10.53477/2668-2028-21-48

THE ISSUE OF INFORMATION TECHNOLOGIES WITHIN CRITICAL INFRASTRUCTURES

Alexandru-Cristian SAMOILĂ
Graduate student, "Carol I" National Defense University
alecsamoila@gmail.com

***Abstract**: Taking into account the need for computerisation and process automation within critical infrastructures, a whole process of choosing the most appropriate software technologies is born, both in terms of security, but also in terms of costs and development opportunities. This problem is encountered by all states, but also by private companies, has favoured the creation of an environment conducive to the development of computing technologies in three directions, namely: in-house software, open-source technologies and proprietary technologies. The current challenge is to find medium and long-term solutions for the rapid interconnection or redesign of these three types of information technology in order to process data from government systems, in order to perform complex analyses that can meet current needs, keeping in -an equable balance of costs and security level and identifying the most effective solution.*

***Keywords**: open source technologies; proprietary technologies; in-house software; technologies in critical infrastructures; informatisation risk.*

Introduction

If in the middle of the twentieth century the computer was intended only for simple arithmetic calculations, today we can hardly find areas in which a computing system cannot facilitate or even take over the work of dozens of people. Due to the natural need of man to simplify his existence, these computing systems have been implemented to the highest levels in society, so the calculating algorithms are increasingly complex, becoming almost impossible to understand even for those initiated, in this domain.

The amazing progress made in a very short time in the IT field, together with the continuous computerisation of all fields, has led to an irreversible dependence of critical infrastructures on IT systems, but also to the performance that seemed impossible to achieve in the past. Thus, the IT component may in itself be a critical infrastructure or it may have a supporting infrastructure role within any critical infrastructure.

The main advantages of informatisation in modern society are also the main threats to critical infrastructure, thus being a double-edged sword:

- **the data processing speed** – governed by the law of Gordon Moore, co-founder of Intel, who stated in 1965 that the number of components in integrated circuits doubled annually since the invention of the integrated circuit from 1958 to 1965. Thus explaining that computing power will double annually. Google officials said in 2020 that Moore's law would be doubled due to the invention of the quantum computer[1];
- **the transport speed of the information** – time intervals that in the past were measurable in weeks or months are now measured in seconds or milliseconds. In 2021, the first quantum network was brought to the public's attention, capable of transporting the information processed by quantum computing systems[2].

[1] https://www.ft.com/content/b9bb4e54-dbc1-11e9-8f9b-77216ebe1f17, accessed at 02.02.2021.
[2] https://www.descopera.ro/stiinta/19608128-china-a-creat-prima-retea-cuantica-integrata-din-lume-care-se-intinde-pe-mii-de-kilometri, accessed at 02.02.2021.

Risk of computing

The immediate risk of informatisation is clear: cyber-aggression tools increase their efficiency while we guide our decisions, budgets and security according to a graphical interface, which we have to give full confidence to. Computerisation has other risks that are much more dangerous for society and why not for all of humanity. Attacks on critical infrastructure through IT systems can lead to real security crises, both nationally or in Europe or globally.

The reality requires the approach of IT risk in terms of three factors:

- threats – events or activities that can affect critical infrastructures, generally originated outside the system but they can start from within the organisation, too and these are the most dangerous;
- vulnerabilities – weaknesses of an IT system (hardware or software) that serves a critical infrastructure;
- impact – is considered to be a short, medium or long term loss or consequence, in which the owner or user of the computer system is directly affected.

The risk at the level of an organization cannot be eliminated, it will always exist. The management of the entity is responsible for reducing it to an acceptable level, thus opening the horizon to the resilience of the IT system that serves the critical infrastructure.

Risk management in software technologies is based on three elements - compliance with public standards, transparency in decision processes (an external audit may be involved) and splitting across developers (the last hardware and software solution produced entirely by a single company was IBM AS400 – Application System/400).

Critical infrastructure such as the electricity grid, oil and gas pipelines, and water distribution systems are fundamental to modern society. Thus, the protection of critical infrastructure is a matter of national security. However, recent incidents involving the Stuxnet malware have shown that critical infrastructure elements are susceptible to cyber-attacks. First and the most alarming cyber-attack reported against a power grid took place in December 2015. Malware infected the electricity utilities of at least three regions, leaving about half of the homes in the Ivano-Frankivsk region of Ukraine without electricity[3].

Technologies based on in-house software vs open-source software vs proprietary software

The phrase "*computer data processing technology*" can be defined as the set of methods, processes and operations applied to computer data in order to obtain a result in a form of a computer solution. This problem being encountered by all states, and also by private companies, has favoured the creation of an environment conducive to the development of computing technologies in three directions:

I. **In-House software** – creating your own technologies involves creating a software product for data processing within your own critical infrastructure, at national or European level, that can be used for other several critical infrastructures. In this case, a dedicated and specialised team in the field of IT&C is needed, where the implementation or development times may be longer, but it requires a detailed knowledge of each security element and a predictability of costs;

II. **Open-source software** – is the practice of implementing or developing certain finished software products, allowing access to interested persons to act freely on the production or development process. This mode of development offers the advantage that more specialists can improve the technology provided with the help of the community, with minimal costs, but also the disadvantage that a malicious person can have access to the source code and can more easily discover a security breach or have the ability to propose a code sequence that will serve

[3] Dragoș Cătălin Barbu, *Improving the protection of critical infrastructures in the IT&C sector by increasing resilience*, accessed at 06.02.2021, https://rria.ici.ro/wp-content/uploads/2016/12/06-art.4-D_Barbu-OK-4.pdf

as a Trojan horse in a future cyber-attack. The staff training process is not perfectly standardised, but the information can be found, most of the time, through a search on the Internet, and which involves a low cost and less time to be implemented. The ability to access the source code by any interested person can raise a security dispute. Although it was initially considered that open-source technologies would suffer a slow disappearance, relying largely on the intrinsic motivation of developers, eventually the practice has shown the opposite, the best example being the open-source digital multimedia encyclopedia project[4];

III. **Proprietary software** – is a solution guaranteed by the developer that can be implemented in a short time than the previous technologies, but having the disadvantage of high cost and the ideology of keeping the customer captive in a maze consisting of contractual clauses and technological limitations. Thus, these technologies represent the practice of private entities to develop software products without disclosing the source code. This ensures a controlled and theoretical development flow, as well as an increase in the level of security by obscuring the source code. For the user, the security level and the specialised support are closely related to the payment of a subscription that allows updates and access to the developer's private resources. Otherwise, serious questions are raised about the level of security. Below, in table no.1 are exposed the strengths and risks for each category.

Table no. 1. Strengths and risks specific to the categories of computing technologies

Technologies	Strengths	Risks
In-house software	- Choosing the desired programming language; - Imposing one's own security standards; - Costs predictability on costs, as well as their decrease in the situation when the number of critical infrastructures that are served by the same software solution increases; - Direct relationship with the team of specialists influencing the creative process; - Elimination of collateral components which involves the elimination of possible security breaches; - The evolutionary maintenance process is under total control.	- It requires a team of specialists for a long time; - Security breaches for outdated system components; - An unidentified security breach in time will be able to be exploited in all critical infrastructures served; - The development and implementation time will be dependent on the needs exposed in the creation process; - The test area is much smaller (summarised at the organisation level); - Poor management - lack of vision and an applied work plan.
Open-source software	- Unrestricted access to technical documentation; - Independence from a certain hardware platform; - Implementation of public standards; - Easy interconnection with other computer systems; - Testing and improving source code, transparently, by different teams globally; - Reduced costs for specialised help; - Identifying and hiring qualified development staff is much easier;	- The need to always have a specialised team; - Sometimes the graphical interface can be underdeveloped, requiring command line knowledge and experience to decode less detailed errors; - The source code being written in a common and public language can be analysed by a potential attacker.

[4] ENCARTA – the premium digital multimedia encyclopedia project, started by Microsoft in 1993 with a considerable investment, was closed in 2009, and the open source multimedia encyclopedia project – WIKIPEDIA – started by the non-profit organization Wikimedia has demonstrated its supremacy and continues to be improved through the unpaid contribution of stakeholders. https://ro.wikipedia.org/wiki/Wikipedia, accessed at 06.02.2021.

Technologies	Strengths	Risks
	- It benefits from a diversified testing market, globally; - The training and implementation process is carried out in an optimised time.	
Proprietary software	- Immediate implementation of a mature technology; - Existence of a specialised technical support team; - Accurate knowledge of the optimal operation capabilities of the system.	- High costs for the acquisition of rights to use; - Dependence on other software solutions owned by the same vendor; - Dependence on a certain hardware platform; - Uncertainty about the future cost of maintenance or development, especially for products that benefit from an annual licensing system; - Uncertainty about the development of technology (the manufacturer may abandon the development of a product considering it unprofitable); - The choice of programming language is exclusively the prerogative of the manufacturer; - Interconnection with other manufacturers' systems often proves to be a cumbersome process and allowed only for approved products.

In the business environment, one of the questions underlying the establishment of a profitable entity is “How do you secure your business?” Similarly, for critical infrastructures, one of the questions is “How to protect the functionality of critical infrastructure and the services provided?” Thus, how to patent or develop proprietary technologies is an applied answer to these questions. The interested entities have built an interdependent virtual environment, which can open communication channels only to the agreed technologies.

Over time, “how to secure business or vital services by including the customer in a closed virtual environment” has become increasingly refined. Each entity is willing to give free rein to the imagination to find solutions to this problem, as the legislative framework is developing much slower than technological progress.

In the earlier versions of securing a business, the use of a computer program was conditioned by its compilation using hardware products developed by the same entity. Subsequently, a licence to use a computer program was granted on the basis of a contractually defined hardware processing power. Then the focus was on growing the business by conditioning interconnections and using proprietary vendor standards. For example, a web portal technology that ensures the display of data in a browser can be interconnected only with LDAP technology that is owned by the same entity, application development can be done only through modules which are interconnected with the portal, possibly based on software developed by the same vendor and available under an annual subscription.

Another question mark falls on the integrity of the developer, it must be at the highest level, otherwise it could provide security breaches for various partners (in the case of the spread of the Stuxnet virus in the top secret network serving the nuclear infrastructure, Iran accused Western corporations for their collaboration with the secret services), while for an open-source technology each line of code is brought to the attention of developers around the world, and it is almost unlikely that a security breach can be left intentionally without being noticed. But the

biggest sign of uncertainty looming over a proprietary technology, at the time of its integration into a national system is the date of withdrawal from production and the galloping increase in the purchase price. Practically, the customer cannot intervene in a company's decision to close the development of a certain product or to migrate it to an inaccessible cost ceiling.

Due to these reasons, open-source technologies are constantly expanding, and entities established as profitable businesses are interested in acquiring small groups of competing programmers, focused on developing open source technologies (Oracle has acquired competitor MySQL[5] and many other database developers les known; the company F5 Networks acquired the competitor NginX[6]).

In order to ensure the existence of entities whose sole purpose is the development of open source technologies, they have offered to sell technical support packages or improved products. Another method found by these entities was the association with an important client, for example the utility suite for spreadsheets and text editing –LibreOffice – obtained the support of the German administration for the development of open source technology after in April 2010 Oracle Corp. bought Sun Microsystems Inc., thus becoming the owner of OpenOffice.org, on September 28, 2010 several members of the OpenOffice community founded The Document Foundation and created a branch of the beta version of the OpenOffice.org suite 3.3[7].

Although the choice of open source technologies seems to be sufficiently tender, the tipping point is given by the human resources specialised in the field of information and communication technology. The budgetary environment cannot compete to attract young specialists, due to a lack of a coherent policy and implicitly due to wage differences from the private environment, thus having to take into account the availability of adaptation to new technologies of existing employees. In the absence of a strong sense of self-motivation, the employee will advocate for a technology that benefits from an easy interface and recognised as having no problems. In parallel, the situation is similar for employees with tasks in editing text and performing spreadsheets, although they are encouraged to use open source technologies such as LibreOffice or OpenOffice, the power of habit or fear of the unknown helps them find the most complex motivations, forcing for the employer to purchase proprietary technology such as Microsoft Office.

Conclusion

In the situation of Romania, the public administration being a sub-sector with critical infrastructures, not having a unitary response to the influx of information generated by the continuous development of data processing technologies, and so each public entity, respecting the public procurement law or regulations hiring specialised staff in the field of information and communication technology, has developed an IT solution based on its own evaluation system.

At the inter-institutional level, the lack of communication and cooperation between state institutions has led to a dissolution regarding the implementation of common used technologies and, implicitly, the realisation of interconnection. This fact corroborated with the need of private entities to secure their business, but also with a rigid legal framework on pay that does not allow the remuneration of information and communication technology specialists at the level set by the free labor market, which has led to a slow progress in the process of interoperability of national information systems and thus to the impossibility of provide a complete overview in a short time.

The use of open-source technology, common to all public administration organisations, would lead to a massive reduction in costs and an increase in security as more experts would

[5] https://www.oracle.com/ro/mysql, accessed at 02.02.2021.
[6] https://www.nginx.com/blog/nginx-is-now-officially-part-of-f5, accessed at 02.02.2021.
[7] https://ro.wikipedia.org/wiki/LibreOffice, accessed at 02.02.2021.

contribute to the security effort by acting in one direction. In the case of using a common technology one of the most pressing problems would be the chain propagation effect of a security breach, so that all participants will be or could be affected by the same insufficient security of the technology used.

The process of migrating proprietary technologies to open-source technologies needs to be strongly supported through training programs and especially through a national support center. If critical infrastructures were to opt primarily for in-house software and open-source technologies, the question is how high is the level of risk in the scenario where these infrastructures would fall victim to cyber-attacks concerted by large companies, in order to prove their supremacy and regain their market share?

BIBLIOGRAPHY

1. https://www.ft.com/content/b9bb4e54-dbc1-11e9-8f9b-77216ebe1f17, accessed at 02.02.2021.
2. https://www.descopera.ro/stiinta/19608128-china-a-creat-prima-retea-cuantica-integrata-din-lume-care-se-intinde-pe-mii-de-kilometri, accessed at 02.02.2021.
3. BARBU Dragoș Cătălin, *Improving the protection of critical infrastructures in the IT&C sector by increasing resilience*, accessed at 06.02.2021, https://rria.ici.ro/wp-content/uploads/2016/12/06-art.4-D_Barbu-OK-4.pdf
4. https://ro.wikipedia.org/wiki/Wikipedia, accessed at 02.02.2021.
5. https://www.oracle.com/ro/mysql, accessed at 02.02.2021.
6. https://www.nginx.com/blog/nginx-is-now-officially-part-of-f5, accessed at 02.02.2021.
7. https://ro.wikipedia.org/wiki/LibreOffice, accessed at 02.02.2021.