AN HOLISTIC APPROACH TO AN INTERNATIONAL DOCTORAL PROGRAM

Louise Yngström
Department of Computer and Systems Sciences, Stockholm University& The Royal Institute of Technology, The IT university in Kista, Sweden.
louise@dsv.su.se

Abstract: The paper discusses forms and structures for an international doctoral program with specialization in information security and information assurance based on an analysis of international educational efforts in the area 1995-2003. The presentation underlines the need for holistic approaches to the IT security area and presents, as an example, the Systemic-Holistic Approach, SHA.

Key words: Systemic-Holistic, Information Security, and PhD Education

1. INTRODUCTION

Many problems within information security are multidisciplinary in nature – there are needs for knowledge from natural sciences as well as law, social sciences and humanities. This becomes problematic in research (as well as in practice) since each science has its own defined knowledge field and well established research methodologies. Basically two world views clash – the formal/hard and the informal/soft. To bridge the gap inter-, multi- and cross disciplinary methods are often used successfully but they demand each participant to have detailed knowledge in each involved discipline. Holism takes the meta-approach where an actual problem is investigated from some generalized system-concept; this may emanate from any area of science but is initially scrutinized as one whole. The result of the systemic analysis will further direct the course of research and actions. This way knowledge from soft and hard sciences is bridged. This paper discusses how to use an holistic approach to a PhD program in information security and information assurance.

The paper is organized as follows: The international doctoral program with a bias towards a holistic approach is discussed. The WISE1-3 conferences are revisited to conclude about holistic and interdisciplinary demands within the area, and to underline the international developments within academic teaching 1995-2003. Finally there is a section on the Systemic-Holistic Approach, developed and used by the author.

2. DISCUSSING THE INTERNATIONAL DOCTORAL PROGRAM

Following the Systemic-Holistic Approach, SHA, (see section 4), the content of any holistic oriented research needs a description of the field of study. Thus the core curriculum of such a PhD program needs to be specified in terms of what courseware in IT security is needed in addition to courseware in science, including scientific and research methodology. I will use the SHA approach for sketching and discussing the international doctoral program with specialization in information security and information assurance; doctorate by research and a professional doctorate; different sectors including academic, military and armed forces, law enforcement, government and private industry. The approach includes in short: delimit the system of study from the environment, define the existing environment, define the system through its inflow, through-flow and outflow, and structure the in-built control system to deal with inner and outer variety

2.1 The system of study

The system itself is the education with its processes, the students including their learning processes, the main advisors including their preferences and knowledge, the department (subject) and university, eventually also the nation, where the PhD candidate is enrolled. I will assume that a professional doctorate candidate will have some home-department apart from his/her company (equivalent).

2.2 The environment

The most important environment will include all the other international departments and universities which are part of this “international federation of doctoral consortium”. Each one is viewed as a system of its own. Defining it this way, each department and university can use their own internal as well as external rules.[1] The environment also encompasses the companies/organizations and many of the problems which will be involved in the research. Particularly in research, there will also be international organizations of various kinds which are either interested in the research, conduct or fund research themselves, are involved in actions which interacts with /parts of/ research, etc.

2.3 The system; its inflow, through-flow and outflow

I will assume that a doctorate will take 3 years of full-time research, and that the candidate will have a bachelor and a master degree (app. 3+2years) prior to entering the PhD education. In an ideal case the candidate will already have studied security in relation to IT on the undergraduate or graduate level. The minimum knowledge in information security (equiv) ought to be somewhere similar to programs described in Proceedings of the WISE conferences (see section 3 of this paper) of an extent to about 1,5 years of full time studies. In addition I would wish the candidate to have studied general science, scientific methodology, research methodology and scientific communications (oral, procedural, and writing including an /under/graduate thesis or project) to the equivalence of approximately 1 year. The candidate entering the PhD program should be a mature person with an urge to learn – and in the ideal case – also have a problem area of interest. Scrutinizing this problem area together with an advisor should result in a provisional and individual research plan. This plan may include courses or specification for courses, and projects. All specifications should be guided by the goal of the PhD, which initially will be rather hazy, but gradually materialize into a clearly defined specification. This implies that I do not favour course-work per se within the PhD education except when the knowledge is identified as a need. This also implies the existence of a present, knowledgeable and interested advisor. Initially the advisor will "point will full hand" towards the goal and its content, but gradually the PhD candidate should take over full responsibilities for his/her research. I really see no principal differences between a professional doctorate and a doctorate by research, except for maybe the scope. Still, both doctorates will need to

[1] Experiences within similar curricula development (Erasmus/Socrates) show that each country has its own regulations and it takes long time to harmonize university educations. Even if Europe is in a process of harmonizing its system of higher education (the Bologna process it will still take time to implement it. An international program probably takes even longer.

show how to use sound scientific methods even though the balances between practical and theoretical work may be different.[2]

This implies that the best way of cooperating internationally is to be able to offer the courses we do give to the international forum, thus for the international doctorate program I suggest IFIP 11.8 members to put up a course catalogue on the web site for this purpose as a start.

When it comes to the "holistic" doctorate, I view the approach as a scientific research methodology that may be used for inter-, multi- or crossdisciplinary problems. This usually implies incorporating knowledge from related fields such as management, economics, law and culture, but may also be used to incorporate aspects of software engineering and information systems. I believe a course on holistic approaches, as indicated in section 4 could be part of the scientific methodology.

2.4 Structure the in-built control system to deal with inner and outer variety

Since I suggest each department and university partaking in the international activities of a PhD program in information security as a system of its own, each department will be left with their own rules. International agreements, such as the Bologna process for European higher education may change this gradually.

3. WISES REVISITED

International Federation for Information Processing, IFIP, has through its working group 11.8 conducted workshops and conferences since 1995 within the wide area of education in information security and information assurance. For the purpose of this paper, the author went through all the proceedings to bring the WG up-to-date with our findings. The analysis shows that the area has matured; the academic international education is converging towards consensus of core knowledge, and there are many detailed examples given of courses, contents, extent and laboratory work. Driving forces seem to have been the ERASMUS/SOCTARES program in Europe and the National Colloquium for Information Systems Security Education in the US - many universities have contributed their knowledge to

[2] This actually implies that I believe a MSc or a MBA towards security should be the preferred professional degrees for people working practically with security outside the academies. A professional PhD could still imply research, but maybe then more directed towards problems of a specific organization.

the success. In 2001 bodies outside the traditional universities, such as police and armed forces joined with their plans and experiences. In 2003 we note reports strongly arguing for holistic, inter- and multidisciplinary approaches to information security particularly for business-oriented education. Didactic questions are starting to appear, in particular distance-education and forms for assessment of programs. Along come also reports from developing countries, changes in profiles of infosec professionals, training approaches for SMEs, teaching PETs, etc. Apart from one paper on forensics and one on IPR, problematisations from legal points of view on information security education on any level is lacking, as is value-oriented questions and extensive comments on educational programs targeting trade&industry. Each of the conferences is characterized through listing of given titles and themes.

3.1 Pre-WISE work

IFIP's working group within the Technical Committee on Security and Protection in Information Processing systems (TC11) number 11.8 Information Security Education, was established in 1991. In 1995 a series of workshops intending to build a critical mass of active international members named *Information Security Education – Current and Future Needs, Problems and Prospects* were initiated to run in parallel with the annual SEC95-98 conferences. Major themes in Cape town, South Africa 1995 were European academic IT security education, Information security education in the business administration environment and Demands for ethical curricula in the information age. The following year, 1996, on Samos, Greece themes were Awareness models, Teaching and learning models and Needs for standard curricula for different groups and levels, in addition to papers on Privacy, Laboratories and Holistics. In Copenhagen, Denmark 1997 themes were extended towards reporting on practical approaches and experiments with a much wider international appearance also including teachers, pupils, data protection officials – and post graduate level. Finally, the forth workshop on a boat on the Danube between Vienna, Austria and Budapest, Hungary in 1998 presented detailed educational programs, mainly academic, from the international scene.

By 1999 the time was ripe to start dedicated international conferences on themes around the teaching and learning of information security. They were named WISE particularly to underline that the teaching and learning about security in IT systems calls for reflections and analyses of what these systems – once made secure in some sense – will be able to accomplish in the real world. "Will they provide for trust in information systems, will they lead to a more secure world, for whom, will they perhaps change existing balances and power structures, will they tend to control individuals, etc.?

The creation of awareness and understanding of the demands for security in IT systems has proven necessary; lacking acceptance with the users will result in inadequately functioning IT security. Also lacking awareness and understanding with the computer scientists and technicians of the demands for security in IT systems from business and user perspectives cause deficient IT security. This is what WISE is about – to present, analyse and discuss what, how, and whom to teach about information systems' and information technologies' security." (Yngström, 1999, p v). The acronym stands for World conference on Information Security Education, suggested by our late 11.8 member Peter Fillery after the 1996 workshop. Hopefully the WISEs will be vehicles not only for how-to-do-reports – even if they are extremely helpful for the international audience – but also for exhibiting and discussing specific research problems incorporated within the teaching of and learning about IT security and information assurance.

3.2 WISE1

Looking back at WISE1 in 1999, themes were introvert and reported in depth on what today would have been called traditional academic IT security education. There were only a few non-academic target groups added and the focus on teaching IT security to trade and industry was almost negligent. Very few research problems were discussed. Titles talk for themselves: Academic Curricula and Curricula Developments in Europe – The ERASMUS/ SOCRATES Approach, Incorporating Security Issues Throughout the Computer Science Curriculum, The Reference Monitor Concept as a Unifying Principle in Computer Security Education, Personnel Training for Information Security Maintenance in Russia, IT Related Ethics Education in Southern Africa, Data Protection in Healthcare and Welfare, A MixDemonstrator for teaching Security in the Virtual University, On the Experiment of Creating the Electronic Tutorial "Vulnerability and Protection Methods in the Global Internet Networking" in Moscow State Engineering Physics for Education of IT Security Professionals, Information Security Best Practice Dissemination: The ISA-EUNET Approach, Amplifying Security Education in the Laboratory, IT Security Research and Education in Synergy, Developing an Undergraduate Lab for Information Warfare and Computer Security, Internet Groupware Use in A Policy-Oriented Computer Security Course, Teaching Computer Security – the Art of Practical Application, Some Aspects of Cryptology Teaching, Explaining cryptosystems for the general public, Approaching the concept of IT security for young users, Introducing IT security Awareness in Schools; The Greek Case, Making information security awareness and training more effective, The Value and Assessment of Information Security Education and Training, The Manual is the Message – an Experiment with Paper based and Web based IT security manuals. (Yngström&Fischer-Hubner, 1999).

3.3 WISE2

In WISE2 the scope had widened, nationally as well as internationally. There were reports on international curricula, important educational problems and impacts also outside established academic institutions such as the police and armed forces, the cyber environment, small enterprises, distance education and societal issues. The inter- or multidisciplinary issue was raised by many authors.

Titles were: Global Impacts, Future Challenges and Current Issues in Training within the Police Computer Crime Unit, Information Warfare and Cyber Warefare: More Than Just Software Tools, Information Security; International Curriculum Projects, The Russian Experience – Information Security Education, Updates on the SOCRATES/ERASMUS Program, Teaching Cyberwarefare Tactics and Strategy, e-Education Frameworks: Applying Generalized Development Strategies to IT Security Courses, An Information Security Education Program in Finland, Information Security Education, Teaching Security Engineering Principles, Core Curriculum in Security Science, Problems in Designing Secure Distance Learning Systems, The Virtual Campus, Action learning in practice, Progress Testing in Distance Learning, A Security Training Approach for UK Small and Medium Sized Enterprises, IFIP World Computer Congress/SEC 2000 Revisited, Teaching Privacy-Enhancing Technologies, Game-Based learning within IT security Education, Human Aspects of Information Security, Awareness and views on Intellectual Property Rights concerning the Internet, Analysis of Teaching GNY-Based Security protocol, Information Security Aspects in the Expert Training Program on Physical Protection of the Objects, Reaching for the Stars – a practical case study in securing computer facilities.(Armstrong&Yngström, 2001).

3.4 WISE3

At the time of WISE3 the area had matured profoundly. There are many detailed curricula reports, including laboratory experiments with different flavours, extensions, levels, depths, widths and target audiences; excellent aids for new-comers. The developed west-oriented world dominates, but also smaller and less developed countries report progress. There are more quests and suggestions for interdisciplinarity, in particular marrying IT security education with education in business administration and intelligence. Computer forensics and information assurance are emergent concepts for education and existing definitions and focuses are problematized. Evaluation appears as a separate subject and the concept of education is widened to include re-training and the activating of alumnae and other external groups. A natural extension of the curricula towards the postgraduate level is present and there are suggested research areas and themes. Titles are: Cyber Security as an Emergent Infrastructure, Teaching Network Security Through Live Exercises, Information Warefare in the Trenches, Changes in the Profile of Security Managers, A Tutoring System for IT Security, Design of a Laboratory for Information Security Education, Integrating Information security and Intelligence Courses, Internet Security Management, Information Security Fundamentals, Australia's Agenda for e-Security Education and Research, Is Security a Great Principle of Computing, IT Security Readiness in Developing Countries, A Program for Education in Certification and Accreditation, Mastering Computer Forensics, Assembling Competitive Intelligence Using Classroom Scenarios, Teaching Undergraduate Information Assurance, Out-come based Assessment as an Assurance Education Tool, Evaluation Theory and Practice as Applied to Security Education, Ten Years of Information Security Masters Programmes, Network Security Scientific and Research Laboratory, A Comprehensive Undergraduate Information Assurance Program, Training the Cyber Warrior, Security Education for Times of Netwar and Peace, Improving Security Awareness Through Computer-based Training, Identification and Integration of Information Security Topics, A Dedicated Undergraduate Track in Computer Security Education (Irvine&Armstrong 2003).

4. AN HOLISTIC APPROACH TO INFORMATION SECURITY AND INFORMATION ASSURANCE

When I first started to study – and later – to teach about information security from a holistic - later called systemic-holistic – base, I did not understand fully that it was a difficult (and to some extent even until today unsolved) scientific problem. My department was one of the first ones to consider computer science and information systems together – to our notion computers process data which in some sort of intelligent process (often involving humans) may be transformed to information. And viewing the IT security problems (initially of privacy) from the point of view of a generalized system, made it easy to state/understand the security problems as problems of integrity. To my understanding no system, not even 'privacy' could be totally without an environment with which is has relations; thus it boils down to some sort of control problem. Cybernetic systems are controlled through feed-back; and in theory they apply 'control from within' (Wiener 1948, Beer 1964, 1968). They appear in various forms. Thus security to me could be viewed from the point of view of building /a/ control system/s/.

The third central part of the holistic approach was General Systems Theory, GST. The purpose of GST(von Bertalanffy 1956,1968) was to further the development of theoretical systems applicable to more than one of the traditional disciplines into a meta-theory. This way analogies and isomorphies can be used from one known area to another. GST rests on five postulates and ten hallmarks, which in essence view the world from formally provable realities where general laws and structures may be transferred from one level to another, from one area to another provided there are strong similarities. Thus assessed research methods could be applied in new fields.

In the theoretical building of the systemic-holistic approach also the Theory of General Living Systems (Miller 1978) took part. Miller delimits his theory to deal with concrete, open, homeostasis aiming complex systems, composed by 19 critical subsystems. Miller himself notes (1978, p 42): "My analyses of living systems uses concepts of thermodynamics, information theory, cybernetics, and systems engineering, as well as the classical concepts appropriate to each level. The purpose is to produce a description of living structure and process in terms of input and output, flows through systems, steady state, and feedback, which will clarify and unify the facts of life".

With the aid of system theories and cybernetics the systemic-holistic approach was structured to facilitate understanding IT security problems as how to construct robust and survivable structures. Now, this was not the way most IT security people viewed their task: I spent time researching how and why people saw the world they did as compared to mine – and what the results were of the different world views. At the time (Yngström 1996) I outlined and discussed some areas as an illustration to why it was/is problematic to understand security in relation to IT:

- A language problem – English is the language used in most scientific communications, whereas many other languages understand 'security' much wider.
- Is cryptography the same as security? Cryptographic functionalities are based on secrecy but used in quite different ways.
- Whose point of view is security for? Most often the view is to protect assets of the firm and not of the individual.
- How is the environment considered? The environment if often implicit – to the developers. It is not necessary the same as understood by the users.
- Information or data security? The two concepts are often used interchangeably giving an unsolid ground for decisions.

- CIA as the main definition/description. As technology and use of IT extends, definitions are not good enough; even these three include contradictions.
- Problems of specifying IT security criteria. We live with that all the time, and I still favour Abrams' (1994) comments that there is not one good model to cover all aspects, despite CC.
- Measurements of security. Today security metrics seem to be a large field for research.

Presented issues contain gleanings from often discussed matters. Certainly they could have been headlined or related differently - this is the whole point with an SHA approach. Many perceive the issues as a mesh of opinions or ideas built on specific knowledge, and somehow – which is not obvious - connected to each other. This is where a generalised concept of a system may be used as a basic model for understanding and structuring matters; expressed by the following steps:

1. Understanding and conceptualisations,
2. Demarcations: delimit the system of study from its environment including defining the relevant environment,
3. Definitions: specify inflows, throughflows and outflows, and
4. Measurements of control: structure controls to deal with relevant varieties.

Following this, the problematic issues mainly dealt with:

1. Understanding and conceptualisations: Language and Cryptology,
2. Demarcations: Whose point of view to take, and Taking account of the environment,
3. Definitions: Information or data, IT security criteria, and Confidentiality, integrity, and availability, and
4. Measurements of control: Measurements of security.

However, few of the issues are unequivocal and someone else might want to classify them as:

1. Understanding and conceptualisations: Confidentiality, integrity, and availability, Whose point of view to take, and Taking account of the environment,
2. Demarcations: Measurements of security, and Information or data,
3. Definitions: Language, and
4. Measurements of control: IT security criteria.

This illustrates exactly why the issues are problematic: they cannot with any kind of certainty be allocated into one model easily understood and agreed upon even amongst involved professionals. Still, the generalised concept of a system can be used differently - to form a base for a *subjective* appreciation of the area which also is objectively communicative to others.

4.1 The Systemic-Holistic Approach spelled out

General Systems Theory had its origin in observations of similar phenomena 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. While perceiving /a part of/ reality, humans are able to reflect on their findings - and in doing so, they will test and change their concepts in order to fit them better to the perceived reality. In this actual process of testing and changing, there is a multi-creating relationship between the perceived reality and the intellectual concepts which in fact constitutes a learning process.

In efforts to control, humans may choose to assume that the reality *is* a system rather than could be looked upon *as* a system through the learning process. The control method used in the first case Checkland labels engineering or hard systems thinking, the second one systemic or soft systems thinking. The main underlined differences between the methods are, that in hard systems thinking perceived realities are treated as existing systems (the ontological entity) and their problems solved by systematic methods, while in soft systems thinking perceived realities are treated as problems (the epistemological entity) and solved by systemic methods. Through soft systems thinking, humans can learn how the concept of a system *reflects* the real world, and may represent one - and possibly changing - understanding of the world. Checkland does not refrain from hard systems thinking and engineering, rather he underlines that soft systems 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 images of the systems and the systems image" [Checkland 1988, p. 40]. By Laufer [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, i.e. cybernetics.

Laufer offers one more explanation of importance to the 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 with two distinct states. Either 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. Or - and 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 authorise, 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 Bertalanffy and General Systems Theory, thus gives grounds for studying the concept of 'system' as an epistemology for viewing and understanding perceived realities. The actual choice of when to change over to hard systems thinking *becomes subjective, but is done consciously,* and becomes a part of the conceptual model and the pedagogics.

General Living Systems Theory forms the third building block to the concept of systems, since it deals with systems that really exist - the ontological 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 supranation; 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 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 interleaved 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 ... neurons run in the same simple way the whole time. You can’t “think” your neurons 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”.

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 when to change from an epistemological to an ontological 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 conceptualisations 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 different contexts. This may also be a suitable mode governing the design, operation, management, and evaluation of secure IT structures.

The conceptual model, called the Systemic-Holistic Model, is very simple; it consists of a three dimensional framework and a Systemic Module as shown in Figures 1.

The framework describes the areas of interest while the Systemic Module acts as an epistemological device for “facts” in the framework. The framework is organised into three dimensions: Content/subject areas, Levels of abstraction, and Context orientation. The Systemic Module presents foundations of General Systems Theory and Cybernetics, Soft System Methodology and General Living Systems Theory. 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.

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 referred to as Beer's three levels of analysis, and the analysis is eventually also applicable recursively in the dimensions separately.

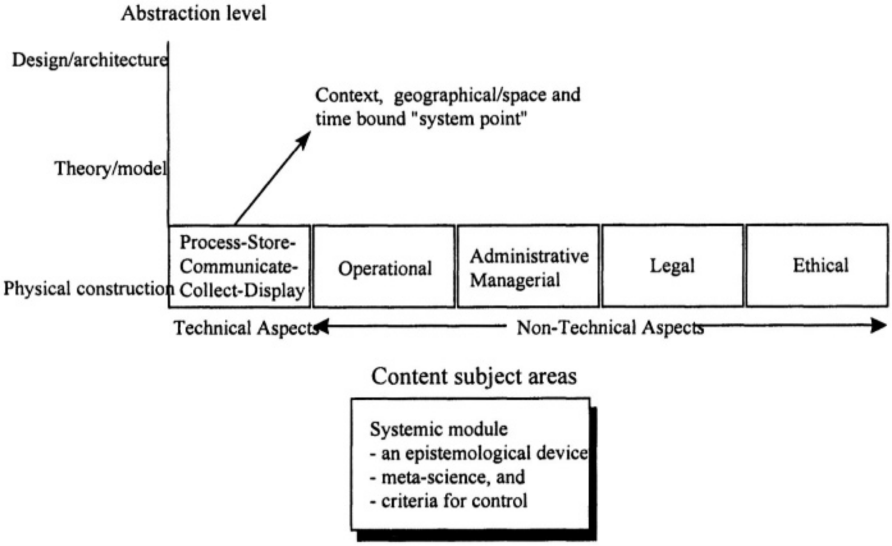

Figure 1. Details of the framework and the methodology for Security Informatics - the Systemic-Holistic Model

4.2 Some critique of the SHA for researching IT security

The most fundamental critique lays with the subjectivity; when a physical person has to decide to change from epistemology to ontology, from systemic/problematic to systematic/hard science. But this, to my understanding, is connected with what efforts we want to make: if we can deal only with one side of the problem, we can use scientific methods proved for these problems, if we want to deal with realities including systems, applications, people, etc in various roles we need a bridging science, such as the SHA approach. Other authors, for instance Fillery-James (1999) Siponen (2003) and Truex et al (1999) have presented similar approaches. The

(2003) and Truex et al (1999) have presented similar approaches. The approach as such may very well be further developed, there are indications that a totally new scientific base, which can bridge the areas of both hard- och soft sciences based on second order cybernetics is under way (Kjellman 2003,2001).The particular approach is called the Subject-oriented Approach to Knowledge, SOA, and has many resemblances with the SHA.

5. REFERENCES

(Abrams, 1994): Abrams, Marshall D., Symbiosis Among IT Security Standatds, policies, and Criteria, in Seizer, R., Yngström, L., Kaspersen, H. and Fisher-Hubner, S. (eds) Security and Control of Information Technology in Society, IFIP Transactions A-34, North-Holland, 1994, pp.145-159

(Armstron&Yngström 2001) Armstrong, H., Yngström, L.,(eds) Linking government, industry and academia to raise information security awareness, education and training in an age of cybercrime, Proceedings of IFIP TC11/WG11.8 Second World Conference on Information Security Education, 12-14 July, 2001, Perth, Australi, Edith Cowan University and IFIP 2001, ISBN 0-7298-0498-4

(Beer 1964) Beer, S., Cybernetics and Management, John Wiley & Sons, 1964.

(Beer 1968) Beer, Stafford, Cybernetics and Management, Science Edition, John Wiley, New York, 1968.

(Beer 1979) Beer, S., The heart of the enterprise, John Wiley & Sons, 1979.

(Checkland 1988) Checkland, P.B., Images of Systems and the Systems Image, Presidential address to ISGSR, June 1987, Journal of Applied Systems Analysis, Vol 15, 1988, pp. 37-42.

(Fillery-James 1999) Armstrong H., (Fillery-James H.L.) A Soft Approach to Management of information Security, PhD thesis, School of Public Health, Curtin university of Technology, Australia, 1999

(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.

(Irvine&Armstrong 2003) Irvine, C.,Armstrong, H., (eds) Security Education and Critical Infrastructure, Proceedings of IFIP TC11/WG11.8 Third Annual World Conference on Information Security Education (WISE3), June 26-28, 2003, Monterey, California, USA, Kluwer Academic Publishers, 2003

(Kjellman 2001) Kjellman A., Sociocybernetics – the path to a science of becoming, presented at the 3rd Int. Conf. On Sociocybernetics in Leon, Mexico, June 2001

(Kjellman 2003) Kjellman, A., Constructive Systems Science – the only remaining alternative?, PhD thesis, Department of Computer and Systems Sciences, Stockholm University, 2003, DSV report serie 03.014

(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, pp. 29-42.

(Laufer 1990) Laufer, Romain, The Question of the Legimitacy 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, pp. 31-61.

(Miller 1978) Miller, James G., Living Systems, McGrawHill, 1978.

(Siponen 2002) Siponen, M., Designing Secure Information Systems and Software. Critical evaluation of the existing approaches and a new paradigm, PhD Theisi, Faculty of Science, University of Oulu, Finland, ISBN 951-42-6789-3

(Truex et.al.1999) Truex, D, Baskerville, R., Travis, J., Amethodical Systems Development: The Deferred Meaning of Systems Development Methods, pre-copy to be printed in Accounting, Management and Information Technologies, 1999.

(von Bertalanffy 1956) von Bertalanffy, L., Main Currents in Modern Thoughts, in Yearbook of the Society for General Systems Research, Vol 1, 1956.

(von Bertalanffy 1968) von Bertalanffy, L., General Systems Theory, Braziller, 1968.

(Wiener 1948) Wiener, N., Cybernetics or Control and Communication in the Animal and Machine, John Wiley & Sons, 1948.

(Yngström 1996) Yngström, L., A Systemic Holistic Approach to Academic programmes in IT Security, PhD thesis, Department of Computer and Systems Sciences, Stockholm University, DSV report serie 96-021,1996 (CC).

(Yngström 1999) Yngström, L.Preface in Yngström, L., Fischer-Hubner, S., (eds) WISE1 Proceedings of IFIP TC11 WG11.8 First World Conference on Information Security Education, 17-19 June 1999, Kista, Sweden. DSV and IFIP ISBN 91-7153-910-7, pp. v-vii

(Yngström&Fischer-Hubner 1999) Yngström, L., Fischer-Hubner, S., (eds) WISE1 Proceedings of IFIP TC11 WG11.8 First World Conference on Information Security Education, 17-19 June 1999, Kista, Sweden. DSV and IFIP ISBN 91-7153-910-7