardware. There are other categories within software such as firmware, the operating system, the general purpose execution environments, and the specific applications that provide services for the organisation.

Nowadays, both hardware and some software resources have basically become like any other raw material undergoing the market process of traditional goods such as metal and minerals. This change in trend is a result of the market evolution and the change in value chains of products provided to customers, where now the added value from manufacturing and distributing these intermediate goods is marginal.

A market dynamic based on reducing costs has been implemented for these assets. This has been made possible due to a standardisation process of the systems as an answer to the Open Systems philosophy present throughout the evolution of computers and telecommunications since the end of the 1970s and the beginning of the 1980s.

This trend has been confirmed after proving the small differentiation between performance presenting models of the same market segment supplied by different manufacturers and the rapid merge of suppliers heavily reduced to just a few dozens in the case of hardware and even less than a dozen in the case of software.

Undoubtedly, there are still very specific performance systems that do not fall under this type of model. It is also true that the virtualisation of the systems (processing, telecommunications, and storage) currently named *hyperconvergence* is reversing this particularity through the substitution of the dedicated systems by a combination of general purpose hardware interconnected and set up in a way that allows to obtain a similar performance to the one of the dedicated system. The difference between one and another lies in the significant cost reduction from the equipment production that is directly passed to the final user since the cost of the software and the services related to set up, maintenance, and support of these technologies make final cost reduction less significant.

Software elements influenced by this trend are mainly the operating systems and applications that can be considered as logic infrastructure for storage and processing that support the information society, such as database and application servers. The scarce value created from selling these products contrasts with the value generated from services related to maintenance and support, which are the ones that bring a significant performance to suppliers, directly or through representatives, mediators, or authorised distributors. In fact, the traditional model of acquiring software packages that allows unlimited use of the software once bought is being substituted by time-limited license models, where it is necessary to upgrade the software periodically to keep the system working. This policy makes it possible to reduce capital expenditures (CAPEX) and orchestrate them in an equivalent financing operation by including the operating expenses (OPEX).

ICT strategies

Under this idea of hardware and software as raw material of scarce added value, the chosen option to acquire them is going directly to the market instead of developing them directly, similarly to what happens for instance to the new alternative hydrocarbons sources; that is, their exploitation is not profitable because of the negotiation prices of traditional exploitation products in the market. Therefore, countries and companies do not even consider developing new platforms. They would be more expensive because there wouldn't be a price reduction for experience and economies of scale. They would also present a worse performance as a result of poorer technology knowledge and the impossibility of using designs from other manufacturers, as these designs are protected by patents.

The efforts needed are considered to be useless: entering an established market like the one that already exists is complicated, and it is not easy to find a model that pays off for the necessary investment.

Such a decision is not free from consequences. Although you get rapid coverage of the basic needs by going to the market, you are also contributing to distort it by reducing the number of available options and taking out the research on these components. Only the few suppliers left are in charge of developing and maintaining these technologies, a task they carry out by focusing on their own interests. This is how they control the market; their control positioning causes the remaining technology to depend on the performance of these elements, and so only new technologies in line with the interests of the suppliers will prosper. This also gives them the chance to attract customers, since there is no other alternative and there is a need for giving continuity to the whole application ecosystem based on the performance of these elements.

If any problems related to this technology show up, they will affect all players involved and, given the fact that only one company has the ability to solve them —as it has total control of the product— priorities under which these problems will be solved will be determined once again by the interests of the supplier.

From an economic perspective, the lack of alternatives has also an impact on the competitiveness of the sector, which is why the supplier can afford to fix prices unilaterally.

A matter of reliance

Using specific hardware and software as infrastructure for the information systems implies the responsibility of relying on the suppliers of such elements and hoping they will take care of preserving information privacy and integrity. In fact, this blind trust is due to lack of evidence proving the opposite. It is easy to prove that this preservation has failed when an information leak is released, but it is very difficult when leaks are not released while other players can keep eliciting strategic information without the user noticing this.

Leaks can happen as a result of programming or design flaws that give place to vulnerabilities potentially exploited to illicitly access the system. They can also happen as a result of the creation of backdoors, after which the manufacturer facilitates the necessary means so that third parties gain access to these systems.

These highly complex systems go against the user on two accounts. Firstly, as functionalities provided grow in number, the number of spots where the programming or design default can take place also increases. Secondly, the complexity of the systems makes it very hard to detect backdoors in the software by using ordinary testing techniques. To make this possible, practices not allowed by usage license would be necessary in many cases, such as reverse engineering for applications.

The risk exists and gives reasons to many players to distrust the solutions available in the market. The most representative cases are China and Russia, discussed below, although other countries are also developing initiatives, motivated not only by the existing risk but also for economic reasons and technology control.

Piracy is another key element concerning system security. In order to skip protection measures set on anti-piracy systems, one must use applications usually developed in environments over which there is no control. Even though pirates skip anti-piracy protection, the software installed in the computer to do so can include other functions such as the introduction of backdoors so that those who developed it can have free access to the pirated devices, and therefore to the information contained in them.

In 2009, the Business Software Alliance (BSA) calculated that the software piracy rate in Russia had gone up to 67%.[1] Also according to the BSA, China has had the highest piracy rate for several years. These numbers significantly represent the risk taken by both countries in their infrastructure.

Initiatives taken by the People's Republic of China

After the end of the Windows XP operating system support and the arrival of Windows 8, the Chinese Government vetoed the installation of the Windows operating system in all governmental systems.[2] Before that, China was part of the program through which the governments and other organisations get access to the source code of the operating system and the main tools of the company. This way, it is possible to analyse the code to diagnose the existence of design or programming

[1] Seventh Anual BSA/IDC Global Software Piracy Study. http://portal.bsa.org/globalpiracy2009/studies/09_Piracy_Study_Report_A4_final_111010.pdf

[2] «*China bans use of Microsoft's Windows 8 on government computers*» Reuters, disponible en http://www.reuters.com/article/us-microsoft-china-idUSBREA4J07Q20140520

defaults and check that there are no backdoors allowing third parties to gain access. Since the source code could not be accessed, the Government decided that using that operating system and its office applications entailed a risk for its information.

On the other side, and concerning hardware, a previous article[3] had already mentioned the digital devices manufactured by China to tackle the US imposed limitation to the exports of co-processors used in computer systems of high performance processing. In 2002, China launched an initiative of public and private cooperation named BLX to create microprocessors initially known as Godson and currently named Loongson[4], as well as for creating the necessary tools for the development and design of systems with such processors. The company does not have foundries of its own to produce the chips, so it outsources to STMicroelectronics[5], a microelectronics company created in 1987 from merger of SGS Microelettronica (Italy) and Thomson Semiconducteurs (France), currently headquartered in Switzerland. The device uses MIPS-64 architecture, which is significant when it comes to installing an operating system because it is not compatible with the x86 architectures used by the devices of the sector leaders Intel and AMD. However, since this architecture cannot be implemented due to license reasons, they have introduced a binary translator in the device that allows the execution of applications developed for these devices with performances only a 30% below the native applications.[6]

A product catalogue has been developed to cover the different needs concerning desktop computers, embedded systems such as routers, and other industrial equipment, which provides considerable technological self-sufficiency to the country.

To avoid the self-imposed veto in software and the hardware imports imposed by the US, the Government of the Popular Republic of China has developed an operating system based in Linux with a double goal: first, to have a great potential tool supported by a long history of success in this operating system that matches or surpasses the performances of other commercial options existing in the market; second, to count on an operating system that works in a native way in the devices that it has developed. An operating system based in Linux can be installed in very different architectures, including the MIPS-64 architecture of the Loongson devices. Therefore, the use of a Linux operating system in a Loongson device makes it possible to exploit to the maximum the device's capability.

[3] RAMÍREZ MORÁN David «¿Es la supercomputación una herramienta geopolítica?», September 2nd 2015, available at http://www.ieee.es/Galerias/fichero/docs_analisis/2015/DIEEEA43-2015_Supercomputacion_DRM.pdf

[4] http://www.loongson.cn/index_en.html

[5] www.st.com

[6] Weiwu Hu et al. «Godson-3: A Scalable Multicore RISC Processor with x86 Emulation» IEEE micro. Vol.29 N.2 2009, available at http://www.computer.org/csdl/mags/mi/2009/02/mmi2009020017-abs.html

Initiatives taken in Russia

The elimination of the Windows operating system in Russia is due to a policy undertaken by Vladimir Putin in 2010 by which he set the year 2016 as the deadline to eliminate all the equipment with a Windows operating system from the public administrations and replace it with open source software.[7]

The Russian Government states that the reason for developing its own computer equipment is to "replace foreign models which do not guarantee the lack of spyware or protection against information leaks"[8]. To achieve this, the Government created the United Instrument Manufacturing Corporation in 2014, a subsidiary from the government-owned Russian company Rostec, which gathers radio and electronic research and production installations.[9]

UIMC recently released the news that it will soon move on to producing the last version of its 8 core microprocessor Elbrus-8C. It is a SPARC architecture device that, as the device developed by China, includes binary translators that allow the execution of x86 architecture instructions, as well as the ARM architectures designed by the English company.

As in China, the development of an operating system based in Linux provides a double solution to the problem of counting on an efficient operating system and exploiting to the maximum the performance of its devices by using SPARC architecture, also found in the ones enabled by Linux.

Other initiatives

North Korea is among the countries that have been forced to launch initiatives to count on information technology that allows them to take profit of associated advantages. In this case, North Korea has chosen to develop its own operating system based in Linux and named Red Star. Information on the release of its third version has been leaked recently.[10]

India is also introducing a new free software solution based on Linux with an

[7] «Putin to put Russian government on Linux by 2015» *Computer World,* available at http://www.computerworld.com/article/2511966/government-it/putin-to-put-russian-government-on-linux-by-2015.html

[8] http://www.eng.opkrt.ru/index.php/news/205-uimc-started-developing-equipment-based-on-russian-processor-and-protected-from-cyberespionage

[9] http://www.eng.opkrt.ru/index.php/corporation/about-the-corporation

[10] http://www.theguardian.com/world/2015/dec/27/north-koreas-computer-operating-system-revealed-by-researchers

operating system called Bahrat Operating System Solutions (BOSS)[11], launched in 2007 and currently on its fifth version. This operating system is meant to replace the Windows operating system from the Government's computers.

Several European countries have also embarked upon the replacement of commercial products for free software tools with similar or equivalent functionalities. For instance, the French Ministry of the Interior has replaced Microsoft computer tools with free software tools[12], as well as the Government of Italy[13], as a consequence of a 2012 law, which says that the free software tools should be the default option for the country's public administrations, or Poland, with the email tools[14]. The Dutch Ministry of Defence is also among the ones using free software.[15]

Diplomacy and technology markets

The US Government recently made public the news of the upcoming implementation of the Windows 10 operating system with an optimised setting to secure all its terminals, from PCs to laptops and tablets. The reason leading to this decision is the enhanced security that this operating system provides compared to former versions, as well as cost reduction given the cut in the number of different systems they still keep.[16]

This type of communication is striking since, although the installation of free software tools in defence fields has been made public in the past, the US Government had never given information on the update of its systems to newer versions of the operating system, excepting the problem caused by the Windows XP.[17]

A piece of news announcing the Government's implementation of a technology solution developed by one of its companies and praising the virtues of technology is an answer to one of the practices that better contribute to exporting defence technology. If, on top of that, we take into account the difficulties that the company is

[11] http://trak.in/tags/business/2015/09/15/boss-os-made-in-india-operating-system-boss-replace-microsoft-windows/

[12] https://joinup.ec.europa.eu/community/osor/news/frances-defence-ministry-dutiful-studies-free-software

[13] https://joinup.ec.europa.eu/community/osor/news/italian-military-switch-libreoffice-and-odf

[14] https://joinup.ec.europa.eu/community/osor/news/frances-defence-ministry-dutiful-studies-free-software

[15] https://joinup.ec.europa.eu/community/osor/news/open-source-advancing-dutch-defence-ministry

[16] http://www.defense.gov/News-Article-View/Article/688721/dod-wide-windows-10-rapid-deployment-to-boost-cybersecurity

[17] GÓMEZ RUEDAS Jesús, «Adiós al soporte a Windows XP en el Ministerio de Defensa: lecciones aprendidas», available at http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO18-2015_WindowsXP_Fin_JesusGomezRuedas.pdf

undergoing to make the general public adopt this product, it is quite obvious that there is an institutional support campaign going on.

A few months ago there was a similar piece of news. The UK Government announced the migration of the computer systems of the Ministry of Defence to a solution based in the cloud and provided by Microsoft: Office 365.[18] In this case, the barrier that had to be brought down was the governments' reluctance towards the idea of information as sensitive as the one treated in the Ministry of Defence abandoning the systems of the organisation and being guarded by external servers controlled by a company. The fact that the adoption was made by the United Kingdom can be linked to the belonging of both countries to Five Eyes, an alliance comprising Australia, Canada, New Zealand, the United States, and the United Kingdom for joint cooperation in signals intelligence.

The decisions taken by China and Russia, as well as their publication in international media, are a quite resounding political message. They sow doubts on the reliability of the systems when it comes to protecting the governments' and also companies' most sensitive information. In fact, the Russian company that manufactures the processing devices states that the reason for developing computer equipment of its own is to "replace foreign models that do not guarantee lack of spyware or protection against information leaks.[19]"

Conclusions

ITC have become an essential capability for the functioning of companies, governments, and organisations. Given their increasing importance, decisions concerning its contracting cannot be limited anymore to the technicians who traditionally selected the best alternative according to their own criteria. It is now necessary to employ a global point of view which includes strategic and industrial policy motivations.

The solutions market currently meets the needs, although there is a certain lack of alternatives. This doesn't only give rise to situations of dependency on certain suppliers, but also to situations with an impact on competitiveness, which is inexistent in some cases.

[18] STONE, Mike «IT transformation in the Ministry of Defence», available at https://governmenttechnology.blog.gov.uk/2014/08/06/guest-post-it-transformation-in-the-ministry-of-defence/

[19]http://www.eng.opkrt.ru/index.php/news/205-uimc-started-developing-equipment-based-on-russian-processor-and-protected-from-cyberespionage

Today there is a widespread tendency to use free software as a solution to the lack of alternatives and the high costs of commercial technology licenses. We must make sure that the guarantees that these solutions provide are good enough accordingly to the nature of the information guarded. As for the better control that these technologies provide —since their code is available for analysis and review—, it is necessary to take into account that such control implies counting on the technical and human resources needed for the analysis and this responsibility cannot depend only on the good performance of a third party.

The solutions currently implemented are a result of long processes of development and optimisation cycles, which restricts significantly the emergence of new players in the market. However, the risk taken is increasing as this doorstep will keep growing indefinitely and will turn into a loss of decision-making ability for those who only participate as the suppliers' customers. Some countries are starting to take measures against it by sacrificing the performance and easy access to technologies to develop capabilities of their own with which they can develop knowledge and deal with a potential limited access to technology.

David Ramírez Morán
IEEE Analyst