AUTHOR'S GUIDE TO DOCTORAL (PhD) DISSERTATION (THESIS)

NATIONAL
UNIVERSITY OF PUBLIC SERVICE
Doctoral Council

TAMÁS JÉRI

Security issues of the Critical Internet Services in the defense sector

author 's description of his doctoral (PhD) dissertation and
official reviews

Budapest
2020.

UNIVERSITY OF PUBLIC SERVICE

DOCTORAL SCHOOL OF MILITARY ENGINEERING

TAMÁS JÉRI

Security issues of the Critical Internet Services in the defense sector

author 's description of his doctoral (PhD) dissertation and official reviews

Scientific supervisor:

Brigadier General Prof. Dr. László Kovács (DSc)
professor

Budapest
2020.

TABLE OF CONTENTS

Budapest, 8th of December, 2020

signature

SCIENTIFIC PROBLEM STATEMENT

Developments in information technology have forced the use of fast and efficient tools and applications in the defense sector. They are an essential part of the day to day work and mostly the primary option to store data. The available internet services, similarly to the internet services used in society, have become ingrained in the life of the organizations and bodies. Without them, the performance of the basic activities would be endangered, so we can rightly call them vital services. The problem, however, is that neither the surveillance nor the protection of these systems and services is fully resolved.

1. Legal requirements

Laws of electronic information security and general rules of electronic administration and trust services combined with the expectations of society raise requirements towards administrative bodies, including the defense sector, which are

- the rules on electronic information security are complied with in all circumstances;
- cases should be handled electronically, if possible;
- the information must be up-to-date, accessible in user-friendly form, and constantly available.

Fulfilling such requirements is vastly different in cyberspace compared to the physical world. In cyberspace, this raises different kinds of challenges and pressure, while at the same time, it could mean an opportunity to take advantage of the latest advancements of technology. Although the implementation highlights quite a few further problems to solve as the safety of information needs to be assured as follows

- the data stored in the organisation's IT system are authentically available only to the extent necessary and with constant availability;
- the administrative process initiated by the citizens at any time should also be stored in the IT system of the organization and the inbound information should reach the relevant stakeholders.

The main problem with the internet services resulting from the commitment received or undertaken is that they should, as far as possible, operate safely in all circumstances, with constant availability, for which several recommendations must be followed.

2. Exploiting the opportunities of the internet

The upside of the internet is definitely the availability and ease of using applications developed by third-party vendors, rather than developing them ourselves. In this day and age, it is relatively simple to find and use an internet service or application for any reason (leisure, self-development, entertainment, productivity, etc), and obviously, their use in the defense sector is no exception.

One of the potential problems is the uncontrolled use of these services which can lead to issues caused by malware, unauthorized access, outage, or performance degradation due to overuse of untrusted services. All of these scenarios could have a significant negative impact on an organization.

In summary, the following scientific problems were identified:

- the issue of vital internet services, despite its importance, has not been scientifically addressed so far, either generally or specifically in the field of defense;
- currently, there are no guidelines or recommendations on what should be done for the security and high availability of online IT services;
    - the introduction of internet services in the field of defense focuses primarily on the expected results, however, in the event of a possible shutdown or outage, no impact study is prepared, prevention is a secondary aspect;
    - the internet services used are of equal value, with no emphasis being placed on those critical services that deserve more than average, continuous attention;
    - the operational responsibilities for the alleged Critical Internet Services are not defined, the centers of gravity and focal points of the services are not known;
    - in the event of a failure of running internet services, the response is self-sustaining, ad-hoc in nature (each at its own discretion).
- the use of internet IT services is not regulated, there is no general recommendation or guidance for it, despite the fact that it means continuous risk-taking.

RESEARCH OBJECTIVES

1. I wish to highlight the existence of the so-called critical internet service.
2. I aim to define what a Critical Internet Service (in the following: CRIS) is, describe its structure, study the aspects of its function, and have an overview of its application generally and in law enforcement.
3. I wish to prove that amongst infrastructures and information infrastructures, internet services can also be critical, as a working infrastructure does not guarantee a functioning service.
4. I wish to investigate the connection between critical infrastructures and critical information infrastructures. Also, to discuss practical methods and recommendations while sustaining a safe and continuously available system.
5. I make recommendations about the safe use and maintenance of internet services considered critical.

I split the research activity into the following tasks below:

- Explore the existence of Critical Internet Services, examine the correlations with information infrastructures
  - define CRIS;
  - explore CRIS generally and specifically in the field of defense.

- Study the components of CRIS, present threats and proper use of service providing
  - components of CRIS, sub-systems;
  - most frequent occurrences of CRIS, its systems, and safe maintenance;
  - recommendations for a safe CRIS.

RESEARCH METHODS

To complete my dissertation, I have used the following research methods:

- study the relevant international and Hungarian literature, legislations and other documents;
- comparative analysis based on survey results;
- generalization as a research method;
- logical analysis: analysis and evaluation of results, identification of connection points, recommendations;
- empirical research: documentation of professional self-experiences;
- attendance of conferences, consultations, and events;
- publication of research results: live presentation at conferences and training sessions, publication as articles and university case studies.

BRIEF DESCRIPTION OF CONDUCTED RESEARCH BY CHAPTER

1. Critical Internet Services is a range of vital services that appear in one of the ever-expanding segments of critical information infrastructures. CRIS can be deduced from the definitions of critical infrastructures (CI), information infrastructures (II), and critical information infrastructures (CII) in the scientific approach, proving that when some internet services are shut down, “life almost stops”. Overall, the survey confirmed the assumption that Critical Internet Services exist and operate in the defense sector, and it can be concluded that no organization would be able to fully perform its tasks or meet its obligations without the availability of vital internet services.
2. With the system-level examination of CRIS the sub-systems and system components, which are equally important when it comes to direct or indirect support of services, were identified. Database management systems are essential "props" of today's information society and with it, as a result and consequence, of Critical Internet Services. Malicious access to the operating system, file system, database manager and database through CRIS can lead to service outages.
3. Due to the dynamic development of IT over the past two decades, the Web, which is also the most commonly used CRIS, has become the dominant information platform on the internet. The hacked or modified websites are a good indication of what it means to exploit errors or lack of attention. The steady increase in the number of internet users is clearly having an impact on e-mail users as well, which prioritizes e-mail addresses as potential targets of attack. Cybercriminals are constantly using e-mail as a tool, which is still the number one yet “legal” tool on the internet utilized for cyber attacks. . I demonstrate how safety can be sustained while the unavoidable maintenance processes are still followed.
4. The recommendations outlined around safety of connections, services, use of services, or general safety procedures are presented in a complex and structured fashion, aimed to help the work of users or providers of Critical Internet Services regardless of their professional background.

SUMMARIZED CONCLUSIONS

In my dissertation, I stated that the operation of internet services is infrastructure-specific. Therefore, the use of scientific explanations of CI, II, and CII are the most appropriate to approach services classified as critical. It is highly subjective what is considered as a vital internet service, hence I formulated the definition of CRIS based on the service activity, the consequences of the service outage, and assuming the availability of infrastructural constraints.

I noted that each CI, CII, or CRIS compose an independent set, although they can be connected. In the case of a connected scenario, the shutdown of KRISZ also affects a significant part of society, or government officials cannot fully perform their duties. In addition to the infrastructural background, I have detailed the necessary elements that provide the „building blocks" of an internet service. I reviewed how one's attachment to internet services develops, what the consequences are, and how they become critical to users.

The theoretical approach was supported by a survey completed by workers of the defense sector, which focused both on the use and provision of internet services. With the survey, I proved that without the availability of certain internet services, law enforcement agencies are not able to fully perform their tasks. It has been proven that internet services define everyday life, their unavailability has a serious impact on operations, so Critical Internet Services do exist according to the hypothesis.

When analyzing given internet services, it was assured that all law enforcement agencies

- operate a website, news feed and electronic administration;
- provides email, webmail access to its employees;
- provides access to its IT system for certain users through an encrypted internet channel.

During the system-level examination of internet services, I found that they can be divided into subsystems and system elements that influence the operation of internet services in accordance with their role in the system. There are unavoidable subsystems, such as databases which are key cornerstones of today's internet services. My research results show that the data stored on those databases impact the quality of the services, and databases are usually targets of malicious activity, hence their uninterrupted operation must be secured on priority. Due to the permanent connection between the database and the internet service, there is also a permanent entry point available for

malicious attacks, which is the user interface of the internet service itself. This means the internet service's user interface must be secured also on priority.

In parallel with the habits of a society that consumes internet services, the manifestations of Critical Internet Services show a similar pattern. The Web is currently the most popular form of information on the internet, with each law enforcement agency maintaining its own website, and publishing both mandatory and optional content. Due to its development, it can have numerous subsystem elements, the possibility of interactivity is provided in it, numerous development and framework systems are available, which of course also allow for errors. I have reviewed what to consider in order to run a stable, fault-tolerant web server, and what security measures need to be taken to prevent Web attacks.

The popularity of electronic mail is on par with the popularity of the Web, and is available for decades now, yet it has a completely different function for Critical Internet Services: it can be a target of an attack and also a tool of an attack. Electronic mail is available throughout the defense sector, each law enforcement agency has its own webmail system available on the internet, and almost every employee can have their own work email address. I pointed out that every person who uses the internet in the world has an average of two e-mail addresses, and the e-mail address is used to embody and identify the person, and e-mail is the main authentication tool for identifying people. I also pointed out the fact that electronic mail on the internet is still the main attack tool, and I have shown what it means to use and exploit a mail system. In the case of e-mail, there is a kind of windmill battle against the mass of malicious codes and spam. In such an environment, without the application of appropriate security measures, this internet service serves as a means for others to carry out a cyber attack.

During the operation of an internet service, there are recurring operational tasks that are unavoidable. I have summarized the solutions and security measures to be followed that can help maintain the availability of internet services in the long run.

The protection recommendations I propose in the dissertation can help their users and operators in a systematic way, in line with the structure of CRIS. Of course, security perceptions and opinions are different. These recommendations got formulated from the perspective of a user with many years of IT administrator experience, who is also involved in various decision-making situations.

NEW SCIENTIFIC RESEARCH RESULTS

I summarize my research results as follows:

1. I formulated the existence of Critical Internet Services, created its definition and content elements.

The criticality of internet services is much more subjective than the tools and services that provide the background, so to prove their existence I had to examine the existing dependencies and the consequences of a possible termination. I revealed that the criticality of internet services depends on the infrastructures behind the services, as well as on the effects and consequences of the shutdown and outage of the given internet service. Considering that the direct consequence of the shutdown of background services is the cessation of internet services, it is evident that the derivation of the Critical Internet Service can be derived from it as a result of the dependency. For the definition, I had to start from the formulations of critical infrastructures and critical information infrastructures, taking into account that the Critical Internet Service is always a subset of the infrastructures above it.

2. I deduced the possible development of the Critical Internet Services.

I pointed out that either due to obligation or own decision, a connection or addiction could develop in users towards certain internet services so they become critical internet services as they become vital to the user. The development of the connection is in the interest of the service providers with the aim that the users turn to the given internet service and return to it regularly. I highlighted how the attachment to internet services that appears in the day-to-day operation of the defense sector can make them vital and critical in a short time, as well as what the addiction transformed from attachment means, and what the consequences may be.

3. I have proven that Critical Internet Services exist both in the defense sector and in everyday life.

Treated as a fact that the defense sector represents a segment of society in terms of the use of the internet, it can be stated that if Critical Internet Services exist in the defense sector, they are present in society and even to a much greater extent. The best way to make the lack of an internet service measurable and scientifically identifiable is by surveying its users objectively. The survey conducted in the defense sector covered both the consumer and service provider sides of the internet, and also examined the consequences of a possible termination or shutdown.

The obligations of online presence defined in current legislations, the (information) infrastructures, the researches focused on the criticality of backend services, and the research done

in the defense sector together prove that internet services can be critical. Consequently this means Critical Internet Services do exist. The summary of the named internet services included in the survey, and also my research on this topic revealed a number of Critical Internet Services in both general and law enforcement applications.

4. By examining the security of Critical Internet Services, I have pointed out their potential vulnerabilities, and I have demonstrated the need for defense and best practices in defense.
The mapping and examination of CRIS's subsystems and system components proved that the internet service is as resilient as the weakest element of its constituent units, and it has become clear that the database as a subsystem element is essential in today's Critical Internet Services. By examining the databases, I have shown that the lack of security of the stored data alone is sufficient for the failure of CRIS. Through the most common internet services, which are also the most common Critical Internet Services, I introduced the Critical Internet Service systems, focused on their safe operation and security issues. By detailing the operation of electronic mail, I pointed out its dual role, as it is a constant target of attack on the one hand, and also functions as an attack tool on the other.

5. I have formulated a protection recommendation for the safe and effective operation and maintenance of Critical Internet Services.
The recommendation can be a comprehensive IT and management tool to maintain Critical Internet Services and ensure their long-term use.

APPLICABILITY OF RESEARCH RESULTS

The structure of the dissertation was structured according to theoretical and practical topics, and one of the research objectives was specifically focused on practical applicability: „I would like to present methods and recommendations which will help to achieve continuous availability while maintaining information security, all in the context of internet services considered critical." The third chapter focuses on the practical implementations, while the fourth chapter also contains practical recommendations, so the application of research results also ensures practical validity.

RECOMMENDATIONS

1. It can be used in the educational activities of the National University of Public Service, especially in the bachelor and master's program of the Faculty of Military Science and Officer Training, and in the subjects taught by the National Security Institute, either as a separate educational material, source work or recommended literature.
2. The conclusions of the certain chapters can serve as a basis for further scientific research, partly as described, such as a broader examination and survey of Critical Internet Services.
3. I recommend the findings in my dissertation to managers and IT professionals working in the defense sector, when creating IT regulations, preparing contracts with IT-related suppliers, or operating internet services.
4. I definitely recommend the sections discussing the security issues of internet services to the owners of companies that use the internet directly or indirectly to generate income, as well as to individuals who operate an internet endpoint in any form on a permanent basis.
5. I recommend the chapter on electronic mail to all internet users with e-mail addresses in order to maintain their own and others' internet security.

LIST OF PUBLICATIONS BY THE DOCTORAL CANDIDATE

Articles published in a peer-reviewed journal:

1. Jéri Tamás: The Security Of Databases In Critical Internet Services, Hadmérnök X. Évfolyam 3. szám - 2015. szeptember ISSN 1788-1919;
Online: http://hadmernok.hu/153_18_jerit.pdf;
2. Jéri Tamás – Pándi Erik – Jobbágy Szabolcs: A hálózatok világa, Hírvillám, I. évf. 1. szám, Budapest, ISSN 2061-9499, 168-177. oldal, 2010.; Online: http://www.comconf.hu/kiadvany/hirvillam_1evfolyam_1szam.pdf;
3. Jéri Tamás – Pándi Erik – Jobbágy Szabolcs: A hálózatok védelmi aspektusai, Hírvillám, I. évf. 1. szám, Budapest, ISSN 2061-9499, 210-220. oldal, 2010; Online: http://www.comconf.hu/kiadvany/hirvillam_1evfolyam_1szam.pdf;
4. Jéri Tamás – Pándi Erik – Tóth András: A kommunikációs infrastruktúrákkal szembeni rosszakaratú tevékenységek:
Hírvillám, I. évf. 1. szám, Budapest, ISSN 2061-9499, 276-288. oldal, 2010.; Online: http://www.comconf.hu/kiadvany/hirvillam_1evfolyam_1szam.pdf;
5. Jéri Tamás: A kommunikációs eszközök fejlődésének kihatásai a büntetés-végrehajtás rendszerére, Hadmérnök VII. Évfolyam 2. szám - 2012. június ISSN 1788-1919; Online: http://www.hadmernok.hu/2012_2_jeri.pdf;
6. Jéri Tamás: Kritikus internetes szolgáltatások, Hadmérnök VIII. Évfolyam 1. szám - 2013. március ISSN 1788-1919; Online: http://www.hadmernok.hu/2013_1_jerit.pdf;
7. Jéri Tamás: A kritikus internetes szolgáltatások biztonságos üzemeltetése, Hadmérnök X. Évfolyam 1. szám - 2015. március ISSN 1788-1919; Online: http://www.hadmernok.hu/151_20_jerit_2.pdf
8. Jéri Tamás: Az adatbázis-kezelők szerepe a kritikus internetes szolgáltatásokban, Hadmérnök X. Évfolyam 1. szám - 2015. március ISSN 1788-1919; Online: http://www.hadmernok.hu/151_19_jerit_1.pdf
9. Jéri Tamás: A Web szerepe a kritikus internetes szolgáltatásokban, Hadmérnök X. Évfolyam 3. szám - 2015. szeptember ISSN 1788-1919; Online: http://www.hadmernok.hu/153_17_jerit.pdf

Article published in a conference publication:

10. Jéri Tamás: A Kritikus Internetes Szolgáltatások alrendszerei, A Haza Szolgálatában konferenciakötet; Társadalom és Honvédelem XVII. évf. 3-4. szám ISSN 1417-7293 2013. 205-214. oldal;

DOCTORAL CANDIDATE'S CAREER AND SCIENTIFIC HISTORY

Personal details

Name:	Tamás Jéri
Date of birth:	8th of July, 1974
Place of birth:	Kalocsa, Hungary

Career history

2020 – Present	Wealth Utilization and Bookkeeping Nonprofit Ltd., Kalocsa, Hungary, Executive
2018 – 2019	Tolna County Penitentiary, Hungary; Commander
2011 – 2017	Prison, Kalocsa, Hungary; Deputy commander
2000 – 2011	Prison, Kalocsa, Hungary; Head of IT department
1998 – 2000	National Command for Penitentiary Enforcement, Hungary; Senior staff
1994 – 1998	Prison, Kalocsa, Hungary; supervisor, guard, instructor, senior instructor

Education

2015	PhD. Doctoral degree; National University of Public Service, Doctoral School of Military Engineering
2010	MSc, Defense Management Systems Management; Miklós Zrínyi University of National Defense
2004	BSc, IT Engineer; Dennis Gabor College
1992	Graduation, Vocational High School of Economics

Language

English, intermediate level

Russian, basic level