9

A Holistic Approach to IT Security

Louise Yngström

Department of Computer and Systems Sciences, Stockholm University and Royal Institute of Technology, Electrum 230, S-164 40 Kista, Sweden
voice 46-8-16 16 10, fax 46-8-703 90 25, e-mail louise@dsv.su.se

This paper presents the Systemic-Holistic Approach developed and used in an academic educational programme in IT security. The programme itself has been presented before in [Yngström 1983, 1988, 1994]. This time the theoretical background to the holistic approach is explained in detail, it is presented how it has influenced the conceptual model of the programme, and how it is taught in the classroom, including reading material. Finally the former presented evaluations are extended with evaluations of the same approach taken in another social environment.

1. INTRODUCTION

The former stated security paradigm "security by openness" seems currently to be shifted towards "security by obscurity". Maybe there was never such a paradigm as security by openness. Discussions on definitions, paradigms, models, and criteria reveal there has existed many different interpretations simultaneously. In order to be able to cope practically with security, it has also been underlined that security needs to be treated holistically [NRC 91, OECD 92], or at least interpretating security demands from other realities than a strict computer science environment [ACM 91, INFOSEC 92]. Many see ethics or moral judgements as one way to cope [see for instance Denning 92, Gordon 94], and most sources turn to training and education for aid.

We have developed an academic educational programme in IT security where a holistic approach is used. The approach facilitates to detect when, what and how biases are used, thus explicitly exposing used definitions, paradigms, models, criteria, environments and values. The programme is based within a regular computer science programme, and has been in operation for ten years. This paper presents the theoretical backgrounds to the holistic approach, how it is used in a conceptual model for the educational programme, and finally some evaluations of the approach.

J. H. P. Eloff et al. (eds.), *Information Security — the Next Decade*

2. THE HOLISTIC APPROACH

2.1. Demands and definitions

There have been demands for the use of holism within IT security, but no real definition has been offered. A dictionary [Longman 1987] gives the following explanation: "based on the principle that a whole thing or being is more then just a collection of parts added together." Holistic in reference to a /computing/ curicula is in [ACM 1991, p 72] commented as "holistic, attempting to reach a wider constituency than any of its predecessors. It is intentionally designed to encourage curriculum innovation and evolution, enabling educators to respond in a timely fashion to future changes in the discipline rather than to simply update earlier models".

General Systems Theory's second hallmarks reads: " all systems have a gestalt, a whole, which cannot be broken down into its constitutional parts and each of the decomposed elements be studied in isolation, but rather /one must/ attempt to view the whole with all its interrelated and interdependent parts in interaction" [Schoderbeck et al 1990, p 38]. The founder of the Society for General Systems Research notes: "There is, however, another remarkable aspect. If we survey the evolution of modern science, as compared to science a few decades ago, we are impressed by the fact that similar, general viewpoints of organisation, of wholeness, of dynamic interactions, are urgent in modern physics, chemistry, physical chemistry and technology. In biology, problems of an organismic sort are everywhere encountered; it is necessary to study not only isolated parts and processes, but the essential problems are the organising relations that result from dynamic interactions and make the behavior of parts different when studied in isolation as within the whole" [von Bertalanffy 1956, p 23]. A similar observation is made almost forty years later: "The growing world network shares many characteristics with biological organisms...The overall system can exhibit behaviors that cannot be seen in an analysis of its separate components." [Denning 1990, p iii].

2.2. Theoretical background to the approach

The approach has been called the Systemic-Holistic approach, and relies on three main building blocks : General Systems Theory including Cybernetics[Ashby 1963, Beer 1964, 1979, Boulding 1964, Schoderbeck et al. 1990, Ackoff 1976 von Bertalanffy 1956, 1968, Wiener 1948], Soft System Methodology [Checkland 1988, 1990] and General Living Systems Theory [Miller 1978, de Rosnay 1975]. In addition explanations and further comments are facilitated by Laufer [Laufer 1985, 1990]

General Systems Theory had its origin in observations of similar phenomenon existing in many different sciences. To study these interdisciplinary, Bertalanffy chose the concept of 'system'. He used 'system' as an epistemological device to describe organisms as wholes, and showed that it could be generalised and applied to wholes of any kind. Checkland developed this further [Checkland 1988] in discussions on the confusion between what exists (the ontological entity) and what is an abstraction (the epistemological entity).

Checkland´s view is that humans can only perceive reality through a methodology which uses abstract concepts. In perceiving realities, humans can consciously reflect on this, and in doing so, they will test and change concepts, in order to fit them better to perceived reality. In the process of testing and changing there is a multi creating relationship between perceived reality and intellectual concepts. When confusing perceived reality - the epistemological entity - with reality - the onthological entity - humans tend to control through engineering rather than through understanding. Controlling through understanding he calls systemic or soft systems thinking, while he calls controlling through engineering hard systems thinking.

The main differences between using the soft systems and the hard systems thinking are the following: in soft systems thinking perceived realities are treated as problems and methods to solve these are systemic, while in hard systems thinking perceived realities exist and are systemic and its methods become systematic. Thus in using soft systems thinking, the human is learning how the concept of system reflects the real world. S/he does not decide once and for all that this 'system' is the world, but rather an -possibly changing - understanding of the world. Checkland does not refrain from hard systems thinking and engineering; rather he underlines, that soft- and hard systems thinking are complementary to each other. But the decision when to change from one to the other is a human subjective one.

The confusion between "what seems to exists" and "what exists" has been labelled by Checkland as "the confusion between the image of the system and the system's image". By [Laufer 1985] it is described as the confusion between the science of nature and the science of culture; what is neither nature nor culture is artificial. And the science of the artificial is the science of systems; that is cybernetics.

Laufer offers one more explanation of importance to the /IT/security area: the main reason for the confusion between what is nature and what is culture is that the ultimate locus of control is undecided. This generates an on-going crisis. Either then, he states, the problem is very simplistic and implies a great number of similar events; in that case a manager can predict future states of the system and is confronted with the relatively safe risk of controlling the probable. More often assumptions cannot be made about the similarity of future events or about their independence, and management is confronted with the problem of controlling the improbable. The results of trying to control and cope with the improbable is to control it symbolically; for instance through laws that authorize, commissions to deal with abuses or prevention, ad hoc commissions to deal with any new emerging problems, security norms produced by suitably composed commissions or public opinion through opinion polls [Laufer 1990].

Checkland and Laufer, following on Bertalanffy and General Systems Theory, thus gives grounds for studying the concept of 'system' as an epistemology for studying and understanding perceived realities. The actual choice of when to change over to hard systems thinking becomes subjective, but is done consciously, and, as we shall see becomes a part of the conceptual model and the pedagogics used in the classroom.

General Living Systems Theory forms the third building block to the concept of systems, since it deals with systems that really exist - the onthological entity. It offers a concrete understanding of how physical realities restrict theoretical models, so frequently used within IT security that we tend to believe that the models are the reality.

General Living Systems Theory [Miller 1978] deals with living, concrete, open, homeostas aiming, systems composed of matter and energy and controlled by information. Matter and energy are considered in their physical form, and information is defined as physical markers carrying information. Thus a living system is composed of physical entities. Moreover, living systems exist on seven levels; cell, organ, organism, group, organisation, nation, and supranational; each level needing nineteen critical subsystems for its survival. Each subsystem is described through its structure and process and through measurable representative variables. The model is recursive on each level. General Living Systems Theory offers knowledge and insights on how to link reality to theoretical models; through understanding of physical realities, restrictions of the domains of different theories can be understood.

Sequentially - because we know no other way of presenting a material - the Systemic-Holistic approach starts with General Systems Theory and Cybernetics which presents the foundations of the epistemology, the way to understand and learn. It is interfoiled with adequate, contemporary /IT / security examples. It is further developed along General Living Systems Theory, exemplifying for instance the following citation from [Hofstadter 1979, p 686] elaborating on the issue "Do words and thought follow formal rules?" "the ultimate answer is "Yes - provided that you go down to the lowest level - the hardware - to find the rules...neurones run in the same simple way the whole time. You can't "think" your neurones into running some non neural way, although you can make your mind change style or subject of thoughts...Software rules on various levels can change; hardware cannot - in fact, to their rigidity is due the software's flexibility!". It also sheds some lights into some obvious reasons to IT security problems; [Hoffman 1992, p 4] "The traditional and widespread von Neumann architecture is inappropriate for systems shared by a large number of users, not all of whom trust each other...The technical communities will have to produce changes in the basic architecture of personal computers to avoid the threat of expensive product liability suits". And some other well known phenomena such as the result of the Harrison-Ruzzo-Ullman model as presented by [Pfleeger 1989, p 255]: "..The first result from HRU indicates that it is possible do decide whether a given subject can ever obtain a particular right to an object. Therefore, it is decideable whether a low-level subject can ever obtain read access to a high level object, for example...As a second result, Harrison et al. show that if commands are not restricted to one operation each, it is not decidable whether a given protection system can confer a given right. This result indicates that one cannot determine in general if a subject can obtain a particular right to an object...the HRU result can be extended: There may be an algorithm to decide the access right question for a particular collection of protection systems, but even an infinite number of algorithms cannot decide the access right question for all protection systems."

Thus General Systems Theory makes it possible to define and investigate systems and their phenomena free from any biases than that of the concept itself. This way paradigms, values and other related entities can be explicitly defined and discussed in context.

None of the presented theories give absolute criteria as to when to change from an epistemological to an onthological treatment to reach security - rather this is directed to be performed in interaction with the phenomena themselves. It becomes a

/subjective/ assessment based on a specific domain of action, a context. But together they indicate how to organise teaching for establishing continuous learning processes in IT security: always to question if "facts" really can be considered as such, and always try to confront facts with context, even with different contexts. This may also be a suitable mode governing the design, operation, management, and evaluation of secure IT structures.

2.3. The conceptual model for IT security education based on the Systemic-Holistic Approach

The conceptual model is very simple; it consists of a three dimensional framework and a systemic module (Figures 1 and 2). The systemic module acts as an epistemological device for "facts" in the framework. It presents the foundations of General Systems Theory and Cybernetics, Soft System Methodology and General Living Systems, as shortly explained above. Through these, security as the concept of control and communication, can be defined, investigated, and explained on a level free from any other biases than the system concept itself. This meta knowledge may then be applied at any level of the three dimensions of the framework; each practical interpretation may thus be viewed as an instance of subject area, level of abstraction and context.

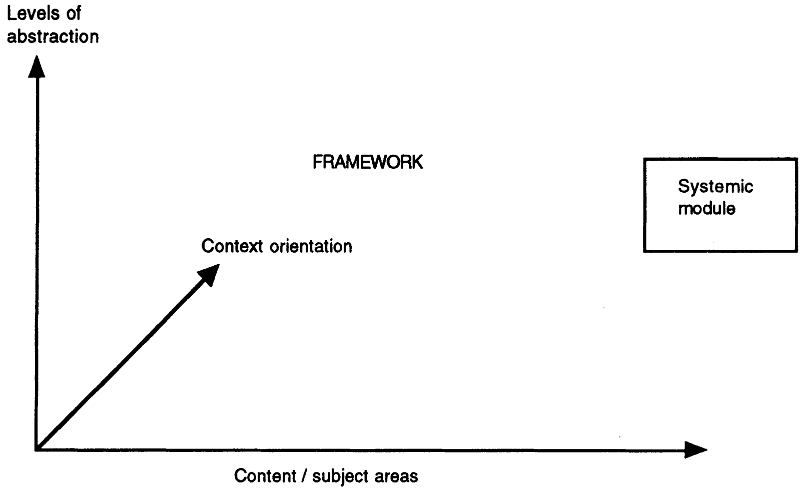

Figure 1. The conceptual model for the comprehensive programme. Overview

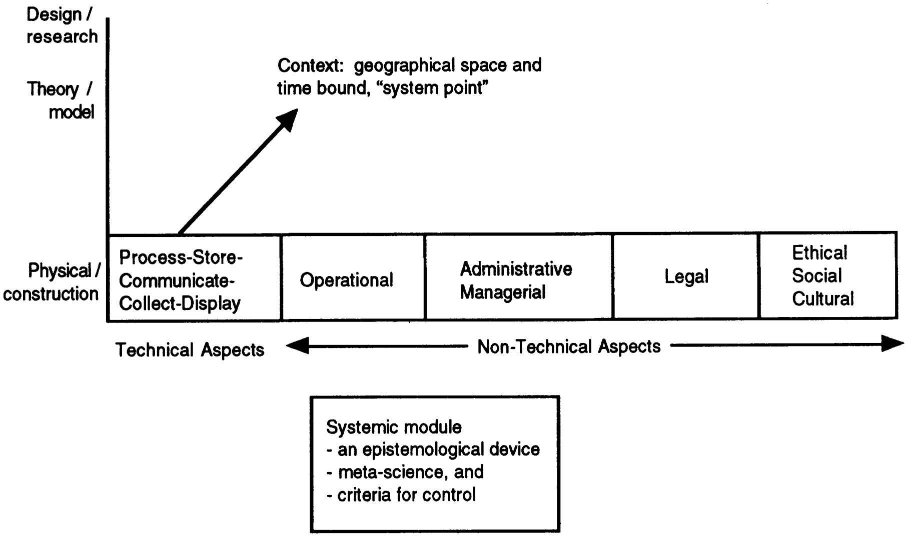

Figure 2. The conceptual model for the programme. Detail.

Also the dimensions of the framework indicate the presence of system theories:
- one dimension is content/subject areas, including technical (collect-process-store-communicate-display)and non-technical (operational-managerial/administrative-legal-ethical/social/cultural) aspects,
- one dimension is levels of abstraction; physical/construction - theory/model - design/research, and
- one dimension is context; geographical space and time reference.

The systemic module and the framework is viewed as a system with the potential to be viable in the sense of [Beer 1979]: in order to establish a control system that will grant viability to a system, three levels need to be analysed; the system itself (system in focus), its environment (the meta system) and the level below the system in focus. Together the three dimensions may be be referred to as Beer's three levels of analysis and the analysis is eventually also applicable recursively in the dimensions separatedly.

During the educational programme in IT security the systemic module and a particular intersection of the dimensions of the framework are combined. This starts by generalisations - the abstract concepts that once were perceived by someone in interaction with reality. Through presenting examples and inviting participants to give or test their own examples, there is a shift from the ontological approach towards an epistemological approach. The results looked for - knowledgeable attitudes and conducts - will foster awareness and assurance that these generalisations are valid for each participant's own perceived realities of security. Thus the systemic module used together with the framework acts as an epistemological device which in itself defines security by using system concepts (1), and through its definitions acts upon the framework (2).

The initial systemic module includes in short: General systems theory, cybernetics, and general living systems theory provide the foundations for survival structures and mechanisms usable for control. Special emphasis is put on negative and positive feed-back mechanisms. This is aiming at creating an understanding for the needed balance between development and control, the two main functions involved in systems' survival. The theory for living systems focuses on how nature constructs its control cycles, and what happens if these are broken. Similarly is studied for the levels individual, group, organisation, national and international. Threat-risk-safeguarding sequences are introduced and studied for general systems and IT systems. Examples of different possibilities to secure system are made over the whole content area and within different contexts. The most important principles from the module, recurring in all other modules are:

- delimit the system of study from the environment,
- define the existing environment,
- define the inflow, throughflow, and outflow, and
- structure the built-in control system so that it can deal with relevant inner and outer variety.

2.4. Detailed content of the systemic module

The Systemic module is the first course in the programme. It is organised into eight lectures, each on a three hours duration. A typical outline of the eight lectures is

1. Introduction to Security Informatics - a holistic view on security and safety

Systems approach, System characteristics, What is a system; sets, objects, relationships, attributes, environments, whole, Diagram of a system, Boundaries of a system. General systems theory: origin, postulates, properties, Classifications, Open and closed systems, Isomorfic systems, Hierarchies of systems, Adaptability of systems, Evolution and growth of systems.

Application of system theories on traditional /Swedish/classifications of risk management and security

Literature: Schoderbek chapter 1-2, Hamilton (in Swedish) overview.

2. Security and control versus risk.

Cybernetics: feedback, closed-loop systems, open-loop systems, first-, second-, and third-order feedback systems (automatic goal attainment, automatic goal changer, reflective goal changer), control and the Law of requisite variety, complexity and Black Box, Basic elements of control systems, Stability and instability of control objects, Examples of cybernetics in organisations. Applications of cybernetics on traditional /Swedish/ classifications of EDP security.

Literature: Schoderbek chapters 3-5, Freese (Swedish) overview.

3. Information Security or Computer Security?

Data versus information, Economics of information, Information theory; measuring information, channel capacity, entropy, Communication; scientific and operational approaches, levels, structures, problems.

Literature: Schoderbek chapter 6

4. Environments for Infosec.
Uncertainty, Change, Complexity, Scanning and decision making, Scanning processes, Information in open systems, Informational flows, Organisational effectiveness, Goals and problem solving; optimization, suboptimization, bounded rationality, problem identification and problem solving.
Literature: Schoderbek chapters 7-10

5. Safety and security in the System perspective.
Theory of living systems: classifications of levels, subsystems, and concepts for living systems. Structures and processes for information handling, matter/energy handling, information/matter/energy handling in systems.
Literature: Miller chapters 1-4

6. Can theory and practise unite?
Application of the concepts of traditional /Swedish/Risk management and EDP security on system theories.
Literature: Hamilton and Freese (in Swedish)

7. Example of system theory as control method.
Structures of control systems, Control hierarchies versus controlled hierarchies, Self regulation, Proactive versus reactive control.
Literature: Beer chapters 1-2, 4, 6, 11-15

8. Discussions and conclusions.
Literature: all above.

Literature in English:
Beer, S: Brain of the Firm. The Managerial Cybernetics of the Organization. second ed., Wiley, New York, 1986.
Miller, J.G.: Living Systems, McGraw-Hill, New York, 1978.
Schoderbek, C.G. et al.: Management Systems, Conceptual Considerations. fourth ed., Business Publ. Dallas, Irwing-Dorsey, London, 1990.
Supplementary: lists of vocabulary in IT security.

Literature in Swedish:
Freese, J. et al.: Datasäkerhet. Praktisk handbok för beslutsfattare. Affärsinformation AB, Stockholm, 1989.
Hamilton, C.: Detta är risk management. Studentlitteratur, Lund, 1985.
Supplementary: ordlistor inom området informations/ADB/data säkerhet (Swedish vocabulary in IT security)

Examinations are typically of a four hours essay-type, with 80% of questions dealing with definitions in relation to system theories and infosec, and 20% analysing a current infosec problem in a system perspective. During 1993/94 one analysing problem dealt with escrew encryption: students were asked to read a specially prepared Swedish text and analyse involved systems, their boundaries, environments and flows. At another examination the problem dealt with reported security breaches in a net at a university. The same questions were asked.

2.5. Evaluations of the systemic module

A thorough study of the effects of the systemic-holistic approach on former students was performed in 1991 and reported in [Yngström 1993]. Specifically was investigated how knowledge in systems theory and related general systems theory, general living systems theory and cybernetics had facilitated assessing and understanding problems, work efficiency and effectiveness, and continuous learning within the field of security and IT security. The population consisted of 71 students out of a total possible of all students ever within the programme of 155.

These students were all at least on their last year of an undergraduate education majoring in security informatics. Their previous theoretical studies were mainly computer science, business administration and law, but also graduates from military or police academies were amongst this group. Many had experiences from the traditional or EDP/IT security areas; varying from a few months up till more than five years of practise. In reference to ordinary third year students their ages were higher with a mean towards their late 30ies.

Results indicated that the use of systems theories as an explicit theoretical foundation, facilitates an interdisciplinary and holistic view of IT security, as well as eases delimiting and specifying work tasks for oneself and others. Former students also have advanced in their careers; knowledge in IT security is favoured for the position of corporate security director.

During the first half of 1993, the author had the opportunity to incorporate a reduced systemic module into an existing Information security course on graduate level at the Faculty of Information Technology at Queensland University of Technology in Brisbane, Australia. In a general course assessment performed through the QUT Student Guild, the overall rating of the whole course was 'Great' or 'God' in 79% of cases. For specifically evaluating the systemic-holistic approach the same questionnaire as used in the second Swedish study refered to above was utilized. This total population consisted of 35 persons, 21 questionnaires were received.

These answers indicate firstly that the Australian students were much younger - the mean towards late 20ies - and few had started their professional careers or had had previous work experiences. Less than one third recorded prior or present work position. If they belonged to outside professional bodies these were related to computing, not to security, auditing or law as recorded in the Swedish study. In reference to prior theoretical studies, they were mainly majoring in one subject and also showed smaller diversity in their theoretical studies as well as practises than the Swedish group. Theoretical studies were recorded in computer science, business administration, military and police sciences, but not in law, which is an increasing subject within the Swedish group of IT security students.

Compilations indicate also positive reactions from the Australian students, although the total answer differ widely from the Swedish group. When it comes to propositions dealing with the students´ own work, overall understanding, theoretical work, products and work methods 50-80% of the group is positive. When it comes to propositions dealing with linkage to other persons´work tasks or detailed work tasks, few record a positive reaction and 90% of the group recorded "the question is not relevant to me". If however, the evaluation is interpreted only on the basis of those who have previous experiences, reactions indicate positive answers with a very similar rate as the Swedish group also for work related questions.

It thus seems reasonable to interpret the results of the two groups assessed as follows: The systemic-holistic approach facilitates to assess and understand problems, increase work efficiency (doing things right) and effectiveness (doing the right things) and foster continuous learning within the field of security and IT security, provided the student has some own experiences to refer to. When students do not have their own work experiences, the systemic-holistic approach still facilitates assessment and understanding of problems, increase of effectiveness (doing the right things) and fostering of continuous learning - but in order also to increase efficiency (doing things right) practise is needed. This is firstly not surprising; the epistemology (what seems to exist) fosters understanding of the onthology (what exists), but does not substitute it totally. Secondly the order as such between doing the right things and doing things right is preferable - once the epistemology gives guiding principles, details can be added during work. In fact, this is a fundamental principle of learning which is also discussed within other areas of engineering subjects with similar results [see for instance Smith 1991].

3. DISCUSSION AND CONCLUSIONS

The need for vehicles to support understanding, using, and coping with different definitions, models, criteria, paradigms, and interpretations in the form of devices and safeguards for IT security is obvious - we shall never find one single one to suit all circumstances. The systemic-holistic approach presented here has shown to act as such, in particular for persons who have already some understanding of what IT security is about. It offers a meta model within which particular views on IT security may be investigated. Moreover, it offers the IT security professional to consciously investigate effects of different alternatives - also from different involved other specialist security areas. It leaves the value judgments to humans, but supports their analyses. In addition, the systemic-holistic approach offers the possibilities to make humane judgements.

REFERENCES

[Ackoff 1976] Ackoff, R., *Designing a National Scientific and Technological Communication System*, University of Pennsylvania Press, 1976

[ACM 1991] *Computing Curricula 1991. Report of the ACM/IEEE-CS Joint Curriculum Task Force.* ACM Press & IEEE Computer Society Press, 1991.

[Ashby 1963] Ashby, R. *Introduction to Cybernetics*, Wiley & Sons, New York, 1963

[Beer 1964] Beer, S., *Cybernetics and Management*, John Wiley & Sons, 1964

[Beer 1979] Beer, S., *The heart of the enterprise.* John Wiley & Sons,1979.

[Boulding 1964] Boulding K., "General Systems as a point of view" in Mesarovic, M., D. (ed) *View on General Systems Theory*, John Wiley & Sons, New York, 1964

[Checkland 1988] Checkland, P.B., "Images of Systems and the Systems Image", Presidential address to ISGSR, June 1987, in *Journal of Applied Systems Analysis*, 15, (1988) 37-42.

[Checkland 1990] Checkland, P.B., *Soft System Methodology in Action*, Wiley & Sons, 1990

[Denning 1990] Denning, Peter J., (ed) *Computers under Attack. Intruders, Worms, and Viruses,* ACM Press, Addison-Wesley Publishing Co., Mass, 1990

[Denning 1992] Denning, D. E., "A New Paradigm for Trusted Systems" in *Proceedings 1992-1993 ACM SIGSAC New Security Paradigm Workshop, September 22-24, 1992, August 3-5, 1993, Little Compton, Rhode Island, USA,* IEEE Computer Society Press 1993

[de Rosnay 1975] de Rosnay, J, *The Macroscope. A New World Scientific System,* Harper & Row Publ., New York, 1975

[Gordon 1994] Gordon, S., "Technologically Enabled Crime: Shifting Paradigm for the Year 2000" in *Proceedings of the Tenth International Information Security Conference, IFIP SEC'94, Curacao, Netherlands Antilles, May 23-27, 1994.* Conference edition

[Hoffman 1992] Hoffman, Lance J.: *Reducing Society's Vulnerability as Computers and Networks Proliferate.* The George Washington University, Institute for Information Science and Technology GWU-IIST-92-19, 1992.

[Hofstadter 1979] Hofstadter, Douglas R., *Gödel, Escher, Bach: an eternal golden braid. A Metaphorical fugue on minds and machines in the spirit of Lewis Carroll.* Penguin Books, Harvester Press Ltd, 1979.

[Laufer 1985] Laufer, R., "Cybernetics, Legitimacy and Society", in Yngström, L., Sizer, R., Berleur, J., Laufer, R. (eds) *Can Information Technology result in Benevolent Bureaucracies? Proceedings of the IFIP TC9/WG9.2 Working Conference,* Namur, Belgum, 3-6 January, 1985, North-Holland, 1985, 29-42.

[Laufer 1990] Laufer, R., "The Question of the Legitimacy of the Computer: An Epistemological Point of View", in Berleur, J., Clement, A., Sizer, R, Whitehouse, D.(eds), *The Information Society: Evolving Landscapes,* Springer Verlag & Captus University Publications, 1990.

[NRC 1991] *Computers at Risk. Safe Computing In the Information Age.,* System Security Study Committee Computer Science and Telecommunications Board Commission on Physical Sciences, Mathematics, and Applications, National Research Council, National Academy Press,1991.

[OECD 1992] *Guidelines for the Security of Information Systems, Organisation for Economic Cooperation and Development,* OECD/GD(92)190, Paris, 1992.

[Pfleeger 1989] Pfleeger, Charles P., *Security in Computing.* Prentice Hall,1989.

[Schoderbek et al. 1990] Schoderbek, P., Schoderbek, G., Kefalas, A., *Management Systems. Conceptual Considerations,* 4:th ed, Irwin, Boston, 1990

[Smith 1992] Smith, R. A.,(Ed) *Innovative teaching in engineering,* Ellis Horwood Ltd, Chichester, 1991

[Wiener 1948] Wiener, N., *Cybernetics or Control and Communication in Man, Animal, and Machine,* John Wiley & Sons, 1948

[von Bertalanffy 1956] von Bertalanffy, L., "Main Currents in Modern Thought" in *Yearbook of the Society for General Systems Research,* Vol 1, 1956

[von Bertalanffy 1968] von Bertalanffy, L., *General Systems Theory,* Braziller, New York, 1968

[Yngström 1983] Yngström, L., "Education in Safety Systems and Security Analysis - Suggestions for a One Year University Program", in Fåk, V. (ed) *Security, IFIP/Sec'83, Proceedings of the First Security Conference, Stockholm, Sweden, 16-19 May 1983,* North-Holland, Amsterdam 1983, p 295-303

[Yngström 1988] Yngström, L., "Experiences from a one-year Academic Programme in Security Informatics", in Caelli, William (ed) *Computer Security in the Age of Information, Proceedings of the Fifth International Conference on Computer and Security,* 19-21 May, Gold Coast, Queensland, Australia, North-Holland, 1988.

[Yngström 1993] Yngström, L., "Evaluation of an academic programme in IT Security 1985-1990", in Dougall, Graham E., Jones, Darren, (eds) *Computer Security: Discovering Tomorrow, Proceedings of the Ninth IFIP International Symposium on Computer Security,* IFIP/Sec'93, Deerhurst, Ontario, Canada, 12-14 May, 1993, 281-294.

[Yngström 1994] Yngström, L., "Education in IT Security at Bachelor and Master Levels Using a Systemic-Holistic Approach" in Seizer R., Yngström, L., Kaspersen, H., Fischer-Hubner, S., (eds) *Security and Control of Information Technology in Society, Proceedings of the IFIP TC9/WG9.6 Working Conference on Security and Control of Information Technology in Society on board M/S Ilich and ashore at St. Petersburg, Russia, 12-17 August, 1993,* North-Holland, 1994.