AARMS Volume 17, Issue 1 (2018)

Contents

ISSN 2498-5392

AARMS Volume 17, Issue 1 (2018) 1–140

AARMS

Academic and Applied Research in Military and Public Management Science

Volume 17
Issue 1
2018

SCIENTIFIC JOURNAL OF THE NATIONAL UNIVERSITY OF PUBLIC SERVICE, HUNGARY

AARMS Vol. 17, No. 1 (2018) 5–12. **10.32565/aarms.2018.1.1**

Juvenile Boot Camps in the Shadow of Tragedies

Magdolna CSUKAI,[1] **Péter RUZSONYI**[2]

Many pros and cons arguments can be read about boot camps in terms of efficiency and application. My article reviews tragedies and deaths occurred in juvenile boot camps processing their background and causes. It is not my purpose to present boot camps in a negative light but to reveal circumstances of tragedies and on the basis of this to prevent their re-occurrence.
Keywords: *boot camps, military drill, tragedies*

Boot Camps

Coming to Being

The idea of boot camps appeared as an alternative to the conventional prison and probation time as it was often experienced—for perpetrators committing a non-violent criminal offence for the first time—that people considered penalty in prison to be too harsh while probation time too lenient. Therefore, in view of such cases, it was deemed necessary to impose new intermediary sanctions such as house custody, electronic surveillance, intensive probation service or boot camp. The latter was one of the most popular forms getting major resonance [1] whose essence is a short "shock prisoning" with a military atmosphere. The roots of its popularity lie in the linked expectations according to which it can reduce recidivation, operational costs and prison population.

Already in 1938, the plan for such boot camp-type of penalty form had been forged for youngsters in England but it was no sooner implemented than in 1948. The then established boot camps were running until the 1970s but did not meet the expectations. [2] The first American new-generation boot camp started operation in Georgia, in 1983, in an adult prison with 50 beds. This soon spread state-wide and such facilities were made not only for adults but youngsters [3] as well, at the time. The first programme developed for youngsters in particular was launched in 1985 in Parish, Orleans, Louisiana. According to statistics, over 75 juvenile boot camp programmes were launched in 33 states [1] in 1997; nowadays this form of penalty can be found all over the world except for Europe. Due to its diversity and variety, several names have been granted for boot camps.[3][2]

[1] Ph.D. student, National University of Public Service, Doctoral School of Military Sciences; e-mail: csukaim@gmail.com

[2] Ph.D., Correctional Brigadier-General, University Professor, Pro-Dean, Head of Department of Corrections, Faculty of Law Enforcement, National University of Public Service; e-mail: ruzsonyi.peter@uni-nke.hu

[3] For instance, such names are Special Alternative Incarceration, Basic Training Program, Intensive Motivational Program of Alternative Correctional Treatment, Regimented Inmate Discipline, Challenge Incarceration, Shock Incarceration and Detention Centre Programme.

General Characteristics

Boot camps established for youngsters may differ in the procedure that applies to the youngsters selected for inclusion in the programme. [4] In general, this does not happen on a voluntary basis but it is the court, prison facility probation service that submits the juvenile perpetrator to a boot camp. However, there are some exceptional cases when a boot camp can host voluntary participants as well; but should in our case if the training be unsuccessful, the person must go to a conventional prison to complete the penalty period. [5]

Youngsters are usually sent to boot camps for a short period of 1 to 6 months, on average 3 months. Thus, the time spent in the camp is brief but all the more intensive as those who have been included must be involved in activities actively for 16 hours daily. [8] This is one of the reasons why the inclusion in such camps is linked to several prerequisites as not everyone is apt to complete such an intensive programme. Although prerequisites vary from programme to programme and from state to state, those who committed no violent criminal offence for the first time may participate in the boot camp programme. By age, generally a wider age range of 10 to 25 years can be considered, [1] but each programme may contain a tighter age range as large difference in the participants' age provides an opportunity for the elders to commit physical abuse to the detriment of the youngers within the camp, [7] consequently this is not recommended. Furthermore, there are camps where age conditions are stricter and participation under 16 is not even allowed because the military drill employed there is overly burdensome for the younger ones. [2] These basic conditions related to the type of criminal offence and age may be complemented with the parent's declaration of consent as well as the necessity of health, physical and psychic fitness.

Based on the critics raised and experience gathered over the years, a continuous development of camps can be detected, during which a transition from the one-to-one copy of military penal camp that broke up both the body and the mind to educational, training programmes was attained. [2] Therefore, nowadays youngsters can participate at various activities after inclusion in a specific boot camp. Currently, most of the juvenile boot camps have three main components: military training in stringent discipline, rehabilitation activities as well as educational and vocational training programmes. [8] These three parts can be interpreted both as a function and a development direction in comparison to the original standard military camps. [6] However, from the point of view of to what degree these areas appear during the programme, large differences can be noticed. Certain camps still place emphasis on discipline and strict physical education, whereas others concentrate on occupational therapy, education and development of capacity for thinking despite the military atmosphere. [3]

Military Drill

Pros and Cons Arguments

Military drill is the core characteristic of boot camps, however, there are divergent opinions as to its strong application in juvenile camps. Perhaps this component has been and still is

exposed to most critics. Also, the interest shown by the media concentrates almost completely on the strict military nature as it has plenty more sensational value than rehabilitation and educational programmes. [6]

In most of the camps, prison officers and detainees wear a military-style uniform and use military terms. The method employed conscientiously by those called drill sergeants is verbal confrontation, which is mainly used to crush the self-esteem of the newly arrived when inclusion takes place [2]: *"You are nothing and nobody, fools, maggots, dummies, mother…s, and you have just walked into the worst nightmare you ever dreamed. I don't like you. I have no use for you, and I don't give a f… who you are on the street. This is my acre, hell's half acre, and it matters not one damn to me whether you make it here or get tossed out into the general prison population, where, I promise you, you won't last three minutes before you're somebody's wife. Do you know what that means, tough guys?"* [9: 30]—this is how an opening speech goes in a boot camp. [9] Besides, the military model comprises tough training, military drills, prompt physical punishment applied when behaving inappropriately, a celebration to be held during inclusion and departure and stringent daily schedule, too. [4]

Those in favour of strict military drills claim that soldiers' personality transforms after being drafted, therefore it is the drilling and discipline that are expected to alter the behaviour of youngsters. It is thought that this way a law-breaking youngster may become a person abiding authority, [1] as training transmits valuable elements from a pedagogical point of view such as emphasis on grooming, setting honour, integrity, and professional liability to the fore as well as respecting traditions. [2] Thus, the camp in accordance with this line of thought shocks participants by the tough physical expectations to make them more inclusive towards the change in personality and deter them from further criminal offences. [9]

Against these critics voice the arguments that current psychological research projects focussing on teenagers imply that they do not react to short-term physical load that comprises threats and humiliation. There are those who worry about participants becoming better perpetrators via their better stamina, becoming more disciplined and smarter than their counterparts being in prison. [9] Moreover, this military model provides room for physical and psychic abuse as it can make many forms of penalty legal that other prison regime would refuse due to its cruelty and inhumanity. [2: 7] All these may lead to excesses on the part of the training staff, which, unfortunately, had been presented in several instances during the existence of boot camps.

Moreover, the effectiveness test of boot camps does not support the necessity for strong military drill. In relation to this, Muscar [9] obtained the result that in boot camps which showed any signs towards reduced deterioration, each had an aftercare with intensive supervision. This indicates that weaker recidivation rate occurs thanks to aftercare and not military-based residential period. It is no coincidence that it is a baseline requirement for professionally serious boot camps to have the aftercare arranged as a part of the work of the institution. [6] The same is backed by Wilson, MacKenzie and Michell's comprehensive research, [3] as well. Their findings indicate that the military approach of boot camps is an inefficient method to reduce the recidivation after the camp.

Selection and Preparation of Personnel

A well-selected and prepared personnel have a vast role to play in the success of boot camps. It is observed in boot camps mainly created for youngsters that the novel missionary consciousness, the dominance of rehabilitation tasks, dealing with youngsters with a previously clean record renew the personnel's morale. However, unfortunately this is only a preliminary state, serious issues may arise as programmes advance. Since a boot camp exerts an enhanced stress to not only youngsters incorporated but also the training personnel, the negative consequence of a burn-out and high turnover can be more rapidly reached here than in normal prisons. Parallel to the growth in the number of such cases, the possibility of harassment and physical abuse within a camp arising from fault or negligence of the personnel increases. [10] To avoid this, the proper selection of personnel, their preparation for work and their further training at regular intervals are key issues.

Thus, the first step is the selection procedure. In this, at least the following factors need to be addressed by all means, which can be grounds for exclusion: physical abuse or negligence of those put to care or supervision of the person; drug or alcohol abuse; serious personal issues currently existing; reports on previous misconducts. In addition, a requirement for training officers can be the experience gathered in earlier military service and many physical conditions – height, weight, condition – as they should be suitable for carrying out the issued tasks as well and serving as a role model for the youngsters. [11]

The second step is the preparation of the selected persons. A boot camp is a special correctional medium, thus it is important that the personnel understand the concept, purpose and structure of the programme. During the preparation, the future personnel is helped to better understand the participating youngsters and themselves, too. Unfortunately, this preparatory training is neglected in some minor boot camps, however, there are camps where especially complex preparatory training is given. For instance, those wishing to work in a boot camp are to complete a 4-week programme in the State of New York. The training material comprises management skills, consultancy techniques, psychology, resuscitation, military formulas, drills. [11] They have even unique training programmes from time to time for further training of those already working there. [10]

Tragedies, Deaths

Although as we mentioned, the physical and mental screening is necessary for most of the boot camp programmes before the youngsters are placed there but reports on deaths and injuries indicate that sometimes youngsters are sent there who either physically or mentally are inapt for the programme. [9] Below we shall present some detailed cases that had a major echo in the media, where death was attributable to the military training and discipline, training personnel, physical load or health conditions.

The case of Mario Cano[4] (age 16) can be classified in the latter category, i.e. health causes; he was one of the teenagers to be the first to die in a boot camp. Mario's death was caused by a blood clot reaching his lungs 4 days after his inclusion in the camp. Although he

[4] Date of death: April the 27th 1984, location: Tucson-based VisionQuest.

was complaining to the training personnel about being ill, they thought he was simulating, therefore he was forced to carry on the physically burdensome physical exercises, during which he collapsed and died. During these short 4 days, camp nurses checked his health condition and no medic had him checked up. [12] Also, Nicholaus Contreraz[5] (age 16) had health issues who died of a massive undiagnosed infestation, after he had lost his conscientiousness during training. Two weeks before his death, Nicholaus told a camp nurse about having breathing difficulties and that he was feeling pain in the chest and experiencing general weakness. He became incontinent and vomited several times a day. Instead of giving him appropriate care, the training personnel accused him of imitating this and started harassing him, thus, he was to undergo plenty of humiliation in the days before his death. [9]

In the history of boot camps, burdensome physical load resulted in several casualties. Among them Gina Scoret[6] (age 14) who collapsed during a 2.6-mile jogging and died, suffering from heat exhaustion. She was overweight and not used to intensive physical exercise but the training personnel forced her to jog uninterruptedly. From time to time, they roped her to themselves to force her make constant motion until she dropped onto the ground. The personnel was waiting 3 hours after her collapse to call the ambulance as they thought her to be simulating feeling sick. [9] Similarly to Gina, Paul Choy[7] (age 16) was unable to complete the 5-mile jogging set for him. As a punishment, the boy had to sit on a wooden platform for 5 hours in the cold. He was not allowed to shiver nor use the washroom for this period of time. Finally, when Paul gave up the exercise, the training personnel jumped on him right away and held him tight to the ground applying a so-called Nelson hold to him. They were holding him on the ground for 10 minutes and no sooner realised that the boy was no longer breathing being technically brain dead. [13] Therefore, in Paul's case also, the brutal excess of the training personnel attributed to the tragedy in addition to the basic physical ineptness. The conditions of the death of Martin Lee Anderson[8] (age 14) have similar characteristics to that of Paul's, feeling sick after a 6-mile jogging and complaining of tiredness. Nonetheless, the training personnel obliged him to complete the jogging as he was also believed to simulate feeling sick. When Martin refused to continue the exercise, several members of the training personnel grabbed him in a way that they blocked his breathing. By the time they realised that the trouble is serious, it was too late, the boy had died. [14] The case was also recorded on a video footage, which was disclosed later on. Unfortunately, there are more who died by the hands of training officers due to being held down or detained: Anthony Green[9] (age 15), Brandon Hadden[10] (age 18).

Besides the health and physical issues raised so far, psychic inaptitude may also lead to tragedies. Suicide—although the examination of specific root causes and background is difficult—may be a sign of psychic inaptitude, which is an isolated case in boot camps either. Anthony Dumas[11] (age 15) took his own life hanging himself with a belt on his double-deck bed. Chad Andrew Franza[12] (age 16) also hung himself attaching the rope to

---

5 Date of death: March the 2nd 1998, location: Arizona Boys Ranch.
6 Date of death: July the 21st 1999, location: South Dakota State Training School.
7 Date of death: February the 4th 1992, location: Rite of Passage.
8 Date of death: January the 6th 2006, location: Bay County Sheriff's Boot Camp.
9 Date of death: May the 21st 1991, location: Brookhaven Youth Ranch.
10 Date of death: October the 15th 1998, location: Healthcare Rehabilitation Center.
11 Date of death: October the 14th 2000, location: Lippman Family Center in Broward County.
12 Date of death: August the 17th 1998, location: Polk County Boot Camp.

the air vent of the air conditioning unit located in his room. Shawn Smith[13] (age 13) was complaining of those abusing him who should be normally helping him then killed himself using the bed sheet attached to his door.

Summary

The strong military drill employed in boot camps entails negative impacts from several points of view. On the one hand, the relation with the aggressive and hostile training staff does not promote rehabilitation nor brings about long-term positive psychological and behavioural changes. On the other hand, enforcing participants to carry out heavy physical exercises may endanger their physical integrity and may even lead to death. [34] To avoid such strategies, more emphasis should be put in any event on physical and psychological assessment tests before including someone in this camp. At the same time, providing the proper specialist medical supervision would be necessary including the preparation of the training staff to be capable of recognising whether a young person is struggling with a serious issue or is just simulating. On the other hand, it is worth noting the maintenance of the proper mental health conditions of the personnel by means of providing regular further trainings or supervisions.

Ultimately, in any event, larger space should be given to various rehabilitation programmes, education, vocational training, employment and aftercare in addition to the military nature in boot camps established for youngsters. Efficiency tests demonstrate that military nature alone cannot achieve positive changes for the participants only if applied together with these programmes.

References

[1] GÜLTEKIN, K., GÜLTEKIN, S.: Is juvenile boot camp policy effective? *International Journal of Human Science*, 9 1 (2012), 725–740. https://doi.org/10.14687/ijhs.v9i1.1978

[2] RUZSONYI P.: Régi és új forma – Érvek és ellenérvek a csizmatáborokról. *Börtönügyi Szemle*, 3 (2000), 1–14.

[3] WILSON, D. B., MacKENZIE, D. L., MITCHELL, F. N.: Effects of Correctional Boot Camps on Offending. *Campbell Systematic Reviews*, 6 (2005), 1–42.

[4] SIMON, J.: They died with their boots on: the boot camp and the limits of modern penalty. *Social Justice*, 22 2 (1995), 25–48.

[5] MACKENZIE, D. L.: Boot camp prisons: components, evaluations, and empirical issues. *Federal Probation*, 54 3 (1990), 44–52.

[6] HUSZÁR L.: Csizmatábor létesítésének alternatívái Magyarországon. *Börtönügyi Szemle*, 3 (1999), 63–69.

[7] TYLER, J., DARVILLE, R., STALNAKER, K.: Juveline boot camps: a descriptive analysis of program diversity and effectiveness. *The Social Science Journal*, 38 (2001), 445–460.

[13] Date of death: October the 30th 2001, location: Volusia Regional Juvenile Detention Center Florida.

[8] LUTZE, F. E.: Are shock incarceration programs more rehabilitative than traditional prisons? A survey of inmates. *Justice Quarterly*, 15 3 (1998), 547–566.

[9] MUSCAR, J. E.: Advocating the end of juvenile boot camps: Why the military model does not belong in the juvenile justice system. *UC Davis Journal of Juvenile Law & Policy*, 12 1 (2008), 2–50.

[10] MACKENZIE, D. L, ARMSTRONG, G. S.: *Correctional Boot Camps: Military Basic Training or a Model for Corrections?* Thousand Oaks: SAGE Publications, 2004.

[11] MACKENZIE, D. L., HEBERT, E. E.: *Correctional Boot Camps: A Tough Intermediate Sanction.* Washington D.C.: National Institute of Justice, 1996.

[12] VisionQuest: The Best Alternative for Some. *Los Angeles Times* (online), June 16, 1985. http://articles.latimes.com/1985-06-16/local/me-2770_1_young-people (Downloaded: 10.12.2016)

[13] RIAK, J.: *Deadly Restraint.* 2006. http://nospank.net/camps.htm (Downloaded: 04.11.2016)

[14] REUTTER, D. M.: Youth Dies in Florida Boot Camp; Cause of Death Questioned. *Prison Legal News* (online), July 15, 2006. www.prisonlegalnews.org/news/2006/jul/15/youth-dies-in-florida-boot-camp-cause-of-death-questioned/ (Downloaded: 11.12.2016)

AARMS Vol. 17, No. 1 (2018) 13–22. 10.32565/aarms.2018.1.2

Thoughts on Technological Diversity and Knowledge Management in Centralised Organizations

Péter KORONVÁRY,[1] Péter SZEGEDI[2]

The diversity of available technology challenges our organizations, leadership and (uniformed and civilian) co-workers day by day. Fiscal limits, conflicting technologies, constant need of unavailable knowledge and various other environmental factors may get centralized organizations with positional power in critical situations in our century. This article tries to bring to front some arguments why knowledge management should be considered as a key part of the necessary solution in avoiding new risks we shall face in the 21st century.

Keywords*: management, leadership, knowledge organization, technology, public administration, military*

A Cavalcade of Opportunities

The world of "smart" tools can astonish anybody who grew up in an age when the regular way to interact with distant friends, acquaintances or relatives was writing a postcard. Even the coming of the telephone (and, do understand it well, we are talking about the wired dial phones grandpas still prefer to use as their fingers are too big to use a mobile) caused serious restructuring in the behavioural patterns as well as that of the living space or the social patterns. Once there will come some historian to write lengthily about how telephones conquered the streets and apartments, where they were stationed, how they were moved within the house or flat, and how they became from status symbols work instruments and, by now, artificial body parts of practically any human being under the sun, and how it became from a highly private act into an openly done one irrespective of place, time or audience.

The purchase of a mobile may be even more troubling. The cavalcade of makes, brands, versions, types, colours and, of course, prices can easily make the average over-aged adult dizzy. If you give a closer look, however, it may be that the various gadgets begin to group into sets. Classification makes orientation a lot easier.

In everyday situations classification is usually done according to the particulars of the potential buyer. Certain people consider design and colour, others also brand and technological specifications, while there are some who follow fashion or function, and most, of course, consider, in one way or another, the price.

There are the most modern high-tech power machines, the automatic super-smart pocket mobiles with more functions one can use in a lifetime and with comparable capacities to a good desktop computer, and in fact with a number of accessories they are capable of executing very similar functions too, and much more. Their most talkative

[1] Assistant Professor of the National University of Public Service; e-mail: koronvary.peter@uni-nke.hu
[2] Senior Officer of the Hungarian Defence Forces; e-mail: szegedi.peter@hm.gov.hu

characteristics for the everyday man are that you need an evening course to learn how to use them and a lifetime to pay its price. And the running costs, if you want to make use of all the utilities at a professional level, they may be unacceptably high for the average wage earner. They are pretty, they are lean, they are the dream of tekkies and the status symbols (and sometimes probably also important multifunctional tools) of top managers. And yes, you can use them even as a telephone.

There are the middle-market bracket mobiles, with less fantastic prices and designs. The difference for the everyday user is mostly formal: their design makes use of more Spartan, more affordable materials, keeping as much as possible the elegance of lines and curves. Functionally they are capable of the same things, probably less efficiently and there may be reasonable differences in the quality of output too, but the everyday mobile buying individuals will see little of this. Evidently, they offer for them a much better value for price than top models, not to mention that they do not have to sell their children's future to pay them. Running costs are usually affordable for most living from a salary as telephone companies from time to time promote such medium-priced gadgets by offering them together with certain really advantageous packages. Their use meeting the full potentials of such a tool, however, may also require relatively more expense per month.

There are also various corresponding "no name" phones on the shelves produced by companies which either will make themselves a name in the future or sink soon into oblivion. They may be a bit heavier, a bit thicker, a bit less elegant in design, but they may also offer potentially interesting solutions due to their technical specifications, special service or better prices.

Also, you may see a number of "out-dated" mobiles on sale. They are relatively slow and have fewer or less worked out or older versions of functions, weaker hardware and software. They are beginning to become "problematic" as—due to the changes in fashion, software offerings and architecture—they are slowly becoming less and less compatible with the network, with the up-to-date software, with the upgrades of older software, they are the lower-market bracket products on sale for those who do not want to spend much and do not really need or want to use the exquisite online services.

Even some of the "mammoths" may turn up—from the back shelves of deep, dark stores, second hand shops, they somehow may find their ways to the customer. They are the museum pieces, sometimes real archaic finds, with all the charms and beauty of antiquity—they are big, massive, thick and "stupid", offering much fewer functions and weaker capacities as today's gadgets. Even so, they sometimes prove to be pretty functional, even surprisingly so. Not much time and children will find too difficult to use them—even their old users will need some time to find out how they actually can send messages on their old gadgets and be surprised how they could use them without any opportunity for reading or writing e-docs, watching films, or linking to the World Wide Web. They are the fountain-pens of the world of 3D information technology. Spare parts, accessories may already be difficult to find, their cooperation with the modern electronic tools is problematic. And even so, there is something interesting happening here…

There are copies of these "mammoths" present in masses in supermarket offerings. They look like mammoth, smell like mammoth, taste like mammoth. However, they are different. They are cheap, small, practical. They are able to offer the user a basic set of functions at a relatively really good level of efficiency and effectiveness. Not the fancy

3D internet highway functions, but the basic ones you really need. They do not overtly multifunction, they are not "smarter" than the user. They offer clean functionality, polished, even sophisticated forms, practicality, but only within a limited range of possible tasks (phoning, messaging, calendar, register, notes etc.). Even if they look like old designs, they are practical and eye-catching. But they are different.

At first the similarity may confuse the inexperienced buyer but not for long. When you take such a gadget in your hands you will feel the difference. The materials are somehow different, better fit for mass production, perhaps, but also lighter, good-looking, easy to hold, good to touch. And they are—you will feel it when holding them—smaller. Even the tips of your fingers will perhaps be too big for them, you will have to use the edge of your nails. And the small screens have basic but comforting pastel colours, not the olden green background, black icons solution. Even the icons are different: easy to interpret, functional but pretty—tailored to the eyes of today's users. And the operations logic has also been made easier to understand. But the biggest anachronism: these gadgets are almost "empty": their mass-produced parts are so small that if the size of such phones would be reduced to the necessary, they would be simply too small to use. Even so, these components may be much more powerful than those of the original models—simply it is not worth to manufacture so weak and outdated parts any longer. With a bit of attention, they may last for ever but if they do not, it's no use to have them repaired. Costs would probably be much higher than the price of a new one. [10]

Overburdening the People

The example of mobile phones can be adapted to practically any equipment group used by our organizations, let them be office equipment, weapon systems or education technology. It shows us that the survivability of old systems may be better than one would at first dare to think. The barrier hardest to overcome may rather be on the human side—the knowledge incurred in their use and functioning may outdate faster than the technical solutions. As the proper maintenance and use of the newer and newer systems may require varying sets of skills and know-how, even changing sets of premises or concepts, organizations will sooner or later face a new problem in the field of the management of human resources development. Even today signs of over specialization may be observed. Operators and even technicians working with up-to-date technologies may not have that old set of skills and know-how necessary to integrate outdated but still functioning machines. The so-called interface problems between human and non-human elements in a process, as well as maintenance problems (e.g. unavailable or too expensive spare parts for older machines) are also recently faced by specialists. Organizational problems do peak, however, when even the necessary specialist knowledge will be of no avail. To get some hands-on experience of the problem, you can try to connect an about 10 years' old printer to a modern laptop and print a page or two. Do you have matching slot to the plug? If not, can you find a solution yourself? Have you got the right driver installed? If not, can you find it on the internet, download and install it? What if you do not find any solution to make the printer work together with your Win10? Can you change back to an earlier system? What about Linux? And if all this is not enough, what if it is an about 25-year-old matrix printer you have to integrate into

your home computer network? In plain English, the real-time lengths of the equipment life cycles are rapidly becoming shorter and shorter.

Today's and tomorrow's operators, technicians and engineers are facing the problem of having to study more and more of the outdated machines in use, while trying to keep up with their rapidly developing profession. Seemingly by the middle of the 21st century a major weakness of any piece of technology may be that it gets outdated much faster than the equipment itself would actually break. In addition, staff fluctuation may become faster than equipment life cycles, therefore old and new technologies may have to gain equal importance in education, training and development. Finally, new generations joining the organization will be socialized to the use of a quite different sets of technology than the previous ones or that the (more or less outdated) mixture used by the organization would require. These three problems will definitely add up to develop new risks of major management crises in our big organizations and systems, especially in the public sphere. Together with the culturally programmed tendency to think of organizational reforms in terms of structural changes instead of process development, the rethinking of human and non-human resource strategies at such highly technology-based, sizeable public organizations like the military ones seems to be unavoidable.

When taking a systemic perspective, a sincere overview of the organizational context seems to make it clear that the integration and comprehensive management of tasks, technologies and know-hows of public organizations, whether military or civilian, must be at regular intervals reviewed and adjusted. And these intervals are to be shorter and shorter in our century. It is of utmost importance that we find ways to permanently renew and improve our resources (both human and non-human) so that the execution of organizational tasks and the attainment of operative as well as strategic objectives remain possible. As long as the procurement of market leading technology for the whole of such big and complex organizations may be financially challenging, if not impossible, special effort is necessary to ensure the integration of old and new pieces of equipment in the very same system. Even if their parallel use makes the system more expensive to operate on the long run, the peculiarities of fiscal thinking and cash-flow may make it unavoidable. Not only the components and spare parts, accessories and complementary tools of ageing equipment may become sooner or later too expensive or even unattainable, but also those management, systems, operational etc. schemes, architectures, structures of concepts, thinking and techniques too in which they originally were meant to fit. Today's processes and problems are partially or wholly different from those they originally were able to handle. In many respects it may be that we are trying to make a 3D coloured cinema with a mid-20th century photographic camera with a 26-picture black-and-white film in it. Lots of time, energy and effort are wasted to solve the unsolvable and to bridge the technological gap between the realities in equipment and the level that would match 21st century contexts and problems.

If creativity and a wide range of technological information is needed to match a whole bunch of ageing equipment with unfitting modern counterparts, education, especially the education of future operative and maintenance staff, including military technicians and engineers, has something to do there. If we have but paper and pencil to solve problems, our officers-to-be have to be taught how to do so. There is however no way to prepare well-functioning specialists by teaching what's new and up-to-date, and then sending them to work with stone-age equipment. Also, however, it is no solution to teach them the use

of "existing" equipment as the gap between the know-how needed by presently purchased technology and the acquired knowledge would be too far away from each other. To train and pay two groups of technical staff is of course unimaginable. To teach old and new technology in their variety to the same set of people would require, of course, much more time and energy. Therefore, the only way out seems to teach a selection of both, using examples from the organization's practice, linked by what is today usually labelled as "creative problem solving". [15]

It is therefore essential that new generations of our technicians and engineers are trained not only in using pen and paper, but also, they are educated in how to solve problems in such a technologically challenged environment. It is not enough for them to learn how current management information systems function and what they can be used for, or how to use a project management software, they should also acquire skills necessary to get to similar results with outdated technology, too. A Gantt chart may be calculated and drawn with pen and paper, if you know how to do it.

In an age when leaders have to be taught how to sign a document with a ceremonial fountain pen it is probably not much of a surprise if calligraphy, the skill of beautiful handwriting has found its way into the curriculum of certain universities. We have to do the same and teach skills that used to be basic a couple of decades ago but seem to be rare and necessary today. Even if students are taught, for example, how to use present documents and have to be able to fill in, following the standards and regulations, certain forms and tables, electronically or on paper, but this is not enough. They have to know what rules to follow when creating a new table. What are those rules of thumb that help them create one that can easily be interpreted by those who will be lucky enough to fill it? What to do if computer networks cease to function and our organizations have to get back to paper-based operations till the servers (or whatever) get repaired? What if the mobile systems cease to function? Or the satellites? Or all these together? What if all these will be part of a much bigger set of symptoms of a complex crisis following a natural catastrophe or terror attack? We need officers—leaders, managers, engineers or technicians—who know what to do under such circumstances, or at least they can find it out. Systemic thinking and creativity have to be integrated into 21st century curricula in an age when everybody has Google, but most of them have no idea how to use it effectively. Seemingly, however, certain professional cultures do not support such ideas. [10]

The increasing speed of technical equipment dropping out of use will be a source of major crisis management problems in our age. To sustain basic operations and continue executing organizational functions without the technology we are so much used to is a task we are going to face on a regular basis. The present imprinted set of rules and regulations, manuals, accepted standards of behaviour etc. will hardly match an operational context "without gadgets" better than that of a technologically up-to-date one. In fact, we do not even need a crisis—such interface problems may be more than enough to build one up and start is. As thirty years ago it was the use of British street phones or the place of postal codes on an envelope that may have caused headaches to tourists and post officers, today all individuals and organizations face a cavalcade of operation systems, linguistic and cultural complexities, the beauties of international English with its non-native varieties, differences in documentation and regulatory background of partner countries and/or organizations, just to mention a few of the non-technological symptoms adding to the developing crisis. [4]

Whether we realize or we don't, we are living in a huge complexity of interface problems where proper, ethical and even—at the first sight at least—logical regulations might add to our problems instead of helping to solve them. Just think of product manuals in the packing telling the same thing in sometimes twenty-something languages printed in 2pt small—and therefore totally unreadable—characters. [10]

Today's technological systems require operating staffs to acquire knowledge and skill sets under the pressure of the urgent need of further improvement. To add further knowledge and skills required by the integration of multi-generational equipment to their burden of continuous development will mean additional education costs and higher fluctuation as such well-trained problem-solving engineers will definitely find better paid jobs with international companies than with our public organizations. Furthermore, their effectiveness will always be strictly limited by the outdated systems they will be requested to operate and maintain. [9] What's more, they will also be bound by their working environment at other levels too—let us think of, for example, the cultural and regulative framework the military and other public organizations exist within. [15]

The speed of technological development is seemingly continuously growing. Public budgets do not allow to introduce the newer and newer generations of modern tools and equipment. Some speak of virtual warfare and virtual client service at government offices, but it is only the gap between the technologically possible and the reality that is widening. We are at a point where the choice between financially feasible working solutions and the "big jump" to close up behind the top technological leaders has to be taken and according to the decision our governments and organizations have to define strategies for the rest of the century. The economic realities of Europe may rule out the high-cost alternatives in most areas of the public activities, but perhaps there is still enough reserve in the system to choose rapid development at least in some small segments. The later strategic decisions are taken, the fewer areas of development we can rationally expect to remain on the menu. [8]

The amortization of our present systems is in a phase when in some cases it is only the historic value of some technologies still in use that can be expressed with a positive number. Our multigenerational systems, however, will seemingly have to be staying in use as long as we can find or train personnel to maintain and operate them. [6] A major hindrance in this respect is the tendency of centralized organizations to neglect the proper management of organizational knowledge development. Without special managerial effort to fight this trend, as a result also organizational innovativeness, internal motivation building, professional and personal development, even organizational development will suffer. [14] Undeveloped, unmanaged knowledge will soon become outdated and irrelevant, useless. With the right management attitude, however, there is a chance that organizational leaders may keep up a situation where operative objectives may be reached; the question is, at what price. [9] There must be other solutions to develop our organizations in a (functionally, economically, socially etc.) more effective way. [10]

Our (higher education, public administration, national defence, law enforcement etc.) organizations typically depend upon the collection, organization, analysis and use of data, information and knowledge. They all take it for granted that a certain idealized system of organized knowledge does exist. Their operations follow codified and standardized processes based on inherited, historic values that are held universally true but are, in fact,

in some respects rather worn out or even atavistic. Tradition, institutions, culture in such organizations are phrases that are often used for hiding partial inertia. [11] Over-centralization, the overt functioning of "survival-orientation" in such systems based on positional power and the required and expected respect of rank are all symptoms that more often than not go together with the exclusion of people at lower organization levels from knowledge and information, and the avoidance of the mere acceptance of the existence of individual know-how of subordinates. [10] As a matter of fact, the exclusive right of the superiors to the possession of knowledge (or even the belief in it!) is a powerful tool to the ideological strengthening of their positional standing. Not only is it against the interests of superiors to collect knowledge attainable within the system bottom-up and to make it available for others, but they also may take such suggestions as a personal attack against their own positions.[12] They will function as powerful filters within the organizational information system letting through exclusively those bits of information they find safe, relevant and important for their own purposes. [1]

Special Leadership Effort Needed

Any organization that manages to bottleneck in its own internal communication channels will become unable to identify movements in their environment. Neither those offering opportunities, nor those causing trouble. With extensive leadership effort, the creation, strengthening and regular development of those systems processes are capable of identifying, analysing and interpreting potential problems. To do so, organization leaders have to see to it that *(1)* the regular collection and restructuring of information does take place unhindered, *(2)* the collected information will be continuously analysed and assessed, processed and shared so that they meet professional standards, *(3)* the necessary resources (units, people, functions, tasks, place, equipment, authorizations, access etc.) are provided so that the processes involved may be run by knowledge management professionals. The creative use of present equipment may certainly reduce costs, for example the use of a Linux operation system and free office software may help to keep older desktops and laptops functioning. [15] [9]

The creation and development of adaptive and agile management of organizational knowledge in line with the organization's strategic objectives is an important part of the solution to the problems of centralized organizations. To set it up, we shall be in need of the support of all the analytic, critical, creative, intuitive, networking, project-management etc. skills available. The development of such skills with the help of available techniques and methodologies such as Total Systems Intervention, [7] de Bono's thinking tools [3] or Action Learning [13] is doable, but the integration of such practices in the daily decision-making processes does need further leadership attention and effort. [15]

The target can be to intentionally prepare public organizations to identify and actively utilize the necessary knowledge(s) in and around to identify and prepare for various environmental effects under a strong leadership. Reforms and structural changes may strengthen the risks of losing professional competencies of the organization, both on the rational-analytic side (explicit knowledge) and on the intuitive one (tacit knowledge). To create an ideal system where the knowledge of the co-workers is permanently available

for each other and the generation and utilization of new ideas are actively maintained by ongoing organization problem-solving processes is an objective they should pursue without cease. [9] Such an active organizational thinking may be able to identify changes in the organization's environments, mission and/or objectives, update organizational SWOT-s and analyse them, identify missing knowledge inputs and potential sources to acquire or develop them, and make sure that the necessary professional know-how as well as organizational knowledge reaches wherever they may be needed in time and in the form best fit for the potential users. [2] [15]

Such organizational knowledge may then be channelled also towards education. While higher education institutions may play a key role in identifying, analysing and introducing the necessary concepts, methodologies and tools in setting up working knowledge systems as well as in the dissemination and circulation of current theoretical and practical knowledge, hands-on experience and practical information from the actual problems arising in the course of their introduction and use may come only from the "battlefield". The education of new generations of young professionals must therefore take place in at least two very different environments that should work together, even intermingle, but never be mixed up and even confused: the university and the workplace. The common effect of the two very different types of experience will create in the learner the necessary "creative chaos", a mental state or space for conflicting inputs necessary to practice "thinking skills" needed so much in the problem-solving process. [12]

There is no learning simulation or seminar assignment that may prepare for the organizational realities. Professionals are made in practice. Education, however, can supply the necessary skills, capabilities and knowledge to see tasks, processes and structures from different aspects and perspectives. The aim is to mentor new and not-so-new generations of professionals to be able to trust and value such generational differences and share with each other what they are good at. [15] If indoctrination and socialization processes in our organizations work against this, and kill in the name of "tradition" all hope for transition, development and change, if we make use of financial and technological limitations as excuses for maintaining the past instead of moving toward the future, we are lost. It does not matter how up-to-date knowledge new colleagues bring to the organization if they are not allowed to use it. [9] Either they will be frustrated and leave the organization, or they will bend to the force of organizational culture and take over outdated patterns of thinking. In both cases, our organizations are bound to lose. It is not enough therefore to educate, train and mentor professionals-to-be, but there is also an urgent need to do the same at least with the core members of the organization. [2]

Centralized complex structures based on positional power—this is how most of our public organizations can be described. The textbook characterization of such systems will be a key element of coming organizational and social crises. Fiscal problems only add to the risks. We have, however, possible (partial) solutions at avail, such as knowledge management. In case we decide to adapt them, centralization and a strong, change-oriented leadership may even be advantageous in preparing for the coming wave of challenges. And then probably statistical proofs of their excellence will also improve. [5]

References

[1] BELÉNYESI E.: Hatékony önkormányzati kommunikáció – a tudás megszerzésének lehetőségei. *Pro Publico Bono: Állam- és Közigazgatástudományi Szemle*, 1 (2011). www.propublicobono.hu/pdf/Belényesi%20E.pdf (Downloaded: 01.10.2015)

[2] BENCSIK A.: *A tudásmenedzsment elméletben és gyakorlatban.* Budapest: Akadémiai Kiadó, 2015.

[3] de BONO, E.: *Six Thinking Hats.* Granica Editions. Boston: Little, Brown and Company, 1986. www.ilahas.com/sirpabs/ ebooks/Social%20Interactions/Six%20Thinking%20 Hats %20-%20Edward%20de%20Bono.pdf (Downloaded: 20.07.2016)

[4] BUDAI B.: Az e-közigazgatás elmélete axiomatikus megközelítésben. *Információs Társadalom,* 9 (2009), 68–79. www.infonia.hu/ digitalis_folyoirt /2009_2/2009_2_budai_balazs.pdf (Downloaded: 01.10.2015)

[5] BUKOVICS I.: A fenntartható „jó állam" paradigmája. *Polgári Szemle*,10 3–6 (2015). www.polgariszemle.hu/?view=v_article&ID=617 (Downloaded: 20.07.2016)

[6] CSEPELI GY.: *A szervezkedő ember: a szervezeti élet szociálpszichológiája.* Budapest: Osiris, 2001.

[7] FLOOD, R. L, JACKSON, M. C.: *Creative Problem Solving: Total Systems Intervention.* Hoboken: Wiley, 1991.

[8] HANDY, C. B.: *Gods of Management. The Changing Work of Organizations.* New York: Oxford University Press, 2016.

[9] *Tudásmenedzsment a tanuló társadalomban, oktatás és készségek.* OECD, 2001. www.oecdbook shop.org/get-it.php?REF=5LMQCR2JCGG1& TYPE=browse (Downloaded: 06.08.2015)

[10] KORONVÁRY P., SZEGEDI P.: Tudásalkalmazás és tudásgondozás. *Hadmérnök,* X 4 (2015), 217–226. www.hadmernok.hu/154_20_koronvaryp_szp.pdf (Downloaded: 17.05.2016)

[11] KORONVÁRY P., SZEGEDI P.: Thoughts on Understanding Our Organizations. *Hadmérnök,* X 4 (2015), 227–236. www.hadmernok.hu/154_21_koronvaryp_szp.pdf (Downloaded: 17.05.2016)

[12] KORONVÁRY P., SZEGEDI P.: Repülőgép üzembentartó szervezetek humán erőforrásának tudásalapú fejlesztése. In. BÉKÉSI B., SZEGEDI P. (szerk.): *Repülőműszaki üzembentartó szervezetek működésével, fejlesztésével kapcsolatban.* (Tanulmánykötet a BSc, MSc hallgatók számára) 49–63. Szeged, 2016. https://ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/10227/Tanulm%C3%A1ny-Repm%C5%B1szaki.pdf?sequence=1&isAllowed=y (Downloaded: 17.05.2016)

[13] KRAMER, R: How Might Action Learning Be Used to Develop the Emotional Intelligence and Leadership Capacity of Public Administrators? *Journal of Public Affairs Education,* 13 2 (2017), 205–242. www.jstor.org/stable/pdf/40212728.pdf?seq=1#page_scan_tab_contents (Downloaded: 17.05.2016)

[14] SÁNDORI ZS.: *Mi a tudásmenedzsment? Tacit és explicit tudás.* http://mek.oszk.hu/03100/03145/ (Downloaded: 17.05.2015)

[15] TOMKA J.: *A megosztott tudás hatalom.* Budapest: Harmat Kiadó, 2009.

AARMS Vol. 17, No. 1 (2018) 23–30. 10.32565/aarms.2018.1.3

Public Service Motivation (PSM) and Job Satisfaction in Case of Hungarian Local Public Service

Gábor HOLLÓSY-VADÁSZ[1]

Public Service Motivation (PSM) originates from psychology and it spreads in other disciplines such as public administration. PSM was developed in the USA and it is also applied in Europe. In this study, I investigated the connection between PSM, job satisfaction, red tape, and resignation satisfaction in case of a Mayor's office of a district in Budapest. I had four hypotheses but I could prove only one. I found a significant connection between PSM factors and job satisfaction. These results may suggest that PSM could affect how public servants are satisfied with their job in the Hungarian public service.

Keywords: *Public Service Motivation, PSM factors, job satisfaction, correlation, regression analysis, motivators*

Introduction

Public Service Motivation as a theory originates from psychology and it spreads in other disciplinaries like socio-biology, economics, organizational behaviour, sociology, political science and public administration. [1] PSM was developed in the USA and also applied in Europe. [2] PSM was inspired by New Public Management and it turned up in the 90's. *"PSM is the motivational force that induces individuals to perform meaningful public service."* [3: 417] The special motives in public service: [4]

1. *Rational:* PSM pays attention that public servants behave in an altruistic way but they also want to maximize their utility.
2. *Norm-based:* the main norm in public sector is to service the public interest.
3. *Affective:* the main element of the affective norm is patriotism of benevolence which refers to the fact that professionals in public service must provide safety to citizens based on basic rights.

Four dimensions of PSM: [5]

1. Attraction to public policy making refers to be exciting to participate in policy making.
2. Commitment to the public interest refers to the desire to service in the public sector which is an altruistic behaviour.
3. Compassion equals to the patriotism of benevolence which is a moral attitude and an emotional stand. Here, compassion refers to provide the basic rights without screening the political preferences or political attitudes of the citizens.
4. Self-sacrifice is *"the willingness to substitute service to others for tangible personal rewards"*. [5: 7]

[1] Ph.D. student, National University of Public Service; e-mail: hvadaszg@gmail.com

In this study, I examine the connection between PSM, job-satisfaction, resigned satisfaction, and red tape. The number of studies examining job-satisfaction have been continuously increasing in the last 40 years. Job satisfaction can modify significantly both the employees' and the organizations' performance. Job satisfaction is also important due to humanitarian reasons. Job satisfaction goes with mental and physical health. [6]

Resigned satisfaction is not a popular research area in public administration. The authors claim the resigned satisfaction is a part of job satisfaction. They defined resigned satisfaction, which is an individual sense that origins from the difference between his/her personal goals and his/her current job status. If individual experiences are in harmony with his/her personal goals and his/her current job status then her or his aspiration to work will increase. If individual experiences are in disharmony with his/her personal goals and his/her current job status then her or his aspiration will decrease. That can be a stress-source. [7]

Red tape refers to a couple of rules, procedures, regulations that do not create beneficial situations. These situations decrease the loyalty to the organizations. Therefore, not all regulations are red tapes, just those that obstruct the employees. Red tape correlates to high insecurity, mistrust, pessimism. [7]

Previous PSM and Hungarian Motivation Studies

In this section of the study, I summarize the results of previous related studies which applied regression models to search for the connection between PSM and job satisfaction. [8] Numerous studies investigated the relationship between PSM and various labels (such as job satisfaction) in this decade. The authors referred to 28 studies but I will refer only to the most relevant articles. [8] The national context could modify the relationship between PSM and job satisfaction.

Firstly, I refer to a cross-cultural study. [6] A previous study used the data of International Social Survey Program on Work Orientations which included six different countries: Germany, Great Britain, the USA, Hungary, Norway and Israel. The authors found the intrinsic rewards (for example autonomy) had the strongest effect on job satisfaction. PSM-fit (compatibility between individual PSM and features of work environment) had a positive effect on job satisfaction. The results suggested that there was no significant correlation between PSM and job satisfaction. [6] Public servants who experienced a smaller gap between PSM and an opportunity to realize their motives were more satisfied with their jobs than public servants who believed they could not do it. In case of Hungary, the authors found the major drivers of job satisfaction (intrinsic and extrinsic rewards) were scored lower by Hungarian respondents than in other countries.

The above-mentioned article was a cross-cultural study so I present a study which examined only one country. I previously referred to a study [7] that tested the connection between PSM, red tape and resigned satisfaction using a regression model. The responders were Swiss public servants speaking French or German. According to the results, Compassion and Self-sacrifice (PSM factors, see above) can be factors of resignation. Commitment and Attraction to public policy do not correlate with resignation. This result refers to a psychological contract between public servants and public organizations. The psychological

contract is *"a subjective perception of the employment relationship and is mainly concerned with expectations about the mutual obligations of employer and employee to the relationship."* [7: 188] The resigned satisfaction is the manifested outcome of breaking the common psychological contract. Another important result of the study is that red tape strengthens the resigned satisfaction.

The above-mentioned articles did not investigate the mediation effect of PSM so I present a study investigating the mediation effect of PSM. [9] The author investigated the relationship between job satisfaction and organizational commitment in case of a Belgian public service. The study also investigated the mediation effect of PSM. According to the results, three PSM factors (Attraction to public policy making, Commitment to the public interest, Self-sacrifice) went with self-reported performance. Compassion did not meet to a professional public administration where it was not allowed to behave compassionately. He hypothesized that job satisfaction and organizational commitment could modify the relationship between PSM and performance. According to his results, the above-mentioned mediators went with all PSM factors. Finally, PSM could produce person-environment fit in the public sector that created satisfaction among the public servants.

In this paragraph, I present the results of the Hungarian motivation studies in public service. In the Hungarian public service [10] there are three different categories of motivation ideas. The first cluster is called 1.0. According to the ideas of the first cluster, motivation is only the satisfaction of biological needs so, a public organization can motivate the public servants only by the satisfaction of biological needs. The second cluster is called 2.0. According to the ideas of the second cluster, employees are interested in avoiding the penalty and they are motivated in searching for rewards. So, these kinds of theories use only outside motivators. The third cluster is called 3.0. The ideas of the third cluster suggest using the inside motivators also. This can be a connection point between Hungarian public service and PSM because PSM also suggests adopting and using the inside motivators. [11] Hungarian authors define the motivation as an intrapersonal drive which is closed to the motivation concept of PSM.

The Goals and Hypotheses of this Study

In the Hungarian public service literature, one cannot find any empirical studies using the PSM concept. [12] Therefore, no Hungarian study investigated the connection between PSM and job satisfaction. The main goal of this study is to investigate the connection between PSM and job satisfaction in case of Hungarian local governments. I have three hypotheses:

1. There are positive correlations between some PSM factors and job satisfaction, according to a previous study. [7]
2. There are positive correlations between some PSM factors and resigned satisfaction according to a previous study. [7]
3. Red tape strengthens the resigned satisfaction according to a previous study. [7]

Methods

I developed a questionnaire which includes four different parts:

1. In the first part of the questionnaire, there are items investigating the demographical status of the respondents such as gender, age, highest level of their education and residence. In this part of the questionnaire the respondents also answered some questions in line with their jobs such as: *a)* What time did they start working in public service? *b)* When did they start working at their current job? *c)* In what hierarchical system do they work?
2. In the second part of the questionnaire, there is a Likert scale to measure the overall job satisfaction.
3. In the third part of the questionnaire, there are scales developed by a previous study to measure PSM factors. [7] The questionnaire includes 4 factors. The first factor includes 2 scales. The second factor includes 4 scales. The third factor includes 3 scales. The fourth factor includes 2 scales. The items were translated into Hungarian.
4. In the fourth part of the questionnaire, there are scales developed by a previous study [7] to measure red tape and resigned satisfaction. The red tape questionnaire includes 3 factors. The resigned satisfaction questionnaire includes 4 factors. The items were translated into Hungarian.

All items of the questionnaire were in the Hungarian language.

Respondents

(n = 40) public servants filled my questionnaires worked in a Mayor's office of a district in Budapest. (n = 12; 28.6%) of the respondents were men and (n = 28; 66.7%) of the respondents were women. The average age of the respondents is (m = 42.78 year; SD = 9.344 year). Table 1 presents the hierarchical level of the employees in public organizations. 73.8% of the respondents were subordinate workers. Table 2 presents the educational level of the employees. The lowest educational level of the respondents was high school, the highest educational level of the respondents was MA/MSc degree.

Table 1. *Hierarchical level of the employees.* [Edited by the author.]

Hierarchical level	Number of employees	Percentage
Top managers	3	7.1%
Middle managers	4	9.5%
Professional advisers	2	4.8%
Subordinate workers	31	73.8%
Summarized	40	100%

Table 2. *Educational level of the employees.* [Edited by the author.]

Educational level	Number of employees	Percentage
High school	3	7.1%
Professional qualification	9	21.4%
BA/BSc	15	35.7%
MA/MSc	13	31.0%
Summarized	40	100%

Results

Firstly, I controlled the reliabilities of PSM, red tape and resigned satisfaction. Table 3 presents the Cronbach Alpha scores. Cronbach Alpha scores must be over 0.7. If it is not over 0.7 that means, the questionnaire is not reliable, therefore, I ignore any other statistical examinations of red tape and resigned satisfaction in this study.

Table 3. *Cronbach Alpha scores.* [Edited by the author.]

Name of dimension	Cronbach Alpha
PSM	0.780
Red Tape	0.571
Resigned Satisfaction	0.297

Secondly, I tested the connection between PSM factors and job satisfaction in a linear regression model based on entry method. In this case, ($R^2 = 0.417$; $p < 0.001$). Table 4 presents the regression model based on entry methods. Commitment to the public interest is only one factor that affects significantly on job satisfaction.

Table 4. *The regression model based on entry method.* [Edited by the author.]

Model	Beta	Significance
PSM Factor 1	-0.092	0.510
PSM Factor 2	0.466	0.010*
PSM Factor 3	0.082	0.610
PSM Factor 4	0.203	0.262

*$p<0.05$

Thirdly, I investigated the internal correlation between PSM factors and job satisfaction. I found 4 significant correlations. The PSM Factor 2 (Commitment to the public interest) has

the strongest effect on job satisfaction. The PSM Factor 3 (Compassion) and PSM Factor 4 (Self-sacrifice) have also a strong effect on job satisfaction. The PSM factor 1 (Attraction to public policy making) dos not have a significant effect on job satisfaction. Table 5 presents the correlation results.

Table 5. *Correlations between PSM factors and job satisfaction.* [Edited by the author.]

Name of PSM factors and scales	Job satisfaction
PSM Factor 1	0.069
PSM Factor 2	0.616**
PSM Factor 3	0.440**
PSM Factor 4	0.493**

*p<0.005; **p<0.01

Discussion

No empirical studies using PSM concept is to be found in the Hungarian public service literature. There is only one Hungarian study that focuses on PSM but that is a theoretical study. [12] This is one of the first studies that empirically investigates PSM in the Hungarian public service. In this study, I investigated the connection between PSM and job satisfaction in case of a Hungarian local public sector. The respondents worked in a Mayor's office of a district in Budapest. The Cronbach Alfa scores of red tape and resigned satisfaction are under 0.7. There could be two reasons for the low reliabilities. The first one might be that only 40 people participated in this study. The low number of respondents is the main limitation of this study. Red tape's Cronbach Alfa score proves the above-mentioned idea because it is close to the acceptable level. The second reason might be that resigned satisfaction concept does not fit into the Hungarian public sector. In the future, some studies should investigate if resigned satisfaction concept can adapt and apply in the Hungarian public sector. However, I had three hypotheses but I could prove only the first one because the red tape and resigned satisfaction could not be statistically analysed.

Although the number of respondents is limited, still I could successfully prove my first hypothesis. Three PSM factors positively correlate to the job satisfaction. If employees score high on Commitment to the public interest, Compassion and Self-sacrifice, they are satisfied with their current jobs. Therefore, public organizations should seek for employees who are committed to the public interest, have compassion and willingness to serve others because these servants are satisfied with their public jobs. My results confirm a previous study [7] that found positive correlations in Switzerland. According to regression results, the PSM Factor 2 can explain 41.7 % of job satisfaction's variance but the other PSM factors do not have significant effects on job satisfaction. The results of correlation and regression analyses suggest that the PSM concept can strongly modify how Hungarian public servants are satisfied with their jobs. My results partially disprove a previous study [6] that found

significant connection between PSM-fit and job satisfaction in their cross-cultural study. I suppose the reason is that the connection can be modified by the national context. [8]

A Hungarian study [13] summarized the managerial responsibilities in the Hungarian public service. The author mentioned that the main responsibilities of managers are to motivate the employees in public sector. One of the main goals of Public Administration and Public Service Development Strategy 2014-2020 [14] is that public employees in the Hungarian public administration should be motivated on high level because it is one of the principles of the Good State Conception. [14] The results of this study and the whole PSM concept can support these processes and there is empirical evidence that PSM is a valid concept in the Hungarian public administration.

References

[1] KOEHLER, M., RAINEY, H. G.: Interdisciplinary foundations of public service motivation. In. PERRY, J. L., HONDEGHEM, A. (eds.): *Motivation in Public Management. The Call of Public Service.* Oxford: Oxford University Press, 2008, 33–55.

[2] MIHALCIOIU, R. M.: Public service motivation. *EIRP Proceedings,* 6 (2011), 834–838.

[3] BREWER, G., COLEMAN SELDEN, S.: Whistle blowers in the federal civil service: new evidence of the public service ethic. *Journal of Public Administration Research and Theory,* 8 3 (1998), 413–439.

[4] PERRY, J. L., WISE, L. B.: The Motivational Bases of Public Service. *Public Administration Review,* 50 3 (1990), 367–373. https://doi.org/10.2307/976618

[5] PERRY, J. L.: Measuring Public Service Motivation: An Assessment of Construct Reliability and Validity. *Journal of Public Administration Research and Theory,* 6 1 (1996), 5–22. https://doi.org/10.1093/oxfordjournals.jpart.a024303

[6] WESTOVER, J. H., TAYLOR, J.: International differences in job satisfaction. The effects of public service motivation, rewards and work relations. *International Journal of Productivity and Performance Management,* 59 8 (2010), 811–828.

[7] GIAUQUE, D., RITZ, A., VARONE, F., BIGET, S. A.: Resigned but satisfied: the negative impact of public service motivation and red tape on work satisfaction. *Public Administration,* 90 1 (2012), 175–193. https://doi.org/10.1111/j.1467-9299.2011.01953.x

[8] HOMBERG, F., MCCARTHY, D.: A Meta-Analysis of the Relationship between Public Service Motivation and Job Satisfaction. *Public Administration Review,* 75 5 (2015), 711–722. https://doi.org/10.1111/puar.1242

[9] VANDENABEELE, W.: The mediating effect of job satisfaction and organizational commitment on self-reported performance: more robust evidence of the PSM-performance relationship. *International Review of Administrative Sciences,* 75 11 (2009), 11–34.

[10] SZAKÁCS G.: *Az emberi erőforrás gazdálkodás fejlesztésének elméleti kérdései a magyar közszolgálatban*. Budapest: Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Kar, 2014.

[11] SZABÓ Sz., SZAKÁCS G.: *Közszolgálati HR-Menedzsment*. Budapest: Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Kar, 2015.

[12] HOLLÓSY V. G., SZABÓ Sz.: A pszichológiai megközelítésű PSM-paradigma jelentősége a magyar közszolgálatban. *Hadtudományi Szemle,* 9 2 (2016), 163–174.

[13] SZABÓ Sz.: Managerial Responsibility and Efficiency in Public Service (Competency-based Solutions). *AARMS*, 15 3 (2016), 271–277.

[14] *Közigazgatás- és Közszolgáltatás-fejlesztési Stratégia 2014–2020.* www.kormany.hu/download/8/42/40000/K%C3%B6zigazgat%C3%A1s_feljeszt%C3%A9si_strat%C3%A9gia_.pdf (Downloaded: 01.09.2017)

AARMS Vol. 17, No. 1 (2018) 31–44. **10.32565/aarms.2018.1.4**

State-Level Analysis Aspects of Comparative Disaster Management

Bendegúz PAPP[1]

In international environments numerous different disaster management systems can be found, whose operation can be also varied because of their differences. Nowadays, there is no common, comprehensive analyzing model which could be adopted for describing and analyzing one state's disaster management system. Through conclusions drawn during the analysis of foreign emergency managements, the different domestic disaster risk management methods can be improved. Hence, the phrase disaster management can be defined in several ways and those approaches determine the analyzation framework of the given country, as well. For a unified interpretation, a model needs to be created which promotes the descriptive analysis. Since the topic is actual, in this paper an analysis model is presented, which can be applied in international environments, and it can also be helpful for domestic research.

Keywords: *qualifying point, analysis level, theoretical model, international emergency management*

Introduction

The primary purpose of this paper is to attempt to offer points for analyzing state-level disaster management systems and actions. The choice of the subject is fundamentally justified by the deficiency of methodology of general description, so the mission of this research is to create a primal analysis framework. Since disaster management expends to a quite big area, one analysis cannot cover every small detail of a state's system, the negotiated aspects offer help to a general, descriptive research.

The developed rating system gives an opportunity to the international disaster science for an ovjective comprehensive model in order to provide a point for comparison of different disaster management systems. Thereby, papers can be helped which pay attention to the emergency management of a country. Moreover, this framework can be used by students and young researchers who would like to get informed about some aspects of foreign or international disaster management.

On the mentioned subject, a rightly related question arises: why is it important to investigate the disaster relief system of different states? Due to global climate change, the number of natural disasters is rising all over the world which challenges the international disaster management. [1] Examining state-level disaster relief, individual systems can be developed, so this research has practical benefits besides broadening one's horizon. Central Europe and Hungary also struggles with more and denser extreme whethear phenomenon

[1] Ph.D. student, National University of Public Service, Doctoral School of Police Science and Law Enforcement; e-mail: papp.bend@gmail.com

and its negative effects, the international scientific horizon could help the disaster relief. [2] The framework introduced here wishes to redound this development process.

Definition of Concept and Interpreting Aspects

According to the International Federation of Red Cross and Red Crescent Societies, disaster management is: *"…the organization and management of resources and responsibilities for dealing with all humanitarian aspects of emergencies."* [3]

It investigates especially preparedness, response, and reconstruction, in order to reduce the disaster's effect on the society. Disaster is an event that requires resources beyond the capability of a community and requires a multiple agency response. It includes any domestic disaster or act of terrorism that:

- suddenly requires a much larger amount of blood than usual, *or*
- temporarily restricts or eliminates a blood collector's ability to collect, test, process and distribute blood, *or*
- temporarily restricts or prevents the local population from donating blood or restricts or prevents the use of the available inventory of blood products requiring immediate replacement or re-supply of the region's blood inventory from another region, *or*
- creates a sudden influx of donors requiring accelerated drawing of blood to meet an emergent need elsewhere. [4]

The word *disaster* can be defined in several ways, depending on the approach or the actual context. David Etkin negotiated the concepts of disaster in his book *Disaster Theory* [5] from a lot of aspects, as he tried to summarize the *state-of-the-art* of disaster science. Nevertheless, if we would like to construct an essential practical definition, then disaster is an event which requires the work of organizations related to disaster management system. As the definition of *disaster* is varied, the expression *disaster management* has also plenty of meanings. If a state-level disaster management is discussed, we need an accurate, exact interpretation of the concept.

The author's first goal is to create and describe three different approaches, which are necessary for understanding the principles of the analysis. Accordingly, this paper interprets disaster management in three different ways: as an organization, as an activity, and as a science.

Disaster management as an organization means a coordinating, managing, and controlling state-related organization. In different democratic countries—where this kind of central system can be found—disaster management is related to the executive power (unlike the legislative power or the head of state-related army). Therefore, it is part of the public administration, and is responsible to the Prime Minister, one or more ministries, or an administrator assigned specifically for disaster causes. This hierarchical system is related to the Ministry of the Interior in Hungary, to the Department of Home Security in the USA, and to the Minister of State for Disaster Management in Japan. The next chapter will discuss this topic in detail.

Disaster management as an activity is covered by home defense. According to Szabó [6] home defense consists of principles, organizations, activities, and other relevant factors

which are related to defending the state from armed forces. This definitioin focuses on its military approach, for the broader concepts we need a security science approach. According to Deák [7] the subject of security can be classified in three categories: sovereignity of state, lives of the citizens, and national wealth.

Under sovereignity, territorial integrity is understood, which covers airspace and waters as well. Sovereignity can be endangered only by human factors: foreign armed forces, violent groups, or other offensive forces. Every threat against the citizens is also the subject of security, which can be caused by military or other human or non-human factors. This can endanger the lives of citizens, the society or the whole civilization. The third category contains threats against national wealth, which includes infrastructure, natural environment, cultural values, and important services.

Based on the above, this paper tries to use a broader definition for the term *home defense.* Accordingly, home defense covers all organizations, activities, and other relevant factors that have a well-defined goal of defending the security of the state, recovery and fighting the threats, consisting of military and civil elements. The military element is made up by the army and law enforcement agencies (e.g. police), the civil element includes defense management, strategic resources and other civil defense organizations. [8] In summary, disaster management is part of the home defense, under civil defense management.

Based on the above, it can be stated that the purpose of disaster management activity is to prepare for emergencies, hazard elimination, remediation, and recovery. Emergency can be caused by three types of events: [9]

- natural disaster like flood, inland water, snow, weathear phenomenon, or geological hazards (earthquake, forest fire);
- civilization-origin disaster like industrial accident, dangerous materials, waste pollution;
- other-origin disaster like epidemic, water pollution, critical infrastructure.

Different emergency situations are the subject of disaster management, so the scope of activities can be sorted based on them. The purpose of practice is defined by Mógor: [10]

- prevention of emergence;
- eliminating the causes;
- reducing harmful effects;
- defense of the citizens' lives and wealth;
- ensuring basic living conditions on the disaster area;
- recovery.

Based on this list, it can be stated that the disaster practice covers all processes related to disasters, so *disaster management activity* means a complex task system. Based on this division, it consists of the following actions:

- planning, organizing, synchronizing;
- implemention, controlling;
- installation, operation;
- informing, alarming; providing data;
- supervision.

Although disaster management differs from country to country, it has different connection network, the subdivision above defines the national practice all over the world.

The last point of this chapter is defining disaster management as a science. Alexander [11] gives seven approaches to disasters: geography, anthropology, sociology, development studies, health sciences, geophysical sciences with engineering, and social psychology. Here, it can be seen that the science of disaster management is a broad, complex science which requires an interdisciplinary knowledge.

However, the aim of disaster science is not only communicating our research and knowledge, the communication, knowledge sharing and cooperation is also needed between the actors in disaster management. These actors include three types: scientific experts, policy makers and practitioners. Scientific experts need an interdisciplinary knowledge, they have to produce scientific results and advices to politicians and practitioners, moreover, they are responsible for innovations in disaster relief. For policy makers there are two main challenges: obtaining timely advice during emergency management and obtaining reliable advice for policy making. The practitioners are responsible for solving global and local disaster-related problems, for working on a more effective communication on risk and creating clear public partnerships. [12]

This paper gives a try to define disaster science and management. It is at the frontier of three main disciplines: political science, public administration science, and technical science.

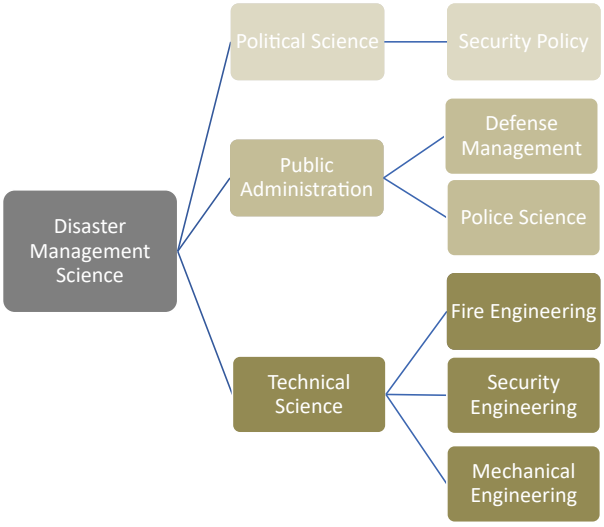

Figure 1. *Scientific classification of disaster management.*
[Created by the author.]

Under political science, security policy deals with disasters and emergencies, especially with their theoretical issues. Formerly, the science of security policy investigated only military security, where the subject of security was limited to the states and their offensive and defensive capabilities. In this approach, the role of the state was only the protection of its territory, airspace and population. According to the exceed security concept, other

meanings are also distinguished: inter alia political, economical, social, and environmental security.

Political security is equal to sovereignity, which occurs on the level of political leadership, so the subject is legitimation, ideology and international judgement. In an economical dimension, the objects of threat are resources and funds related to society's well-being. Social security deals with language, culture, religion, national identity, tradition, habits. The last category is the environmental security, where disaster management takes place. Here, the subject of investigation is the protection of the biosphere of the planet (or the state in a narrow sense). This includes every change which endangers the living conditions of the population or the society in a direct or indirect way. In this ecological sector disaster management is affected by all questions, as the environmental security covers all environmental dangers. [13]

The categorization of the science of public administration is more difficult, because—as a new research area—there is no general accepted circumscription. Political philosophy started investigating issues related to public administration quite early—from the 19th century, so a lot of definition was created, however, as the modern science it became part of university education relatively late. Broadly understood, public administration covers all topics which deal with the connection between political power, burecracy and the society (virtually every aministration issue). [14] This discipline has two relevant subdisciplines related to disaster management: defense management and police science. Defense management's research area is the defense of the population, and other defense issues related to the population: organization theory and practice, public management, humane resource management, leading management. Police science's definition is a difficult question as well, although according to Kersten, the police science' task is every state-level, local, or citizens' intention, activity, and attitude related to public order and security. [15] So, disaster management aspects of police science are: civil protection and coordination tasks. Based on the above, disaster management aspect of public administration covers—unlike security policy—practical areas of disaster management.

The third relevant category is technical science, within that fire engineering, security engineering, and mechanical engineering. Fire engineering is a part of civil engineering, its main areas are infrastructure, planning of buildings and fire prevention systems, so it supports the fire and industrial security within disaster management. Security engineering includes planning of alarm and protection systems, so its main task is building and developing disaster alert system. The most relevant area of mechanical engineering is planning and maintaining the toolkit of disaster management.

Nevertheless, we have to mention the auxiliary sciences of disaster management. First of all, other technical sciences belong here, where the main areas are environmental, conservation, water management, vehicle, and agricultural engineering. Jurisprudence plays an important role in creating and analyzing law, rules, rights and obligations related to disaster management. Psychology's research interest is coordination of the society, trauma and experience processing after emergencies. Media science has become indispensable through public informing during disasters. Meteorology as an auxiliary science ensures forecasting natural disasters and supporting preparation. Pedagogy plays also an important role, through training in schools and training of disaster relief personnel. Naturally, this list could be continued, this chapter tried to enumerate only a few of the most notable ones.

At a global level, science and technology will play a central, more important role in disaster management, so specifying the *state-of-the-art* is essential. The disaster management science's importance is outstanding in the *2030 Agenda for Sustainable Development* and other international agreements addressing Disaster Risk Management. In conclusion it can be stated, that the science of disaster management needs a comprehensive, interdisciplinary approach, as its experts come with various, multicoloured background. Disaster science has to provide science-based advice for disaster management policy-makers and practitioners, as well as scientific-based analysis for preparedness and response coordinating activities. [16]

Analysis Levels of Disaster Management Organization

As described above, the science of disaster management does not have a unified theoretical framework which could provide analytical method for examining its main fields. The international literature usually describes the national organization of a country, and it applies an appropriate framework which suits the given country's structure.[2] In other cases, [20] when the author strives for a general introduction, the disaster relief process is being presented, not the general trends of disaster management structure. Thus, a general analytical framework of structure is subordinated in the international literature.

When disaster management is discussed as a state-level organization, the following problem is faced immediately: plenty of countries—especially among the developing ones—does not have an integrated countrywide institution, sometimes a general disaster management strategy is also missing. The build-up of a system of disaster relief can be dated in the middle of the 19th century [21]—and due to developing differences, it extremely differs from country to country. Nevertheless, if a state does not have a central coordinating body, it still has some level of infrastructure and practice in fighting disasters.

In the following, an organizational model will be introduced, which can be applied to disaster management structure of all countries and provides a point for analyzing them. Due to deficiencies in some countries mentioned above, deficient levels can be found, or—in exceptional cases—the whole level could be missing. However, the model as a whole can be applied in those cases, too. The analysis of disaster management as an organization can be interpreted in four levels: mega-, macro-, meso-, and microstructure. The differentiation of the individual levels is based on their different function during relief.

Megastructure indicates the highest level of emergency management; the legal framework is meant here. Constitutional aspects of disaster management and civil defense, laws, regulations, government or ministerial level boundaries, provincial, county, local, and other, grass-roots handlers belong here. Apart from this, all the international foundations, treaties, hostages, and the provisions ratified by the state are included. In its intensity, the level extends to all written document which governs disaster prevention actions.

The next level is the level of *macrostructure*, the political level in other words. This includes all disaster management actors at the level of political decision-making. Primarly,

[2] For example, Mógor [17] goes by a method which can be used only in Hungary's case, Hanny's [18] method only in China's case, and the analysis of the Japanese Prime Minister's Office [19] shows specialities of the Japanese structure.

ministries, departments, divisions, experts, and secretaries are covered, which control and coordinate the bigger or smaller field of emergency management. If there is a central coordinating body which controls disaster-related organizations at all levels, those are also part of the macrostructure, as being the subject of political leadership owing to their extensive responsibilities. That is to say, the level of macrostructure contains the central management, its controllers, and affiliated officers of the state.

The level of *mesostructure* is the core of disaster relief. It consists of all organizations, facilities and units involved in preventive, remedial, defective and planning processes of actual disaster management activities. At that level, fire departments, civil protection organizations, meteorological services, industrial security organizations, coastal guard, civilian police, police officers, military, rescue units, volunteer units are discussed, which are taking up the task of deconstruction. Research institutes, monitoring centers that participate in preventive, controlling, and coordinating processes, or any disaster response council (provincial, county, municipal) under the national level, belongs to the level of the mesostructure. The majority of papers, documents and books, which discuss state-level disaster management, carry out their research at the level of macro- and mesostructure.

Microstructure is the smallest, but most varied level, this is the society-related aspect of emergency management, practically, every human resource-related phenomenon belongs here. Due to its wideness, the spectrum of analysis is quite extensive and the elements can be the following: public information system and informing practice, school education, material of the university training, framework and possibilities of training, social perception, cultural embedding, disasters-related folk traditions. Since this level does not cover a specific organizational unit, we can not undertake in a study to discuss all aspects of this level. In a comprehensive work, it is reasonable to focus only on training and information-alert elements of disaster relief.

Disaster Management Activity

In this chapter, the concept of disaster management activity will be introduced based on relevant international literature. Unlike the organizational structure, international organizations and researchers choose the aspect of activity when analyzing disaster management with a general intent. At international disaster science, two structures are applied, which in this paper will be called *vertical* and *horizontal* aspects. At vertical level, the individual disaster types and their special relief methods are discussed, its question is: *against what?* In case of horizontal level, the linear process is the subject of investigation, the describing of the state-level *disaster management cycle* is the target. Its question is *how?*

In the negotiation of the *vertical* level, over the analysis of each type of disaster, possible special prevention, prevention and preparation processes need to be included as well. There are several principles for defining each group: the origin of the disaster, the magnitude of the damage, and the quality of the necessary measure. The most applied division is the International Federation of Red Cross and Red Crescent Societies' one which follows categorization by origin. Accordingly, two disaster types are distinguished: natural and technological (also known as human origin) ones.

Within natural disasters, geophysical (earthquakes, landslides, tsunamis and volcanic activity), hydrological (avalanches and floods), climatological (extreme temperatures, drought and wildfires), meteorological (cyclones and storms/wave surges) or biological (disease epidemics and insect/animal plagues) can be differentiated. Technological ones include environmental degradation, pollution and accidents, technological or man-made hazards (complex emergencies/conflicts, famine, displaced populations, industrial accidents and transport accidents). [22]

The systematization of Dey and Singh is more thorough than the classification of the Red Cross, its approach also uses the aspect of the disaster's origin.

Table 1. *Types of Hazards.* [23]

Types	**Hazards**	
Geological	1. Earthquake 2. Tsunami 3. Volcanic eruption	4. Landslide 5. Dam burst 6. Mine fire
Water & climatic	1. Tropical cyclone 2. Tornado and hurricane 3. Floods 4. Drought 5. Hailstorm	6. Cloudburst 7. Landslide 8. Heat & cold wave 9. Snow avalanche 10. Sea erosion
Environmental	1. Environmental pollutions 2. Deforestation	3. Desertification 4. Pest infection
Biological	1. Human/animal epidemics 2. Pest attacks	3. Food poisoning 4. Weapons of mass destruction
Chemical, industrial and nuclear accidents	1. Chemical disasters 2. Industrial disasters	3. Oil spills/fires 4. Nuclear accidents
Accident related	1. Boat/road/train accidents/ air crash, rural/urban fires, bomb/serial bomb blasts 2. Forest fires	3. Building collapse 4. Electric accidents 5. Festival related disasters 6. Mine flooding

Disaster types can be categorized according to their peril, though this classification may vary considerably between countries and regions. The figures below were made by the author based on the data of The International Disaster Database, aiming to illustrate the danger of disasters. Figure 2 shows deaths caused by disaster types worldwide.

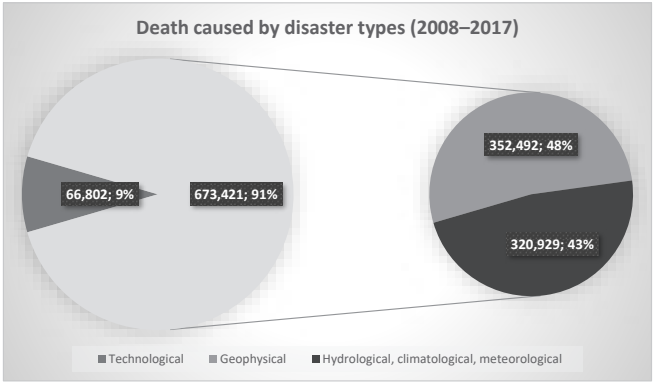

Figure 2. *Deaths caused by individual disaster types (2008–2017).*
(Created by the author based on [24].)

As it can be seen, in the period from 2004 to 2013, disasters of technological origin had the least victims, with traffic accidents (45,810) in the majority. 91% of the deaths were caused by natural disasters, mainly geophysical types. Within geophysical disasters there are almost entirely tsunamis and earthquakes, and as they often occur at the same time, the deaths of both have been registered (351,817) the most. The most dangerous type among natural ones was the category of climatological, meteorological and hydrological disasters, the most relevant ones were wind storms (166,123) and extreme temperature (73,568 persons).

On Figure 3, the same categories are shown, although it is based on the magnitude of damage in million dollars caused by the disaster:

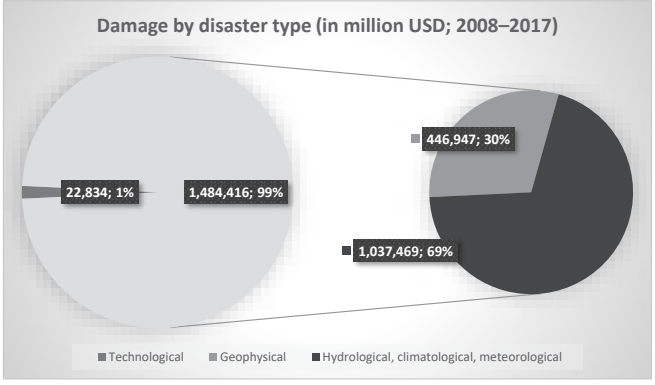

Figure 3. *Magnitude of damage by disaster types (in million USD, 2008–2017).*
(Created by the author based on [24].)

Figure 3 also accounts for the damage occurring over the nine-year period starting in 2004. The rate between technological and natural disasters is similar to before (the danger of natural disasters is overwhelming), but the rate of technological disasters has dropped from

9% to 1%. In case of disasters with natural origin, however, the rate has been reversed, the damage caused by geophysical disasters is 30% as the number of all disasters. Almost all the damage caused by geophysical disasters (USD 446.05 billion) was caused by earthquakes and tsunami. In the other category, wind storms (USD 544.70 billion) and floods (USD 358.42 billion) can be classified as rather dangerous ones.

The other level of disaster management activity is the *horizontal* level, in other words, the disaster management cycle. According to Corina Warfield *"the Disaster management cycle illustrates the ongoing process by which governments, businesses, and civil societies plan for and reduce the impact of disasters, react during and immediately following a disaster, and take steps to recover after a disaster has occurred."* [25] Its three main phases are: pre-disaster, emergency response, and post-disaster ones.

The pre-disaster phase is primarily aimed at risk reduction and preparation. At this stage, besides disaster management organization, the active contribution of political decision-making, executive power, and smaller, provincial, and municipal governments are needed. Creating a legal background is essential for the development of a successful defense system, which although belongs to the public policy, the professional background is provided by disaster management. Preventive measures include all monitoring activities which collect and analyze data about risk and vulnerability, they serve as a basis for defense measures and relief models. In conlusion, the pre-disaster phase contains all measures which support the development of defense task system, also including training, education and planning the alarm system. [26]

The emergency response section can be divided into two additional units: primary and long-term intervention. Most of the steps and measures planned in the pre-disaster phase are fulfilled in this one. In the primary phase, local organizations intervene and act according to their pre-agreed principles and action plans, the central body and the political body are collecting data, evaluating the event and determining additional measures. As part of the long-term phase, the problem gets explored, the compensation gets defined and ordered. The central organization is responsible for the provision of special emergency rescue tasks and organizes the civil defense tasks (protection of the population, supply of food and drinking water, medicine supply, trauma management). The duration of emergency response phase is short, up to a few weeks. [27]

The post-disaster phase's main task is restoration and reconstruction, rehabilitation of the population's condition, reparation of the damage and rebuilding the infrastructure. The aim is to reach a pre-disaster status or a higher level of welfare, which means re-establishing the information system, education system, public administration, economic infrastructure, and stability. This phase also includes lessons learned, evaluation of data, and the foundation of the development strategy that anticipates preparation and prevention. Quick recovery can take months to months, while full reconstruction for up to years. [27]

Levels of Disaster Management Analysis

In order to be able to resemble individual state-level disaster management organizations in a scientifically modest way, an analysis of an elementary aspect is required. Each level of examination has been designed to make a broad comparison possible through the analyzed

data. Elements of analytical levels and critical elements are summarized by the following outline. When editing, the author used Rihmer's lexicographical work [28] as an initial point.

Possible aspects of state-level analysis of disaster management (outline)

I. Information about the country (background)

a) Geographical feature of the country, broadly the region, possible environmental risk factors:
   - natural environment: large footprints, mountains, deserts, rivers, coasts, features of weather phenomenon (rain, drought, temperature);
   - social-economical environment: distribution of population, urbanization, industrialization, infrastructural facilities.

b) Relevant disaster types:
   - categorization by frequency, economic damage, and affected people;
   - presenting specific, typical disaster types of the region.

II. Analysis of the system

c) Megastructure (legal framework):
   - appropriate sections of constitution, law, decrees;
   - international contracts, statutes;
   - action plans, strategy.

d) Macrostructure (political level):
   - ministries, state organs, subordinate organs, divisions, specialists, ministers, politicians and referents who are responsible for the whole or a part of emergency management;
   - central, coordinating body (if any).

e) Mesostructure (practical units):
   - fire-fighters, civil defense organizations, meteorological services, industrial security organizations, coastguards, police, gendarmerie or military personnel, rescue units, voluntaries, research centers, agencies, think-tanks, advisory offices.

f) Microstructure (social aspects):
   - informing organizations, media;
   - educational institutes, offices responsible for training the society;
   - disaster awareness in the society;
   - cultural phenomenon, habits, beliefs, traditions, folktales;
   - other social phenomena related to disasters and emergency management.

III. Analysis of activity

g) Vertical level (*against what?*):
   - characteristics of coping with disaster types;
   - special challenges and methods.

h) Horizontal level (*how?*):
   - applying disaster management cycle to the country;
   - each phase, practical application of plans.

IV. Qualitative analysis

i) Presenting the actual disaster relief through a case study;
j) Experiences based on fieldwork and observation;
k) Criticism of practical operation.

Naturally, this system can be expanded, according to new challenges and hazards.

Summary

The purpose of the author was to set up an analysis model for presenting and analyzing state-level disaster management organizations and their activity. The created framework is useful for only a general description of a country's emergency management; a detailed analysis is possible only with further enlargement. The proposed levels interpret disaster management from two aspects: as an organization and as an activity.

It is advisable to begin the analysis with a generic country presentation; accordingly, the geographical features and typical disasters of the region should be presented. The country system can be examined at four levels, which gives the mega-, macro-, meso- and microstructure level. The actions can be analyzed on two axes, which is displayed in a vertical and horizontal dimension. The analytical earnings are suggested by a case study or some other criterion criticism that emphasizes the presentations, organizations, and action plans presented earlier, and can therefore serve as a basis. At the end of the analysis, a case study or other criticism is suggested which supports the practical application of previously presented institutions, organizations and action plans and can serve as a basis for evaluation.

The various domestic disaster management sciences' primer purpose is to support its own state-level system and activity. For efficient work, however, the knowledge of international scientific methods and experiences are indispensable, by which the individual domestic processes can evolve. In this sense, the number of international disaster research will hopefully grow, this paper would like to join them as well.

Acknowledgement

Supported BY the "ÚNKP-17-3-2-NKE-9 code ÚNKP – New National Excellence Program of the Ministry of Human Capacities".

References

[1] KUTI R., FÖLDI L.: Extreme weather phenomena, improvement of preparedness. *Hadmernök*, 7 3 (2012), 60–65.
[2] KUTI R., NAGY A.: Weather Extremities, Challenges and Risks in Hungary. *Academic and Applied Research in Public Management Science*, 14 4 (2015), 299–306.

[3] *About disaster management. International Federation of Red Cross and Red Srescent Societies.* www.ifrc.org/en/what-we-do/disaster-management/about-disaster-management/ (Downloaded: 31.08.2017)
[4] BLANCHARD, W.: *Guide to Emergency Management and Related Terms, De initions, Concepts, Acronyms, Organizations, Programs, Guidance, Executive Orders & Legislation.* A Tutorial on Emergency Management, Broadly Defined, Past and Present, 2008. http://training.fema.gov/EMIWeb/edu/docs/terms%20and%20definitions/Terms%20and%20Definitions.pdf (Downloaded: 22.09.2017)
[5] ETKIN, D.: *Disaster Theory.* Amsterdam: Elsevier, 2016. https://doi.org/10.1016/B978-0-12-800227-8.00002-8
[6] SZABÓ J. (szerk.): *Hadtudományi Lexikon.* Budapest: Magyar Hadtudományi Társaság, 1995.
[7] DEÁK A.: *Biztonságpolitikai kézikönyv.* Budapest: Osiris, 2007.
[8] ISASZEGI J. (szerk.): *Magyarország védelmi igazgatása a közigazgatás új környezetében.* Budapest: HM Zrínyi Nonprofit Kft. – Zrínyi Kiadó, 2014.
[9] ETKIN, D.: *Disaster Theory.* Amsterdam: Elsevier, 2016.
[10] MÓGOR J.: *Katasztrófavédelemins.* Budapest: CompLex Kiadó, 2009.
[11] ALEXANDER, D.: *Confronting Catastrophe.* Washington D.C.: Terra Publishing, 2000.
[12] CLARK, I., de GROEVE, T., MARÍN FERRER, M., POLJANŠEK, K., FAIVRE, N., PETER, D., QUEVAUVILLER, P., BOERSMA, K. E., KRAUSMANN, E., MURRAY, V., PAPADOPOULOS, G. A., SALAMON, P., SIMMONS, D. C., WILKINSON, E., CASAJUS VALLES A., DOHERTY B., GALLIANO, D.: Future challenges of disaster risk management. Chapter 6. In. POLJANŠEK, K., MARÍN FERRER, M., de GROEVE, T., CLARK, I. (eds.): *Science for disaster risk management 2017: knowing better and losing less*. Luxembourg: Publications Office of the European Union, 2017.
[13] GAZDAG F. (szerk.): *Biztonsági tanulmányok – Biztonságpolitika.* Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2011.
[14] *Public Administration: An Art or a Science. Management Study Guide.* http://managementstudyguide.com/public-administration-an-art-or-science.htm (Downloaded: 19.10.2017)
[15] KERSTEN, J.: Was versteht man unter „Polizeiwissenschaft“ – Eine programmatische Standortbestimmung. *Neue Kriminalpolitik*, 24 1 (2012), 8–10.
[16] BOWER, A., BLOCK, J., DALI, M., FAIVRE, N., FELL, T., GHISLAIN, P., HAPPAERTS, S., KAVVADAS, I., KOCKEROLS, P., MOLNAR, A. M., QUEVAUVILLER, P., VILLETTE, F.: Current status of disaster risk management and policy framework. Chapter 1. In. POLJANŠEK, K., MARÍN FERRER, M., de GROEVE, T., CLARK, I. (eds.): *Science for disaster risk management 2017: knowing better and losing less.* Publications Office of the European Union, Luxembourg, 2017.
[17] MÓGOR J.: *Katasztrófavédelem.* Budapest: CompLex Kiadó, 2009.
[18] HANNY Á.: *Katasztrófavédelem a Kínai Népköztársaságban.* Budapest: Tajvani Véndiákok Magyar Egyesülete, 2013. http://mytaiwan.hu/wpcontent/uploads/2013/12/Hanny-%C3%81kos-Akatasztr%C3%B3fav%C3%A9delem-a-K%C3%ADnai-N%C3%A 9pk%C3%B6zt%C3%A1rsas%C3%A1gban.pdf (Downloaded: 22.09.2017)
[19] 内閣府：日本の災害対策． 日本の内閣府 Tokyo, 2015.
[20] KHAN, H., VASILESCU, L. G., KHAN, A.: Disaster Management Cycle – a Theoretical Approach. *Management and Marketing Journal*, 6 1 (2008), 43–50.

[21] SZILÁGYI J., SZABÓ K.: *A tűzrendészet fejlődese az őskortól a modern időkig.* Budapest: BM Könyvkiadó, 1986.
[22] *Types of disasters: Definition of hazard. International Federation of Red Cross and Red Crescent Societies.* www.ifrc.org/en/what-we-do/disaster-management/about-disasters/definition-of-hazard/ (Downloaded: 23.08.2017)
[23] DEY, B., SINGH, R. B.: *Natural hazards and disaster management.* Delhi: Natural Hazards and Disaster Management, 2006.
[24] GUHA-SAPIR, D., BELOW, R., HOYOIS, Ph.: *The CRED/OFDA International Disaster Database.* Brussels: Université Catholique de Louvain. www.emdat.be (Downloaded: 17.01.2018)
[25] WARFIELD, C.: *The Disaster Management Cycle.* Kóbe: The Global Development Research Center. www.gdrc.org/uem/disasters/1-dm_cycle.html (Downloaded: 05.09.2017)
[26] PAPP B.: Állami szintű katasztrófavédelem elemzési szempontjai nemzetközi környezetben. *Védelem Tudomány* 2 1 (2017), 263–284.
[27] KHAN, H., VASILESCU, L. G., KHAN, A.: Disaster Management Cycle – a Theoretical Approach. *Management and Marketing Journal*, 6 1 (2008), 43–50.
[28] FÓRIS Á., RIHMER Z.: A szótárak minősítési kritériumairól. *Fordítástudomány,* 9 1 (2007), 109–113.

AARMS Vol. 17, No. 1 (2018) 45–52. **10.32565/aarms.2018.1.5**

Designing Complex Technical Rescues with a Proprietary Application (Computer Program)

Csaba HAJDU,[1] Rajmund KUTI[2]

Handling emergencies caused by different environmental and civilization catastrophes, [1] (e.g. extreme weather, flood, severe industrial accidents involving dangerous substances, possible terror activities) is an ever-increasing challenge for damage control rescue entities. Efficient executing of these tasks requires ever increasing preparedness of intervention units, constant technical equipment development, introduction of new technical rescue tactics and complex intervention plans.

Executing such a complex rescue plan is an extremely complicated task. At a given situation more units are to be coordinated in several disaster areas (sites). Several special technical rescue tasks have to be pre-planned to increase the efficiency of the interventions. The authors would like to help these planning efforts by an originally developed proprietary force-unit calculation application (software) program, described in this article. The possible applications, technical requirements, detailed usage steps are also described.

Keywords: *complex technical rescue, disaster relief planning, force-unit calculation, originally developed proprietary application (software) program*

Introduction

In case of simple accidents with a high number of occurrence technical relief operations usually are not problematic. It is easy to identify force-equipment to be used in such relief efforts based on similar past events. In more severe cases after evaluation, the Operations Control decides the forces and equipment to be alarmed. Their work is supported by different expert programs and databases. [2] If the alarm call is not received by Operations Control, but by the given facility or voluntary fire rescue then the Commanding Officer (CO) decides about the units and technical equipment to be mobilized. In this situation based on past experience the CO quickly evaluates whether the mobilized units and equipment is sufficient for the rescue effort. The decision is only verified on the actual disaster site, where the alarm level can be modified by the fire, rescue operation site commander. These decisions can be highly supported by an application which helps in allocation of the force-equipment. [3]

Such a decision supporting application is developed which helps the users especially in force-equipment allocation and alarm level determination.

[1] MSc student, Budapest University of Technology and Economics; e-mail: h12csaba@t-online.hu
[2] Ph.D. (Military Technology), Associate Professor, Széchenyi István University, Department of Mechatronics and Machine Design; e-mail: kuti.rajmund@sze.hu

Planning Basics

Planning technical rescue operations is not an easy task. It is expedient to plan operation steps in advance for better coordination, accuracy and saving time and life. In rescue operations units use special gear and technical equipment.

First, the list of available systematized equipment (gear) in Hungary has to be created in an equipment library. Special vehicles which carry rescue equipment, different special substances used in fire rescue operations are included in this library.

Manpower necessary for operation of the equipment which has to be taken into account during planning is defined in the professional guidelines for the equipment.

A User-Friendly User Interface is developed. During rescue operation time component is crucial, so simple handling, easy overview, speed, reliability are primary requirements. Experiences gained during past rescue operations are also taken into account.

During application planning tasks to be executed by fellow rescue organizations had to be also overviewed. It is known that gas body suits are very heavy to use as it is very hard to move in them and the respiratory equipment exhausts the rescue officer, so they have a very limited energy and time for actual work. Consequently, backup manpower has to be planned and provided by the application.

Overview of Computer Force-Equipment Calculation

The hardware and configurational requirements of the application program are average. It can be run on every PC where the NET framework is installed (deployed).

The calculation is based on the available technical equipment and on required manpower defined in the operation's security manuals (directives). The application user has to enter only the rescue site and the required technical equipment quantity in input fields (left white), and the special substances if necessary. Based on the planned number of squads the application offers the alarm level qualified with BM regulation 39/2011 (XI. 5.) about "Common regulations about fire and rescue operations." If special substances are to be carried, the application offers special (emphasized) alarm execution (which is also displayed).

During rescue operations there can be additional tasks that cannot be foreseen. To address these situations additional preplanning is required, to avoid reclassifying and regrouping of tasks. The application gives possibilities for these.

The layout of User Interface of Force-equipment calculation application program with extensions is given on the next diagram.

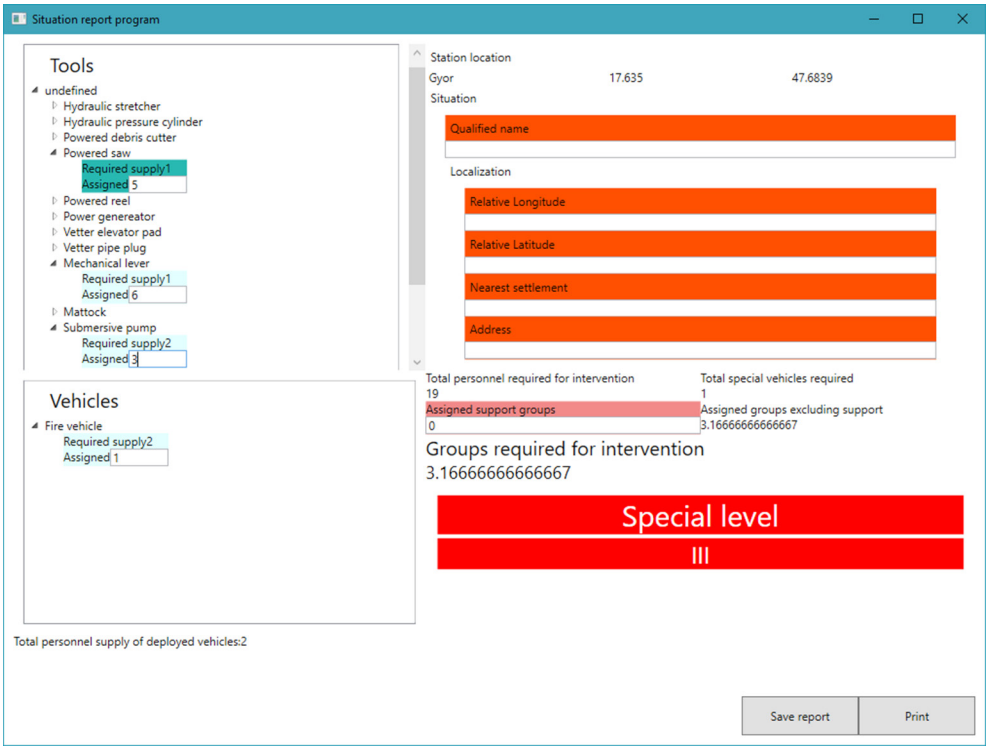

Figure 1. *Target program operation example.* [Edited by the authors.]

Filing out the input fields is easy as it is only possible to input data in the white fields. Other fields are write protected, to avoid overwriting of mathematical formulae.

Where numbers are displayed in red, the computer fills them automatically.

The lowest red bar is the calculated alarm level by the application program based on input data.

Structure of the Recommender System

The Recommender System process has two components. The process and the components are identified on Figure 2. With the target program an alarm level can be set for an incoming rescue operation. The second component *(Inventory description editor)* generates the list of equipment according to regulations with the help of an internal *generator component* interpreting the abstract description. This list is used by the *target user program.* During the execution of the program the list of the available force-equipment must not be changed.

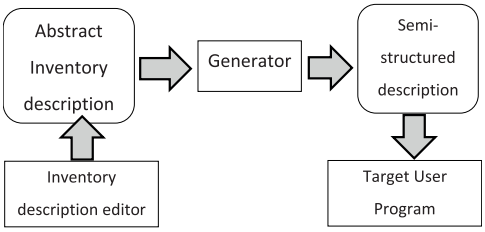

Figure 2. *Description of the configuration generation process.* [Edited by the authors.]

The list is produced by an Eclipse-based editor. A force-equipment can be modelled as a labelled weighted element, where the weight corresponds with the personnel needed to operate the equipment. Breaking down on the context of the problem vehicles are differentiated from other equipment. The model is based on Eclipse-Ecore (Eclipse Modelling Framework – EMF); [5] there is a possibility of creating a textual description language. The Xtext [6] [7] framework provides an efficient way to produce a text editor fitting the problem-specific language that is derived from the meta-model of the inventory description. The text language should be unambiguous and transparent like natural languages in order to be easy to learn even without programming skills and experience. This editor generates a semi structural file (in XML format) after every change.

The target program reads equipment (device) inventory generated description. The user has limited possibilities to change certain fields. The number of deployable force-equipment and the description (unique name, alarm site, etc.) of the alarm can be changed only. The input data should be strictly controlled by the program. Exemptions and bad data should be treated also (e.g. negative or fractional number of deployable units etc.). After data input the report can be saved in a text format or printed out on the default printer.

The usage can be demonstrated through a simple example; an alarm about a vehicle accident carrying gaseous explosive material comes in. The necessary assets are detached from the equipment library for emergency handling. This is increased by the weighted manpower necessary for the unit. If a vehicle (e.g. technical rescue, special substance) is necessary, the alarm level automatically escalates to extensive (critical) and the number of manpower needed to operate the vehicle is added to the result. According to regulations, the number of squads (per 6 person) can be determined. The program recognizes complete and half squads. Further squads can be assigned for tasks not foreseen.

In summary the complete deployable weighted manpower for operation of vehicles and equipment can be produced. (Figure 3)

$$|personnel| = \sum_{i=0}^{|vehicles|} capacity(vehicle[i]) \times count(vehicle[i]) + \sum_{i}^{|tools|} capacity(tool[i]) \times count(tool[i])$$

Figure 3. *Final manpower equation.* [Edited by the authors.]

The structure of the developed meta-model is depicted on the following UML Class diagram (Figure 4), the basis of the textual tool describing an inventory set. Notice that the inventory contains two distinctive categories of inventories: vehicle and tool inventories. Both inventories are filled with corresponding tools and vehicles, both elements derived from an abstract inventory element type. Also, the inventory contains information about the location of the emergency station (name, latitude and longitude).

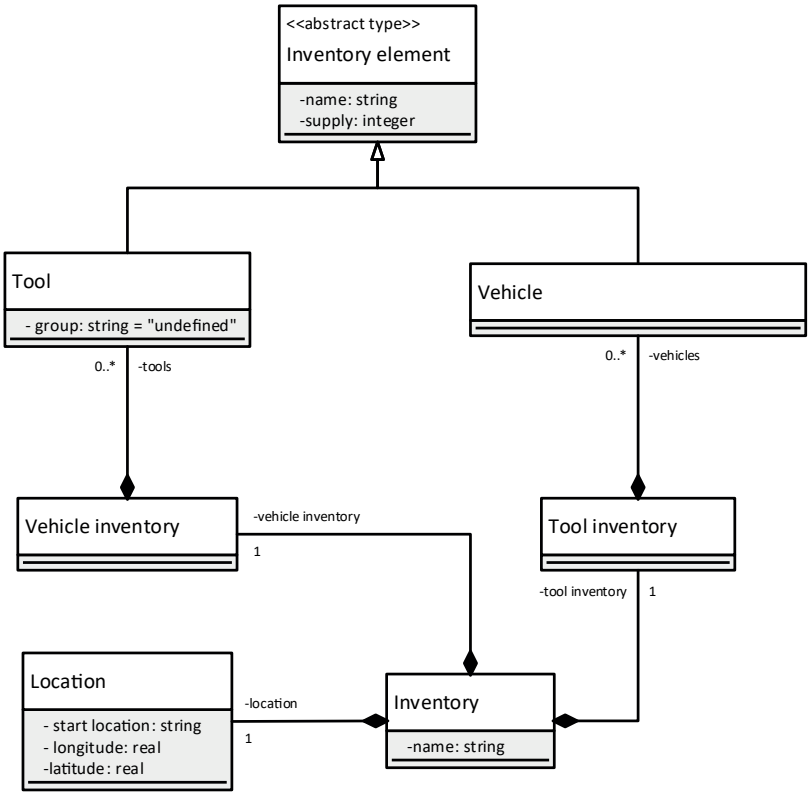

Figure 4. *Structure of inventory meta-model.* [Edited by the authors.]

The equipment library can be abstractly modelled in context of the problem. In the library vehicles are differentiated from other equipment because deploying even one vehicle leads to another level of alarm. In the problem context vehicles and other equipment can be characterized with common attributes (name, manpower required for the operation etc.). Common devices can be rated in groups for an easier overview. For program operation and ordering of an alarm it is necessary to note from which station the alarm was originated. It is feasible to store these data in the configuration of the Target Application (e.g. station name, city, geographical coordinates etc.).

Description Language

The description language follows the syntax of ALGOL/Pascal that fits into the meta-model of the equipment library. Equipment library is described in a structural form, so first the universal description of the equipment library should be given (unique name for the equipment library). After that the vehicles and further equipment can be characterized. The attributes of certain equipment are given divided by line space. All characteristics should be given—excluding groups of equipment. (Figure 5)

```
inventory DefaultInventory
  toolinventory
    tools
      tool Squirt
        supply: 2
        group: Liquid actuator
      end tool
      tool Precision drill
        supply: 1
        group: General tool
      end tool
      tool Powered hammer
         supply: 2
      end tool
      tool Powered debris cutter
         supply: 3
         group: Powered tool
      end tool
…
      tool Powered mattock
         supply: 1
         group: Technical rescue tool
      end tool
      tool Powered reel
         supply: 2
         group: Technical rescue tool
      end tool
    end tools
  vehicleinventory
    vehicles
      vehicle Fire vehicle
        supply: 2
      end vehicle
      vehicle Daru
         supply: 2
      end vehicle
      vehicle Chemical container
         supply: 2
      end vehicle
      vehicle Technical Rescue Vehicle
         supply: 2
      end vehicle
    end vehicles
   station
         location Gyor
                  latitude 47.6839
                  longitude 17.635
         end location
end inventory
```

Figure 5. *Equipment library description example.* [Edited by the authors.]

The equipment library was uploaded with data concerning systematized equipment associated with the number of required operating personnel. The equipment library can be extended after procurement and systematization of a new equipment.

The handling of the Application is easy, UI is user friendly, different deployment scenarios can be evaluated, tested in short time. The result of the tests can be printed out. Further steps can be decided after result comparison. The data is stored in a structural form after the program is run, allowing further data analysis and evaluation.

Conclusion

After testing the application, the conclusion is reached that it can be of valuable help in supporting decisions about alarm level determination.

Handling is easy, results are quickly displayed, results can be printed out if required. Databases (libraries) are extendable, so newly developed equipment can be included. This is crucial for the up to date operation.

It is also proved that the application is capable of analysis of past technical rescue operations. The result of this analysis can be used for case studies.

Summary

The developed application program supports decision making of pre-planned tasks and personnel assignment for rescue operations therefore these operations are quicker and easier executed.

The application program can be used for situation training planning, stored data is saved, can be printed out data and the necessary force-equipment is perspicuously laid out. The validity of the proposed alarm level, the availability of necessary equipment can be evaluated during drills, so gained experience can be used during live rescue operations.

Complex, combined technical rescue operations are becoming efficient if the parts of the system are chosen according to the task goal. To achieve that a complex technical rescue operation reaches suitable results, all the following factors are necessary:

- suitable equipment,
- appropriate staff with protecting gear,
- trained and prepared personnel,
- appropriate tactics.

Decision supporting computer applications and experience gained on pre-planned technical rescue drills (exercises) support the elaboration of appropriate rescue tactics.

Increased attention should be focused on possibilities offered by Information Technology (IT) also. The main goal is however that the rescue operation should be started in the shortest time frame from the event with the greatest efficiency and optimal usage of available resources (equipment), so the damage handling (liquidation) can be done more quickly.

References

[1] HALÁSZ L., FÖLDI L., PADÁNYI J.: Climate Change and CBRN Defense. *Hadmérnök*, 7 3 (2012), 42–49. http://hadmernok.hu/2012_3_halasz_padanyi_foldi.pdf (Downloaded: 15.08.2017)

[2] MOLNÁR R.: A tűzoltói beavatkozások hatékonyságát növelő fejlesztések az egységes katasztrófavédelmi rendszerben. *Műszaki Katonai Közlöny,* XXVII 3 (2017), 131–145. http://hhk.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/PDF_2017_3sz/2017_3sz.pdf (Downloaded: 20.09.2017)

[3] KUTI R.: Komplex műszaki mentések tervezésének lehetőségei. *Védelem Online. Tűz-és Katasztrófavédelmi Szakkönyvtár,* 233 (2010), 1–7. www.vedelem.hu/letoltes/anyagok/233-komplex-muszaki-mentesek-tervezesenek-lehetosegei.pdf (Downloaded: 20.09.2017)

[4] PADÁNYI J., FÖLDI L.: Tasks and Experiences of the Hungarian Defence Forces in Crisis Management. *Bilten Slovenske Vojske,* 17 1 (2017), 29–46.

[5] *Eclipse Modeling Framework (EMF).* www.eclipse.org/modeling/emf/ (Downloaded: 20.09.2017)

[6] BETTINI, L.: *Implementing Domain-Specific Languages with Xtext and Xtend.* Birmingham: Packt Publishing, 2013.

[7] *XTEXT homepage.* www.eclipse.org/Xtext/ (Downloaded: 20.09.2017)

AARMS Vol. 17, No. 1 (2018) 53–70. **10.32565/aarms.2018.1.6**

Smart Military Electrical Grids

Zsolt VÉGVÁRI[1]

Today's society is increasingly dependent on electricity and the armed forces also face this problem. In this regards the issue of providing electricity in field conditions when power lines are not available is extremely interesting. The technology of the generators used in the fields has developed only at a minimal level over the past half century while the demand for electricity has multiplied. Logistics becomes more and more difficult and fuel caravans are one of the most vulnerable parts of military actions. Smart grid technologies based on RES[2] *are no longer a novelty for civil engineering. How are these used in military environments and what are the limits of their application? These are the questions I would like to find some answers to.*

Keywords: *smart grids, hybrid power supply, field power supply*

Global Challenges of Energy

Energy is an indispensable element of our modern civilization. In prehistoric times people were a part of the nature and they used their environment like any other organism, but about 5,000 years ago mankind began to change the environment in order to survive. The creation and the maintenance of the artificial environment needed a lot of energy but the available energy—manpower and animal power—was limited for centuries. By and by mankind discovered how to use the power of water and wind but the real breakthrough was the spread of fossil energies. Now the total energy consumption of the World is more than 13 billion tonnes oil equivalent (TOE)[3] [1: 8] and the 85% of this amount comes from fossil sources.[4] Nowadays sustainable development is a keyword in modern science and the yield, the transportation and storage of the necessary energy is a really big challenge for us. Unfortunately, by using this extremely huge amount of energy, human activities changed the climate of the whole planet so only bringing up the energy is no longer enough, we have to find better and cleaner ways than ever before.

Since of its development electrical energy is getting a bigger part of the energy consumption of the World. In 2017 it was 24,816.4 TWh. [1: 46] In SI units this 89,339 million GJ means that one third of the primary energies turned into electricity[5] before the final use.

---

[1] Lieutenant Colonel, Senior Executive Officer in the Defence Technology Research Centre of the Hungarian Ministry of Defence; National University of Public Service, Doctoral School of Military Engineering; e-mail: vegvari.zsolt@hm.gov.hu

[2] Renewable Energy Sources.

[3] One-litre of crude oil contains about 38.5 MJ energy in SI units. One-litre crude oil is 0.85-0.95 kg so one ton contains about 41.8 GJ. 13,276.3 million TOE = 555,852.1 million GJ.

[4] Crude oil, natural gas and coal.

[5] The efficiencies of the methods of producing electrical energy are very different. A PV panel has only 20-25%, but the best power plans have about 50%. In this calculation I counted half of the total used primary energy changed into electricity.

Now it's the most important secondary energy[6] because of its flexibility and easy usability. Electricity can be produced from any other kind of energy. Usually we use generators powered by heat energy of fossils, nuclear reaction, water or wind but there are methods for direct transformation too. Semiconductor devices can generate electrical energy directly for example from temperature difference (Peltier-cells) or solar radiation (solar cells or PV cells[7]). Of course, it is similarly simple to transform the electricity into any needed types of end use energy. The high voltage electric power line is the most economical way of energy transport because its loss is less than 1% every 100 kilometres. [2] The greatest challenge of electricity of our days is storage. Batteries are very easy to handle but their energy density[8] is substantially less than fossil fuels.

Electrical Energy Issues in the Security Domain

Energy is also very important for the defence sector. In ancient times warfare was absolutely based on manpower and horsepower, but after the industrial revolution it changed totally. In WWII a daily operation of a single soldier took 4 litres of oil equivalent energy. In the Vietnam War it was more than 33 litres of oil equivalent and during the Iraqi mission a single allied soldier needed 81 litres of oil equivalent of energy a day. [3: 2] Based on these data we can conclude that defence is an extremely energy-intensive field of the human activities and the energy necessity of the military actions expectedly will grow in the near future.

Until the beginning of the 20th century armies didn't use electricity at all. The first electrical military devices—the telephones were released during WW1 but their petty consumption was able to be supplied by batteries. Between the world wars radio equipment became the most important communication device but the energy demand of the contemporary vacuum tube amplifiers and other circuits was extremely high compared to the telephones. Because of the low energy density of the batteries the needed electricity was no more "portable", it had to be generated "in situ". Interestingly enough, not so many other electric devices were used by armies. Petroleum was commonly used for camp lighting and the primary source of heating was simple firewood.

After WW2 camp lighting fully changed into electrical systems; then air conditioners, computers and other electrical devices also appeared. Now no modern armies can exist without electrical energy and this is especially true for the deployed units, as temporary military camps are totally based on electricity. As we can see, electricity is an essential part of temporary military accommodation if the military operations are taking place where there is no infrastructure or it is damaged, so the very comfortable and cheap wired power supply is unavailable. Producing the necessary energy under these harsh conditions is already a really serious challenge. However, the expected demands will increase even on the basis of currently existing technologies and we must be aware that most of the future technologies are also significant electrical consumers. The development potential of

---

6 Primary energy means energy sources that can be found in nature like fossils or renewable energies. Secondary energies are carriers of energy transformed from primaries by human engineering.

7 In the photovoltaic devices the incoming photons between semiconductor layers induce electron flow without any concomitants like motion, noise or heat.

8 Energy density is the amount of energy stored in a given space or weight for example J/m^3 or kWh/kg.

traditional armament technologies are getting narrower and the future weapons will need an extremely huge amount of energy—in most cases in electrical form. [4: 7]

The Evolution of Electricity Production in Field Conditions

As it was mentioned, the first military electrical devices were supplied by batteries, but further on by using radios, the electricity demand exceeded the possibilities of battery technology, so application of electric rotating machines was needed for electrical power generation. The first electric rotating machines were based on human muscle strength and were called "pedal-generators". As radios needed DC, these types of equipment applied dynamos.[9] This solution was very simple, reliable and there was no need for fuel supply but its performance was limited to the human body. That is why lots of countries developed their own generators powered by gasoline engine in the 1930s of the last century. These developments were independent but similar demands resulted in very similar devices. [5: 571]

Figure 1. *German TP5 pedal-generator before WW2.* [17]

At the same time almost exclusively, radio equipment needed field electricity independently from those vehicles that had an on-board electric grid. It means that the majority of field generators were a part of a radio station. Most of the armies were not fully mechanized, for example the Hungarian forces also used horse drawn wagons to transport their radios so

[9] Dynamo is a type of electric rotating machine providing direct current (DC).

the weight of the generators was very important. These generators used gasoline. The diesel engines had better efficiency but their construction was more complicated and that was not an advantage in field conditions. As most of the vehicles also consumed gasoline there was no need to create a new fuels supply chain. Lying cylinder arrangement were often used in order to reduce the resonance. The air cooled, two-stroke boxer engines were very undemanding and easy to maintain. [5: 572]

Figure 2. *A typical small gasoline generator US GE-12-G from WW2. It has a 0.5 kW air-cooled 2-stroke 2-cylinder engine and produces 12 volts DC.* [5: 572]

The applied electrical rotating machine was usually a dynamo, even though it was already well known that alternators[10] were more efficient and their performance was less dependent on the rotating speed of the engine. Alternators produce alternate current, but radios needed direct current, and the contemporary rectifiers were big, heavy and also made significant power loss. [6] As 80–90% of the power consumption of radios was made by heating the vacuum tubes, the actual power supply didn't depend on the working mode. This almost constant power demand was favourable for dynamos. The engine, the fuel tank, the dynamo and the attached connectors, etc. were installed on a simple welded steel frame without any cover in order to reduce the weight.

After WW2 diesel engines were widespread in land vehicles and their usage in field generators became more favourable owing to their better efficiency. Later on, more and more parts of the equipment of the camp accommodation became electrified and most part of the used electrical devices was the same as the ones used in the barracks. As the deployed units increasingly needed the same electrical power as in their peace-time quarters, the same electrical networks were installed in the temporary camps, too. The critical

[10] An alternator is a type of electric rotating machine providing alternate current (AC).

info-communication elements still kept their individual small generators but all other consumers were linked into a grid supplied with one really big generator. Nowadays these generators are one of the most important pillars of the field logistic supply system. Their power contains hundreds of kW-s and can supply even a full battalion. Normally these sets are towed or self-propelled ones, and rarely mounted in a standard commercial container.

Figure 3. *US MEP–805A 3 tons towed military generator driven by a John Deere 4 strokes diesel engine. Max output is 30 kW AC. It has EMP proof capability and quiet working method for tactical missions.* [18]

During real military missions the primary goal is always completing the mission, the secondary goal is reducing the casualties and only then can saving money or the environment be considered. So, if we need more electrical power in the future for our deployed military units it might seem a simple logistic question. Theoretically we can use more generators and we can consume more fuel but in fact it's a little bit more difficult. It is well known that the most vulnerable parts of the military missions are the supply lines. More supply caravans mean more expensive logistic background and the casualties also will spectacularly rise. If we want to reduce the dependency on fuel supply of our deployed forces, we could improve the efficiency of electrical power generation or we can gain electricity from other sources in the field.

Unfortunately, there are no real possibilities to improve sensibly the efficiency of generators. The efficiency of the alternators can reach 95%, so these machines belong to the best ones that were ever made by humans. [7: 187] Diesel engines have much worse efficiency, only about 40%. It is slightly better than gasoline engines, but there are still technical barriers for further efficiency increasing. The development trends of diesel engines—for example turbo charging —create complicated structures but their increase of efficiency is only 1–2% and the complex machines are more expensive, need more maintenance and more often fail. Practically the heat loss of any kinds of heat machines can't be decreased below 50–60%.

Theoretically there are several ways of using the remaining heat by Peltier-cells, steam engines or Stirling-engines but these types of equipment are also expensive, complicated and make only a minimal improvement.

A camp-size nuclear plant would be technically appropriate for the advanced states but for now it seems to be too risky for their own troops. There are several projects for using hydrogen or methanol fuel-cells in the field but the technology is still in its elementary stage. Scientists are looking for more persistent electrodes and cheaper catalysts than platinum. If this technology was much more mature then it even would need a separate fuel supply chain, and this would be a logistic nightmare. Probably the only real alternatives of fossils for deployed units are the renewable energy sources at this moment. Using of RES becomes less and less particular in the civil economy, but their integration into an independent military grid means a very different challenge.

RES in Military Fields

Renewables are natural resources that can replenish themselves naturally over time. Practically these resources can be gained but their left quantity won't be less. Basically, five main types of RES are available in the biosphere of Earth. Biomass (including all wasted or cultivated organic materials), solar radiation, wind power, geothermic energy and hydro power. Some researchers separate tidal and ocean waves but in this article, it makes no sense for this separation.

There are dozens of projects all over the World with the target to integrate biomass into the fuel supply chain. In most cases biomass can reduce the dependency on fossils and has favourable effects on the economy and the environment. By this criteria biomass could be very useful for armies during their peace-time activities but unfortunately, it's not a proper choice for the deployed forces. Namely, it's not worth establishing a new logistic supply system because the energy density[11] of biofuels is less than the refined petroleum derivate. [8]

[11] Energy density is the amount of stored energy in a given space or weight. The SI unit is the J/m3 but sometimes it's better to use a weight-related one. For example, hydrogen gas has very good energy density related to its weight and much worse related to its volume.

Figure 4. *The 1520 tons ITS Commandante Foscari patrol vessel is a part of the Italian Green Fleet Program propelled by "Green Diesel" acquired from vegetable oils and tallow. This fuel conforms to F76 NATO navy fuel standard.* [19]

Hydro power is a very clean and economic source of electricity but it has two attributes which essentially excludes it from military operations. [9: 304] Gaining the energy of water needs enormously big and heavy infrastructure that is not mobile at all. In most cases of the possible military operations there is not enough water even for drinking. Using the heat of the Earth in the battlefield is similarly problematic because the equipment of geothermal harvesting is heavy and not easy to deploy and dismantle. [10: 19] In some parts of the Earth the geothermal gradient[12] is low or the lithosphere is too massive to enable the drill.

Solar and wind power seem to be the right choice for deployed military troops. These are well scalable, mobile enough and do not need too many infrastructural parts. These are available almost in all regions of the Earth but of course their intensity is very changeable. Unfortunately, whereas the gained energy from bio, hydro and geothermal sources are accurately predictable, wind and solar intensity are really unreliable. [11: 46–50] It means that wind and solar energy can't be used individually but we can take their advantages mixed with conventional generators in the same grid.

[12] Geothermal gradient is the rate of the increasing temperature towards the interior of Earth. The average rate is 3 C° per 100 meters but in Iceland it could be even ten times better.

Table 1. *The important features of RES in terms of military applicability.*
[The author's compilation.]

Renewable	Biomass	Hydro	Geothermal	Wind	Solar
scalability	n/a	bad	medium	good	very good
reliability	good	good	very good	medium	bad
mobility	n/a	none	very bad	medium	good

Classifying Micro Grids and their Components

Military grids are based on civil micro grid technologies so it's inevitable to examine their structure. An electrical grid can be very simple. If we have a power source (a plant in the power grids), a consumer and they are connected with a power cable, that's a grid. On a smaller scale if the power source is a generator we're talking about micro grids. Of course, depending on the number of sources and consumers, junctions can be created and the topography of the whole system would be very complicated but that's still a simple grid. The electrical grids of deployed units are always micro grids, because battalions or bigger units never settle down close to each other and it is not an expedient to connect them into a bigger energy network.

If a grid contains conventional plant(s) or generator(s) and some RES too, that's a hybrid grid. In the civil electrical power infrastructure micro grids are invested for economic reasons and they're connected into a big power grid. If a micro grid works independently without any power line connection, that's a so called off-grid or an "island." [12: 31] Usually the temporary military electrical networks are off-grids, even if those have got the capability to connect power lines, their typical working method is "island."

The last and the least clear type we have to know is the smart grid. In a smart grid there is a central control unit which has the information about both demand and supply and by these data it has the capability to change the direction and the amount of energy flow. Big power grids are always "smart" but of course there is the possibility of manual control. If conventional generators and RES are mixed into a hybrid system, there is the theoretical possibility of the manual management but it's not really lifelike during a military action. In the military applications hybrid grids are always "smart" ones.

It is very important, that if an island solution uses some RES, the system has to contain a storage unit in order to supply electricity when RES is not working until the generator starts. It's usually a battery group or it can be a hydrogen fuel cell with a water separator[13] or both. Other solutions like mechanical (gravity) storages are still in their technological beginning and their size doesn't allow using them in some parts of temporary military facilities. In most cases the power sources are not directly connected with the consumers but via the storages. It makes continuous load for batteries and current transformers make losses but on the other hand this structure ensures the constant quality of power supply.

[13] When there is a surplus of solar energy the water separator uses this electricity for making hydrogen stored in a tank. When there is not enough light, hydrogen is driven to a PEM cell making electricity.

There are a lot of ways of gaining the energy of solar radiation. Some solar plants work similarly to a conventional TPP[14] where high pressure steam rotates a turbine on a common axis with an alternator, but the heat making steam is not produced by burning fossils. Large-scale mirror systems can focus the light of the sun into a point where the temperature can reach hundreds of degrees. This solution hasn't enough mobility for military applications so when we're talking about solar power in military smart grids, we mean using PV cells.

As we can see the possible building blocks of micro grids are the followings:

- control unit and its sensors,
- generator(s),
- RES (in military applications that is wind and/or solar),
- storage unit (batteries or/and hydrogen cells),
- cables and switches,
- current transformers,
- power line interface(s).

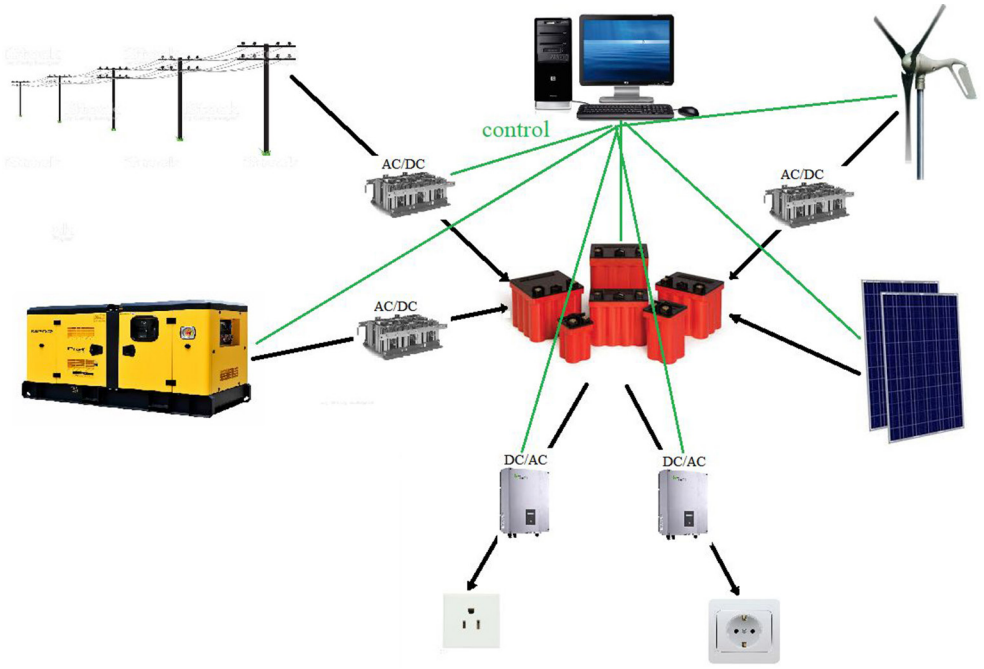

Figure 5. *A possible "full-scale" smart grid structure.*
[Edited by the author.]

According to the actual needs some parts may be missing. UPS[15] infrastructure can be seen like a special type of micro grids. When the primary goal is to improve the reliability of the electricity supply, the micro grid is only a small capacity battery and a generator.

[14] Thermal Power Plant.
[15] Uninterruptable Power Supply.

When the main power line is interrupted the generator starts immediately and the battery supplies the network between them. In some civil applications when the main reason of building a micro grid is economy the storage unit and the generator is commonly missing because of its price, and the micro grid essentially is a PV farm with a control unit and transformers. While the generated local power is more than the required, the surplus is fed into the network, otherwise the network recoup the local power generation. As it was mentioned, the military micro grids mostly don't have connectors for civil power lines.

Military smart grids are made in order to get the possibility of gaining RES in field. In this application RES means almost exclusively solar power. These types of equipment have to be very mobile and must face the difficult circumstances required by military standards. Normally their structures are very similar but the current size of the components depends on the intended mode of use and the geographic position. Let's see some examples. An unmanned remotely controlled communication station can be supplied for an extremely long time without any local maintenance if it has a special smart grid. In this case the working time is limited by the locally stored fuel for generator, so the target is to minimize its run time. It means an extremely large PV surface and a massive storing capacity compared to the load of the station.

In a temporary camp the number of very expensive batteries can be reduced as the refuelling of the generator(s) is easy and more PV panels can be used. In some applications like quick reaction auxiliary power supplies, the stored energy capacity is a determinative attribute but the generator can be very small or completely abandoned.

The closer we are to the equator the angle of incoming photons is closer to 90° which significantly raises the efficiency of solar panels. [13: 34] It is logical that for the same real PV power in northern places more panels are needed. There are some different PV materials in the market and they have different qualities.

Table 2. *Comparison of PV types.*
[The author's compilation.]

Technology	**Monocrystalline**	**Polycrystalline**	**Thin Film**
Material	silicon	silicon	amorphous silicon, CdTe,[16] CIGS[17]
Cost	moderate	low	moderate
Efficiency	15–24%	16–20%	8–12%
Heat Resistance	moderate	high	high
Temperature Co-Efficiency	moderate	high	minimal
Weight	high	high	low
Flexibility	none	none	good
Longevity	high	moderate	poor

[16] Cadmium Telluride.
[17] Copper Indium Gallium Diselenide.

Table 3. *Comparison of battery types and fossils based on their energy density.*
[The author's compilation.]

Material/technology		Maximal energy density	
		volume prop.	weight prop.
alkali batteries		~100 Wh/l	~150 Wh/kg
Electric batteries	plumbate-acid (Pb-acid)	~40 Wh/l	~25 Wh/kg
	nickel-cadmium (NiCd)	~150 Wh/l	~100 Wh/kg
	nickel metal-hydride (NiMH)	~300 Wh/l	~150 Wh/kg
	lithium-ion (Li-ion)	~650 Wh/l	~250 Wh/kg
	lithium polymer (Li-polymer)	~700 Wh/l	~250 Wh/kg
	lithium ferrophsophate ($LiFePO4$)[3]	~200 Wh/l	~100 Wh/kg
	lithium-air	~2,000 Wh/l	~1,700 Wh/kg
	lithium-sulphur	~1,500 Wh/l	~1,000 Wh/kg
liquid hydrogen		~2,500 Wh/l	~39,000 Wh/kg
Fossil fuels	fire wood (dry)	~700 Wh/l	~3,000 Wh/kg
	black coal	~9,000 Wh/l	~6,500 Wh/kg
	liquid gas	~7,000 Wh/l	~12,000 Wh/kg
	gasoline	~9,500 Wh/l	~12,000 Wh/kg
	diesel	~10,500 Wh/l	~13,500 Wh/kg
uranium–235		$\sim 4.7\times10^{12}$ Wh/l	$\sim 2.5\times10^{10}$ Wh/kg

The Working Method of Military Smart Grids, Advantages and Disadvantages

The working method of an average military island smart grid is quite easy and it can be described in three simple steps:

1. RES charge the batteries and the consumers load energy from them via an inverter.[19]
2. The RES input doesn't cover the output and the batteries are discharging.
3. The charge of the batteries falls below a predefined level when the generator starts and recharges the batteries again.

[18] The lithium-ion batteries almost dominate the smart grid technology because of their energy density but in some applications lithium ferrophosphate can be very useful because of its slightly higher temperature tolerance.

[19] An electronic converter that changes DC to AC.

Figure 6. *A recorded daily working diagram of a real smart grid.* [20]

As it was mentioned several times the goal of using smart grids is to reduce the fuel consumption. But how is this accomplished? It seems very easy: when the sun shines there is no need for the generator to work. It's absolutely true but there is another reason why these structures can save fuels compared to conventional generators. And this is coming from the characteristics of diesel engines. The efficiency of diesel engines (and all other types of heat-engines) depends on the load. It's only a very narrow band close to the maximum of load when the efficiency is optimal. In other bands it can be extremely poor and even close to zero. For example, when the load is zero a conventional generator can't stop and it has to work continuously without producing electricity as it is shown very conspicuously in Figure 7.

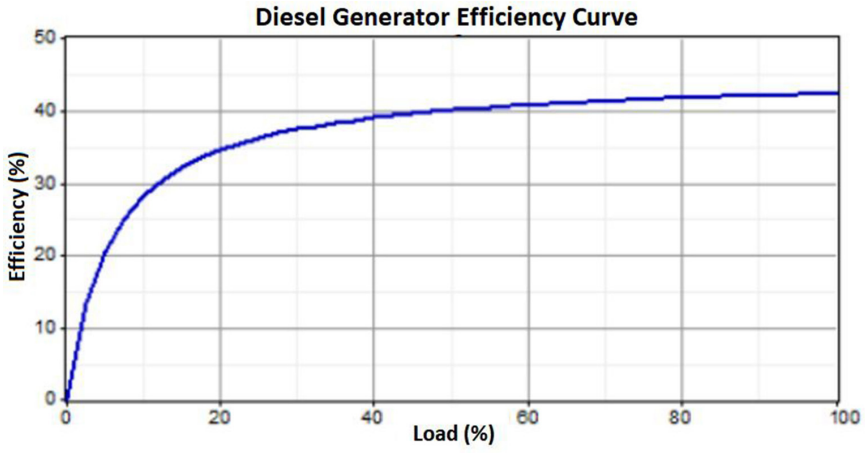

Figure 7. *The efficiency of a typical diesel generator vs load.* [21: 753]

If we check again Figure 6 we can see that diesel engine started only 3 times that day and worked for 7 hours but this time it was working constantly on its optimal load. This process is so effective that it alone results up to 40% in fuel savings.[14] The efficiency of the process was revealed only during the developments of hybrid systems but since then a number of independent international practical studies has been completed with similar results. The decreasing operating time and the optimum load have other positive gain as the maintenance cost and reliability of the applied diesel engines have improved spectacularly.

Table 4. *The generations of generators.* [The author's compilation.]

Generation	**0.**	**1.**	**2.**	**"2.5"**	**3.**
Power source	muscle	gasoline	diesel	buffered diesel	hybrid
Typical application period	1910–1930	1920–1950	1940–now	2015–now	2010–now
Current	DC	DC	AC	AC	AC
Supply theory	decentralised	decentralised	centralised	decentralised	decentralised
Maximal thermal efficiency	n/a	18–24%	28–36%	36%	36%
Relative efficiency	n/a	1	1.5	2.1[20]	2.1–3[21]
Relative weight[22]	5	1	1.4	1.8	2
Relative efficiency vs. weight	n/a	1	1.07	1.17	1.5
Relative noise	0.1	1	1.2	0.7[23]	0.3[24]
Relative visibility[25]	0.2	1	1.2	1.3	2

The main advantage of the military smart grid systems is the decreasing fuel consumption that results longer independent mission time and improved survivability for troops. The battery power greatly improves the reliability of supply and a well-designed system requires less maintenance despite its more complex structure. The decentralized supply model assumes several smaller grids but these can be connected into a bigger one which further enhances the resilience of the supply. Of course, long power cables make some loss and as they behave like a kind of antenna the vulnerability of the system raises against electro-magnetic effects. To avoid those effects further items like high voltage transformers and surge protectors are required.

Unfortunately, RES has an undesirable effect on the shielding of the camps. PV panels need direct solar radiation so those can't be camouflaged and the glitter of the large panels

[20] The efficiency of a conventional diesel engine +40% surplus.
[21] The efficiency of a buffered diesel +estimated solar power under normal continental conditions.
[22] The output power compared to the weight of the device.
[23] Of course, the noise of the diesel engine is always the same, but in buffered or hybrid systems it works significantly less.
[24] Of course, the noise of the diesel engine is always the same, but in buffered or hybrid systems it works significantly less.
[25] The output power compared to the size of the device.

can reveal the location of the camp from very far. From this point of view, the application of wind power is even more risky. For more efficient power production, a larger pole is needed but that extremely raises the visibility. These kinds of equipment are very noisy and the large moving rotors have surprisingly big radar cross-section.

The fuel consumption of the grid can be reduced up to 40–80% depending on the actual implementation [15] but it can't counteract the fact that these devices are extremely expensive. Primarily because of the cost of batteries—the investment cost of such device is three-five times more than the cost of a conventional generator. Because of the more complicated structure these are larger and heavier than normal diesel generators and that means more logistic demand. Due to their more numerous components their full deploy time is much longer and if the batteries are charged then hybrid systems can be loaded immediately and there is no need for warm up time and it is not necessary to wait for the full installation.

The Main Types of Existing Systems

As it was noted before, military smart grid technology is totally based on the civil grids so the most important developers are civilian energy companies. Around the turn of the Millennium they recognized that the demands of armed forces are similar to some conventional civil applications. In Europe NATO and EDA[26] recognised the military significance of this technology and strongly support its spread.

Now the main scenes of the appearance of these devices are "Capable Logistician" international military logistics exercises. These events are organized by MLCC[27] and supported by NATO ESCD.[28] The last exercise was held in Várpalota, Hungary where more than 2,000 soldiers of 27 nations were practicing co-operation during 2 weeks. [12: 3] It was the first time in Europe when military smart grids were not only exhibited but were integrated into the power supply system of the exercise. So far, no country has ever deployed smart grid system but some of them plan to do so. Besides the developer companies two major military projects are being conducted. NATO ENSEC COE[29] has a great experimental equipment in Vilnius built by the German company, Pfisterer and EDA deployed another one in Mali built by the British BAE Systems. [16]

In fact, the first military smart grids are already existing products with ruggedized design. These types have high performance according to industrial needs. Their military versions are normally built in a standard container in order to be easily transferable. These are designed for supplying temporary camps, independently deployed medium size military units for longer time so their full installation takes more time, up to some hours.

The design principles of these kinds of equipment are as follows:

- RES can be wind or solar power. The applied devices are usually fixedly installed on the roof of containers or tents;

[26] European Defence Agency is an independent European organization in Brussels, Belgium. Its main purpose is to provide place to co-operation of the European military developments.

[27] Multinational Logistic Coordination Centre is an independent international organization in Praha, Czech Republic. Its main purpose is to develop military logistics and organize military logistic events.

[28] Emergency Security Challenges Division in the Headquarters of NATO in Brussels, Belgium.

[29] Energy Security Centre of Excellence is a NATO organization in Vilnius, Lithuania.

- the power management system prefers RES but it also has a powerful diesel generator in order to secure and stable energy supply constantly;
- these are modular. Each container can be assembled to the specific needs of the user. These are easily scalable for output from 25 kw to 1 mw;
- consumers can be prioritised;
- these operate remotely without local supervision;
- generators and PV panels can be a third-party product or an existing item;
- containers contain only the management system and the batteries. In order to use the highest energy density Li-ion batteries the containers are air-conditioned that eliminates the temperature dependency of capacity of these kinds of batteries.

Figure 8. *The equipment of Dutch ESTechnologies operating on CL15 exercise in Várpalota supplied a battalion-size camp.*[30] [The author's photo.]

Later on, another type of military smart grid emerged driven by military needs. These small-size mobile devices have variable possible applications. These are usable for supplying quick move and installing smaller military units like a platoon or company. These are also usable for temporary strengthening a micro grid or temporary maintaining a facility during a blackout. Their typical application is the solar-trailer (a towed chassis with quickly expellable PV panels) but there are also some other construction principles.

The design principles of these kinds of equipment are as follows:

- these are very mobile, lightweight units. Their full installation time is only some minutes;
- RES can be only solar. Panels are quickly deployable and redeployable using some

[30] The total PV surface is 120 m^2 with 18 kW nominal power. The white container contains the management system and 140 kWh total capacity battery group. PV panels arrived in the red container. The orange box in the middle is the standard Caterpillar diesel generator. The green box is the power interface of the tent camp.

mechanical assistance;
- only PV sets and power transformers are compulsory. Diesel generators or even batteries may be absent in some cases;
- the most applicable battery type is Lithium-ferrophosphate. As air-conditioned housing is not possible, so the preferred feature of this type is that its capacity is less dependent on the temperature although the available energy density is lower than Li-ion;
- these are only partially modular. Only the size of the batteries or the types of the inverters can be changed.

Figure 9. *The theory of the British Renovagen is very special and compact. The trailer contains the retractable solar-carpet and the inverters. The tractor Land Rover helps the quick deploy.* [The author's photo.]

Summary

Overall, we can state that military smart grid is a very innovative and modern technology. Using these systems causes a really substantial reduction in fuel consumption unlike the residual heat-recovery or additives and emulsions in the diesel engine. Despite all that, their explosive propagation is not expected because of the price of the essential batteries. But as the battery costs fall, this kind of equipment will become more and more common in the armed forces and other law enforcement agencies.

According to some calculations the great investment is already recoverable during peace-keeping or peace-enforcing military operations as within a few years—if we calculate with extremely high fuel prices (3 EUR/l)—the transportation and storage costs will be very high. However, the spread of container type smart grids is more likely where the main aspect is to reduce vulnerable fuel supply caravans and increase survivability of our troops.

In some cases, it is worth considering the settlement of a bigger smart grid in a permanent military facility where there are no power lines within hundreds of kilometres. In Hungary all the facilities owned by the army are connected to the domestic electrical network therefore the application of larger systems in Hungary is currently not planned. At this moment the Hungarian troops performing service abroad are supplied by allied logistic units but if we deployed a bigger Hungarian contingent independently it would be worth taking into account the acquisition of a smart grid.

The situation is much simpler for the mobile military smart grids. For these devices, the lower price can even be further reduced with the proper scaling and omitting the unnecessary parts. Due to their high degree of mobility, they can be an ideal addition to the telecommunication stations, command and control centres and field medical facilities. These kinds of equipment are particularly suitable for ensuring the power supply of unsupervised military bases.

References

[1] *BP Statistical Review of World Energy.* London: British Petrol, 2017.

[2] PARMAR, J.: Total Losses in Power Distribution and Transmission Lines. *EEP – Electrical Engineering Portal,* 19.08.2013 http://electrical-engineering-portal.com/total-losses-in-power-distribution-and-transmission-lines-1 (Downloaded: 19.11.2017)

[3] BRYCE, R.: Gas Pains. *The Atlantic,* 05.2005. www.theatlantic.com/magazine/archive/2005/05/gas-pains/303897/. (Downloaded: 30.08.2017)

[4] VÁNYA L.: *Irányított energiájú fegyverek.* Budapest: Nemzeti Közszolgálati Egyetem, 2013.

[5] VÉGVÁRI ZS.: A katonai aggregátorfejlesztés- és gyártás történeti áttekintése, különös tekintettel a villamos forgógépek magyarországi gyártására 1927–1954 között. *Katonai Logisztika,* 24 különszám (2016), 564–579.

[6] HERMAN, S. L.: *Electrical Transformers and Rotating Machines.* New York: Delmar, Cengage Learning, 2012.

[7] CHAPMAN, S. J.: *Electric Machinery Fundamentals.* New York: McGraw-Hill, 2012.

[8] ROOS, D.: *Biofuels vs. Fossil Fuels.* 20.08.2012. http://auto.howstuffworks.com/fuel-efficiency/biofuels/biofuel-fossil-fuel.htm. (Downloaded: 02.09.2017)

[9] GERŐCS I.: *The military and the renewables. Hadtudományi Szemle,* 5 1–2 (2012), 300–314.

[10] GUPTA, H., ROY, S.: *Geothermal Energy: An Alternative Resource for the 21th Century.* Amsterdam: Elsevier Academic Press, 2007.

[11] VÉGVÁRI ZS.: A megújuló villamos-energiaforrások felhasználásnak lehetőségei harctéri körülmények között. *Hadmérnök,* 11 1 (2016), 41–56.

[12] VÉGVÁRI ZS.: A Smart Energy koncepció és eszközei a CL15 logisztikai gyakorlaton 1. rész. *Haditechnika,* 49 6 (2015), 30–34.

[13] MERTENS, K.: *Photovoltaics: Fundamentals, Technology and Practice.* Chicester: John Wiley & Sons Inc, 2014.

[14] ZOTOS, A.: *Renewable Energy Sourced Camp Smart Microgrid.* Brussels: EDA Energy and Environment WG, 2017.

[15] VÉGVÁRI ZS.: A Smart Energy koncepció és eszközei a CL15 logisztikai gyakorlaton 2. rész. *Haditechnika*, 50 2 (2016), 44–48.
[16] WOODMAN, J.: *Smart Energy Camp Final Report*. Farnborough: BAE Systems, 2016.
[17] *Wehrmacht.* Awards.com. www.wehrmacht-awards.com/forums/showthread.php?p=7823476 (Downloaded: 01.03.2018)
[18] *Pinterest.* www.pinterest.co.uk/pin/391813236323258580/?lp=true (Downloaded: 01.03.2018)
[19] *100528-N-3136P-207.* www.navy.mil/view_image.asp?id=86206 (Downloaded: 01.03.2018)
[20] *Flyer broshure of Pfisterer's CrossPower system.*
[21] NOUR, M., ROHANI, G.: Prospect of Stand-Alone PV-Diesel Hybrid Power System for Rural Electrification in UAE. *International Journal of Renewable Energy Research*, 4 3 (2014), 749–758.

AARMS Vol. 17, No. 1 (2018) 71–86. **10.32565/aarms.2018.1.7**

Hungarian Participation in the EU-Led African Military Operations

János BESENYŐ[1]

Africa is a high priority region to the European Union. Therefore, the European Union launched independent missions in the unstable regions of the African continent regularly since 2003, in order to restraint and eliminate local conflicts and prepare local armed forces for mission. Hungary was involved in a wide range of tasks in recent years from June 2005. We contributed to the success of these missions, our soldiers served on the highest respectable level among others in the Darfur, Congo, Chadian, Somali and Mali operations as well as in the elimination of piracy in this region. After all, it is likely that the European Union will continuously count on our country's participation in its peace-supporting missions. In the study I would like to present nine major operations, and the ultimately cancelled Libyan mission. I detail the case-specific objectives and implementation through first-hand experience, which was gained during my deployment. As far as Hungary is concerned, I wish to demonstrate the Hungarian soldiers' admirable work during these missions, besides, I would like to concentrate on the background and conditions of our participation.

Keywords: *European Union, Africa, Congo, Darfur, Chad, Naval Operation, Somalia, Mali, Libya, Central Africa, Hungary, peacekeeping, piracy, humanitarian activity, military training*

The EU Operation "Artemis"

The EU Operation "Artemis" (DRC Artemis) [1] was the EU's first fully independent mission in the African continent, which was carried out without NATO support between the 12th of June and the 07th of September 2003. Although the mission operated under the aegis of the EU, the management and leadership were clearly in French hands.

Starting the operation was a need, since bloody conflict between the Hema and Lendu tribal militias broke out in the Democratic Republic of the Congo's Ituri province with a total population of 4.5 million. Soon, other nationalities also got involved in the clashes.[2]

The UN forces in Congo (United Nations Mission in the Democratic Republic of the Congo–MONUC) were unable to bring the clashes under control, therefore the UN Secretary General on the 19th of May called the European Union—as it had strategic interest in Africa—on the implementation of a limited operation, which was adopted by the UN Security Council Resolution No. 1484 on 30 May with the following mandate: [2]

- enforcing stability in Bunia by a limited military operation, securing the airport;

[1] Ph.D., Colonel, Head of a Research Section in the Hungarian Ministry of Defence; e-mail: besenyo.janos@gmail.com

[2] The city had approximately 300,000 inhabitants, who belonged to the Alur, Hema, Lendu, Ngiti, Bira and Ndo-Okebo tribes. [1]

- performing security tasks (facilitating the solution of the Hema–Lendu conflict);
- humanitarian activities, protecting refugees and civilians;
- supporting operation of MONUC, protecting UN operatives and facilities.

Originally, the EU operation was an Interim Emergency Multinational Force. It was designed for three months and for a limited area of operations, until the UN Mission in the Democratic Republic of the Congo takes over control of the province. Seventeen countries participated in the French-led mission with 2,548 personnel. [3: 59] [4] [5] The EU Operation "Artemis" command was located in Paris, led by the French Lieutenant General Bruno Neveux. The strategic headquarters worked in the Ugandan Entebbe city, commanded by the French Major General Jean-Paul Thonier, while the "Outpost Command Centre" was set up in the operational field in Bunia. French air force units and civilian firms' Lockheed C–5 and Antonov 124 aircrafts provided the transportation of troops and logistics supply between Uganda and Bunia. The first European peacekeepers arrived in Bunia on the 6th of June, where the airport was secured without any problems, the troops could begin collecting their weaponry. Up to the 8th of July, the broad-mandated, well trained and equipped European units cleaned the city from armed groups, where life returned to normal. By the end of July, they also managed to stabilize the security situation in the suburbs. Meanwhile, the UN raised the amount of its employees to MONUC by 10,800 personnel and began securing the previously Artemis-guarded areas. [6] Withdrawal of European troops began in the middle of August and ended on the 7th of September. On the 25th of September they mopped up the headquarters in Uganda.

The balance of mission was definitely positive, which encouraged the EU for further participation in the continent's processes.[3]

Lieutenant Colonel János Tomolya served in the mission headquarters in Paris as chief military personnel officer. Since he graduated from the French military academy, he was the most likely to be chosen for the French-Hungarian negotiations. Originally, Hungary did not intend to take part in the mission, but the political leadership believed that participating in the Congo operation could be beneficial as an applicant for EU membership. Finally, the appointed officer hadn't been deployed to operational field, but with national limitations to the headquarters in Paris.

EU Support to AMIS (Darfur)

The EU support to African Union's enhanced Mission to Sudan (AMIS/Darfur) operation [7] —between June 2005 and December 2007—was the next African mission, where Hungarian soldiers were sent. The mission was preceded by a conflict between nomads (Arabs) and agricultural (black) tribes in February 2003, the escalation of which was accelerated by the Sudanese government-paid Arab militias' activities. [8] Fulfilling their ambitions and in reaction to the international pressure, the AU launched a peace-support operation (AMIS) in the region, which had to deal with a wide range of problems from the beginning. Initially,

[3] In spite of this, the mission faced with such problems like strategic air transport capabilities or the inefficient logistics supply.

the EU only provided financial and logistical support to AMIS, but later the support grown so diverse, they provided help through a joint support operation, [9: 117–118] which received a mandate in the following activities: [7]

- operating and supporting AMIS II;
- general and specialized training of African soldiers;
- managing and implementing tactical-strategic air transports;
- logistics supply, consulting 2012—advisory group;
- police assistance;
- participating in humanitarian programs.

From the beginning of the mission Hungary has been among those, who offered observers for the operation, as the political leadership rightly assessed that Africa is a major priority for the EU foreign policy. Besides the crisis in Sudan, the humanitarian disaster in Darfur made enormous impact on the world press. World-wide political support helped the work of organizations, searching for solution, through which our participation could generate great advantages in foreign policy.[4]

Leaders of the Hungarian Defence Forces appointed Major Ferenc Kajári to AMIS as an unarmed military observer from June 2004 to June 2005, who served as chief reconnaissance officer in one of the camps (Kabkabiya). The Major carried out classic peacekeeping/observer tasks, within the framework of which he took part in the everyday operation of camps, went patrolling and investigated ceasefire violations. Besides he endeavoured to be a neutral party and build a good relationship between the conflicting parties. The African Union's military leadership was so pleased with Major Kajári's work, they asked the European Union for further deployment of Hungarian troops. Thereby I got an opportunity to serve in El-Fasher headquarters in June 2005 as an (logistics) advisor. I've spent only six months in the mission, during which—as the camp supply department Deputy Commander—I was responsible for the nearly 12,500 deployed soldiers and police units (food, air and ground transportation, fuel, water security, and the operation and fire protection of the camps). Due to the sharp deterioration of the security situation in December I had been recalled from the mission, additionally Hungary withdrew its earlier offers to make further Hungarian soldiers serve in Darfur.

EU Advisory and Support Mission in the Democratic Republic of the Congo

During the operation, the Africans' attitude toward us "white" advisors was challenging. On the basis of the misconceived "African ownership" they asked financial, logistical support and a lot of work from the donors without taking any of our advice on the deficiencies. Almost every aspect of our supply (food, accommodation, hygiene, provision of drinking

[4] This is proven by the fact that one of the leaders of the EU mentioned to a member of the Hungarian EU representation in Brussels that Hungary was the only one among accession countries, that offered an observer which is a good breakaway opportunity among the member countries. According to him, the offers to Darfur mission is a—not only, but important—sign for the countries' readiness to respond, which helps the EU in crisis management, active and responsible participation in humanitarian disasters.

water etc.) was problematic and it didn't meet any of a common norm either. Despite all this, we earned the recognition of our work from the AU, and the EU as well. Instead, at home it was decided that we should take part rather in the European Union Security Sector Reform Mission in the Democratic Republic of the Congo (EUSEC RD Congo) which was launched on 2nd May 2005. Hungarian soldiers still serve in this mission. [9] Following the peace agreement, which ended the second Congolese civil war, an official request for peacekeeping arrived from the African country. Answering this, the Hungarian leadership decided to participate—with a limited amount of personnel—in the Congolese security sector reform. The mandate of "EUSEC RD Congo" lasted for one year, with a budget of only € 1.6 million. The operation was given a mandate in the following activities: [10]

- supporting Congolese government;
- supporting the security and cooperation of the countries, which are surrounding the African Great Lakes;
- supporting the reform in the administration and financial system of the military, transforming the Defence Sector;
- cooperating with the European Union Police Mission in Kinshasa (the Democratic Republic of the Congo), peacekeeping mission (EUPOL Kinshasa is aiming to reform the security of the Democratic Republic of the Congo);
- humanitarian activities.

From the beginning of the mission, the Hungarian Defence Forces was represented. First by one, later by three soldiers. However, the lack of officers who were able to communicate in English and French created difficulty in deployment, so Lieutenant Colonel István Papp was recalled from pension for service in Kinshasa, who then was closely involved in setting up the mission. [11] This deficiency remained in the later stages,[5] so the majority of officers were not sent in the Congo on a yearly mission, but for at least two or three years. Colonel Sándor Nagy was also a senior officer, who returned home after four years. Following the respectable work of Colonel Papp, the EU asked another flag officer for the position of financial officer, and for this, Major Zsigmond Csajági was deployed.

The main duties of the two flag officers were linked to the military transition. At first, they took part in the registration and check of the military personnel. Additionally, another Hungarian officer arrived, who was responsible for the operation's IT tasks.

Meanwhile, Lieutenant Colonel Papp left the mission, so that a system evolved where Hungary regularly sent two military advisers to the mission. In the last period this commitment decreased by 1 personnel/mission, since we weren't able to fill both positions at the same time. By the summer of 2015, eleven Hungarian officers and flag officers served in the mission.

Since the registration process could not be controlled from the capital, involved personnel spent most of their time in several camps on the operational field. It was also important because some of the local military leaders caused serious financial damage to the country with different types of fraud (larger amount of staff have been reported, they promoted people for financial rewards etc.).

[5] Teaching French would be efficient for our further involvement in Africa; unless this language-knowledge, operation in North- and Middle-Africa is nearly impossible.

Obviously, the European advisors' activities hurt the interests of several military leaders and warlords. Thereby Europeans received serious threats more than once and their lives were in danger, as well. Hungarian experts worked as consultants in the Defence Secretary's Office, Army General Staff, Joint Operational Committee and in the Committee for disarmament, demobilization, reintegration of former combatants, which was also responsible for decommissioning child soldiers. They also took part in the transformation of military structure, the Congolese army's internal control on financial and human resources, and the training of Congolese officers and flag officers.

In addition, they played an important role in disarmament and humanitarian programs. These projects, however, could not be completed in a year, so each year the mandate of the EU mission was extended again and again, and the personnel was increased to 60 people instead of the starter 8 officers. The annual budget reached 10.9 million Euros. [9: 107] Up to now, the EUSEC carries out major tasks in the field of logistics, supply systems, the operation of the military preparation and training. Over the past few years, the mission provided a few tangible results, however, it is considered more successful than the UN operation (MONUSCO) with its 20,000 personnel, both internationally and in the Congo.

Although very good circumstances were provided for advisers at the Kinshasa headquarters, during fieldwork, often the most basic tools were missing. The complicated and bureaucratic system of the EU made operations difficult, which could easily extend the execution of an operation by a year. [12: 350–351] In the meantime, the mission set up offices in several other locations outside the capital, leaving only one Hungarian soldier at the headquarters. The others performed service in Kisangani, Bukavu, Goma, Bunia and elsewhere, where 18 integrated brigades were set up by the former government forces and opponent militias.

The "rural" services were more dangerous in comparison to the duty in the capital because of the weaker influence of the Government, so soldiers earned special hazard allowances as a compensation. Getting used to very different climatic conditions meant particular problems for the Hungarian soldiers, as well as daily infections such as malaria, Ebola, dysentery, typhoid or cholera. Through the past ten years in the ongoing operation, ten Hungarian officers served in the mission. The shifts were sometimes problematic but we were able to maintain the required amount of Hungarian participation.

European Union Military Operation in the Democratic Republic of the Congo

Hungarian soldiers also undertook other operations in Congo, such as ensuring the Congolese parliamentary elections in the frame work of the EUFOR RD Congo. The operation was established by the UNSC 1671 decision, which was launched following the UN and the Congolese Government's request in 2006. The tasks started on 12th June 2006 and lasted until 30th November 2006. Some of the EU member states did not support the Franco–German-led operation and considered it unnecessary, thus they were not—or only limitedly—involved.[6] [13: 99]

[6] Javier Solana met with the Defence Ministers of the reluctant countries on 22nd February, and managed to convince them in participating in the operation.

In the framework of the mission, the local elections in June were secured by 21 European member states, Turkey (with 2,275 soldiers and police officers) and the USD 20.9 million budget. [9: 111] According to the former Hungarian offers, logistics and HR professionals were sent instead of combat troops.[7] [14: 117]

The EUFOR RD Congo received a mandate in the followings: [15]

- securing the Congolese parliamentary elections in accordance with the UNSCR 1671 decision;
- supporting the operation of MONUC;
- supporting the Congolese Government;
- implementing security tasks;
- protection of civilians;
- securing the airport in Kinshasa;
- humanitarian activities.

The mission was led by the German Lieutenant General Karlheinz Viereck and the French Major General Christian Damay. Operations related to planning and coordination were handled at mission headquarters in Potsdam,[8] [16] while the implementation of the daily activities was carried out in the airport in Kinshasa N'Djilli Operation Headquarters (OHQ) (1,075 people). Most of the mission forces (1,200 people) were deployed to Gabon's capital, Libreville. Had an attack occurred in Kinshasa, they could easily interfere from Libreville. According to the plans, a French battalion (400 people) strategic reserve force was established in Europe. Although, eventually actual deployment of this reserve didn't take place. [13: 102] [17: 363–364] Due to certain reasons, the three Hungarian officers were sent with national restrictions. They served in the mission headquarters in Potsdam, despite the fact that the EU's military leadership planned them in the area of operations. Hungarian flag officers carried out the tasks related to the logistics of the mission and performance of personnel.

In addition to the fact that some of the European states refused to send troops to the operation, cooperation between EUFOR RD Congo and MONUC was also problematic. They faced certain managerial and logistical challenges (lack of airlift capacity), but the operation finally reached its goal as both rounds of the elections could take place without any problems, so according to the plans, EUFOR RD was completed on 30th November 2006. However, some teams were withdrawn only in December and the EU headquarters in Potsdam was mopped up in February, 2007.

EU Military Operation in Eastern Chad and North-Eastern Central African Republic (EUFOR Tchad/RCA)

The next operation in which Hungarian soldiers took part was the EU Military Operation in Eastern Chad and North-Eastern Central African Republic mission. The mission was

[7] In this case, we were not the only nation that refused to send "combat" troops in the operation, several other countries have decided to take part in the operation with only a few staff officers with national restrictions.

[8] Namely the Henning von Tresckow barrack in Deltow, near Potsdam. One of the EU's OHQ with multinational capabilities (originally five nations, more if needed).

established in reaction to the conflict in western Sudan (Darfur) and its regional impacts—mainly on Chad and the Central African Republic—and the mentioned countries' unstable internal political situation. The operation lasted from 28th January 2008 until 15th March 2009. Four (personnel, logistics and medical) officers were sent to the mission. The operation received a mandate in the following activities: [18]

- guarantying regional security, cooperation with the bodies of the UN, Chad, Central African Republic;
- patrolling;
- protecting civilians and refugees, reintegrating them, securing international civilians;
- delivering humanitarian aids.

Two headquarters had been established based on past experience. Strategic Command in Paris[9] [19] was led by Irish Lieutenant General Patrick Nash, while the operational headquarters in Chad (in N'djamena and Abechi) worked under the guidance of French Major General Jean-Philippe Ganascia. The three battalions were deployed to Iri, Forchana and Goz Beida and cities, while a company-sized unit served in the Central African Birao. 23 EU member states as well as Albania, Croatia and Russia[10] [14: 120] were involved in the mission with—in total—3,396 people. [17: 380]

Similarly, to other missions, EU did not use any NATO equipment or assistance.[11] [9: 110] On the other hand they cooperated very well with the organization, using the previous experience from Operation EUFOR RD Congo. Unlike the previous short-term and limited operations, the EUFOR CHAD operated with a budget of EUR 119.6 million, moreover it was not only in Chad for over fifteen months, but played a significant role in the Central African Republic, as well. [14: 118] Actually, it was the "trial run" for EU's long-term operations. Despite the limited mandate and several difficulties (logistical problems, slow mobilization, high OHQ accommodation costs), it was performed successfully. [12: 398–399] Through this, the EU enhanced 'Europeanisation' of peace operations in Africa, and it did not just become equal with the African Union, but it surpassed the other regional organization's level of success.

The Hungarian leadership—as a result of former experience of the Congolese operations—contributed to the work at operational field. Major Ferenc Nagy carried out transport coordination and several planning tasks in Chad. [20] Command of the mission assessed the work of Hungarian officers positively, which was partly due to the work of Major Antal Csaba Kiss doctor, who prepared an analysis on the health risk of the mission, which was a great help for the armed forces of Chad.[12] All officers mentioned that cooperation with local people and the French soldiers was problematic since—despite the fact that English was

9 Namely EU's Mont Valérien OHQ in Paris, Saint-Cloud. One of the EU's OHQ with multinational capabilities (originally five nations, more if needed).

10 Participation of Russia was greatly important as the EU still didn't have the needed airlift capability, thus the success of the mission was highly dependent on the Russian helicopters.

11 Berlin Plus mechanism.

12 This document was so successful that when the EU planned to launch a mission in Libya, the HDF was asked to make the Major or some other medical officers write the health-risk analysis.

the official language—the majority spoke only French and interpreters weren't continuously provided.

European Union Naval Force Somalia. Operation Atalanta

The EU NAVFOR Atalanta/EU Naval Operation in the Somali Republic was established by the UN Security Council 1816 resolution on the 2nd June, 2008. Receiving one of the greatest attention among EU missions, it is currently operating on the Red Sea, Gulf of Aden and the Indian Ocean. [21] As an indicator of the mission we could mention piracy-generated security [22] [23] and world economic issues.[13] [24] The mission operated with approximately 20 crafts, that—in cooperation with regional organizations (UN, NATO) and other national contributions (USA, Russia, China, India, Japan, South-Africa)—controlled 3.7 million square meters of the ocean. The operation received a mandate in the following activities: [14: 121]

- supporting the EU's CSDP;
- combatting piracy, securing trade routes, protection of civilian ships;
- escorting ships of UN World Food Program and other humanitarian convoys;
- supporting the operation of AU's mission in Somalia (AMISOM);
- supervision of fishing in the Somalian shores.

The British-led HQ of the mission (1,400 personnel) was located in Great-Britain, Northwood,[14] [9: 113] while the convoy's "temporary" base port works was in Djibouti. The average annual budget of the operation was 8.3 million Euros, charged to the ATHENA mechanism. [25] Through trade routes patrols and the supervision of civilian commercial ships' convoy routes, effective cooperation was established with countries in the region (Madagascar, Kenya, Somalia, Djibouti, India, Yemen, Mozambique etc.), and with various civil and professional organizations (shipping, insurance companies), too. Thereby they could act in a more coordinated and more effective way against pirates.

Although the activities of the mission were declared successful, the EU doctrine against the pirates was only published two and a half years after the commencement. Additionally, it was misinterpreted by several member states. Besides, the operation still does not have sufficient intelligence, enough helicopters suitable for patrol, efficient medical insurance and tankers. [12: 456–460] A similar problem is the lack of unified regulations against piracy. Several member states are freeing captured pirates, who are about to carry out further attacks. The fact, that its mandate was extended until 12 December 2016 demonstrates the importance of the operation.

Hungary joined the mission at the beginning of the operation, where three IT Non-commissioned officers were sent with national restrictions. However, this was not a problem compared to the past, since the non-commissioned officers served at the Northwood headquarters and needn't go to the area of operations. Their duty was the registration of

[13] According to a research of the non-profit One Earth Future Foundation (2010) this amount added up to approximately 7–12 billion dollars.

[14] The all-time commanders' stay in the area of maritime operations in the marine convoy flagship.

merchant vessels on a special website ("Mercury"), their track and support if needed. Thus, they were in daily contact with not only the Navy but also with civil shipping companies. [26] Merchant ships who have registered on the website were gathered in a group with the EU NAVFOR units and went together to the dangerous waters so that they received protection from pirates. The Hungarian non-commissioned officers served in yearly shifts until 2010, when Hungarian military contribution was withdrawn.

European Union Training Mission—Somalia (EUTM-S)

Later, when the EU invited Hungary to another operation, the idea of sending a special-force unit emerged but finally it was not realized. In replacement, we took our share in the EU Training Mission in Somalia (EUTM Somalia), which began its operation on 10 April 2010 and lasted until December 2016 with the following mandate: [27]

- supporting the implementation of the Djibouti Agreement;
- support for the Temporary Federal Government and government organizations,
- enhancing the operation of AMISOM;
- training Somali government soldiers on the basis of UNSC Resolution No.1872.

The Spanish-led small (125 people) mission worked first time in Uganda where on an annual basis 3,600 Somali soldiers were trained. In December 2013, it moved to Mogadishu, where the headquarters was established at the international airport, while the train continued on Jazeera base. The mission had an annual budget of 11.6 million Euros, which provided the operation of a liaison office in Nairobi as well as a support group in Brussels. In the operation, in addition to the company and battalion commanders, lower ranked leaders, trainers and specialists (officers, non-commissioned officers) were trained, while the Ugandan Army was responsible for the training of the ordinary soldiers. [28] The Somalis were trained in the field of infantry, military police, civil-military cooperation, mechanics and intelligence. In addition, they also acquired knowledge in human rights and humanitarian tasks. At the same time, the mission provided advisors assigned to the Somali Ministry of Defence and General Staff who are also involved in the Somali army reform.

Our country was involved in the operation from the beginning, in which three lawyer officers were sent per a shift. The officer started his duty six week before his deployment in Brussels, where he carried out the preparation of documents regulating the operation. Later, he stayed in Kampala, in the mission headquarters. Trainers were placed in the tent camp of Bihanga, western Uganda. The training was performed by mixed nationality groups accompanying Ugandan soldiers who were responsible for the daily activities of Somalis. Hungarians formed a group with the Germans. Due to their similar readiness and mentality, this group was among the most successful ones. [29] [30]

The first group drew up the rules and guidelines for the next deployed units. Hungarians were responsible for the non-commissioned officers' training, which was conducted six times a week for four months. Theoretical and practical training took place twice a day, exams were written weekly. Hungarian trainers held this system—with minimal changes—in Somalia, too. The training was held in Somali language, so that Hungarians were forced to use interpreters. Breaking with the past trends, our soldiers had no national limitations in this mission,

they arrived with small arms, thus they were able to defend themselves. Although some very dangerous situations occurred, Hungarian soldiers didn't need to use their weaponry. During the mission, Hungarian soldiers worked under Spartan conditions in Uganda. They lived in tents. They received better conditions in Mogadishu. So far 18 Hungarian soldiers participated in the operation. Although the mission was engaged in small and limited activities, its effectiveness was indisputable.[15]

EU Military Operation in Support of Humanitarian Assistance Operations in Libya

Hungarian trainers were already in Uganda on 1st April 2011 when a recent mission of the European Union, the Libyan Operations (EUFOR Libya) started. Its basic task was to support humanitarian organizations and civilian population in the civil war-torn Libya by various activities (convoy escorts, medical insurance). Operational plans were made for these tasks; however, no actual request was received from humanitarian organizations, moreover, European states had different opinion on launching the mission.[16] [31]

The mission had a budget of EUR 8 million, in spite of this, just the 110-strong preparatory staff was set up in Rome, the actual process had not been launched. The EUFOR Libya was given a mandate for the following activities: [12: 425–426]

- protecting Libyan civilians, securing their evacuation;
- creating safe living conditions during the conflict;
- support the work of humanitarian organizations operating in Libya.

The preparatory staff wrote four drafts for the Libyan operations, which covered all of the previously planned tasks. The four plans required four health insurance plans as well. Lieutenant Colonel dr. Tamás Bognár was involved in the preparation process, who was responsible for preventive medical activities and the health risk assessment, as well. He was replaced by Lieutenant Zita Makrai, who continued to carry on the Lieutenant Colonel's duties. At first, Lieutenant Colonel Bognár was sent with national restrictions to EUFOR, but following the request of EU, national limitations were released and Lieutenant Colonel Bognár could travel to the area of operations in Libya. [32]

The two Hungarian officers had double duties. On the one hand they were involved in health planning tasks, which means that they had to organize health care in accordance with the operational plans, thereby ensure that injured personnel receive the required treatment in time. The second task was preventive care, in the framework of which, they prepared mission participants for Libyan health conditions. Although the operation hadn't start, risk analysis and other health programs—carried out by the Hungarian staff—were awarded with widespread recognition of the Hungarian military health care.

---

15 Recruiting and integration of Somalis to the Somalian army has nothing in common with the EUTM SOMALIA personnel, due to this fact a very limited feedback came from the results of the training.

16 Some of the European countries did not participate coordinated in the EU operation, but according to their own interests in NATO operations against Libya played a role. Thus, the EU was not capable of effective independent operation in the Libyan conflict. Therefore, several experts mentioned the operation as "an April joke".

EU Training Mission in Mali (EUTM Mali)

As a result of the Libyan civil war, thousands of formerly Gaddafi-linked Tuaregs returned to Mali, where they burst-out the centuries-old conflict and proclaimed the Azawad, the independent state of their own. Since radical Islamic terrorist organizations (AQIM, Mujan, Ansar Dine) joined the conflict, an international coalition was formed (first involving the French and the EU, later also the AU and the UN) and ousted radicals. [33]

Following, the UN–EU joint mission, the MINUSMA was established. On 18th February 2013, the French-led, 580-strong EU Training Mission in Mali replaced its mandate. It was responsible for the preparation of specified units of the reorganized Malian army. The Council of the European Union defined a 15-month long duration for the mission, run by 23-member countries on a budget of 12.3 million Euros in 2014. On 15th April 2016 it was extended until the 18th of May, with a budget of 23 million Euros and the following mandate: [34]

- according to the declarations of the Mali National Committee on 29th January 2013, enhancing the restoration of constitutional order;
- restoring and securing the Western-African state's statehood, territorial integrity and sovereignty;
- repelling international terrorist organizations and organized crime;
- training the newly-organized Malian Army units;
- advisory tasks related to the reconstruction and employment of the Malian Army.

Headquarters of the mission is located in Bamako, while the training centre operates in Koulikoro, 60 km away from the capital. European policymakers declared in the first days that personnel of the EUTM MALI won't participate in combat operations and they keep to this record ever since. [35]

Hungary was among the first who offered soldiers, according to the Government's decision to contribute with 15 (during replacement period up to 30) personnel. A liaison officer, six medical trainers and three soldiers belonged to the first group, who travelled in March and April 2013. The liaison officer served at the headquarters in Bamako. The medical staff worked in the German–Austrian field hospital, while the six infantry soldiers—belonging to the MH 5th Istvan Bocskai Infantry Brigade, 5/24. Gergely Bornemissza Reconnaissance Battalion—were deployed to Koulikoro to train the snipers of the Malian army.

The first two battalions of the Hungarian soldiers participated in a ten-week training. In addition to the training, they made an English-language preparatory document, on the basis of which the next, Portugal staff continued their duty. [36] In the further period of the mission, only the liaison officers and medical staff remained in Mali. As the EU extended the mandate of the mission we sent out new trainers, who—in cooperation with the Portuguese—carried out the training of Malian snipers. Hungarian soldiers have been sent out without national restrictions, using their own weapons. African conditions, the relatively short and busy training period, weaknesses in logistic support, monotony in supply meant the biggest challenge for Hungarians. Besides, the official language of the mission was French, what was rarely spoken among Hungarian soldiers. Up to now, sixteen Hungarian soldiers served in the mission.

European Union Military Operation in the Central African Republic (EUFOR RCA)

Invitation to take part in the European Union operation in the Republic of Central Africa (EUFOR RCA) [37] was launched during the operation in Mali. The EUFOR RCA was launched on 10th February 2014 by the Council Decision 73/2014/CFSP. EUFOR RCA reached full operational capability on 15th June 2014. It's end was planned for 15th December 2014 by the UN Security Council in Decision no. 2181 (2014), which was later extended until 15 March 2015 with the following mandate: [38]

- EUFOR RCA participates in the stabilization and securing the situation in Bangui, until this task is transferred to the supervision of the AU operation (MISCA);
- protection of the civilian population, improving their living conditions, ensuring the operation of humanitarian aid;
- support the MINUSCA mission until it reaches full operational capability.

Under the guidance of Major General Philippe Pontičs, strategic command was located in Larissa (Greece), while the operation headquarters (led first by Brigadier General Thierry Lion, eight months later by Brigadier General Jean-Marc Bacquet) operated in Bangui. The EU approved 25.9 million Euros as operation costs, which later was increased by 5.7 million. The EUFOR RCA (mainly included French personnel of the total 750 people) occupied the M'Poko airport in Bangu on the 30th of April. Later, step-by-step, in cooperation with the French "Operation Sangaris", they shrivelled armed groups from the capital. Part of the mission's activities were transferred to the new EU advisory mission, the Brigadier General Dominique Lauge-led EUMAM RCA (with a budget of 7.9 million Euros), which concentrated on the reorganization and training of the Central African armed forces. [39]

According to the Hungarian Government's decision, 6 staff officers (during replacement period up to 12 people) were deployed partly to the mission's operation headquarters and partly in the operation field headquarters in the capital city of the Republic of Central Africa. Their mandate in the EUFOR RCA lasted until the previously defined operation's mandate, but not longer than 15th March 2015. Actually, three staff officers were sent to the headquarters. Colonel Vekerdy, who played a significant role in the operations area, ended his service on 13th March 2015.

EUNAVFOR MED Operation Sophia

EUNAVFOR MED was launched in May 2015, [40] in reaction to the overwhelming flow of migrants, who tried desperately to reach European shores through the Mediterranean Sea. Although, the mandate of the mission until 2015 September was primarily reconnaissance and patrolling of the central Mediterranean, in accordance with the common security and defence policy of the EU, it was supplemented by countering human smuggling from Northern Africa, contributing to the implementation of the UN arms embargo on the high seas off the coast of Libya, [41] as well as training of the Libyan Navy Coast

Guard and the Libyan Navy.[17] [42] Following the expansion of the mandate, the mission had been renamed EUNAVFOR MED Operation Sophia. Its licenses include intercepting, scanning, impounding and diverting ships of human smuggler units on international waters.

Since January 2016 to November 2016, the operation saved more than 110 thousand people, who departed on insufficient fishing boats, longing for a miracle to reach Europe. [41] According to the estimates of the European External Action Service (EEAS) operation Sophia's activities resulted in 99 suspected smugglers and 337 boats were removed from criminal organizations' set of tools. [43] So far, 25-member states are represented in the mission, which has an ongoing mandate until 27th July 2017. [39: Art. 11] The common costs of the mission, financed by the Member States, amount to EUR 11.82 million for the one-year mandate. [44]

In November 2016, the HQ operated with 159 people, of which 99 were coming from Italy and 60 from the other Member States (Belgium, Bulgaria, Cyprus, the Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Latvia, Lithuania, Malta, the Netherlands, Poland, Slovenia, Spain, Sweden, the United Kingdom). [45] Hungary contributed with three senior officers, who were responsible for planning, organizing and synchronizing information operations and aviation activities with the applied "conventional" military assets. [4]

Conclusion

The current EU operations show that the African continent is not indifferent for the EU and the regional organization definitely wants to take part in addressing African conflicts, which are influencing the security of Europe at several levels, as well. Out of the 29 operations of CSDP, 16 was carried out in Africa. This conclusion could be also based on the fact that since 2008, the EU participated only in African operations. However, it seems that a significant amount of the member countries refuses to undertake serious role in these operations, so it is likely that they will continue to participate with limited mandates. Furthermore, according to recent experience, the EU doesn't wish to take part in peace enforcement in the African continent, rather in peace support operations (such as training and advising).

Hungary is among the top ten-member countries considering the amount of deployed personnel to EU missions, but not to Africa, rather to the Balkan.[18] Although Hungary isn't "a key player" in the black continent and in previous years the majority of the Hungarian political and military leadership was sceptical about our involvement in African missions, it is increasingly clear that we can't exclude ourselves from the African events. This is indicated by the change in the Hungarian foreign affairs priorities, the "opening to the South" process. Therefore, it would be worthwhile to process our experiences in Africa, on the basis of which preparations should began for a possible operation. Simultaneously removing

[17] Two ships of the deployed units (San Giorgio and Rotterdam) welcomed 78 Libyan trainees of the Libyan Navy Coast Guard in 2016, in order to improve security of the Libyan territorial waters and enhance search and rescue activities in Libyan territorial waters, as well.

[18] Hungary deployed 304 personnel to the EUFOR mission in the Balkans. Additionally, we also serve in 21 individual positions.

existing shortcomings (French-knowledge) should take place. It is clear that there are several areas (intelligence, reconnaissance, logistics, water purification and health), where the EU is struggling with shortages and where the EU appreciates Hungarian participation (even despite the relatively small number of employees!).[19] Therefore, these areas are proposed to be further developed in accordance with our possible future African engagement.

References

[1] TOMOLYA J.: Operation "Artemis": The First Autonomous EU-led Operation. *AARMS*, 14 1 (2015), 121–132. www.uni-nke.hu/document/uni-nke-hu/aarms-2015-1-tomolya.original.pdf (Downloaded: 29.03.2017)

[2] EEAS: *ARTEMIS/DRC.* www.eeas.europa.eu/csdp/missions-and-operations/artemis-drc/index_en.htm (Downloaded: 29.03.2017)

[3] RODT, A. P.: *The European Union and Military Conflict Management: Defining, Evaluating and Achieving Success.* London: Routledge, 2014.

[4] SODER, K.: *EU crisis management: an assessment of member states' contributions and positions.* www.ies.be/files/Soder-D1-NOT4WEB.pdf (Downloaded: 29.03.2017)

[5] TÜRKE A. I.: *The Operation Artemis in the Democratic Republic of Congo, CERPESC – Sorbonne.* www.academia.edu/9502774/The_Operation_ARTEMIS _in_the_Democratic_Republic_of_Congo (Downloaded: 29.03.2017) (As well as based on statements of Colonel János Tomolya.)

[6] UN: *Operation Artemis. The lessons of the Interim Emergency International Force.* http://pbpu.unlb.org/PBPS/Library/Artemis.pdf (Downloaded: 29.03.2017)

[7] EEAS: *EU Support to AMIS (Darfur).* www.eeas.europa.eu/csdp/missions-and-operations/eu-support-amis-darfur/index_en.htm (Downloaded: 29.03.2017)

[8] BESENYŐ J.: The first military operation between the European Union and the African Union. The European advisors' role in Darfur. *AARMS*, 6 4 (2007), 771–784. www.zmne.hu/aarms/docs/Volume6/Issue4/pdf/18bese.pdf (Downloaded: 29.03.2017)

[9] MAYS, T. M.: *Historical Dictionary of Multinational Peacekeeping.* Lanham: Scarecrow Press, 2010.

[10] EEAS: *EUSEC RD Congo.* www.eeas.europa.eu/csdp/missions-and-operations/eusec-rd-congo/index_en.htm (Downloaded: 29.03.2017)

[11] BESENYŐ J.: Beszámoló a kongói EUSEC misszióról. *Afrika Tanulmányok*, II 4 (2008), 28–33. www.afrikatanulmanyok.hu/application/essay/734_1.pdf (Downloaded: 29.03.2017)

[12] BESENYŐ J.: *Magyar Békefenntartók Afrikában.* Budapest: Katonai Nemzetbiztonsági Szolgálat, 2013.

[13] ENGBERG, K.: *The EU and Military Operations: A Comparative Analysis.* London: Routledge, 2013.

[14] KOUTRAKOS, P.: *The EU Common Security and Defence Policy.* Oxford: Oxford University Press, 2013.

[19] Loading professional duties with Hungarian officers cost less and their operational losses add up fewer than sending a greater amount of infantry personnel.

[15] EEAS: *EUFOR RD Congo.* www.eeas.europa.eu/csdp/missions-and-operations/eufor-rd-congo/index_en.htm (Downloaded: 29.03.2017)
[16] TÜRKE, A. I.: *Potsdam – Un QGM européen (III.)* http://europavarietas.org/csdp/csdpblog/potsdam_qg_europeen (Downloaded: 29.03.2017)
[17] KOOPS, J. A.: *The European Union as an Integrative Power: Assessing the EU's "effective Multilateralism" with NATO and the United Nations*. Brussel: Vubpress, 2011.
[18] EEAS: *EUFOR Tchad/RCA.* www.eeas.europa.eu/csdp/missions-and-operations/eufor-tchad-rca/index_en.htm (Downloaded: 29.03.2017)
[19] TÜRKE A. I.: *Mont Valérien – Un QGM européen (II.)* http://europavarietas.org/csdp/csdpblog/mont_valerien (Downloaded: 29.03.2017)
[20] MARSAI V.: A szomáliai kalózok és az EU Atalanata-missziója. *Nemzet és Biztonság*, 4 4 (2011), 66–76.
[21] SOUFIS, E.: *Case Study of European Union Antipiracy Operation "Naval Force Somalia": Successes, Failures and Lessons Learned for the Hellenic Navy.* Monterey: Naval Postgraduate School, 2012. www.hsdl.org/?view&did=726089 (Downloaded: 29.03.2017)
[22] BOWDEN, A. (ed.): *The economic cost of Maritime Piracy.* (One Earth Future Working Paper.) http://oceansbeyondpiracy.org/sites/default/files/attachments/The%20Economic%20Cost%20of%20Piracy%20Full%20Report.pdf (Downloaded: 29.03.2017)
[23] MARSAI V.: Szomália és kalózai I. *Haditechnika*, XLV 3 (2011), 9–12.
[24] EEAS: *Countering Piracy off the coast of Somalia.* www.eeas.europa.eu/csdp/missions-and-operations/eu-navfor-somalia/index_en.htm (Downloaded: 29.03.2017)
[25] ISS: *Seminar reports. Lessons from Atalanta and EO counter-piracy policies.* www.iss.europa.eu/uploads/media/Atalanta_report.pdf (Downloaded: 29.03.2017)
[26] EEAS: *Military training mission in Somalia (EUTM Somalia).* www.eeas.europa.eu/csdp/missions-and-operations/eutm-somalia/index_en.htm, (Downloaded: 29.03.2017)
[27] NILSSON, C., NORBERG, J.: *European Union Training Mission Somalia, a Mission Assessment.* FOI-R–3870–SE. 13.04.2014.
[28] BESENYŐ J.: Portré: Horváth Csaba Zsolt százados, EUTM Somalia. *Afrika Tanulmányok*, VI 3 (2012), 55–74.
[29] BRATTBERG, E.: *Opportunities lost, opportunities seized: the Libya crisis as Europe's perfect storm.* Brussels: European Policy Centre, 2011. www.epc.eu/documents/uploads/pub_1310_opportunities_lost.pdf (Downloaded: 29.03.2017)
[30] HANSEN, L. K., NIELSEN, K. L.: *EU Strategic Culture and the 2011 Libyan War.* www.ecsa-c.ca/wp-content/uploads/2014/11/3A_Hansen-and-Nielsen.pdf (Downloaded: 29.03.2017)
[31] EEAS: *EUFOR Libya.* www.eeas.europa.eu/csdp/missions-and-operations/eufor-libya/index_en.htm, (Downloaded: 29.03.2017)
[32] BESENYŐ J.: War at the background of Europe: The crisis of Mali. *AARMS*, 12 2 (2013), 247–271. http://uni-nke.hu/uploads/media_items/aarms-vol-12_-issue-2_-2013.original.pdf (Downloaded: 29.03.2017)
[33] EEAS: *EUTM Mali.* www.eeas.europa.eu/csdp/missions-and-operations/eutm-mali/index_en.htm, (Downloaded: 29.03.2017)
[34] WIKLUND, C. H., SKEPPSTRÖM, E.: *European Union Training Mission Mali – Challenges and Opportunities. Peace Operations Project, FOI Memo 4797.*

www.foi.se/Documents/European%20Union%20Training%20Mission%20Mali-%20Challenges%20and%20Opportunities.pdf (Downloaded: 29.03.2017)

[35] BESENYŐ J.: Magyar műveleti tapasztalatok Maliban. *Honvédségi Szemle*, 142 2 (2014), 78–92. www.honvedelem.hu/container/files/attachments/42782/hsz20142.pdf (Downloaded: 29.03.2017)

[36] NIRMARK, A.: *EUFOR RCA: EU force or farce?* www.cidob.org/publicaciones/opinion/europa/eufor_rca_eu_force_or_farce (Downloaded: 29.03.2017)

[37] EEAS: *EUFOR RCA*. www.eeas.europa.eu/csdp/missions-and-operations/eufor-rca/index_en.htm (Downloaded: 29.03.2017)

[38] EEAS: *EUMAM RCA*. http://eeas.europa.eu/csdp/missions-and-operations/eumam-rca/index_en.htm (Downloaded: 29.03.2017)

[39] *Council Decision 2015/778 of 18 May 2015 on a European Union military operation in the Southern Central Mediterranean (EUNAVFOR MED).* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015D0778 (Downloaded: 29.03.2017)

[40] EEAS: *European Union Naval Force – Mediterranean Operation Sophia.* https://eeas.europa.eu/sites/eeas/files/eunavfor_med_-_mission_14_february_2017_en.pdf (Downloaded: 29.03.2017)

[41] EEAS: *EUNAVFOR MED: operation SOPHIA training ships San Giorgio and Rotterdam welcomes on board the Libyan trainees.* https://eeas.europa.eu/headquarters/headquarters-homepage/16066/eunavfor-med-operation-sophia-training-ships-san-giorgio-and-rotterdam-welcomes-board-libyan_fi (Downloaded: 29.03.2017)

[42] EUROPEAN COMMISSION: *Infografika – Az EU földközi-tengeri műveletei 2016-ban.* www.consilium.europa.eu/hu/infographics/saving-lives-sea-november-2016/ (Downloaded: 29.03.2017)

[43] EEAS: *EUNAVFOR MED activity update to 31 December 2016*. https://eeas.europa.eu/csdp-missions-operations/eunavfor-med/3790/eunavfor-med-operation-sophia_en (Downloaded: 29.03.2017)

[44] EEAS: *EUNAVFOR MED Op SOPHIA – Six Monthly Report 1 January–31 October 2016.* Brussels: Council of the European Union, 2016. http://statewatch.org/news/2016/dec/eu-council-eunavformed-jan-oct-2016-report-restricted.pdf (Downloaded: 29.03.2017)

[45] DÓRA L.: Magyar részvétel a mediterrán térségi műveletben. *Honvédelem* (online), 2015. 10. 20. https://honvedelem.hu/cikk/54195_magyar_reszvetel_a_mediterran_tersegi_muveletben (Downloaded: 29.03.2017)

AARMS Vol. 17, No. 1 (2018) 87–140. **10.32565/aarms.2018.1.8**

Application of Science–Technology–Society Studies in Information Security Research

Review of Journals for Theory and Advanced Research Design[1]

András NEMESLAKI[2]

The research question and problem statement I posed to answer simply has been: what kind of patterns and specific discourses can be identified around the keywords of "information security" and "social construction" in information systems and its related reference fields such as social sciences, management studies, decision sciences extended to psychology. We may start summarizing the conclusions by stating that "information security" and "social construction" in the SCOPUS domain offers a wide range of literature in the social sciences and related subject areas; the initial search resulted in 406 article hits, whose basic bibliographic parameters with keywords and abstracts were downloaded. I categorized this sample according to the journals H-index, the Scimago Journal & Country Rank (SJR) Q1–Q4 ranking and the individual papers' citations, into five—so-called structural—clusters. Three papers were identified as the highest referenced and most influential, and analysed separately. The other were clustered as follows: 30 papers were classified into CL1, a high impact cluster due to its high citation and H-index, 122 papers were grouped into CL2, a mature cluster, due to their publishing date and medium referencing, 71 papers fell into CL3, a high potential cluster, due to their high H-index and recent appearance and, finally 152 papers were clustered into CL4, the mainstream of the sample due to their medium impact and wide spread of publishing dates. These clusters were further analysed with basic text mining techniques: word counting, key word analysis, textual clusters and N-Gram analysis, and concordance analysis. I found that clusters are different as far as the academic discourse on information security evolves, and each contain unique added value to the social construction of information security amongst users, institutions, technology and public policy. Finally, conclusion and further research opportunities are presented.

Keywords: *information security, social construction, SCOPUS data analysis, text mining, literature review*

[1] The work was created in commission of the National University of Public Service under the priority project PACSDOP-2.1.2-CCHOP-15-2016-00001 entitled "Public Service Development Establishing Good Governance" in the Ludovika Workshop.

[2] CSc (Ph.D.), Professor of Information Systems, National University of Public Service; e-mail: nemeslaki.andras@uni-nke.hu

Introduction

This contribution is positioned as an integral part of a comprehensive research program executed at the National University of Public Service, which aims to bring together the top down and bottom up dilemmas of information security strategy process. [1] Based on Giddens' structuration and Venkatraman's strategic alignment theories we developed arguments for the application of "social construction" as a metaphor both for gaining understanding of the bottom up agencies and emergencies, and for the top-down trickling of strategies through institutions and policies in information security.

The objective of this paper is to examine how the notion of information security is viewed through the lens of the Science-Technology-Studies program (or sometimes referred as Science-Technology-Society both resulting in the acronym STS). I argue that this proposition is important both for practice and for theory, since the complexity of policies, governance and funding needs guidelines and insight to address the challenges of society in the cyberspace. Information security for individuals, organizations and very importantly to governments is pivotal amongst these challenges, and the reforms and activisms represented by the "broad churches" of STS provide a rich platform to enhance the discourses of scientific and technological knowledge in socio-political contexts. [2]

By taking a grounded theory approach within this framework, I present an exploratory analysis of reviewing the available contemporary scientific research in the field of information systems management and its transdisciplinary subject areas. As a corpus, I chose SCOPUS Scientific Journal Ranking and Journal Search database, mainly due to its broadness and easy access.

The research question and problem statement I posed to answer simply has been: what kind of patterns and specific discourses can be identified around the keywords of "information security" and "social construction" in information systems and its related reference fields such as social sciences, management studies, decision sciences extended to psychology. It is important to note, that I excluded in this paper the review of literature in engineering, computer science and natural sciences—references in these subject areas were only taken into consideration in case the outlets have been cross-listed with social sciences or humanities.

In the next sections, I present the research in the following structure; first a definition and brief review of the search terms are outlined as a conceptual background, then the concept of the research model and research design is shown, including the description of the methods and tools used throughout the study. This is followed by an in-depth discussion of the gathered data and several quantitative and qualitative analyses are displayed. Finally, the findings are summarized, together with the implications taking the limitations and validity into consideration.

Concepts and Definitions

We have three central topics in this review: STS, information security and social construction.

Science Technology Studies – STS

In the course of my proposed research design, they are investigated in the STS framework for three key reasons. Firstly, due to the fact, that STS has an active standpoint; it is often referred to as an "engaged program" assuming actions, creating solutions both conceptual and pragmatic. [3] This approach perfectly fits with the contemporary dilemmas of cyber-security challenges. Secondly, STS is inherently social and treats scientific and technological development as a complex social process, and considers that solutions/products of these developments are not "natural" by themselves. [4] This is especially relevant with information technology and information system applications, since they are all created, programmed, designed by humans where the "sciences of the artificial" apply. [5] And finally, the third reason to embed this work into the STS domain, is the broader context of politics and the role of governance at high and low levels to address the new digital world especially in terms of cyber-threats. Scholars in the STS program have developed clear arguments that not only science and technology forms politics and government, [6] but, and this is probably a more important direction in this case, the political neutrality of science and technology is also questionable [7]—several technological paradigm changes have happened thanks to government interventions or even high level political influences (space programs, the trickling effects of military technology, or even the internet). The STS approach, in conclusion, is broad enough in scope and in breadth to connect theories and practices, institutions and emergencies, not only to theorize information security but also for supporting pragmatic public policy programs, as well.

Information Security – ISec

In the proposed scheme of research design the epistemology of information security is connected to STS. As [8: 838] puts: "a key focus in ISec research is finding ways to motivate end users, employees and consumers to improve protection of their individual and organization information assets". Naturally, ISec is not only a user-oriented terminology, it is generally entailing protection against threats, originating "outside" of institutions, but as it has been investigated recently quite often from "inside" organizations. [9]

While having in mind, that protection of all kinds of data and related processing resources—such as systems and individuals—is a very old concept, and not related to computers or communication technologies at all, in the course of this study I inherently attach ISec to information communication technologies. The main reason for this is the fact, that ICT has become so ubiquitous that it is inseparable from our daily life. [10] ICTs have amplified, transformed and enabled breakthrough innovations to threaten the confidentiality, integrity and availability (the so-called "CIA principle"), that is the assurance of information and IT-security. Technologically these threats take various forms such as viruses, malware, worms, e-mail spam, spyware, Trojan horses, Nigerian-letters—quickly changing variations of malicious codes penetrating into information systems and compromising their functioning. [11] As we showed earlier, the rich social context of ISec has been recognized and intensively investigated, for instance [12] a framework has been developed organizing the challenges into three categories:

- data processing integrity: ensuring that content is correct and reliable,
- system access and protection: data is available, retrievable and properly restricted,
- system structure and usage: how easily information is comprehended and protected.

Furthermore, beyond the classic theories of human and organizational interactions with ICT—such as TAM, [13] UTAUT [14] or sociomateriality [15]—new theories are brought to investigate these extended social challenges such as criminology, [16] general deterrence or protection motivation theories (GDT, PMT) from psychology literature. [8]

Apart from the theoretical compositions of ISec, we have looked at our practical experience in educating information security managers for central and local government institutions. According to the expectations and curriculum requirements, these people have to be in charge of the security of the electronic information systems, and be aware of the legal, administrative, safety and quality management bases of their work. They should be able to perform assessing risks at a high level, be able to control the security of systems, and handle the incidents which occur. Topics they need to acquire in their CISO trainings are:

- *General knowledge areas of management, technology and legislation:*
  - Quality management,
  - Technologies of security,
  - Security policy,
  - Legal and administrative areas,
  - Organization and management.
- *Information Security Systems Management Areas:*
  - Information security standards,
  - Management of information systems,
  - Information security strategy and leadership,
  - Information security organizations.
- *Information Security Process Management Areas:*
  - Information security program,
  - Application of information security technologies,
  - Information security awareness exercise,
  - Security of information systems,
  - Information security of networks,
  - Testing and auditing information security.
- *Incident and Security Risk Management Areas:*
  - Risk assessment and risk management,
  - Practical risk management of intrusion,
  - Incident management and continuity planning,
  - Practical incident management exercise.

Government strategies and institutional legislation for governing information security is expressed and enforced through security policies, decrees, laws and organizational arrangements. In this context, general knowledge and compliance—often addressed as awareness—to these guidelines and directives are imperative elements of ISec. [17] There is a stream of research in this context arguing that both compliance and motivation of users/employees/civil servants can be achieved by raising policy awareness, systematic

enforcement and regular maintenance of technological and human procedures in information security management. [12] [18]

Finally, for conceptualizing on ISec, the "CIA principles" over the last years have been appended with the notion of privacy, authenticity and trustworthiness—which have become integral conditions for all electronic services.

Social Construction of Technology – SCOT

The academic school of SCOT emerged in the discourses about interaction and influence between technology and society. SCOT can be positioned as an alternative to technological determinism, which is a typical engineering world-view, taking technology-related strategies governed by rationality, accurately designed, economically clear and unambiguous investment [4]. In this world-view, quite opposite to SCOT, there is no need for social interpretation of technology solutions, the wider environment is not interesting for how technology evolves, since it is gradually adapting to the effects of technology.

The essence of the SCOT theory is that it does not deal with the highly controversial cause-and-effect relationship between the interaction of society and technology but considers human communities as part of technological innovations. [19] Bijker's book on bicycle, Bakelite and fluorescence flashlight presents details of SCOT through the elaboration of the technical history of these three stories. [19] [4]

Bijker explains the connection between relevant social groups (RSG), the individuals who have similarities in their attitude and behaviour; they share the same technology frame and therefore they have the same interpretive flexibility. The technology frame consists of several elements, all conceptualized by the particular RSGs, like the functionality of the given technology artefact, possible ways it addresses solving the users' problems, the scientific theories underlying its working, the affordances with which it offers intuitions for use, what kind of knowledge it requires to operate, how it was designed, tested and implemented. The essence of interpretive flexibility is that technology frames are different amongst RSGs, the same artefact gets rather different translations about their meaning, use, and value. This leads to the situation that technologies with the same set of functionalities and applications might lead to substantially different problem framing and solutions—or constructions, using STS language.

The interpretation of technology is provided by the shared meaning developed in the given RSGs. Dialogues within the RSGs reinforce the technological frames as the artefacts develop in one way or another. This leads to the situation that isolated RSGs have more and more powerful frames, which in return determine the RSG's impact on the development direction of the artefact. When RSGs are not isolated they dispute with each other, and as long as there is no socially accepted interpretation represented by the most dominant RSG, that technology can be regarded as unstable because its evolution is characterized by many competing variants and experiments. Stabilization or closure is reached when one of the RSG's technology interpretations becomes dominant, and a macro level consensus emerges for the particular artefact. The "flexible" interpretation of technology is thus eliminated and the social meaning of the work becomes stabilized.

According to Bijker's case study on the development of bicycles, the so-called "safety" bicycles have long been awaited, because of the rather diverse relevant social groups in the nineteenth century. For instance, at that time the group of athletic men were the most dominant, and bicycles as artefacts were interpreted according to them as technologies for acrobatic achievements, sport, and masculinity requiring manly skills and competitiveness. Other groups, like women's cyclists, were far less significant, as the early asymmetrical bicycle for them meant high risks, discrimination due to the lack of fitting with acceptable female attire, unreliability and many inconveniences. The safety bicycles got stabilized in their present form, when the artefact allowed more RSGs to realize that the technology frame can be altered, and travel, commuting and leisure can also be part of the interpretive flexibility. [19] Bijker's example of the bike has demonstrated the many experiments, attempts, trials dead-lock directions, often in parallel, but always in accordance with one seemingly dominating interpretation of a particular RSG, and technological framework.

I propose SCOT as a powerful concept to deepen our understanding about the challenges of the cyberspace, since for example, the Internet itself can be easily associated with numerous RSGs and their interpretation of technology. Hackers take it as an environment for solving puzzles and breaking lock pads, armies look at it as new theatres for war, suppliers as new markets for products, administrations as a more and more risky channel to reach citizens, and ordinary users as a jungle of threats and dilemmas regarding their life in the cyber world.

In any case, contribution of SCOT literature might reveal the non-linear pattern of development in security management, and importantly some of the driving forces behind the twist-and-turns of adapting information security compliance.

Research Model and Methodology

This design and methodology were exploratory in nature, and its objective has been to provide a first level insight to a robust text mining research design, based on these results. As part of this work, I tested several open-source text analysis tools, developed in R platform, or using other general application packages. In the course of this paper I cannot discuss the experiences and results, regardless that experimentation has been a valuable effort resulting in creating a toolkit for "easy text-mining". To the conclusions and limitations of this approach I return in the last section of the paper.

Research Model

The research model is summarized in Figure 1. I used keyword search on the terms of information security and social construction. This solution proved to be useful to provide substantial amount of hits, because the inclusion of STS as a key phrase would have limited the search too much.

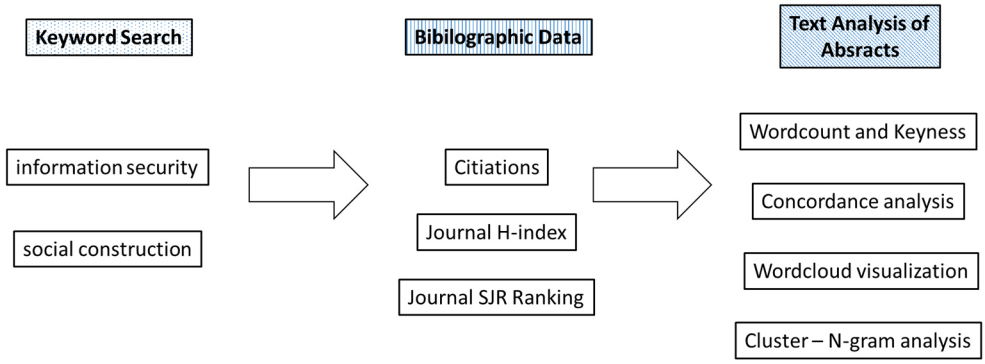

Figure 1. *Research Model.* [Created by the author.]

The second part of the design focused on structural analysis of the bibliographic data—amongst these two are describing the journal (the H-index and the quality ranking) and one particularly the given paper (number of relevant citations).

Finally, in order to get a textual insight to the topics I ran four basic text analysis methods on the corpus of the abstracts of the papers.

Research Methodology

For implementing the design, I used three research methods, a keyword search on the SCOPUS database, a two-step cluster analysis using SPSS, and the text analytics using AntConc,[3] COWO[4] and VOSviewer.[5] In this section I only describe SCOPUS and the sample resulting of the keyword search, the rest of the methods will be introduced in the next, discussion section. The Scopus abstract and citation database is available by Elsevier since 2004 at www.scopus.com. The largest percentage of materials consist of scientific and technical items, and references can be traced back to the 1960s. The database items include books and monographs as well, not only journals, in several languages, but mostly in English. Science Direct, Elsevier's full-text database using SCOPUS is available at www.sciencedirect.com . It provides PDF and other exportable formats of natural, medical, technical journals and books. More than 3,800 journals and 35,000 books can be searched for keywords, author name, title, image, etc.

There are 27 subject areas (e.g. Decisions Sciences, Social Sciences or Computer Science) available for national and periodical ranking, with a total of 313 subject categories (for instance "law" with more than 400 journals is a subject category under the "social sciences" subject area), 8 regions (Africa, Latin America and North America, Western and Central Europe, Pacific region) or country and year (1996-2015). For journal ranking

[3] www.laurenceanthony.net/software/antconc/
[4] http://clementlevallois.net/portfolio.html
[5] www.vosviewer.com/

and targeted search, it is sufficient to provide the journal's title, ISSN number, or the name of the publisher. One can also search for documents by type (journals, book series, or even indexed conference proceedings).

The keyword search on "information security" and "social construction" ran in 8 subject areas and only selecting academic journals (conferences, books were omitted):

- Social Sciences,
- Business, Management and Accounting,
- Arts and Humanities,
- Psychology,
- Decision Sciences,
- Economics and Finance,
- Psychology (Medicine),
- Multidisciplinary.

In order to get an insight to the relevance of the hits, I used three indicators, SCOUPS SJR ranking, the journal H-index and the papers' citations.

Ranking of scientific journals in SCOPUS is assessed by the "SCImago project". The Scimago Journal & Country Rank ranking was developed by researchers in 2009, who are dealing with information analysis, retrieval and presentation of publication data. To determine the index, the number of references should be weighted by the number of references in the referenced journal. SJR journal-based ranking can be divided into groups of high-quality documents—s quartiles (Q) form—on the basis that the document provides specialty prestigious journals which:

- Q1 – "Excellent:" The top 25% of the ranking based on the SJR metrics of the industry.
- Q2 – "Good:" 50 to 75% of the ranking based on the SJR metric.
- Q3 – "Medium:" 25% to 50% of the ranking based on the SJR metric.
- Q4 – "Poor:" The lower 25% of the rankings of the SJR metrics for the industry.

The ranking is publicly available on the official website: www.scimagojr.com. SJR numbers can be sorted and other data can be seen, such as the country in which the publication was made, the H-index, the number of references in the year selected and within 3 years, the number of publications in the year chosen and within 3 years. It is important to note, that journals can be ranked in more subject areas and categories at a time, and the same journal can have different ratings in these areas.

Description of the Sample and the Corpus

The initial search resulted 406 article hits, whose basic bibliographic parameters with keywords and abstracts were downloaded. Yearly distribution can be seen in Figure 2.

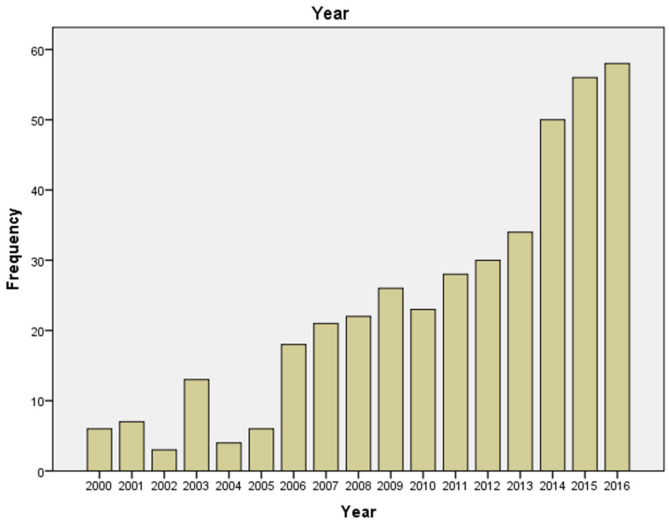

Figure 2. *Papers' yearly distribution between 2000–2016. (Search terms: information security AND social construction.)* [Created by the author.]

It is interesting to notice that publication on this topic started with waves in the early 2000s and until 2013 there was a steady growth in this topic. Then, from 2014 for some reason a boost started and it seems like the social context with information security started to boom.

Distribution between SCOPUS Subject Areas and the journals SJR ranking quality is summarized in Table 1.

Table 1. *Distribution of the corpus by subject areas.* [Created by the author.]

		Subject Areas (SBJA)							
		Business and Management	Social Sciences	Psy-chology	Decision Sciences	Arts	Eco-nomics	Multi-discip	Medi-cal
		Count	Count	Count	Count	Count	Count	Count	Count
SJR	Q1	34	88	20	22	1	9	3	2
	Q2	25	41	7	7	0	3	0	1
	Q3	12	29	3	3	0	0	1	0
	Q4	4	5	2	2	0	0	2	0

As it was accepted, most hits came from Social Sciences and the Management subject areas but the relevant number of publications contains the search words in decision science, and psychology, as well. It is important to note that several journals have more listings—we took the first and the one which harmonizes the journal "title" and genre.

Table 1 also shows that the journals are high quality, the majority of them are Q1 and Q2 SJR ranked. Table 2 lists the most relevant journals of our sample—these are the journals with Hirsch-index higher than 100 at the time of the data collection. As we can see there

are 28 journals amongst the most relevant which all together hold 46 papers of the initial 406. Not surprisingly the ones which included more than one paper with our search word combination are "information system" related (MISQ, Information Sciences, or Journal of MIS) or embedded in decision sciences (DSS, Info Science and Technology, Information and Management). We also find journals from medicine, psychology and social sciences but these are just general indicators without really looking into the content of the papers.

Another important indicator for a paper's relevance is its citation number. This is what we present in Figure 3. Naturally, one has to be careful with judging relevance by citation only, especially in the case of recent papers, since it takes time for a publication to reach readership and climb its citation number. Regardless, a first look at the highest numbers show some interesting insights on what academic readership quotes and refers to a lot. The highest number is a total of 725 references for one article while at the other end we have 41 papers which have 1 SCOPUS citation. All together 311 papers were cited at least once until the time of this essay.

In Table 3 I show the most highly sited papers with our keyword search together with their subject areas. We can see that all papers are Q1 indexed, and from high impact journals (not necessary IF because we use a different database). Six items come from the Decision Science subject area from very high H-indexed journals, two from Business Management and Accounting and one-one from Psychology and Economics.

Table 2. *Journals with a H-index greater than 100 and the papers in the corpus.*
[Created by the author.]

	Journal	**H-index**	**Papers**
1.	*Academy of Management Journal*	252	1
2.	*Journal of Applied Psychology*	218	1
3.	*Quarterly Journal of Economics*	205	1
4.	*Management Science*	198	1
5.	*Social Science and Medicine*	195	2
6.	*Research Policy*	178	1
7.	*MIS Quarterly: Management Information Systems*	177	4
8.	*Ecological Economics*	151	1
9.	*Journal of Organizational Behaviour*	134	1
10.	*World Development*	133	1
11.	*Information Sciences*	131	3
12.	*Tourism Management*	130	1
13.	*Information Systems Research*	128	1
14.	*Information and Management*	128	2
15.	*Global Environmental Change*	120	1
16.	*Journal of Business Ethics*	120	2
17.	*Global Environmental Change*	120	1
18.	*Journal of Management Information Systems*	119	5
19.	*Psycho-Oncology*	113	1
20.	*Journal of the Association for Information Science and Technology*	112	3
21.	*Computers in Human Behaviour*	111	2
22.	*Decision Support Systems*	109	3

	Journal	H-index	Papers
23.	*Journal of Experimental Social Psychology*	108	1
24.	*Accident Analysis and Prevention*	108	2
25.	*Cyber-psychology, Behaviour, and Social Networking*	106	1
26.	*Appetite*	104	1
27.	*Accounting, Organizations and Society*	103	1
28.	*Behaviour Research Methods*	103	1
	Total		46

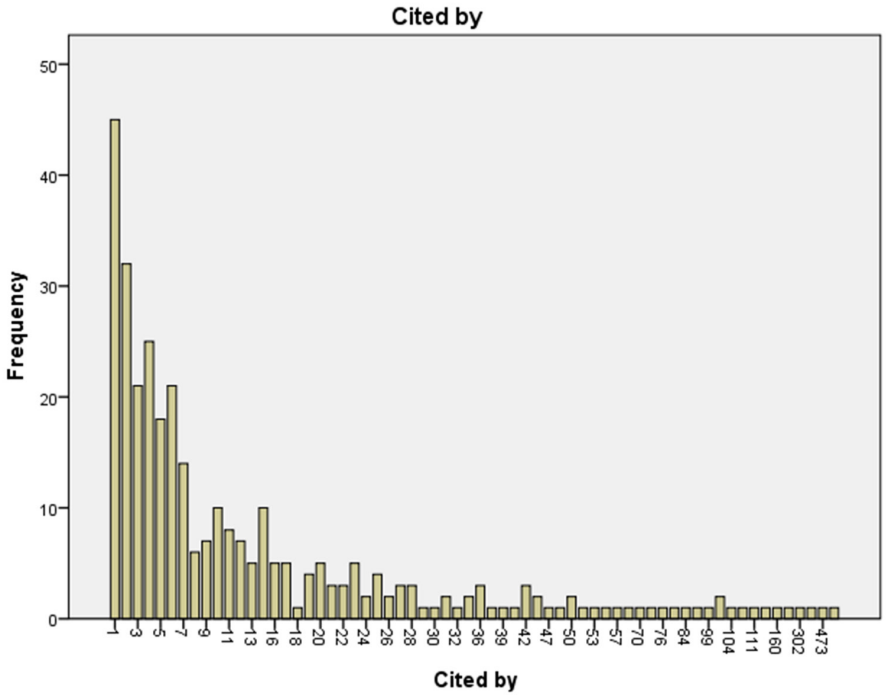

Figure 3. *Number of citations in Scopus.* [Created by the author.]

They are rather mature papers, the oldest was published in 2003 and the most recent from this list is also six years old. This is again in alignment with the citation cycle, but also indicates the fact that when technology issues get mixed with social impact analysis, more time is needed for assessing results and publish findings of robust research results.

Table 3. *The top cited papers with the search phrases and their subject areas.*
[Created by the author.]

Authors	Title	Year	SJR	H	SBJA	Journal	Cites
Kim D.J., Ferrin D.L., Rao H.R.	A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents	2008	Q1	109	DS	Decision Support Systems	725
Ariely D., Loewenstein G., Prelec D.	"Coherent arbitrariness:" Stable demand curves without stable preferences	2003	Q1	205	ECON	Quarterly Journal of Economics	473
D'Arcy J., Hovav A., Galletta D.	User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach	2009	Q1	128	DS	Information Systems Research	315
Johnston A. C., Warkentin M.	Fear appeals and information security behaviours: An empirical study	2010	Q1	177	DS	MIS Quarterly: Management Information Systems	302
Yousafzai S. Y., Pallister J.G., Foxall G.R.	A proposed model of e-trust for electronic banking	2003	Q1	94	BMA	Technovation	176
Workman M., Bommer W.H., Straub D.	Security lapses and the omission of information security measures: A threat control model and empirical test	2008	Q1	111	PSCHY	Computers in Human Behaviour	160
Li X., Hess T.J., Valacich J.S.	Why do we trust new technology? A study of initial trust formation with organizational information systems	2008	Q1	68	BMA	Journal of Strategic Information Systems	130
Iivari J., Huisman M.	The relationship between organizational culture and the deployment of systems development methodologies	2007	Q1	177	DS	MIS Quarterly: Management Information Systems	111

Authors	Title	Year	SJR	H	SBJA	Journal	Cites
Kim D.J.	Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study	2008	Q1	119	DS	Journal of Management Information Systems	109
Guo K.H., Yuan Y., Archer N.P., Connelly C.E.	Understanding nonmalicious security violations in the workplace: A composite behaviour model	2011	Q1	119	DS	Journal of Management Information Systems	104

In Table 4 I attached the authors' keywords to the papers, so at a quick glance, the topics can be identified in the case of the top cited papers. As a result of this visual check, and verifying by reading the abstract of the missing keywords, I decided to omit this paper from further analysis, since the topic had no connection to information security in the context of information systems or cybersecurity.

Table 4. *There is a significant correlation between journal H-index and citation—even in the dynamic field of info security.* [Created by the author.]

Authors	Paper Title	Author keywords
Kim D.J., Ferrin D.L., Rao H.R. 725	A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents	Antecedents of *trust;* Consumer trust; Electronic commerce; Internet consumer *behaviour*; Perceived risk; Privacy and security; The role of trust; Trusted third-party seal
Ariely D., Loewenstein G., Prelec D. 473	"Coherent arbitrariness": Stable demand curves without stable preferences	No Keywords (After analysing the abstract, the paper is omitted from the analysis)
D'Arcy J., Hovav A., Galletta D. 315	User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach	End-user security; General *deterrence* theory; IS *misuse*; IS security; Security countermeasures; Security management
Johnston A.C., Warkentin M. 302	Fear appeals and information security behaviours: An empirical study	Coping appraisal; Countermeasures; *Fear* appeals; Information assurance; Information security; Persuasive communication; *Protection motivation* theory; *Threat appraisal*
Yousafzai S.Y., Pallister J.G., Foxall G.R. 176	A proposed model of e-trust for electronic banking	Electronic banking; *Perceived risk; Trust*

Authors	Paper Title	Author keywords
Workman M., Bommer W.H., Straub D. 160	Security lapses and the omission of information security measures: A threat control model and empirical test	Information security; *Omissive behaviours; Protection motivation theory; Social cognitive theory; Threat control model*
Li X., Hess T.J., Valacich J.S. 130	Why do we trust new technology? A study of initial trust formation with organizational information systems	e-Government; *Initial trust;* National identity systems; Organizational information systems; *Subjective norm; Technology adoption;* Trusting attitude; Trusting bases; Trusting beliefs; Trusting intention
Iivari J., Huisman M. 111	The relationship between organizational culture and the deployment of systems development methodologies	*Competing values model;* Information systems developers; Information technology managers; *Organizational culture;* Software engineering; Systems development; Systems development methodology
Kim D.J. 109	Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study	*Cross-cultural comparison;* Culture impacts; *Self-perception-based trust;* Transference-based trust; Trust in e-vendor; Type I and Type II cultures
Guo K.H., Yuan Y., Archer N.P., Connelly C.E. 104	Understanding nonmalicious security violations in the workplace: A composite behaviour model	information systems security; *nonlinear construct relationships;* nonmalicious *security violation;* perceived identity match; perceived security risk; relative advantage for job performance; *workgroup norms*
Cao L. 100	In-depth behaviour understanding and use: The behaviour informatics approach	*Behaviour analysis;* Behaviour computing; *Behaviour informatics;* Decision making; Informatics

Discussion of Results: Structural Cluster Analysis of the Papers

Four papers have outstandingly high citations, these were removed from the sample. These four are the following:

Table 5. *The four most cited papers for the keyword combination (information security and social construction).* [Created by the author.]

Authors	Title	Year	Journal	Vol	No	Pages	SJR	H-index	SA
Kim D.J., Ferrin D.L., Rao H.R.	A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents	2008	Decision Support Systems	44	2	544-564	Q1	109	Dec. Sci.

Authors	Title	Year	Journal	Vol	No	Pages	SJR	H-index	SA
Ariely D., Loewenstein G., Prelec D.	"Coherent arbitrariness": Stable demand curves without stable preferences	2003	Quarterly Journal of Economics	118	1	73-105	Q1	205	Econ. Fin.
D'Arcy J., Hovav A., Galletta D.	User awareness of security countermeasures and its impact on informa on systems misuse: A deterrence approach	2009	Information Systems Research	20	1	79-98	Q1	128	Dec. Sci.
Johnston A.C., Warkentin M.	Fear appeals and information security behaviors: An empirical study	2010	MIS Quarterly	34	3. SPEC. ISSUE	549-566	Q1	177	Dec. Sci.

After reading the title and the abstract, based on the content I decided to omit the Ariely paper, because it had no relevance to the ontology of information security in its context of our research. The remaining four, on the other hand, perfectly fit our topic and were kept for further analysis, and treated as seminal papers of the field.

The 382 papers remaining in the sample were further classified by Two-Step Cluster Analysis using three variables: year of publication, citation number and H-index of the journal where the paper appeared. Results indicated in Figure 4 show fair values of silhouette measure of cohesion and separation and showing that the importance of three predictor variables are above 0.77 confirming high predictability. Summary of the mean values and population of each cluster can be seen in Figure 5.

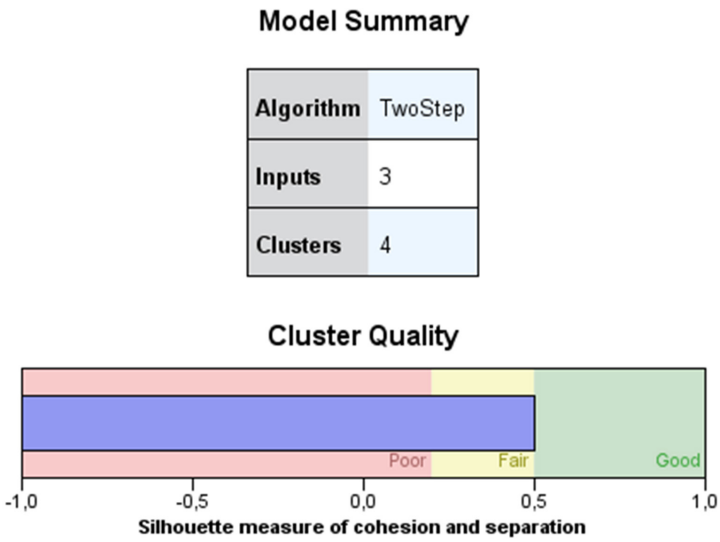

Figure 4. *Model Summary of the Two-Step Cluster Analysis in SPSS.* [Created by the author.]

8% of the papers (30 articles) got clustered into C-1. These papers were published in high H-index outlets, they are mature given the average age of 10 years (2007) and probably these factors contributed to their presently very high citation average (72.53 citation/papers). According to these features these papers were labelled as high-impact papers regarding our topic.

122 papers (32%) were classified into the second cluster—C–2—which I labelled as mature contributions, given the fact that their timing is similar to C–1, but the mean value of citation is almost 6 times lower (12.97 citations/paper) and these contributions have appeared in less highly indexed journals (H = 37.68).

The third cluster, C–3, contains 71 articles (19%) and might be considered as recent contributions, since they are around 3 years in circulation (2014). They were published in high impact journals (H = 86.13), but probably due to the relative freshness their citation number is significantly lower than the first two clusters'. For these reasons I marked these contributions as promising future since dynamically their relevance will grow.

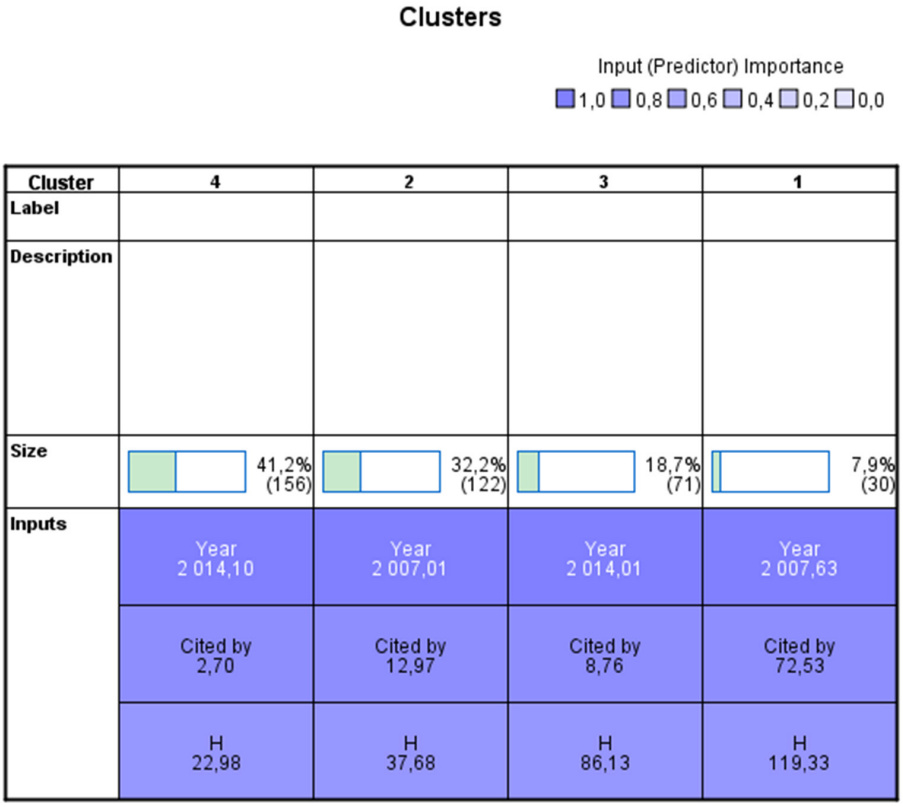

Figure 5. *Description of the four clusters.* [Created by the author.]

Finally, we can see 41%—the highest number—of papers in C–4, the fourth cluster. In terms of age these papers are almost identical to C–3, but they are significantly different as far as the lower impact (Citation = 2.7/paper—one fourth of C–3) and lower ranking of

journals is concerned (H = 22.98). These papers are structurally contemporary, but both in their prestige and impact bear the features of mainstream contributions—on average showing less potential than C–3, but reaching a wide group of readership regardless.

In order to get deeper insights to the four clusters, two evaluation fields were introduced, the variable of journal SJR classification (Q1–Q4) and the subject areas of the papers. These values were not used in determining the clusters, but their distribution helps us structuring the corpus better.

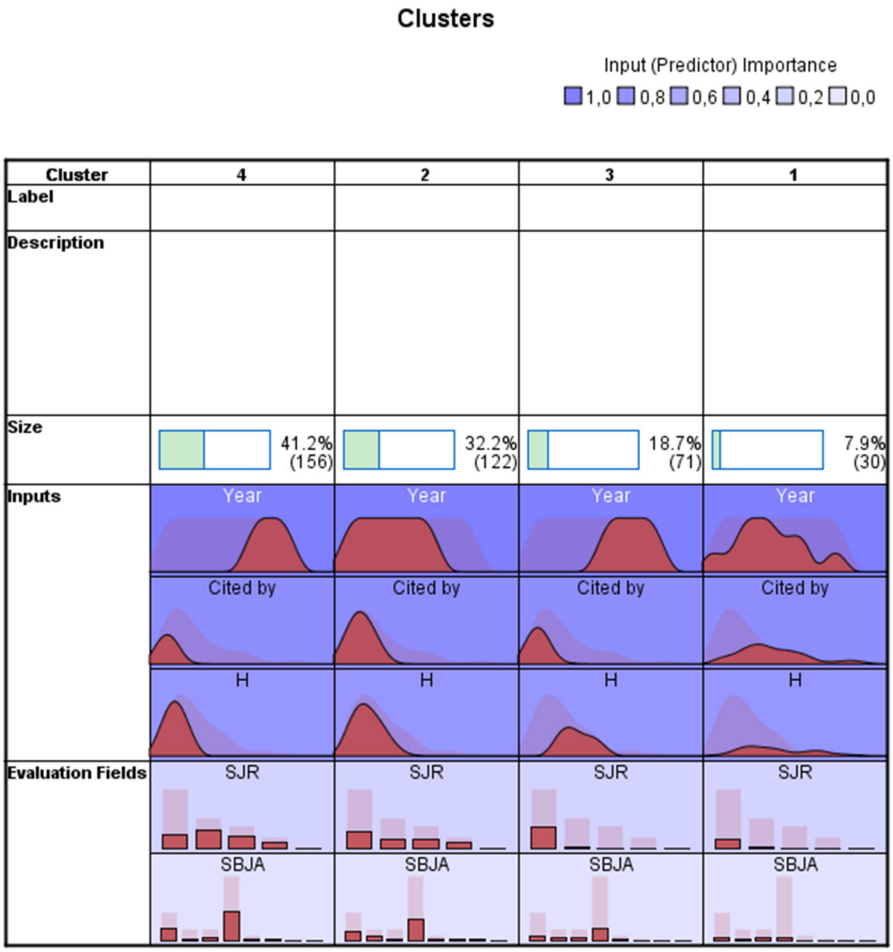

Figure 6. *Visualization of the clusters by including two evaluation fields and value distributions.* [Created by the author.]

In Figure 6 similarities and differences are visualized of the four clusters both for input and evaluation variables. Given the fact, that the evaluation fields are categorical variables "shape of distribution" is more narrative than the SPSS outputs of means. I would like to draw the attention of the reader to the interesting visual fact regarding the subject areas, that the C4, the mainstream cluster, holds significantly more submissions in

business-management-accounting and decision sciences (the first and fourth column), and the modus of the SJR ranking is Q2 journals, while in the other clusters topically decision science dominates and the journals are Q1 level mostly.
Cluster differences can also be studied by comparing the block-box diagrams in Figure 7 and Figure 8.

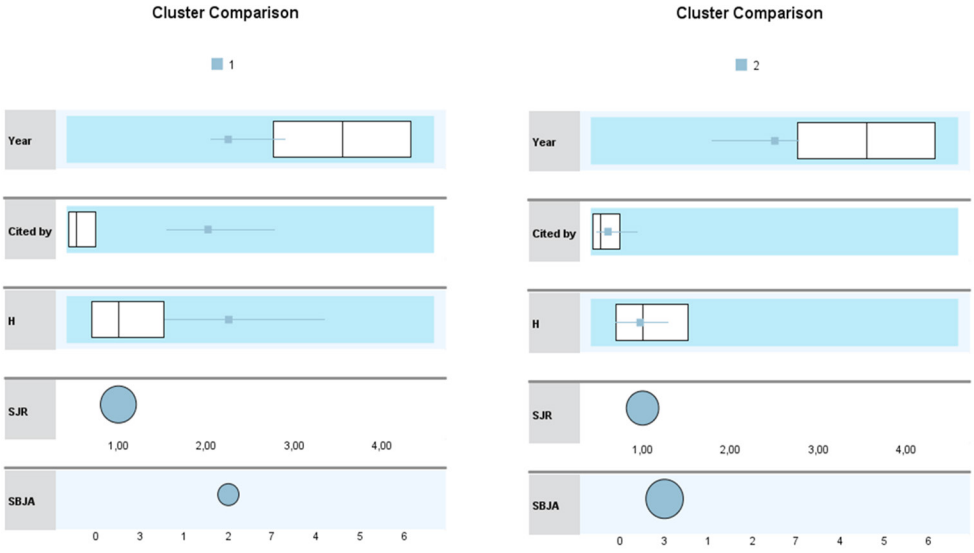

Figure 7. *Comparison of cluster variables for C1 and C2.* [Created by the author.]

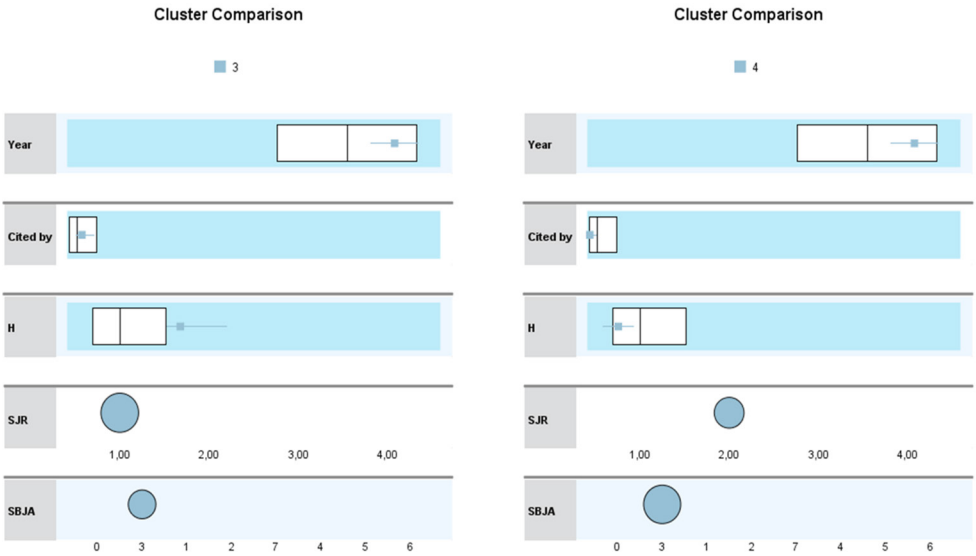

Figure 8. *Comparison of cluster variable for C3 and C4.* [Created by the author.]

The scatter-plot diagrams of the clusters provide several additional observations and implications for further analysis of our corpus. (Figure 9)

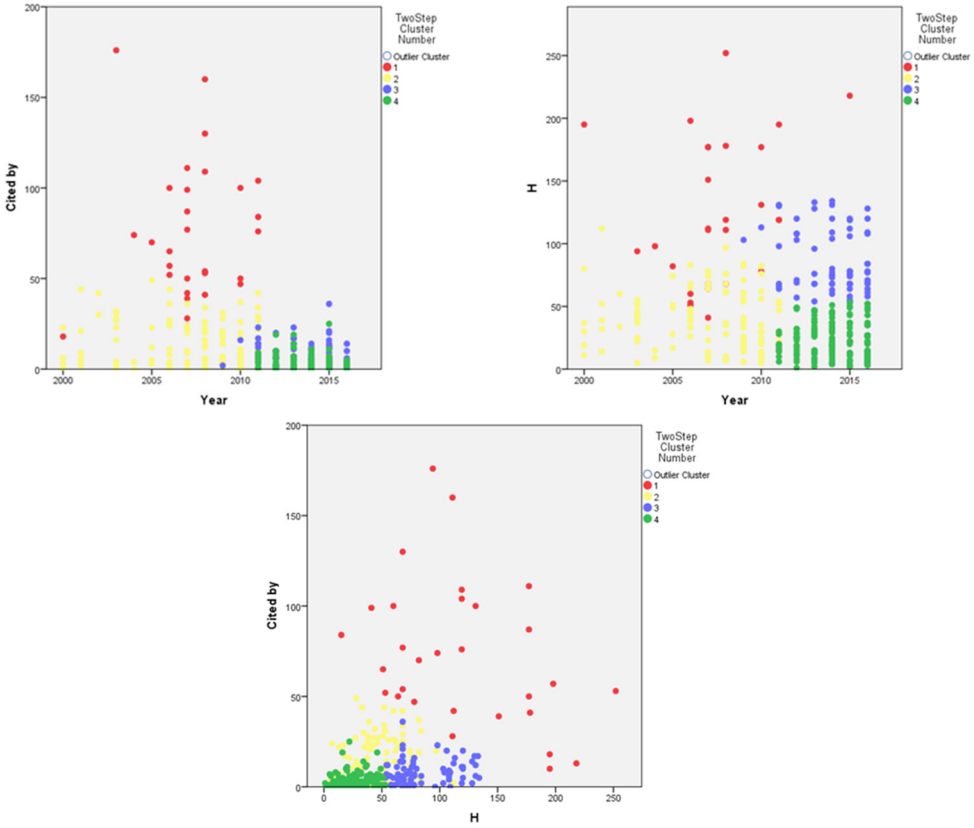

Figure 9. *Scatter plot diagrams of the abstract "points"—according to publication years, citationand journal H-index.* [Created by the author.]

For instance, the first scatter-plot in Figure 9 nicely demonstrates the high impact C1 is populated in the centre of our publication period of 2000-2016 and how much the cluster is elevated in terms of the citations above the others. This is then further emphasized in the second and, especially the third plots. This last one nicely shows the visual difference between C3 and C4 which are similar in terms of citations, and position on the year axis, but different in terms of journal impact. In the second plot this is indicated basically by C3 "sitting on" C4 demonstrating its higher potential for future impact. We can also see, how the mainstream cluster C2, spreads through the years and gives space from around the early 2010s to the green and blue clusters of C3 and C4, yet taking the main bulk of present citations between the high impact C1 and most recent C3 and C4.

Concluding the cluster analysis, we can safely say that the articles show a structured pattern based on their three cluster inputs and also regarding their two evaluation variables. We found five different groups analysing these parameters; the first being a small

set of "outliers" in terms of their citation number consisting of three papers in the topic of information security and social construction. Then, the second highest impact is a set of 30 papers in C1 with high citation numbers and impact, the only dilemma with them being the relative timeliness issue regarding information security given that these are around 10-year-old contributions. The third most relevant group is the next 71 papers in C3 which are relatively contemporary—3 years on average—and appeared in high impact journals. Our assumption is that these contributions have topics, methodologies and issues discussed which will be the next high impact cluster in some years. Finally, C2 and C4 are papers in similar quality journals, where C4 cluster members are more recent—probably covering different topics—and therefore also less cited. My assumptions are that C4 is potentially the next mainstream just like presently C2 covering both topically and methodologically ordinary craftsmanship of our profession—decent but breakthrough research in the field of information security.

In order to find out how the clusters differentiate, and weather the assumption based on the cluster variables hold, in the next chapter I present the result of the text analysis of the abstracts.

Discussion of Results: Text Analysis of the Abstracts

Based on the results of the two-step cluster analysis, I created five separate text files containing the 386 abstracts, and consider these as the main corpus for simple text mining and contextualizing the accumulated knowledge.

Table 6. *Text mining corpus merged from the abstract files.* [Created by the author.]

	File name	Cluster	Number of abstracts
1.	abstract_big_three.txt	Outlier three paper	3
2.	abstract_cluster_1.txt	CL1	30
3.	abstract_cluster_2.txt	CL2	122
4.	abstract_cluster_3.txt	CL3	71
5.	abstract_cluster_4.txt	CL4	156

Given the fact, that this amount of information does not have the depth of the full texts only the basic, simplest text processing methods were applied using AntConc 3.4.4., a freely available but robust multiplatform tool for carrying out corpus linguistics research and data-driven learning, developed by Anthony Laurence at the Faculty of Science and Engineering at Waseda University in Japan.

Word Counting

The first, and simplest way to look into the textual information of the corpus is to run word counts and compare word frequencies across the different clusters. For this I designed the following method.

Figure 10 shows the user interface, how the wordlist was created on the five files composing the abstract corpus. As a result, 82,700-word tokens were created using 7,920 different word types. This list then was used as the keyword list range, or as a corpus reference, compared to which I calculated the so-called keyness variable for each cluster file.

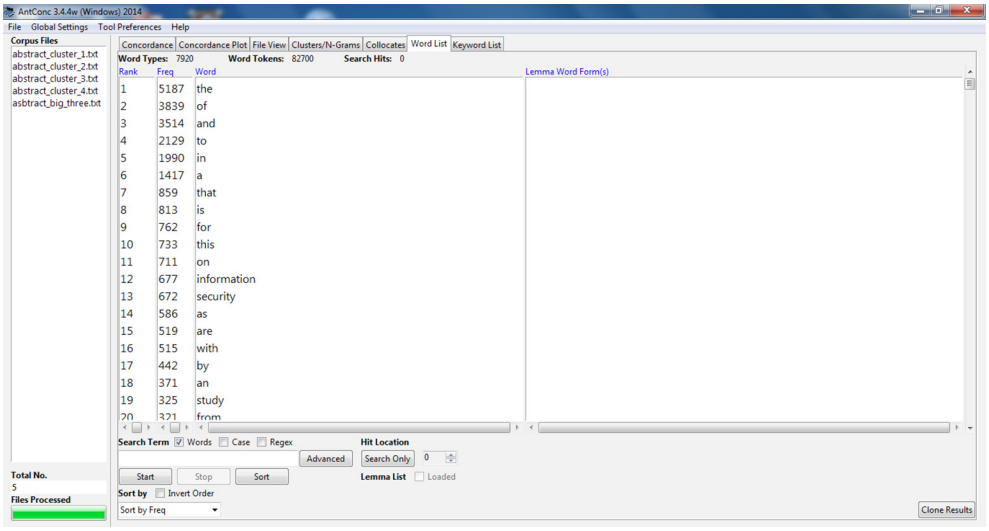

Figure 10. *Wordlist creation with AntConc on the Corpus.* [Created by the author.]

The analysis goes beyond a simple word count, since it shows which words are unusually frequent (or infrequent) in comparison with the words in a reference corpus. This allows us to identify characteristic words—hopefully unique to the individual clusters—as part of a genre.

Keyness is calculated using the Log Likelihood method. [20] When using either Log Likelihood or Chi-squared as the statistical measure, the following significance values apply:

- 95^{th} percentile; 5% level; $p < 0.05$; critical value = 3.84;
- 99^{th} percentile; 1% level; $p < 0.01$; critical value = 6.63;
- 99.9^{th} percentile; 0.1% level; $p < 0.001$; critical value = 10.83;
- 99.99^{th} percentile; 0.01% level; $p < 0.0001$; critical value = 15.13.

Taking this into consideration, I chose the 99% level of significance, using 7.00 as a critical keyness value. Accordingly, a word was considered a keyword—compared to the reference corpus—in case its keyness value was greater than 7.00. Results of the five different clusters are the following:

Three Top Cited Paper (Outlier Cluster)

Table 7. *Keyword keyness of the three most cited papers in the sample.* [Created by the author.]

	Freq.	**Keyness**	**Keyword**	**Verification with concordance analysis KeyWord in Context (KWIC)**
1.	8	51.608	misuse	IS misuse, misuse of information systems
2.	6	29.815	fear	fear appeals
3.	4	25.345	purchasing	purchasing decision, purchasing behaviour
4.	5	21.907	end	end user
5.	3	21.475	appeals	fear appeals
6.	8	21.291	trust	trust, reputation, privacy concerns,
7.	5	18.534	computer	computer users, computer monitoring, the context of computer security and information assurance, computer security actions, human-computer interaction,
8.	6	17.782	users	end user, IT user, computer user
9.	3	17.632	severity	severity of social influence, severity of sanctions severity of sanctions, certainty of sanctions,
10.	3	15.846	sanctions	
11.	2	14.317	certainty	
12.	2	14.317	efficacy	
13.	2	14.317	mitigation	
14.	4	13.786	consumer	consumer behaviour, consumer disposition to trust, consumer decision
15.	4	12.593	consumers	
16.	4	12.288	suggest	
17.	4	12.288	threat	threat to organizations, threat to punishment
18.	2	12.252	deterrence	
19.	3	11.962	actions	
20.	4	11.855	internet	Internet consumer
21.	6	11.081	model	deterrence theory model, conceptual model
22.	3	10.433	awareness	
23.	15	10.158	is	IS misuse, IS security
24.	2	9.938	reputation	
25.	2	9.938	website	
26.	3	9.726	user	
27.	4	9.248	perceived	perceived risk, perceived threat, perceived certainty and severity, perceived severity of sanctions
28.	2	8.520	incidents	

	Freq.	Keyness	Keyword	Verification with concordance analysis KeyWord in Context (KWIC)
29.	4	8.308	impact	impact is not uniform, impact the actions of end users, impact of sanction perceptions
30.	3	7.827	perceptions	
31.	1	7.158	describing	
32.	1	7.158	infusion	
33.	1	7.158	originate	
34.	1	7.158	posture	
35.	1	7.158	sanction	
36.	1	7.158	SETA	security education training awareness

In order to get a contextual understanding of the keywords, I copied results of the concordance analysis for those words, where the frequency of occurrences was greater than 4.

High Impact (C1) cluster

In Table 8 given the large number of significant keywords, I only went through the concordance analysis where the frequency of occurrence is higher than 10.

Table 8. *Keyword keyness of the High Impact Cluster (C1) in the sample.* [Created by the author.]

	Freq.	Keyness	Keyword	Verification with concordance analysis KeyWord in Context (KWIC)
1.	27	37.78	behaviour	behaviour analysis, modelling, informatics (BI), patterns
2.	14	34.95	SaaS	Software as a Service solutions, adoption, literature
3.	26	29.34	people	people requiring institutional care, technology supporting people, people become victims
4.	10	27.42	IFAC	IFAC Swiss registered non-governmental organization
5.	10	27.42	Obama	Obama campaign 2008
6.	16	25.71	culture	culture of secure behaviour, organizational culture, cross-culture, rational culture, Type I, II.
7.	22	25.70	perceived	perceived security, perceived privacy, perceived importance
8.	8	20.75	trusting	
9.	7	19.20	ISS	
10.	8	18.68	campaign	
11.	25	18.44	systems	information systems, information system development, information system field
12.	25	18.20	trust	trust determinants, trust formations, trust in people, trust in technology

	Freq.	Keyness	Keyword	Verification with concordance analysis KeyWord in Context (KWIC)
13.	7	18.02	rivals	
14.	7	16.96	retirement	
15.	6	16.46	dementia	
16.	6	15.29	bi	
17.	8	14.70	everyday	
18.	5	13.71	accreditation	
19.	6	13.32	methodologies	
20.	10	12.56	ability	perceived work ability
21.	8	12.31	behavioural	
22.	7	12.21	initial	
23.	5	11.56	aids	
24.	8	11.30	internal	
25.	9	11.26	type	
26.	4	10.97	contravention	
27.	4	10.97	telecare	
28.	5	10.68	banking	
29.	5	10.68	rational	
30.	10	10.65	housing	“Construction” context
31.	9	10.46	external	
32.	4	9.84	homes	
33.	8	9.56	complex	
34.	7	9.54	patterns	
35.	6	9.23	deployment	
36.	5	9.19	codes	
37.	5	9.19	solutions	
38.	4	8.88	his	
39.	6	8.72	outside	
40.	9	8.72	job	
41.	34	8.68	research	*Methodologically Related*
42.	5	8.55	relative	
43.	12	8.53	organizations	virtual organization, individuals and organizations
44.	8	8.45	identity	
45.	13	8.30	organizational	organizational systems, organizational change, organizational culture
46.	3	8.23	arena	
47.	3	8.23	Beijing	
48.	3	8.23	dwelling	
49.	3	8.23	neighbourhood	
50.	3	8.23	normative	
51.	3	8.23	outlaw	
52.	3	8.23	qual	

	Freq.	Keyness	Keyword	Verification with concordance analysis KeyWord in Context (KWIC)
53.	3	8.23	workgroup	
54.	5	7.97	attitudes	
55.	5	7.97	virtual	
56.	10	7.93	processes	processes of abstraction, social process, governance process, decision-making process
57.	6	7.79	intentions	
58.	7	7.52	identification	
59.	7	7.52	outcomes	
60.	8	7.47	user	
61.	5	7.43	standard	
62.	4	7.35	shaping	
63.	4	7.35	vendors	
64.	3	7.13	bases	
65.	3	7.13	hospitals	
66.	3	7.13	prompt	
67.	3	7.13	punishment	

Mature cluster (C2)

The mature cluster has only 12 significant keywords, in alignment with the assumption that this cluster characteristically is "mainstream" that is not different from the corpus averages.

Table 9. *Keyword keyness of the Mature Cluster (C2) in the sample.* [Created by the author.]

	Freq.	Keyness	Keyword	Verification with concordance analysis KeyWord in Context (KWIC)
1.	57	22.545	health	health care and social security
2.	34	17.074	attachment	children attachment, attachment to the house
3.	28	12.809	disclosure	information disclosure and non-disclosure, property disclosure, ISIS
4.	25	12.446	home	working from home, home-based work
5.	16	9.809	family	family in the social setting (not related)
6.	44	9.577	different	different colleagues, different environments, different IT, different disciplines, different mechanisms
7.	117	9.291	IT	IT as a security problem, IT-based signals, IT features, cooperation with IT vendors, IT professionals
8.	10	7.646	drug	Medical terms, *Not Related*
9.	10	7.646	mother	Social terms, not related.
10.	23	7.457	ICT	ICT use, ICT innovation, ICT adoption, ICT operations
11.	17	7.379	children	children safety and security

	Freq.	Keyness	Keyword	Verification with concordance analysis KeyWord in Context (KWIC)
12.	21	7.077	communities	different IS communities, communities of practice, diverse communities, on-line communities

There are two interesting general features however, the first one is the non-related health and social security topics, which naturally need to be omitted from information security context analysis, but apart from this we can also find more "classic" IS topics such as the IT and ICT terms, the questions of use and adoption along with the diversity issues of technology, people and communities ("different").

High Potential Cluster (C3)

Keyness in the high potential cluster indicates the major difference of these abstracts firstly around the phrases of teaching, instruction and scripts. By running the concordance analysis of these terms, we can see however, that some of these contributions are strictly related to education. The cluster is more relevant in terms of the contributions of Social Media or Social Networking Cites, which is a rather important stream of research in information security. Closely coupled with this the term of information sharing and social capital.

Similarly, safety in a very broad context seems to be a relevant term, followed by the topics of privacy which has not gained keyness in other clusters.

Similarly, to the terms of teaching, food security—although a very relevant area of security management—needs to be omitted from further analysis due to its distance from information security.

Table 10. *Keyword keyness of the High Potential Cluster (C3) in the sample.* [Created by the author.]

	Freq.	Keyness	Keyword	Verification with concordance analysis KeyWord in Context (KWIC)
1.	28	36.921	teachers	teachers reactions to scripts
2.	105	31.851	we	
3.	16	19.686	scripts	scripts in education
4.	14	17.955	instruction	instruction in the educational context
5.	13	17.627	SNS	Social Networking Sites, sharing behaviour, SNS users, ethical challenges, norms of using SNS, self-presentation
6.	12	16.271	scripted	scripted instruction method
7.	23	16.079	sharing	information sharing, sharing behaviour, knowledge sharing, process of social sharing
8.	9	12.204	millennials	
9.	26	12.147	network	social capital, SNS, social network analysis, network monitoring, management protocol, network operators, network structure, learning network, emerging network

	Freq.	Keyness	Keyword	Verification with concordance analysis KeyWord in Context (KWIC)
10.	31	11.68	safety	safety management, safety leadership, safety outcomes, safety participation, safety information
11.	10	11.615	illegal	illegal immigrants
12.	8	10.848	ca	
13.	8	10.848	eco	
14.	8	10.848	froebelian	
15	8	10.848	montessori	
16.	8	10.848	projection	
17.	8	10.848	snapchat	
18.	10	10.762	insecure	insecure information flow, insecure group conditions
19.	18	10.001	method	Related to research methodology
20.	22	9.711	energy	future energy systems, long term energy security, energy industries
21.	7	9.492	deduplication	
22.	7	9.492	humanitarian	
23.	7	9.492	ISDB	
24.	7	9.492	kindergarten	
25.	7	9.492	procedural	
26.	7	9.492	wri	
27.	9	9.444	abuse	
28.	9	9.444	scenario	
29.	27	9.081	food	food security—*Not Related*
30.	26	8.52	perceived	perceived usefulness of SNS, perceived privacy risk, perceived control and barriers
31.	28	8.512	privacy	privacy SNS users, privacy concerns, privacy vs publicity
32.	7	8.495	born	
33.	7	8.495	dissatisfaction	
34.	7	8.495	fisheries	
35.	6	8.136	congress	
36.	6	8.136	healthy	
37.	6	8.136	intergroup	
38.	6	8.136	neutralization	
39.	26	7.962	users	users are concerned, potential users, users permissions
40.	7	7.616	investigations	
41.	8	7.4	Facebook	
42.	6	7.149	clustering	
43.	6	7.149	conservation	

Recent mainstream cluster (C4)

In Table 11 from the 4th row the keyness log likelihood is only significant on the 1% level, so I did not execute concordance analysis, the key differences of this cluster are clearly seen from the keyword list. Discussion and research is focusing on all kinds of managerial issues, business and entrepreneurship and organizations.

Table 11. *Keyword keyness of the Mainstream Cluster (C4) in the sample.* [Created by the author.]

	Freq.	**Keyness**	**Keyword**	**Verification with concordance analysis KeyWord in Context (KWIC)**
1.	58	11.133	cloud	cloud services adaption, cloud storage, cloud service providers, benefits and risks of cloud computing
2	138	7.995	management	information security management, knowledge management, management of…, disaster management, environmental management
3.	2578	7.333	the	Grammatically interesting.
4.	23	6.566	entrepreneurs	
5.	23	6.566	malls	
6.	25	6.535	shopping	
7.	76	6.52	construction	understand the problem of social construction, discursive construction of security, construction of regulatory institutions
8.	63	6.285	business	
9.	28	5.773	supply	
10.	28	5.294	computing	
11.	18	5.139	cilicia	historical research—*Not Related.*
12.	17	4.853	rough	historical research—*Not Related.*
13.	34	4.773	organisations	
14.	89	4.716	factors	
15.	35	4.649	media	
16.	22	4.606	border	historical research—*Not Related.*
17.	15	4.282	indexes	
18.	15	4.282	smart	
19.	17	4.26	schemes	

As we identified in the cluster analysis, most papers appear in the business and management subject area listing, so this result is according to expectations. Apart from management, the cloud topic appears in this cluster in the context of service, storage and management adoption. It is interesting to note, that a special form of cloud computing—the SaaS topic—shows with very high frequency in C1, the high impact cluster.

Visualization of Clusters

In Figure 11 the visualization of the full corpus of the abstracts can be seen, followed by a zoom to the centre in Figure 12.

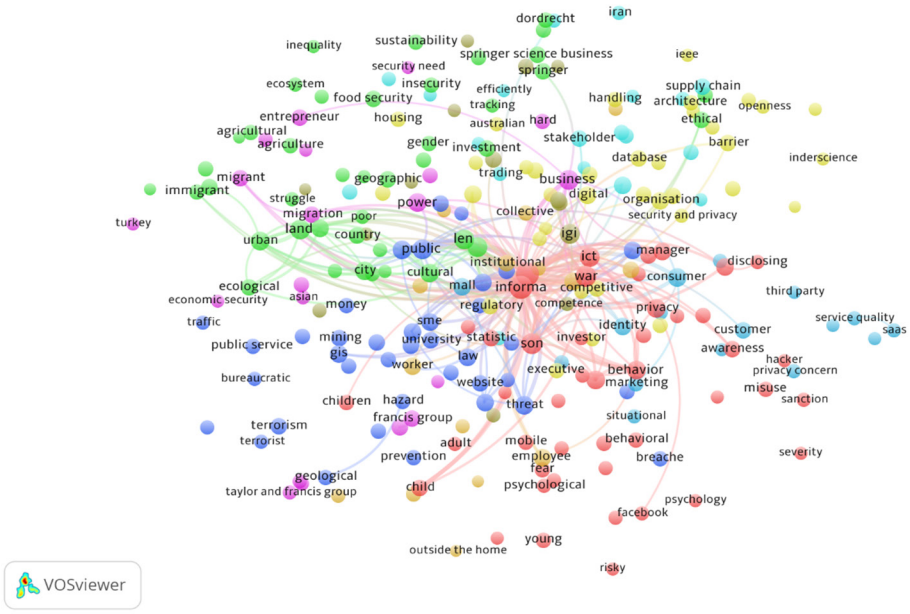

Figure 11. *Visualization of the full corpus (C1–C4 and top three cited papers).*
[Created by the author.]

The centre of the cluster-network shows terms such as information security, ICT, awareness, privacy; and other areas also appear such as national security, law, cyber or identity. In Figure 13, Figure 14, Figure 15 and Figure 16 the four main clusters are visualized—the outlier three-element cluster did not contain enough words in the abstracts to run the analysis. These series of figures provide a more structured insight to the discourses on information security.

The high impact CL1 cluster indicates discourses on three main word clusters, a core security topic, a managerial/organizational topic and a cultural/environmental topic.

CL2, the mature paper cluster holds much more abstracts and Figure 14 is a richer word cloud network. The major differentiators which we can see are the discussion on social securities in family setting (child, mother etc.), a broader set of topics on technology (architecture, ICT, technology) and business. What is also important in this cluster is the appearance of public administration, bureaucracy and criminal justice.

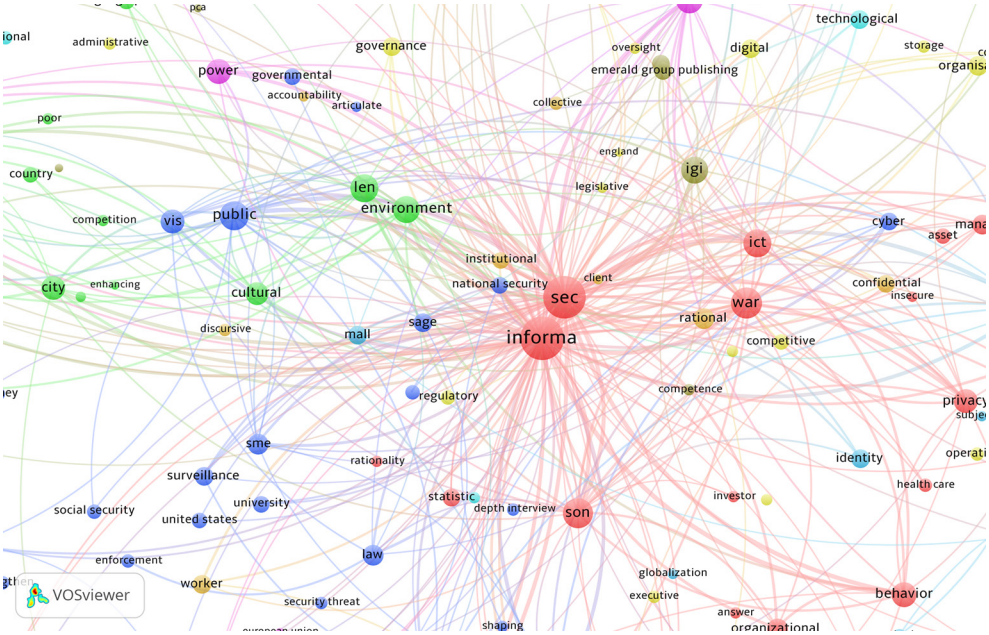

Figure 12. *Centre of the corpus network (information security).* [Created by the author.]

In CL3, what we called high potential cluster, Figure 15 shows also some new terms such as surveillance, security and privacy, employee and ethical. CL2 and CL3 both indicated topics of urban development and "city;" juxtaposing these terms with the keyness analysis we see that the smart city discourses appear in these clusters.

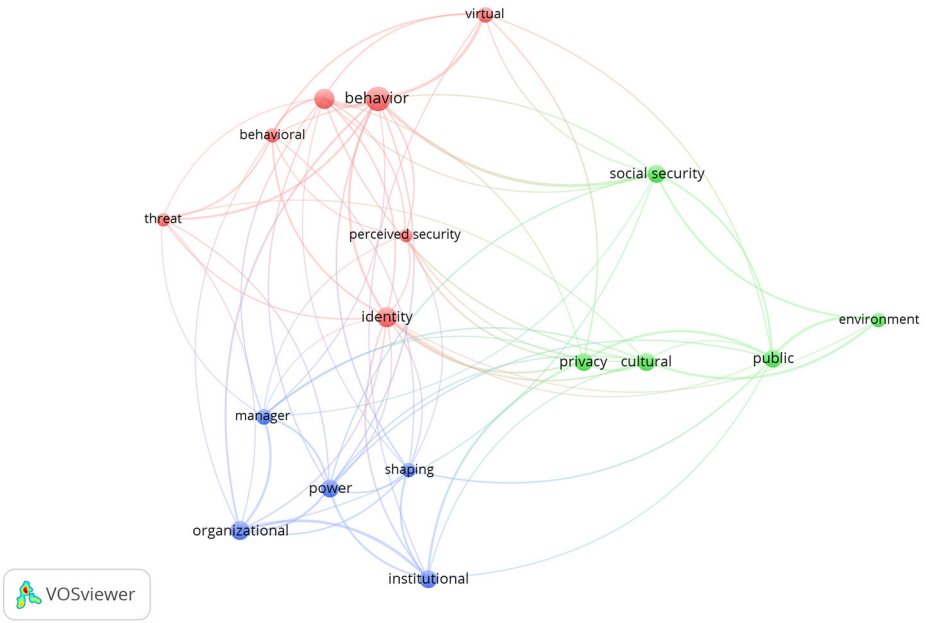

Figure 13. *VOS viewer visualization of CL1 text—high impact cluster.* [Created by the author.]

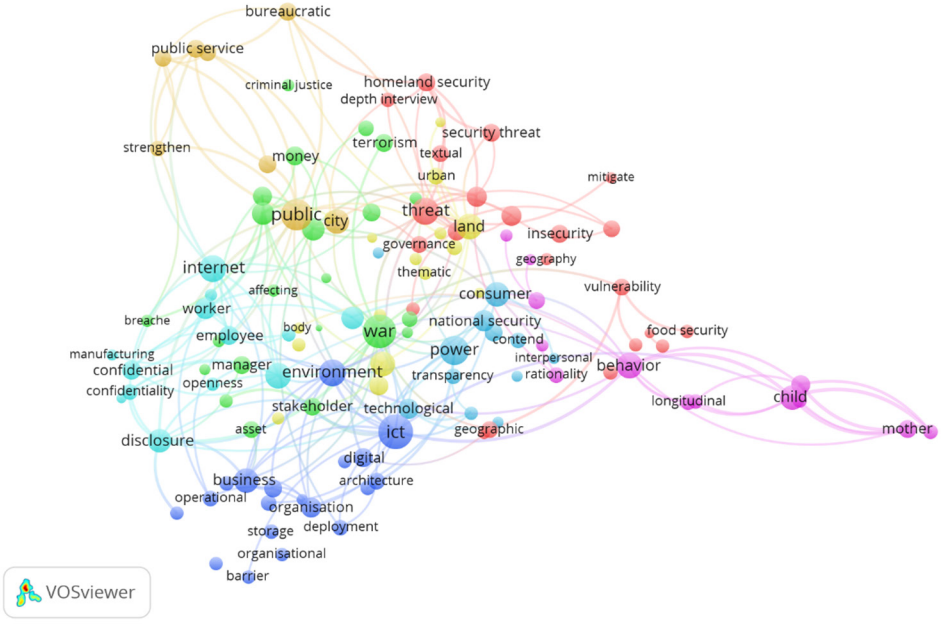

Figure 14. *Visualization of CL2 text Mature Cluster.* [Created by the author.]

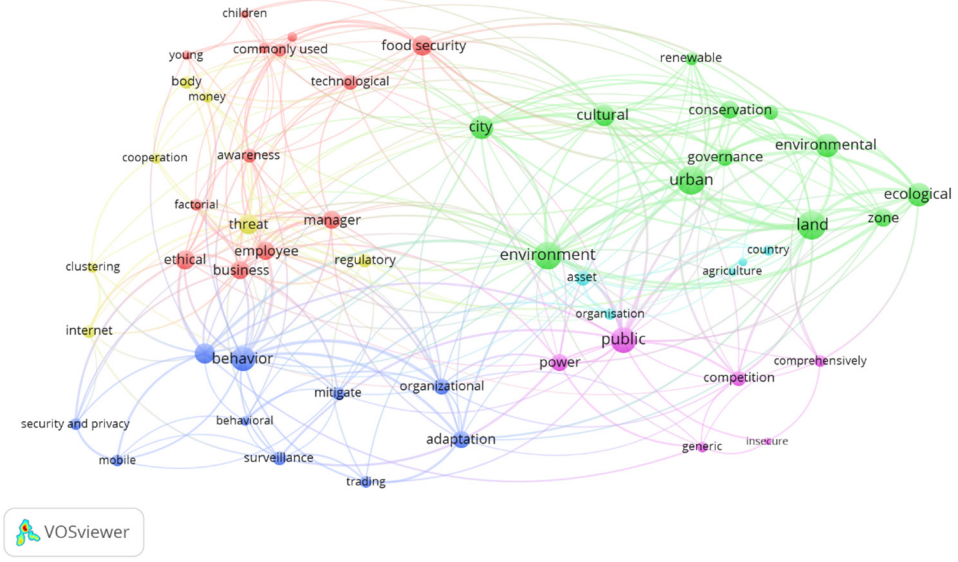

Figure 15. *Visualization of C3 text—High Potential Cluster.* [Created by the author.]

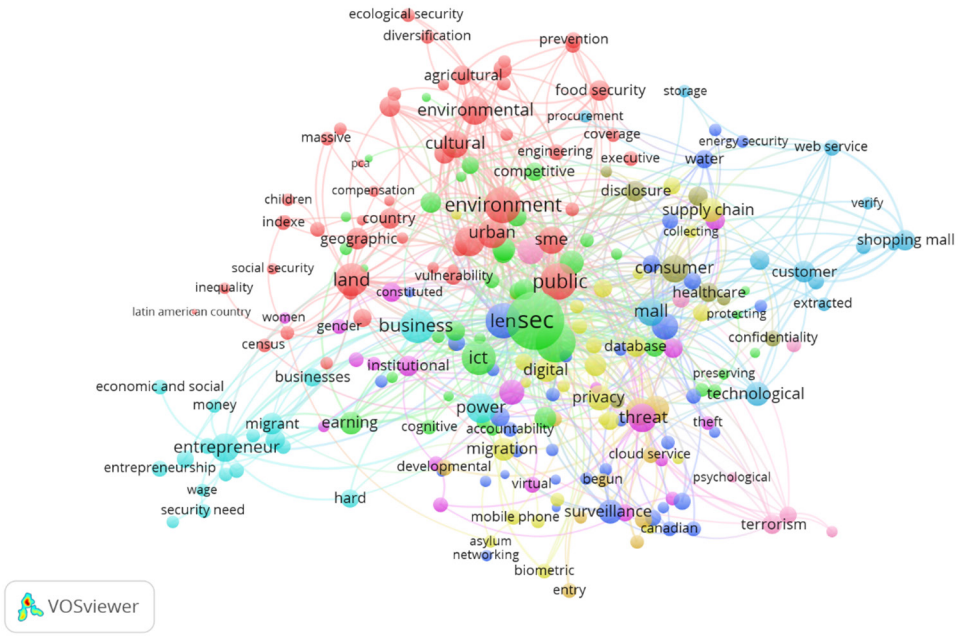

Figure 16. *Visualization of C4 text—Mainstream Cluster.* [Created by the author.]

Figure 16 visualizes the most populated mainstream cluster; discussion which appear in the relatively low H-index papers and probably have achieved the maturity of citation level. This figure is the most similar to the entire corpus: however, issues of healthcare and the family security topics are missing—therefore this cluster can be considered more relevant to the notion of "information security", epistemology related to its cyberspace and ICT context.

Results of Word Clustering and N-Gram Analysis

In order to further contextualize the corpus, I ran a simple word clustering analysis using AntConc clustering and N-gram applications. Then, based on these results which are presented in Table 12, Table 13, Table 14, Table 15, Table 16 I checked the highest frequency clusters in their concordance and for the purpose of further research I summarized them in the Appendix. These outputs, I hope, serve as useful inputs for a more specific literature analysis in the areas of how information security gets socially constructed.

The technique of cluster analysis in AntConc takes a search word, set by the analyst, and lists all the word cluster containing this word according to the defined minimum and maximum cluster element. As it is indicated in the Appendix, I chose minimum 2 and maximum 4 words in a cluster. N-gram analysis, contrary to cluster, does not require a search word—this algorithm basically lists all the clusters with minimum 2 and maximum 4 members in our case. As the Appendix shows, in our corpus there has been 2,378 such cluster types and 27,813 different so-called N-Gram tokens, that are separate two, three, four-word phrases. For handling this huge amount of data, I applied an initial filtering of those clusters which do not appear more than 5 times in the whole corpus.

When the N-gram result was received, I ran a word search on the keywords of my interest: information in Table 12, security in Table 13, social in Table 14, construction in Table 15, and technology in Table 16. These tables contain the frequency of the clusters, the range which is showing in how many text files of the entire corpus can the cluster expression be found, and probability indicates the likelihood that the second word in the cluster follows the first. In the Appendix the concordance tables indicate the corpus files, which are useful for checking which specific papers, in which of our five structural clusters have been dealing with the particular issue. These concordance analyses were only run for the high-frequency word clusters—in most cases where the frequency was higher than 10.

Given the self-explanatory nature of the textual result, I do not present comments to the following tables, the reader is invited to go through the terms, and counter position it with the more detailed concordance analysis in the Appendix. I draw the main conclusions in the next, last section of the paper.

Table 12. *N-Gram Results: Information.* [Created by the author.]

	Freq.	**Range**	**Prob**	**N-Gram Result:** Information
911	20	4	0.01	information about
912	7	4	0.003	information about the
913	43	4	0.021	information and

	Freq.	Range	Prob	N-Gram Result: Information
914	16	4	0.008	information and communication
915	9	4	0.004	information and communication technologies
916	5	4	0.002	information and communication technology
917	5	4	0.002	information assets
918	5	3	0.002	information disclosure
919	6	3	0.003	information exchange
920	7	2	0.003	information for
921	14	3	0.007	information in
922	15	4	0.007	information is
923	6	3	0.003	information management
924	25	4	0.012	information on
925	5	2	0.002	information on the
926	5	3	0.002	information personal
927	7	3	0.003	information processing
928	5	2	0.002	information provided
929	6	3	0.003	information provision
930	7	3	0.003	information quality
931	98	4	0.048	information security
932	6	3	0.003	information security and
933	6	3	0.003	information security is
934	15	3	0.007	information security management
935	5	2	0.002	information security policies
936	8	3	0.004	information security policy
937	17	3	0.008	information sharing
938	5	2	0.002	information sharing and
939	8	2	0.004	information society
940	6	3	0.003	information sources
941	19	4	0.009	information system
942	43	5	0.021	information systems
943	5	3	0.002	information systems is
944	5	3	0.002	information systems security
945	32	5	0.016	information technology
946	9	3	0.004	information technology it
947	5	3	0.002	information that
948	6	3	0.003	information the
949	7	3	0.003	information to
950	5	4	0.002	information was

Table 13. *N-Gram results: Security.* [Created by the author.]

	Freq.	Range	Prob	N-Gram Result: Security
1546	103	5	0.051	security and
1547	9	4	0.004	security and privacy

	Freq.	Range	Prob	N-Gram Result: Security
1548	6	2	0.003	security and the
1549	7	4	0.003	security are
1550	6	3	0.003	security as
1551	5	2	0.002	security at
1552	5	2	0.002	security at the
1553	5	4	0.002	security but
1554	5	4	0.002	security has
1555	22	4	0.011	security in
1556	7	2	0.003	security in the
1557	5	2	0.002	security information
1558	12	4	0.006	security is
1559	15	4	0.007	security issues
1560	21	4	0.01	security management
1561	6	3	0.003	security measures
1562	6	2	0.003	security needs
1563	31	4	0.015	security of
1564	7	3	0.003	security of the
1565	11	5	0.005	security policies
1566	5	3	0.002	security policies and
1567	13	4	0.006	security policy
1568	6	2	0.003	security practices
1569	13	3	0.006	security requirements
1570	5	4	0.002	security research
1571	5	2	0.002	security risk
1572	5	2	0.002	security risks
1573	14	4	0.007	security the
1574	6	2	0.003	security threats
1575	7	3	0.003	security to

Table 14. *N-Gram results: Social.* [Created by the author.]

	Freq.	Range	Prob	N-Gram Result: SOCIAL
1604	24	4	0.028	social and
1605	5	3	0.006	social and environmental
1606	10	2	0.012	social capital
1607	6	3	0.007	social information
1608	5	2	0.006	social learning
1609	7	3	0.008	social media
1610	7	3	0.008	social network
1611	8	3	0.009	social policy
1612	12	3	0.014	social representations
1613	6	2	0.007	social representations of
1614	20	4	0.024	social security

	Freq.	Range	Prob	N-Gram Result: SOCIAL
1615	9	3	0.011	social support
1616	5	2	0.035	society the
1617	10	2	0.128	socio economic
1618	11	3	0.141	socio technical

Table 15. *N-Gram Results: Construction.* [Created by the author.]

	Freq.	Range	Prob	N-Gram Result: Construction
456	6	3	0.018	construction and
457	7	2	0.021	construction industry
458	35	3	0.105	construction of
459	9	3	0.027	construction of a
460	11	3	0.033	construction of the

Table 16. *N-Gram Results: Technology.* [Created by the author.]

	Freq.	Range	Prob	N-Gram Result: Technology
1697	6	3	0.035	technologies and
1698	6	2	0.035	technologies of
1699	16	4	0.045	technology and
1700	9	3	0.025	technology in
1701	7	2	0.02	technology is
1702	9	3	0.025	technology it

Conclusions, Implications and Limitations

We may start summarizing the conclusions by stating that "information security" and "social construction" in the SCOPUS domain offers a wide range of literature in the social sciences and related subject areas, even if the technical areas are excluded from the search.

By categorizing the academically classified journal submissions according to the journals H-index, SJR Q1–Q4 ranking and the individual papers' citations, we classified our sample to five—so-called structural—clusters. First, I identified the top four highest cited papers, amongst which one was omitted due its lack of relevance. The remaining three were published in Decision Support Systems, Information Systems Research and MIS Quarterly. Two of them deal effectively with ISec and explore the concept of deterrence and fear; and one deals with trust especially in the context of e-commerce.

After running a two-step cluster analysis on the remaining papers, I received four other clusters; one containing highly citied and high H-index articles (CL1 – High Impact Cluster), second populating relatively older papers with high references (CL2 – Mature Cluster), a third with relatively recent papers published in high H-index outlets (CL3 – High Potential Cluster) and finally a fourth published in mainstream journals and achieving a saturation with their citation (CL4 – Maturity Cluster). The textual analysis of the abstracts in these

structural cluster reveals a pattern of ISec discourses characterized by key words and textual clusters.

Running N-Gram analysis with AntConc in the range of 2–4 words has resulted in 2,378 N-Gram types and 27,813 N-Gram tokens, while creating textual clusters with the help of CoWo and VosViewer produced 245 nouns organized into 9 clusters with 9,680 connections of co-occurrence.

In the top three papers cluster topics revolve around misuse of information systems, the concept of fear and trust. These papers take a strongly end user viewpoint to ISec through the lens of the term computer. Keyness in this group is also determined by the use of sanctions and their severity regarding social influences.

Papers in the high impact cluster (CL1) demonstrate keyness in terms of deeper discussions in behavioural analysis and patterns. People are also centred, especially in the context of technology relationship and becoming victims of security breaches. I found also high keyness key words as culture, trust and the general concept of perception in connection with several terms such as privacy, importance, and security. This cluster is unique by focusing on organizations and processes in general and in the context of virtual organizations and individual accounts, as well. An interesting stream of research got assigned to this structural cluster, and that is the documentation of the 2008 Obama campaign, exploiting social media the first time in the history of political elections.

The mature cluster (CL2) is adding value in terms of information disclosure and non-disclosure topics, and more frequent use of the terms IT and ICT in many contexts. These are the papers which deal mostly with the exposure of communities, especially in the context of their differences and diversities. Differentiation of this cluster was also stemming from a non-related stream of research which is using information security in a different context: these are the papers in healthcare and social-security issues of families. These papers need to be omitted from further analysis.

High potential cluster (CL3) is different in the focusing on discourses related to social networking and social media, which is also closely intertwined with information sharing and networks. Users' trust, privacy and perception are also high level of keyness in this cluster. We found non-related differentiators as well; the topics of teaching, scripts and education—in non-security related cases—have to be left out from further analysis. The situation is similar, although less obvious, in the cases of energy and food security, which are more connected to general security problems in our modern social environment, but they are also distant from ISec in its ICT context.

The last and most populated cluster—the mainstream cluster (CL4)—logically has the least number of key words with high keyness value, being close to the word list of the corpus. However, the terms management and construction appear mostly in this cluster in connection with security, regulatory institutions and social construction. There are some historical papers—discussing security of states in ancient Roman times—which need to be left out, due to their lack of topical relevance.

Textual clusters reveal two other important discourses in ISec, which can be seen from Figure 11 to Figure 16. The first of these textual clusters is connecting the topics of national security, governments, homeland security, public administration, law enforcement and terrorism. The second embraces the areas of urban, cities, smartness, environment and ecosystems.

As a conclusion I hope researches find the clusters and the organized topics relevant to anchor their research to them, or to find ways to more easily identify where the research adds value to the already existing body of knowledge in the ISec domain. Naturally, these endeavours might only be valid within the limitations of this study, which at the same time gives place to implications for further improvement of research.

Amongst these limitations I have to mention the need to extend the analysis to full papers not only texts and get a deeper insight by running a co-citation analysis to find more connections between the topics, authors and journal styles. Secondly, keywords need to be refined—cybersecurity for instance is also an important phrase which might reveal other types of contributions in the area. Finally, the range of publication outlets might also be extended, indexed books, conference proceedings also contain threads of relevant discussions and worthy for analysis.

Despite these limitations the analysis is convincing that social construction of technology framework reveals new domains of discussion about information security and a large body of literature is available to create programmable actions addressing the complex challenges of information security.

Appendix. Results of N-Gram cluster analysis.

Minimum words: 2. Maximum words: 4. Minimum Range: 2. Minimum frequency: 5. N-Gram types: 2,378, N-Gram Tokens: 27,813.

	Concordance Analysis Results: information and communication	**Range**
1	… to empower managers, IS engineers, and information and communication technology users wit	abstract_cluster_1.txt
2	…actices surrounding hospitals' new investments in information and communication technologies tend to	abstract_cluster_1.txt
3	…networks. For the Internet and other information and communication technologies to sup…	abstract_cluster_2.txt
4	…of surveillance countermeasures. In this context, information and communication technologies have be	abstract_cluster_2.txt
5	…is possible to create multiple identities. Information and communication technologies were se	abstract_cluster_2.txt
6	…and influenced by the degree that information and communication technology are part	abstract_cluster_2.txt
7	…manipulation of sensible information. These new information and communication technologies (ICT)	abstract_cluster_2.txt
8	…fossil fuel peak. The effects of information and communication technologies and tec	abstract_cluster_3.txt
9	…critical understanding of the role of information and communication technology (ICT) in	abstract_cluster_3.txt
10	Advances in information and communication technologies have le …	abstract_cluster_4.txt

11	…licies. Through the proposed approach, education, information and communication are seen as keys	abstract_cluster_4.txt
12	…, which is a multidimensional model. Information and communication technologies (ICTs)	abstract_cluster_4.txt
13	…reluctant to support proper freedom of information and communication. In short, they have	abstract_cluster_4.txt
14	…effort to address issues related to information and communication technology. Technol	abstract_cluster_4.txt
15	…factors that influence the adoption of Information and Communication Technologies (ICT) b	abstract_cluster_4.txt
16	…and the latter's use of information and communication technology (ICT) in	abstract_cluster_4.txt

	Concordance Analysis Results: information technology	**Range**
1	company initiatives, especially those involving information technology. The interweaving of top-do	abstract_cluster_1.txt
2	ICT diffusion dynamics within three large information technology (IT) literate Australian co	abstract_cluster_2.txt
3	in their OC by implementing different information technology (IT) features that should s	abstract_cluster_2.txt
4	studies pay any serious attention to information-technology-related security issues. Th	abstract_cluster_2.txt
5	Dyson, M. Hendriks, S. Grant (Eds.) Information technology and indigenous people, Idea	abstract_cluster_2.txt
6	service, and health workers. Innovations in information technology in the past decade or	abstract_cluster_2.txt
7	ompetitive advantage for organisations worldwide, information technology professionals, consumers an	abstract_cluster_2.txt
8	service, and health workers. Innovations in information technology in the past decade or	abstract_cluster_2.txt
9	become known as India's premier information technology (IT) hub and a magnet	abstract_cluster_2.txt
10	roles of two different criminal justice information technology (IT) security systems-that	abstract_cluster_2.txt
11	systems are discussed. Past research on information technology (IT) security training and	abstract_cluster_3.txt
12	the use value of domain ontology. Information technology has dramatically increased	abstract_cluster_3.txt
13	costs and expand markets by deploying information technology through new and existing bu	abstract_cluster_3.txt
14	findings to decrease CA occurrences. Unethical information technology (IT) use, related to activi	abstract_cluster_3.txt
15	and makes extensive use of spatial information technology and can be widely applied	abstract_cluster_3.txt
16	to the CAI. Economic growth and information technology development has stimulated	abstract_cluster_4.txt

	Concordance Analysis Results: information technology	Range
17	agencies to adopt innovative forms of information technology in order to survive and	abstract_cluster_4.txt
18	electronic commerce (B2C e-commerce) information technology applications in order to ob	abstract_cluster_4.txt
19	with which to interpret cloud-based information technology outsourcing. Purpose – Emp	abstract_cluster_4.txt
20	support and reinforce the contributions of information technology to the development process.	abstract_cluster_4.txt
21	turn to (b) key imperatives of information technology-development linkages and th	abstract_cluster_4.txt
22	knowledge society through the provision of information technology (IT) green services. Furthe	abstract_cluster_4.txt
23	factors are presented. These factors are information technology (IT) tools, information sys	abstract_cluster_4.txt
24	of cyberspace. Failure to engage with information technology, and globally mediated sex,	abstract_cluster_4.txt
25	organizational flexibility. This study presents information technology executive's perspective and	abstract_cluster_4.txt
26	and management, namely, law, economics, sociology, information technology and information resources m	abstract_cluster_4.txt
27	that, for example, advanced equipment and information technology can be harnessed to handle	abstract_cluster_4.txt
28	which are (electronic trust, financial resources, information technology infrastructure, perceived r	abstract_cluster_4.txt
29	Computing opens a new chapter in Information Technology. It has its roots in	abstract_cluster_4.txt
30	advantages in certain effects of globalization, information technology, scientific and technical p	abstract_cluster_4.txt
31	such as airports, special economic zones, information technology parks, real estate ventures	abstract_cluster_4.txt
32	practice of IS security are discussed. Information technology executives strive to align	asbtract_big_three.txt

	Concordance Analysis Results: ICT in, ICT and	Range
1	new ICT unless effective use of ICT and performing operations electronically (eBus	abstract_cluster_2.txt
2	awareness, often combined with mistrust regarding ICT and ICT service providers, costs, lack	abstract_cluster_2.txt
3	service providers, costs, lack of internal ICT and management knowledge, Network infrastructu	abstract_cluster_2.txt
4	particular, to engage more fully with ICT and develop sustainable business practices: 1)	abstract_cluster_2.txt
5	in Colombia regarding the adoption of ICT and independent variables identified in the	abstract_cluster_4.txt
1	new information and communication technologies (ICT), in continuous development, have expanded als	abstract_cluster_2.txt

	Concordance Analysis Results: ICT in, ICT and	Range
2	role of information and communication technology (ICT) in humanitarian action, this article explores	abstract_cluster_3.txt
3	prism through which the role of ICT in humanitarian action is explored is	abstract_cluster_3.txt
4	policies that foster the implementation of ICT in SMEs based on an analysis	abstract_cluster_4.txt
5	use of information and communication technology (ICT) in business processes. Also, the characterist	abstract_cluster_4.txt

	Concordance Analysis Results: technologies of, technology in	Range
1	over time, have long been governmental technologies of control. I further argue that	abstract_cluster_2.txt
2	assesses the threat assessments produced through technologies of risk management and the development	abstract_cluster_2.txt
3	management and the development of new technologies of surveillance. Third it describes t	abstract_cluster_2.txt
4	article explores how biometrics function as technologies of embodiment that both redefine and	abstract_cluster_2.txt
5	technology is one of the core technologies of IoT deployments in the healthcare	abstract_cluster_4.txt
6	then move on to the newer technologies of social media and apps. This	abstract_cluster_4.txt
1	or change individuals' initial trust in technology. In this study, a research model	abstract_cluster_1.txt
2	that focused on the use of technology in supporting people with dementia to	abstract_cluster_1.txt
3	and health workers. Innovations in information technology in the past decade or two	abstract_cluster_2.txt
4	framework for understanding the role of technology in intelligence. The focus is on	abstract_cluster_2.txt
5	and health workers. Innovations in information technology in the past decade or two	abstract_cluster_2.txt
6	the various security requirements of RFID technology in IoT, many RFID authentication scheme	abstract_cluster_4.txt
7	to adopt innovative forms of information technology in order to survive and flourish.	abstract_cluster_4.txt
8	try to overcome such conflicts: through technology. In West Africa, the secure 'Seahorse'	abstract_cluster_4.txt
9	work that analyses the implementation of technology in enterprises in emerging countries, t	abstract_cluster_4.txt

	Concordance Analysis Results: technology and, technologies and	Range
1	ing personality, cognitive, calculative, and both technology and organizational factors of the insti	abstract_cluster_1.txt

	Concordance Analysis Results: technology and, technologies and	Range
2	M. Hendriks, S. Grant (Eds.) Information technology and indigenous people, Idea Group Publi	abstract_cluster_2.txt
3	sites facilitates the distribution of military technology and strategy across numerous scales of	abstract_cluster_2.txt
4	subject to the coercive power of technology, and appropriate the narrow technologic	abstract_cluster_2.txt
5	reflect a broader celebratory ethos of technology and commerce. To understand technologie	abstract_cluster_2.txt
6	GII. As a result, the associated technology and information systems become targets	abstract_cluster_2.txt
7	National Institute of Standards and Technology) and academic databases (e.g. Google	abstract_cluster_3.txt
8	makes extensive use of spatial information technology and can be widely applied to	abstract_cluster_3.txt
9	as spokespersons for the interactive data technology and the retail investor. We examine	abstract_cluster_4.txt
10	is an attempt to introduce a technology and a business model for centralising	abstract_cluster_4.txt
11	was affected through advances in modern technology and promises of wealth and material	abstract_cluster_4.txt
12	cyberspace. Failure to engage with information technology, and globally mediated sex, is discusse	abstract_cluster_4.txt
13	namely, law, economics, sociology, information technology and information resources management fo	abstract_cluster_4.txt
14	source, intrinsic criteria of data, communication technology, and integrity among various criteria.	abstract_cluster_4.txt
15	It has its roots in internet technology, and like the Internet, it is	abstract_cluster_4.txt
16	in the area of science and technology and integrated forecasting of socio-eco	abstract_cluster_4.txt
1	governance of populations occurs through new technologies and techniques of social control. Con	abstract_cluster_2.txt
2	driven by continued demographic growth, new technologies and the desire of many as	abstract_cluster_2.txt
3	especially in the light of developing technologies and the growth of e-commerce.	abstract_cluster_2.txt
4	The effects of information and communication technologies and technological innovation after en	abstract_cluster_3.txt
5	of life, one building on information technologies and critical functions of infrastruct	abstract_cluster_4.txt
6	1970s, to current debates over emerging technologies and global innovation, the academic c	abstract_cluster_4.txt

	Concordance Analysis Results: information systems and information system	Range
1	This paper extends an area of information systems research into a marketing of	abstract_cluster_1.txt
2	developed. Recent trust research in the information systems (IS) field has described trust	abstract_cluster_1.txt
3	lementing e-government systems and organizational information systems in general. This exploratory s	abstract_cluster_1.txt
4	to be „the weakest link" in information systems (IS) security management in th	abstract_cluster_1.txt
5	and action and the security of information systems are increasingly a focus of	abstract_cluster_1.txt
6	identifies four security issues (access to Information Systems, secure communication, securit	abstract_cluster_1.txt
7	ation, security management, development of secure Information Systems), and examines the extent to	abstract_cluster_1.txt
8	three viewpoints: a meta-model for information systems, the research approaches used,	abstract_cluster_1.txt
9	for studying information security from an information systems viewpoint, with respect to res	abstract_cluster_1.txt
10	and philosophy), are particularly necessary. Most information systems research takes for granted the	abstract_cluster_1.txt
11	uences shape organizational actions for improving information systems security. A case study of	abstract_cluster_1.txt
12	also enrich existing research models on information systems continuance. Moreover, the Saa	abstract_cluster_1.txt
13	nformation security awareness of staff, including information systems decision makers, in higher edu	abstract_cluster_1.txt
14	insidious motivators for organizations to adopt information systems security (ISS) approaches. Ext	abstract_cluster_1.txt
15	paper investigates the social representations of Information Systems (IS) security of different com	abstract_cluster_2.txt
16	discussed the framework and value of information systems (IS) security standards and ce	abstract_cluster_2.txt
17	the evolution of an Ireland-India information systems offshoring relationship. By tr	abstract_cluster_2.txt
18	and agenda in the development of information systems to support the process of	abstract_cluster_2.txt
19	adulthood. Digital technologies like geographic information systems (GIS) pose new problems for	abstract_cluster_2.txt
20	a research agenda, Cartography and Geographic Information Systems. 22 (1) (1995) 5-16]. Such imp	abstract_cluster_2.txt
21	States Bureau of Indian Affairs, geographic information systems, and cultural assimilation, in	abstract_cluster_2.txt
22	coherent system of controls consisting of information systems and procedures. This system-ba	abstract_cluster_2.txt

	Concordance Analysis Results: information systems and information system	Range
23	of this article is to identify information systems security risks in local govern	abstract_cluster_2.txt
24	information. Some of the most important information systems are those that produce the	abstract_cluster_2.txt
25	a result, the associated technology and information systems become targets for information	abstract_cluster_2.txt
26	on increasing the development of secure information systems. In particular, we introduce a	abstract_cluster_2.txt
27	related to the development of secure information systems; we identify limitations of ex	abstract_cluster_2.txt
28	discipline for the development of secure information systems, its principles and the challe	abstract_cluster_2.txt
29	of the most widespread problems affecting information systems. Security breaches at companie	abstract_cluster_2.txt
30	problem. For prompt deployment in legacy information systems, it would be desirable to	abstract_cluster_3.txt
31	in terms of the threat to information systems (IS) security. While there is	abstract_cluster_3.txt
32	is related to the misuse of information systems resources) and a three-item	abstract_cluster_3.txt
33	intent. Market surveillance systems (MSSs) are information systems that monitor financial markets	abstract_cluster_3.txt
34	factors are information technology (IT) tools, information systems integration and information se	abstract_cluster_4.txt
35	given the highest importance to the information systems integration. Then, IT tools an	abstract_cluster_4.txt
36	considered. In addition, findings indicate that information systems integration has the highest co	abstract_cluster_4.txt
37	in supply chain, key indices for information systems integration and information se	abstract_cluster_4.txt
38	Latin American countries like Chile. Hospital information systems (HISs) accelerate hospital-rel	abstract_cluster_4.txt
39	nity demographic and discourse data, geographical information systems maps, and comprehensive photog	abstract_cluster_4.txt
40	to identify what the most effective information systems are for the self-builders	abstract_cluster_4.txt
41	consumers' trust. Intentional insider misuse of information systems resources (i.e., IS misuse)	asbtract_big_three.txt
42	work from criminology, social psychology, and information systems. The model posits that user	asbtract_big_three.txt
43	findings of this research contribute to information systems security research, human-compu	asbtract_big_three.txt
1	trust in a more complex, organizational information system, there are a number of	abstract_cluster_1.txt

	Concordance Analysis Results: information systems and information system	Range
2	to hinge on top management championing information system security initiatives and propag	abstract_cluster_1.txt
3	of risk and its effect on information system (IS) risk management. Design/me	abstract_cluster_2.txt
4	they require new business, operational and information system models that extend 30 years or	abstract_cluster_2.txt
5	project was the creation of an information system to ascertain and characterise a	abstract_cluster_2.txt
6	and the Police Computer Network and Information System of Turkey (POLNET). By delineat	abstract_cluster_2.txt
7	technology (remote sensing (RS) and geographic information system (GIS). We constructed an ecolo	abstract_cluster_3.txt
8	source of the security of an information system, rather than rational design ch	abstract_cluster_3.txt
9	The main modification involved integrating an information system with the MBWA in order	abstract_cluster_3.txt
10	as many tours as managers). The information system collected information about saf	abstract_cluster_3.txt
11	on examples relating to the Visa Information System, I show that processes of	abstract_cluster_4.txt
12	data on kin connectivity with geographical information system (GIS) data in a rural	abstract_cluster_4.txt
13	risk assessment (ERA) based on geographic information system (GIS) was built. To identify	abstract_cluster_4.txt
14	Electronic health network (EHN) is an information system providing functions involved in	abstract_cluster_4.txt
15	prefer to use either the Integrated Information System (IIS) that the Ministry of	abstract_cluster_4.txt
16	of Labour has initiated or Payroll Information System (PIS) that is proposed by	abstract_cluster_4.txt
17	in computer science (CS) and computer information system (IS) programmes. The course del	abstract_cluster_4.txt
18	towards Europe, namely Eurodac, the Schengen Information System (SIS II) and the Visa	abstract_cluster_4.txt
19	System (SIS II) and the Visa Information System (VIS). This paper tries to	abstract_cluster_4.txt

	Concordance Analysis Results: information systems security	Range
1	uences shape organizational actions for improving information systems security. A case study of	abstract_cluster_1.txt
2	insidious motivators for organizations to adopt information systems security (ISS) approaches. Ext	abstract_cluster_1.txt
3	of this article is to identify information systems security risks in local govern	abstract_cluster_2.txt

	Concordance Analysis Results: information systems security	Range
4	of the most widespread problems affecting information systems. Security breaches at companie	abstract_cluster_2.txt
5	findings of this research contribute to information systems security research, human-compu	asbtract_big_three.txt

	Concordance Analysis Results: information security policy and information security policies	Range
1	between the uptake and application of information security policies and the accompanying	abstract_cluster_2.txt
2	significant relationships between the adoption of information security policies and the incidence or	abstract_cluster_2.txt
3	paper, we investigate the tension between information security policies and information secu	abstract_cluster_2.txt
4	learning cues influence employee awareness of information security policies and ultimately diffe	abstract_cluster_4.txt
5	utsourcing. Purpose – Employees' compliance with information security policies is considered an ess	abstract_cluster_4.txt
1	availability. While the importance of the information security policy (InSPy) in ensuring th	abstract_cluster_2.txt
2	gement, particularly development and execution of information security policy, awareness, compliance	abstract_cluster_3.txt
3	and situational factors that lead to information security policy violation intentions.	abstract_cluster_3.txt
4	situational factors and intentions to violate information security policy. This study represents	abstract_cluster_3.txt
5	meta-traits and their influence on information security policy violation intentions.	abstract_cluster_3.txt
6	in-house employees in terms of information security policy awareness. Based on da	abstract_cluster_4.txt
7	thereby resulting in diminished levels of information security policy awareness. These findi	abstract_cluster_4.txt
8	advance social cognitive theory by incorporating information security policy awareness as an import	abstract_cluster_4.txt

	Concordance Analysis Results: information security management	Range
1	its implications for the practice of information security management. Copyright This p	abstract_cluster_2.txt
2	he evaluation model include project construction, information security management, special construct	abstract_cluster_2.txt
3	incorporating the identified key issues into information security management systems (ISMS). Or	abstract_cluster_2.txt
4	opportunistic behaviour, therefore, confidence in information security management can be achieved. T	abstract_cluster_2.txt

	Concordance Analysis Results: information security management	**Range**
5	to explore the management role in information security management. Various studies h	abstract_cluster_3.txt
6	for a more holistic approach to information security management. In this paper, us	abstract_cluster_3.txt
7	explore specific managerial activities to enhance information security management. We found that num	abstract_cluster_3.txt
8	is considered an essential component of information security management. The research aims	abstract_cluster_4.txt
9	priori assumption about user intent, P3. Information security management and choice of coun	abstract_cluster_4.txt
10	propositions can form a basis for information security management, making the object	abstract_cluster_4.txt
11	(IT) tools, information systems integration and information security management. The findings indi	abstract_cluster_4.txt
12	integration. Then, IT tools and, ultimately, information security management are considered. In	abstract_cluster_4.txt
13	indices for information systems integration and information security management are also referred.	abstract_cluster_4.txt
14	the mechanisms which structure e-democracy. Information Security Management System (ISMS) is a	abstract_cluster_4.txt
15	management, Crisis management, Change management, Information Security Management System, etc. Risk	abstract_cluster_4.txt

	Concordance Analysis Results: security and privacy, privacy and security	**Range**
1	these tools also raised significant national security and privacy considerations. Finally, the	abstract_cluster_1.txt
2	usability, transparency, quality-assured content, security, and privacy) vary in their impact	abstract_cluster_2.txt
3	Mobile applications build part of their security and privacy on a declarative permission	abstract_cluster_3.txt
4	the declarative permissions model on which security and privacy services of Android rely	abstract_cluster_3.txt
5	method bias cannot be completely eliminated. Security and privacy are the two major	abstract_cluster_3.txt
6	hallenged ethical issues about users' information security and privacy. SNS users are concerned	abstract_cluster_3.txt
7	we devise mechanisms covering three important security and privacy issues of EHN including	abstract_cluster_4.txt
8	attain legitimacy. Given the rising IT security and privacy concerns, organizations are i	abstract_cluster_4.txt
9	lack of confidence in ICT's security and privacy, a perception of ICT	abstract_cluster_4.txt

	Concordance Analysis Results: security and privacy, privacy and security	**Range**
1	and the public at large. Accordingly, privacy and security are active topics of	abstract_cluster_1.txt
2	contribute toward a broad understanding of privacy and security not simply as technical	abstract_cluster_1.txt
3	embedded in social and cultural contexts. Privacy and security are difficult concepts to	abstract_cluster_1.txt
4	move away from narrow views of privacy and security and toward a holistic	abstract_cluster_1.txt
5	technologies designed to support self-expression, privacy, and security for global civic networks.	abstract_cluster_2.txt
6	a deeper understanding of customers' perceived privacy and security (CPPS) by investigating priva	abstract_cluster_4.txt
7	organisations to do this because when privacy and security practices are clearly disclos	abstract_cluster_4.txt
8	ones being the digital divide, the privacy and security concerns and the availability	abstract_cluster_4.txt
9	followed by a section on data privacy and security issues. The concluding sectio	abstract_cluster_4.txt

	Concordance Analysis Results: threat to, and safety and security	**Range**
1	contrast, external rivals pose a lower threat to personal status, so people are	abstract_cluster_1.txt
2	and society in terms of the threat to information systems (IS) security. While	abstract_cluster_3.txt
3	be required to combat this growing threat to IS security. As we approach 2015	abstract_cluster_3.txt
4	(ISDB) of employees is a serious threat to organizations. However, not much empiric	abstract_cluster_3.txt
5	to privacy). Insiders represent a major threat to the security of an organization'	abstract_cluster_3.txt
6	systematically treated as a national security threat to the United States. The scope	abstract_cluster_3.txt
7	or social engineering, is an omnipresent threat to a large number of commercial	abstract_cluster_4.txt
8	terrorism primarily as a crime, a threat to the state's security or	abstract_cluster_4.txt
9	study area and the degree of threat to the coastline. The sustainable civilizat	abstract_cluster_4.txt
10	.e., IS misuse) represents a significant threat to organizations. For example, industry sta	asbtract_big_three.txt
1	classrooms, elbow room, as well as safety and security. The swiftness and considerab	abstract_cluster_2.txt

	Concordance Analysis Results: threat to, and safety and security	Range
2	ips, personal values, cultural identity, physical safety and security, aesthetic preferences, and un	abstract_cluster_2.txt
3	by a case study of the safety and security measures adopted in the	abstract_cluster_2.txt
4	2010 FIFA World Cup partners, is the safety and security of local and international	abstract_cluster_2.txt
5	the authors argue that such a safety and security strategy should be informed	abstract_cluster_2.txt
6	is often assumed that perceptions of safety and security may influence individuals' des	abstract_cluster_2.txt
7	be used, what components (quality, quantity, safety, and cultural acceptability) they were inte	abstract_cluster_3.txt
8	anxiety among the public concerning the safety and security of their personal and	abstract_cluster_4.txt
9	the state's ability to provide safety and security online. This disparity present	abstract_cluster_4.txt
10	accept the trade-off between increased safety and diminished control that accompanies a	abstract_cluster_4.txt
11	commentary that addresses issues pertaining to safety and security to garner an overarching	abstract_cluster_4.txt

	Concordance Analysis Results: socio-technical	Range
1	evaluation model with 5 dimensions based on Socio-Technical model and Stakeholder Theory, whic	abstract_cluster_2.txt
2	this research is to analyse the socio-technical consequences deriving from the dig	abstract_cluster_2.txt
3	is an overview of the possible socio-technical risks that a panel of	abstract_cluster_3.txt
4	a high frequency of occurrence of socio-technical information security risks caused	abstract_cluster_3.txt
5	operate within the context of larger socio-technical systems, wherein they interact – b	abstract_cluster_3.txt
6	with a thorough analysis of its socio-technical context, thereby considering not o	abstract_cluster_3.txt
7	interactions among the actors in the socio-technical system. The requirements models of	abstract_cluster_3.txt
8	a central role in advancing the socio-technical project that is constituted by	abstract_cluster_4.txt
9	This paper looks at cities as socio-technical systems consisting of patterns of	abstract_cluster_4.txt
10	them down into an agent-based socio-technical model. This method is useful	abstract_cluster_4.txt
11	evaluation of the informational stability of socio-technical systems, which are influenced by	abstract_cluster_4.txt

	Concordance Analysis Results: information society	Range
1	while neither the general literature on information society nor security studies pay any	abstract_cluster_2.txt
2	international norms to deal with the “information society,” so that “risk society” does	abstract_cluster_2.txt
3	market of electronic commerce. In the information society, to promote private dynamism a	abstract_cluster_2.txt
4	quite a late achievement of the information society, although, in theory, it could	abstract_cluster_4.txt
5	of Russia’s moving towards the information society, new possibilities open up of	abstract_cluster_4.txt
6	of the opportunities offered by the information society. A methodology is formulated o	abstract_cluster_4.txt
7	of education in the conditions of information society. A concept is put forward	abstract_cluster_4.txt
8	In the globalization era and the information society, data security and protection	abstract_cluster_4.txt

	Concordance Analysis Results: construction of	Range
16	interests are closely aligned in the construction of regulatory institutions at the int	abstract_cluster_4.txt
17	This paper focuses on the discursive construction of ‘security’ in a particular context	abstract_cluster_4.txt
18	Part of the project is a construction of a future intelligent city named	abstract_cluster_4.txt
19	a much larger exercise involving the construction of four new science buildings around	abstract_cluster_4.txt
20	are to better understand the ‘social construction’ of the problem and subsequent policy	abstract_cluster_4.txt
21	through an examination of the social construction of the Heartbleed bug. It demonstrate	abstract_cluster_4.txt
22	vehicle of public participation in the construction of a new political order. This	abstract_cluster_4.txt
23	contribution of this study is the construction of structural and measurement models	abstract_cluster_4.txt
24	using contemporary street maps, and the construction of a comprehensive database by using	abstract_cluster_4.txt
25	synthesis of the management objective, the construction of a dynamic expert system, ensuring	abstract_cluster_4.txt
26	Coordination emerges in SEOP through the construction of a new institutional design, articu	abstract_cluster_4.txt
27	of date of planting, land terracing, construction of drainages, cover cropping and maki	abstract_cluster_4.txt
28	trees, planting of cover crops and construction of drainages across farmland. Age, ac	abstract_cluster_4.txt
29	at different levels of internationalization and construction of the world system’s new	abstract_cluster_4.txt

	Concordance Analysis Results: construction of	Range
30	external factor on the anti-government construction of the issue. This study suggests	abstract_cluster_4.txt
31	at Korykos and Elaiussa Sebaste. The construction of isodomic towers is the only	abstract_cluster_4.txt
32	that this concern led to the construction of the isodomic towers. No archaeolog	abstract_cluster_4.txt
33	hypothesis. Eastern Rough Cilicia witnessed the construction of a road network and bridges	abstract_cluster_4.txt
34	led to a boom in the construction of public buildings in the cities	abstract_cluster_4.txt
35	is proposed. An approach to the construction of the so-called vector of	abstract_cluster_4.txt

References

[1] KOVÁCS L., NEMESLAKI A., ORBÓK Á., SZABÓ A.: Structuration Theory and Strategic Alignment in Information Security Management: Introduction of a Comprehensive Research Approach and Program. *AARMS,* 16 1 (2017), 5–16.

[2] SISMONDO, S.: Science and Technology Studies and an Engaged Program. In. *The Handbook of Science and Technology Studies, Third Edition.* Cambridge: MIT Press, 2008. 13–31.

[3] HACKETT, E., AMSTERDAMSKA, O., LYNCH, M., WAJCMAN, J.: *The Handbook of Science Technology Studies, Third Edition.* Cambridge: MIT Press, 2008.

[4] HOWCROFT, D., MITEV, N., WILSON, M.: What We May Learn from the Social Shaping of Technology Approach. In. *Social Theory and Philosophy for Information Systems.* Chichester: John Wiley & Sons, 2004. 329–371.

[5] SIMON, H.: *The Sciences of the Artificial.* Third edition. Cambridge: MIT Press, 1996.

[6] PEREZ, C.: Technological revolutions and techno-economic paradigms. *Cambridge Journal of Economics,* 34 1 (2010), 185–202. https://doi.org/10.1093/cje/bep051

[7] WINNER, L.: Do Artifacts Have Politics? In. *The Social Shaping of Technology.* 2 ed. London: Open University Press, 1999. 28–40.

[8] BOSS, S. R., GALLETTA, D. F., LOWRY, P. B., MOODY, G. D., POLAK, P.: What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Quarterly,* 39 4 (2015), 837–864.

[9] POSEY, C., ROBERTS, T. L., BENJAMIN, P., BENNETT, R. J., COURTNEY, J. F.: Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors. *MIS Quarterly,* 37 4 (2013), 1189–1210.

[10] YOO, Y.: Computing in everyday life: A call for experiental computing. *MIS Quarterly,* 34 2 (2010), 213–231. https://doi.org/10.2307/20721425

[11] KIM, S. H., KIM, B. C.: Differential Effects of Prior Experience on the Malware Resolution Process. *MIS Quarterly,* 38 3 (2014), 655–678.

[12] LI, C., PETERS, G. F., RICHARDSON, V. J., WATSON, M. W.: The Consequences of Information Technology Control Weaknesses on Management Information Systems:

The Case of Sarbanes-Oxley Internal Control Reports. *MIS Quarterly,* 36 1 (2012), 179–203.

[13] DAVIS, F. D.: Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13 3 (1989), 319–340.

[14] VENKATESH, V., MORRIS, M. G., DAVIS G. B., DAVIS, F.:User acceptance of information echnology: Toward a unified view. *MIS Quarterly*, 27 3 (2003) 425–478.

[15] CECEZ-KECMANOVIC, D., GALLIERS, R. D., HENFRIDSSON, O,. NEWELL S., VIDGEN, R.: The sociomateriality of information systems: Current status, future directions. *MIS Quarterly*, 38 3 (2014), 809–830. https://doi.org/10.25300/MISQ/2014/38:3.3

[16] WANG, J., GUPTA, M., RAO, H. R.: Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications. *MIS Quarterly*, 39 1 (2015), 91–112.

[17] BULGURCU, B., CAVUSOGLU, H., BENBASAT, I.: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, 34 3 (2010), 523–548. https://doi.org/10.2307/25750690

[18] KNAPP K. J., FERRANTE, C. J.: Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations. *Journal of Management Policy and Practice*, 13 5 (2012), 66–80.

[19] BIJKER, W. E.: *Of Bicycles, Bakelites and Bulbs: Toward a Theory of Sociotechnical Change.* Cambridge: MIT Press, 1995.

[20] RAYSON, P.: From key words to key semantic domains. *International Journal of Corpus Linguistic*, 13 4 (2008), 519–549. https://doi.org/10.1075/ijcl.13.4.06ray

AARMS Vol. 17, No. 1 (2018) 139–140.

Authors' Guide

AARMS is a peer-reviewed international scientific journal devoted to reporting original research articles and comprehensive reviews within its scope that encompasses the military, political, economic, environmental and social dimensions of security.

Manuscripts and editorial correspondence should be addressed to
Prof. Dr. László KOVÁCS, Editor-in-Chief
National University of Public Service
P. O. Box 15, H-1581 Budapest 146
Hungary
Phone: +36-1-432-9000/29-004
Mobil: +36-30-9359-776
Fax: +36-1-432-9208
E-mail: aarms@uni-nke.hu

Manuscript Submission Form. All manuscripts should be accompanied with a completed Manuscript Submission Form signed by the author who will be responsible for all correspondence and proofreading ("Corresponding Author"). Manuscript Submission Form can be requested from the Editorial Office through mail, fax or e-mail or can be downloaded from the website of the journal.

Form of the manuscript. Manuscripts (text, tables and illustrations) should be submitted in triplicate. Although every effort will be made to guard against loss, it is advisable that authors retain a copy of all materials submitted. Text (in English only) should be typed double spaced on one side of a good quality paper, with generous margins, and bear the title of the paper, name of the author(s), and the institute where the work has been carried out. An abstract of 50 to 150 words should precede the text of the paper stating briefly the main results and conclusions of the work. It should be suitable for use by abstracting services. Authors are encouraged to use descriptive headings, e.g. Introduction, Methods, Results, Discussion, Conclusion, Acknowledgements (if any), Appendix, Notes, References, etc. The paper should preferably not exceed 32 typewritten pages (about 40,000 characters) including tables and references. The approximate location of tables and figures should be indicated on the margin.

Tables and Figures. Tables, each bearing an informative title, should be self-explanatory and numbered consecutively. Black-and-white or gray scaled illustrations should be selected carefully and the number kept to the essential minimum. The author's name, the title of the paper, and the serial number of the figure should be written on the back of each print. Figure captions should be brief and collected on a separate sheet.

References. References should be to peer-reviewed literature whenever possible, so technical reports, conference proceedings, and other "gray literature" should be referenced only when no other source of the material is available.

References should be numbered in order of occurrence in the text, where the numbers are given in square brackets as, e.g. [12]. In the References section, the bibliographic elements of the numbered references should be given according to the following examples:

For a journal article
[1] WRIGHT, S.: Surfaces of Selective Value Revisited. *The American Naturalist*, 131 1 (1988), 115–123.

For a book
[2] WALLACE J. M., HOBBS P. V.: *Atmospheric Science: An Introductory Survey.* Cambridge: Academic Press, 1977.

For a chapter in a book or monograph
[3] KAUFMANN, S. A., JOHNSEN, S.: Co-Evolution to the Edge of Chaos: Coupled Fitness Landscapes, Poised States, and Co-Evolutionary Avalanches. In. LANGTON, C. G., TAYLOR, C., FARMER, J. D., RASMUSSEN, S.: *Artificial Life II, SFI Studies in the Sciences of Complexity,* 325–369. Boston: Addison-Wesley Publishing Company, 1991.

Web references
As a minimum, the full URL should be given and the date when the reference was last accessed. Any further information, if known (DOI, author names, dates, reference to a source publication, etc.), should also be given. Web references can be listed separately (e.g., after the reference list) under a different heading if desired, or can be included in the reference list.

[4] NULAND, V.: *2012 Conference on a Middle East Zone Free of Weapons of Mass Destruction (MEWMDFZ), Declaration of USA Department of States.* Washington D.C., 23 11 2012. www.state.gov/r/pa/prs/ps/2012/11/200987.htm (Downloaded: 14.04.2013)

Submission in electronic format. Definitely no electronic version of the manuscript is supposed to be attached to the original submissions. Such attachments will not be archived or kept for later use by the Editorial Office. In case of acceptance, the authors are kindly asked to send an electronic version of the final, accepted manuscript (on magnetic or optical media or via e-mail). In case of any doubt, always the printed paper copy of the manuscript is considered authoritative.

Copyright Transfer Form. Accepted manuscripts cannot be published unless a Copyright Transfer Form is completed and signed by the Corresponding Author. Copyright Transfer Form can be requested from the Editorial Office through mail, fax or e-mail or can be downloaded from the website of the journal.