NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(HFM-259)TP/948

www.sto.nato.int

STO TECHNICAL REPORT **TR-HFM-259**

Human Systems Integration Approach to Cyber Security

(Démarche d'intégration humain-systèmes appliquée à la cybersécurité)

Final Report of Research Task Group HFM-259.

June 2020

Distribution and Availability on Back Cover

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(HFM-259)TP/948

www.sto.nato.int

STO TECHNICAL REPORT **TR-HFM-259**

Human Systems Integration Approach to Cyber Security

(Démarche d'intégration humain-systèmes appliquée à la cybersécurité)

Final Report of Research Task Group HFM-259.

The NATO Science and Technology Organization

Science & Technology (S&T) in the NATO context is defined as the selective and rigorous generation and application of state-of-the-art, validated knowledge for defence and security purposes. S&T activities embrace scientific research, technology development, transition, application and field-testing, experimentation and a range of related scientific activities that include systems engineering, operational research and analysis, synthesis, integration and validation of knowledge derived through the scientific method.

In NATO, S&T is addressed using different business models, namely a collaborative business model where NATO provides a forum where NATO Nations and partner Nations elect to use their national resources to define, conduct and promote cooperative research and information exchange, and secondly an in-house delivery business model where S&T activities are conducted in a NATO dedicated executive body, having its own personnel, capabilities and infrastructure.

The mission of the NATO Science & Technology Organization (STO) is to help position the Nations' and NATO's S&T investments as a strategic enabler of the knowledge and technology advantage for the defence and security posture of NATO Nations and partner Nations, by conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance, of the NATO Nations and the partner Nations, in support of NATO's objectives, and contributing to NATO's ability to enable and influence security and defence related capability development and threat mitigation in NATO Nations and partner Nations, in accordance with NATO policies.

The total spectrum of this collaborative effort is addressed by six Technical Panels who manage a wide range of scientific research activities, a Group specialising in modelling and simulation, plus a Committee dedicated to supporting the information management needs of the organization.

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS System Analysis and Studies Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These Panels and Group are the power-house of the collaborative model and are made up of national representatives as well as recognised world-class scientists, engineers and information specialists. In addition to providing critical technical oversight, they also provide a communication link to military users and other NATO bodies.

The scientific and technological work is carried out by Technical Teams, created under one or more of these eight bodies, for specific research activities which have a defined duration. These research activities can take a variety of forms, including Task Groups, Workshops, Symposia, Specialists' Meetings, Lecture Series and Technical Courses.

The content of this publication has been reproduced directly from material supplied by STO or the authors.

Published June 2020

Copyright © STO/NATO 2020
All Rights Reserved

ISBN 978-92-837-2272-4

Single copies of this publication or of a part of it may be made for individual use only by those organisations or individuals in NATO Nations defined by the limitation notice printed on the front cover. The approval of the STO Information Management Systems Branch is required for more than one copy to be made or an extract included in another publication. Requests to do so should be sent to the address on the back cover.

Table of Contents

List of Figures

List of Tables

HFM-259 Membership List

CO-CHAIRS

Professor Yantsislav YANAKIEV
Bulgarian Defence Institute,
Bulgaria
Email y.yanakiev@di.mod.bg

Dr. Antoon Johannes VAN VLIET
TNO Unit Defence Safety & Security
the NETHERLANDS
Email: tony.vanvliet@tno.nl

MEMBERS

Dr. Oleksandr BUROV
Institute of Information Technologies
and Learning Tools
UKRAINE
Email: a_burov@yahoo.com

Dr. Natalia DERBENTSEVA
DRDC – Toronto Research Centre
CANADA
Email: natalia.derbentseva@drdc-rddc.gc.ca

Dr. David GREATHEAD
DSTL
UNITED KINGDOM
Email: dgreathead@dstl.gov.uk

Dr. Julie MARBLE
Johns Hopkins University Applied Physics Lab
(JHUAPL)
UNITED STATES
Email: julie.marble@jhuapl.edu

Dr. Peter SVENMARCK
Swedish Defence Research Agency FOI
SWEDEN
Email: peter.svenmarck@foi.se

Ms. Susan TRAEBER-BURDIN
Fraunhofer Institute for Communication,
GERMANY
Email: susan.traeber-burdin@fkie.fraunhofer.de

Dr. Carsten WINKELHOLZ
Fraunhofer Institute for Communication
GERMANY
Email: carsten.winkelholz@fkie.fraunhofer.de

Human Systems Integration Approach to Cyber Security

(STO-TR-HFM-259)

Executive Summary

PURPOSE

The NATO Science and Technology Organization (STO) Human Factors and Medicine (HFM) Panel 259 Research Task Group (RTG), titled Human Systems Integration Approach to Cyber Security, was established to promote cooperative human-centred research activities in a NATO framework on the complex phenomenon of cyber security as a socio-technical system. The idea was to implement a common research perspective to study cyber security that focuses on the interrelatedness between technology and software developments, concepts, strategies and doctrines, organizational processes improvement and human performance.

More precisely, the goals of the HFM-259 RTG were:

- Identification and mitigation of potential cyber security vulnerabilities due to the role of people in the system;
- To study specific issues related to selection, education, training and retention of cyber force, and to identify the spectrum of Knowledge, Skills, and Abilities that IT experts need for efficient performance;
- To suggest possible approaches to improve resilience to cyber attacks at individual, team and organization level;
- To develop human factors support tools for enhancing individual and group cyber security sensitivity; and
- Improving human-machine interfaces in cyber security.

RESULTS, SIGNIFICANCE TO NATO AND PRACTICAL IMPLICATIONS

The foundation for the application of the Human Systems Integration (HSI) approach to cyber security is laid out in Chapter 2. The chapter defines the general human system integration approach and its domains and discusses how these domains apply to cyber security.

The central point in the NATO STO HFM-259 Program of Work was the development of the Human Systems Integration Framework for Cyber Security. This framework was a necessary step to gather and collate available information (reports, papers, concepts, doctrines, strategies, etc.) with respect to human factors involved in cyber security. The underlying assumption was that humans are significant nodes in cyber system, and therefore their behaviour influences the (in)security of this system. As a next step we tested the developed framework via subject-matter-expert interviews in each participating nation and implemented the ontology into software system (database and tool), which included populating with collected sources. The primary step in the development of the HSI framework to study cyber security was the actual coding process.

The team coded 230 information sources.

At the final stage we used the developed knowledge base and analytical tool to study interrelationships among different concepts, factors, actors, etc. and to write this Technical Report.

Chapter 3 describes the development of the HSI Framework for Cyber Security, its structure, validation, and population with information sources. Chapter 3 also discusses the types of analyses that could be conducted using the framework. The analyses provide useful insights into how different aspects of user behaviour and cognition increase or decrease cyber security.

The following four chapters, i.e., Chapters 4 – 7, discuss some of these theoretical and practical insights in more detail. Chapter 4 focuses on the individual perspective and examines how understanding of various aspects of human cognition, decision making and resulting behaviour can inform our understanding of cyber security. Chapter 5 takes on an organizational focus and examines factors associated with security policy management and its effectiveness, i.e., Information Systems Security Policy compliance. Chapter 6 presents some initial recommendations for how to recruit, select, train, and retain cyber security personnel. Chapter 7 discusses the general overarching cyber security considerations for learning and education.

The last three chapters discuss the efforts to disseminate the work (Chapter 8), offer a general discussion of the findings (Chapter 9) and provide a list of the sources used to inform this work (Chapter 10).

In brief, the NATO STO HFM-259 team developed and tested an HSI framework to study cyber security, knowledge base and used sophisticated software tooling to analyse the role of human factors in cyber security. The products of our work (database and tool) are available to be used by NATO STO and interested national institutions of the contributing nations: Bulgaria, Canada, Germany, the Netherlands, Sweden, Ukraine and the USA.

We believe that our report will be useful for both cyber security experts and military commanders for better understanding of individual and organizational factors influencing cyber security, raising cyber security awareness and building cyber security culture, mitigating insider threats, as well as improving selection, education, training and retention of cyber force.

Démarche d'intégration humain-systèmes appliquée à la cybersécurité

(STO-TR-HFM-259)

Synthèse

OBJET

Commission sur les facteurs humains et la médecine (HFM) de l'Organisation pour la recherche et la technologie (RTO) de l'OTAN.

Le groupe de travail (RTG) 259, intitulé « Démarche d'intégration humain-systèmes appliquée à la cybersécurité », a été créé pour favoriser les activités coopératives de recherche axée sur l'humain dans le cadre OTAN, à propos du phénomène complexe qu'est la cybersécurité en tant que système sociotechnique. L'idée était d'appliquer une perspective de recherche commune à la cybersécurité, qui se concentre sur l'interdépendance entre les progrès de la technologie et des logiciels, les concepts, stratégies et doctrines, l'amélioration des processus organisationnels et les performances humaines.

Plus précisément, les objectifs du RTG HFM-259 étaient les suivants :

- Identification et atténuation des vulnérabilités potentielles de cybersécurité, dues au rôle des personnes dans le système ;
- Étude de questions particulières liées à la sélection, l'éducation, la formation et la conservation de la cyberforce et identification du spectre des connaissances, compétences et aptitudes dont les spécialistes des technologies de l'information ont besoin pour être performants ;
- Suggestion de démarches possibles pour améliorer la résilience face aux cyberattaques au niveau individuel, de l'équipe et de l'organisation ;
- Mise au point d'outils de soutien des facteurs humains, améliorant la sensibilité des individus et des groupes à la cybersécurité ;
- Amélioration des interfaces humain-machine dans le domaine de la cybersécurité.

RÉSULTATS, IMPORTANCE POUR L'OTAN ET IMPLICATIONS PRATIQUES

Le fondement de l'application de la démarche d'intégration humain-systèmes (HSI) à la cybersécurité est exposé au chapitre 2. Ce chapitre définit la démarche générale d'intégration humain-systèmes et ses domaines et discute de l'application de ces domaines à la cybersécurité.

L'élaboration d'un cadre d'intégration humain-systèmes pour la cybersécurité était au cœur du programme des travaux du HFM-259 de la STO de l'OTAN. Ce cadre constituait une étape nécessaire pour réunir et collationner les informations disponibles (rapports, articles, concepts, doctrines, stratégies, etc.) au sujet des facteurs humains impliqués dans la cybersécurité. Selon l'hypothèse sous-jacente, les humains représentaient des nœuds importants du cybersystème et leur comportement influençait la sécurité ou l'insécurité de ce système. Nous avons ensuite testé le cadre élaboré en interrogeant des spécialistes de chaque pays participant et avons mis en œuvre l'ontologie dans le système logiciel (base de données

et outil), ce qui incluait de l'alimenter avec les sources collectées. L'étape principale d'élaboration du cadre HSI visant à étudier la cybersécurité était le processus de codage réel. L'équipe a codé 230 sources d'information.

À l'étape finale, nous avons utilisé la base de connaissances et l'outil d'analyse mis au point pour étudier les interrelations entre les différents concepts, facteurs, acteurs, etc., et pour rédiger le présent rapport technique.

Le chapitre 3 décrit l'élaboration du cadre HSI destiné à la cybersécurité, sa structure, sa validation et son remplissage à l'aide des sources d'information. Le chapitre 3 traite également des types d'analyses qui ont pu être menées à l'aide du cadre. Les analyses en question fournissent de précieuses connaissances sur la manière dont les différents aspects du comportement et de la cognition de l'utilisateur augmentent ou diminuent la cybersécurité.

Les quatre chapitres suivants, autrement dit, les chapitres 4 à 7, détaillent quelques-unes de ces connaissances théoriques et pratiques. Le chapitre 4 se focalise sur l'individu et examine en quoi la compréhension des divers aspects de la cognition humaine, de la prise de décision et du comportement qui en résulte peut éclairer notre compréhension de la cybersécurité. Le chapitre 5 adopte un point de vue organisationnel et étudie les facteurs associés à la gestion de la politique de sécurité et à son efficacité, autrement dit, le respect de la politique de sécurité des systèmes d'information. Le chapitre 6 présente quelques recommandations initiales en matière de recrutement, sélection, formation et conservation du personnel de cybersécurité. Le chapitre 7 discute des considérations générales de cybersécurité relatives à l'apprentissage et à l'éducation.

Les trois derniers chapitres traitent des actions de diffusion des travaux (chapitre 8), présentent les conclusions de manière générale (chapitre 9) et fournissent une liste des sources utilisées pour les présents travaux (chapitre 10).

En bref, l'équipe du HFM-259 de la STO de l'OTAN a mis au point et testé une base de connaissances et un cadre de HSI pour étudier la cybersécurité et s'est servi d'outils logiciels sophistiqués pour analyser le rôle des facteurs humains dans la cybersécurité. Les produits de nos travaux (base de données et outil) sont à la disposition de la STO de l'OTAN et des institutions nationales intéressées au sein des pays contributeurs (Bulgarie, Canada, Allemagne, Pays-Bas, Suède, Ukraine et États-Unis).

Nous estimons que notre rapport sera utile à la fois aux spécialistes en cybersécurité et aux commandants militaires et leur permettra (i) de mieux comprendre les facteurs individuels et organisationnels qui influencent la cybersécurité ; (ii) d'améliorer la sensibilisation à la cybersécurité ; (iii) d'établir une culture de la cybersécurité, en atténuant la menace interne ; et (iv) d'améliorer la sélection, l'éducation, la formation et la conservation de la cyberforce.

Chapter 1 – INTRODUCTION TO NATO STO TASK GROUP HFM-259: HUMAN SYSTEMS INTEGRATION APPROACH TO CYBER SECURITY

Yantsislav Yanakiev
Bulgarian Defence Institute "Prof. Tsvetan Lazarov"
BULGARIA

1.1 BACKGROUND

Cyber domain is, and will continue to be a very important element of the battlefield. It can be argued that the greater part of the military operations in the future will, at least, start in cyberspace and operations will most probably be conducted therein during the period of the conflict, hence the growing importance of its control [1].

While technological solutions are being developed to enhance cyber security, there is growing awareness that besides a technical approach, the role of human performance, decision making, and organizational culture are critical to foster the effectiveness of responses to developing cyber threats [2], [3], [4], [5].

Current studies show that human factor may be a system's 'weakest link' [6], but may also be a powerful resource to detect and mitigate cyber threats [7], [8]. In the same time, the variety of human factors involved in cyberspace and the absence of a consistent theory seem to hinder the focused development of integrated approaches to cyber security. Moreover, there is a lack of research attention devoted to the role of organizational culture and processes to increase cyber security capacity. Finally, further research is needed to improve the state of cyber security Education, Training, Exercises, and Evaluation (ETEE), plus identifying specific lessons that we are learning in both training and operations.

To summarize, the challenge for both collective and national security is to minimize the risks of cyber as a threat.

The NATO Policy on Cyber Defence [1] establishes that cyber defence is part of the Alliance's core task of collective defence, confirms that international law applies in cyberspace and intensifies NATO's cooperation with industry. The top priority is the protection of the communications systems owned and operated by the Alliance.

In addition, the European Union Cybersecurity Strategy: An Open, Safe and Secure Cyberspace (European Commission 2013) also defines the cyber threat among the most important for the Union and the Member States (MS) [9].

In order to respond to the challenges of human factors in cyber security, the HFM Exploratory Team 129 (HFM-ET-129) Human Factors in Cyber Security was established to map out diverse dimensions of how human factors can improve cyber security.

The HFM-ET-129 identified several areas of most critical and urgent needs and the knowledge gaps to address in cyber research agendas of NATO and the nations that can be defined as Psychosocial, Cultural, Conceptual

and Organizational dimensions of cyber security. The common perspective for these research needs is that the interaction between users, cyber security specialists, interconnected organizations, and technologies form a socio-technical system that balance security needs with operational needs.

The HFM-ET-129 identified as the most urgent human factors needs that require further collaborative research in the framework of NATO Science and Technology Organization the following:

- Approaches to improve selection, education, training and retention of a cyber force (IT experts);
- Approaches to improve cyber awareness of all defence personnel;
- Methods, techniques and tools to bridge the gap between the cyber force and the operational community in terms of perceptions of cyber threat, procedures and practices for prevention;
- Techniques to enhance organizational resilience to cyber attacks;
- Methods to improve control behaviour via cyber security policies and targeted Education and Training (E&T);
- Identification of the specific characteristics of a malicious insider's behaviour and methods or tools to identify this potential threat; and
- Definition of the role of the military commanders to mitigate cyber threat.

The conclusion of HFM-ET-129 was that we need a common research perspective to study cyber security that focuses on the interrelatedness between technology and software developments, concepts, strategies and doctrines, organizational processes improvement and human performance.

Taking into account the recognized gaps in the study of cyber security, in 2015 NATO Science and Technology Board (STB) set up a new Research Task Group (RTG) Human Systems Integration Approach to Cyber Security (NATO STO HFM-259), sponsored by the Human Factors and Medicine (HFM) Panel.

Five NATO member countries were represented in the group: Bulgaria, Canada, Germany, the Netherlands, the UK (2015 – 2016) and the USA. In addition, two nations, Sweden and Ukraine, – members of the Partnership for Peace (PfP) Initiative – also contributed to the research activities.

1.2 OBJECTIVES AND MAIN TOPICS OF RESEARCH

The goals of the Research Task Group HFM-259 can be summarized as follows:

- Identification and mitigation of potential cyber security vulnerabilities due to the role of people in the system;
- To study specific issues related to selection, education, training and retention of cyber force, and to identify the spectrum of Knowledge, Skills, and Abilities that IT experts need for efficient performance;
- To suggest possible approaches to improve resilience to cyber attacks at individual, team and organization level;
- To develop human factors support tools for enhancing individual and group cyber security sensitivity; and
- Improving human-machine interfaces in cyber security.

The main topics in the focus of the research are:

- Recruitment, selection, training and maintenance of the cyber force;
- Identification and mitigation of potential cyber security vulnerabilities due to the role of people in the system;
- Improving human-machine interfaces; and
- Securing against the insider threat.

1.3 SCOPING THE PROBLEM

The implementation of the Program of Work (PoW) of NATO STO Task Group HFM-259 went through several key activities.

The work started with a desktop research within each nation represented in the group to identify any existing tools for tracking human-focused cyber vulnerabilities (phishing, human errors that lead to vulnerabilities, etc.). The focus was on existing approaches to identify malicious and non-malicious insider threats; an overview of human reliability analysis basics and the Human Reliability Analysis Method (SPAR-H); and improving Human-Machine Interfaces (HMIs) and Knowledge, Skills, and Abilities (KSA) of Cyber Force personnel and IT personnel needed to effectively implement their tasks, cultural factors and cyber security, etc.

The focal point in the NATO STO HFM-259 PoW was the development of Human Systems Integration (HSI) Framework for Cyber Security. This framework was a necessary step to gather and collate available information (reports, papers, concepts, doctrines, strategies, etc.) with respect to human factors involved in cyber security. The underlying assumption was that humans are significant nodes in cyber system, and therefore their behaviour influences the (in)security of this system.

1.4 FRAMEWORK DEVELOPMENT

The development of the Framework went through several sequential steps. First, we started with identification of major relevant human and machine factors and actors that constitute the socio-technical system “cyber security”. Second, we continued with identifying the potential relationships between the actors and factors, developing a morphological field.

As a third step, we identified different types of Subject Matter Experts (SMEs) to interview in order to validate the initial HSI framework to study cyber security. Additionally, we developed an interview protocol and organized an SME study in each represented nation to validate the initial framework. The targeted experts included engineers, operator SMEs, Reliability SMEs, Systems Engineers and Design SMEs, as well as policy makers. After integrating SME feedback from each nation, the final framework structure was developed. The framework is discussed in more detail in Chapter 3.

Besides, we tried to identify a platform for framework implementation and we explored different options like MS Excel, MS Access, Image, and others, as potential platforms. Furthermore, we started collecting relevant information sources (reports, papers, strategies, doctrines, etc.) and stored them in the RTG HFM-259 repository on Science Connect website.

The fourth step was to implement the ontology into software system (database and tool), which included populating with collected sources and pilot of the coding to test and improve the organization/structure of the database and coding process. The primary step in the development of the HSI framework to study cyber security was the actual coding process. The team coded 230 information sources.

The development of the analytical tool was also an important step to finalize the implementation of the ontology into software system. There were predefined scripts for querying the knowledge base with different points of entry such as (educational and training, metrics, frameworks of human performance and error analysis, etc.). Finally, yet importantly, we used the developed knowledge base and analytical tool to study interrelationships among different concepts, factors, actors, etc., and to writing this Technical Report (TR).

The next chapters reflect a number of perspectives that the research team deemed relevant in order to achieve our ambition in coming to grips with the topics addressed. These are the contributions of the participating nations based on their field of expertise. All of these take a certain point of view and elaborate this point of view. What they have in common are the human factor in cyber security and the attempt to integrate all other factors in socio-technical system applying human systems integration paradigm. These perspectives are:

- Chapter 2 – Cyber security: The human systems integration perspective
  Yantsislav Yanakiev
- Chapter 3 – Human behaviour in Cyber Security: A knowledge base perspective
  Tony van Vliet
- Chapter 4 – Human behaviour, cognition and decision making: An individual perspective
  Julie Marble
- Chapter 5 – Cyber security: An organizational perspective
  Natalia Derbentseva and Susan Träber-Burdin
- Chapter 6 – Recruitment, selection and training of IT/Cyber personnel
  Peter Svenmark
- Chapter 7 – Cyber systems: A potential protective and organizational means perspective
  Oleksandr Burov
- Chapter 8 – Dissemination and interaction
  Yantsislav Yanakiev
- Chapter 9 – Discussion and Conclusion
  Tony van Vliet

1.5 RESEARCH TEAM AND AUTHORSHIP

Name	Organization	Chapter(s) Author(s)
Professor Y. Yanakiev, Dr. Sc., Co-chair	Bulgarian Defence Institute “Prof. Tsvetan Lazarov”, Bulgaria	1, 2, 8
Dr. A.J. van Vliet, Co-chair	TNO Unit Defence Safety and Security, The Netherlands	3, 9
Dr. N. Derbentseva	DRDC, Canada	5

Name	Organization	Chapter(s) Author(s)
Dr. J. Marble	JHUAPL, USA	4
S. Traeber-Burdin	Fraunhofer, Germany	5
P. Svenmarck	FOI, Sweden	6
O. Burov	Institute of Information Technologies and Learning Tools, Ukraine	7

1.6 REFERENCES

[1] NATO. (2011). Defending the Networks: The NATO Policy on Cyber Defence. NATO Policy on Cyber Defence, endorsed by Allied Defence Ministers, June 2014. Brussels, Belgium: NATO.

[2] Karlsson, F., Astrom, J., Karlsson, M. (2015). Information security culture – State-of-the-art review between 2000 and 2013. Information and Computer Security 23(3):246-285. doi: 10.1108/ICS-05-2014-0033.

[3] Forsythe, C., Silva, A., Stevens-Adams, S.M., Bradshaw, J. (2012). Human Dimensions in Cyber Operations Research and Development Priorities. SANDIA Report (Vol. SAND 2012-9188). Albuquerque, NM: Sandia National Laboratories.

[4] Bowen, B.M., Devarajan, R., Stolfo, S. (2012). Measuring the human factor of cyber security. Homeland Security Affairs, Supplement 5, Article 2.

[5] Leggitt, J.S., Shechter, O.G., Lang, E.L. (2011). Cyberculture and Personnel Security: Report I – Orientation, Concerns, and Needs. Monterey, CA: Defense Personnel Security Research Center.

[6] Nohlberg, M. (2009). Why humans are the weakest link. In: M. Gupta and R. Sharman (Eds.), Social and Human Elements of Information Security. Hershey, PA: Information Science Reference / IGI Global.

[7] Winkelholz, C., Traber, S., Kruger, F., Gunther, H., Flemisch, F., Semling, C., Wlczek, N., Schaub, H. (2014). Human factors for cyber defence: Human systems integration for resilient, cooperatively automated cyber defence systems. Brussels, Belgium: European Defence Agency.

[8] Sasse, M.A., Brostoff, S., Weirich, D. (2001). Transforming the 'weakest link' – A human/computer interaction approach to usable and effective security. BT Technology Journal 19(3):10.

[9] European Commission. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. (2013). Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, p. 20. Brussels, Belgium: European Commission, High Representative of the European Union for Foreign Affairs and Security Policy.

Chapter 2 – CYBER SECURITY: THE HUMAN SYSTEMS INTEGRATION PERSPECTIVE

Yantsislav Yanakiev
Bulgarian Defence Institute "Prof. Tsvetan Lazarov"
BULGARIA

2.1 APPROACHES IN DEFINING HUMAN SYSTEMS INTEGRATION

The idea of Human Systems Integration (HSI) emerged in the mid-1980s as a modern concept of coordination and integration of multiple human-centric domains that impact systems design at each acquisition phase. It recognises the human as a critical component in any complex system [1].

This is an interdisciplinary approach aimed at facilitating optimization of overall system performance in both material and non-material solutions. HSI is deeply rooted in the military-industrial complex and it is related to the efforts to manage defence acquisition process more effectively. The concept of HSI was born and developed in the USA and Canada. The corresponding concept applied in the UK is Human Factors Integration (HFI) [2].

Several different approaches to defining the concept of HSI are presented and compared below.

The International Council on Systems Engineering (INCOSE) defines HSI as "the interdisciplinary technical and management processes for integrating human considerations within and across all system elements. It is an essential enabler to systems engineering" [3], p. 183.

The official U.S. Air Force definition of HSI reads that "HSI is the integrated and comprehensive analysis, design and assessment of requirements, concepts, and resources for system manpower, personnel, training, environment, safety, occupational health, habitability, survivability, and human factors engineering, with the aim to reduce total ownership cost while optimizing total mission performance" [4], p. 61.

The comparison of the components of the two definitions, presented in Table 2-1, shows that the INCOSE definition of HSI is reflected in the official U.S. Air Force definition.

Table 2-1: Components of the INCOSE and the U.S. Air Force Definitions of HIS.

INCOSE Definition Components	U.S. Air Force Definition Components
As a *technical strategy*, HSI helps to ensure that human performance issues are addressed early, effectively, and iteratively throughout the acquisition process.	'...*comprehensive* analysis, design, and assessment of requirements, concepts, and resources...'
As a *management strategy*, HSI helps to ensure that human-related concerns are properly considered in an acquisition program.	'...*integrated*..." [within and across multiple system elements]…, with the *aim to reduce total ownership cost*, while *optimizing total mission performance.*'

According to the U.S. Defence Acquisition Guidebook, Human Systems Integration is defined as "a robust process by which to design and develop systems that effectively and affordably integrate human capabilities and limitations. HSI should be included as an integral part of a total system approach to weapon systems development and acquisition….The total system includes not only the prime mission equipment, but also the people who operate, maintain, and support the system; the training and training devices; and the operational and support infrastructure" [5], p. 233.

Figure 2-1 represents the main elements of HSI as discussed in the U.S. Air Force Human Systems Integration Handbook [6], 9-10.

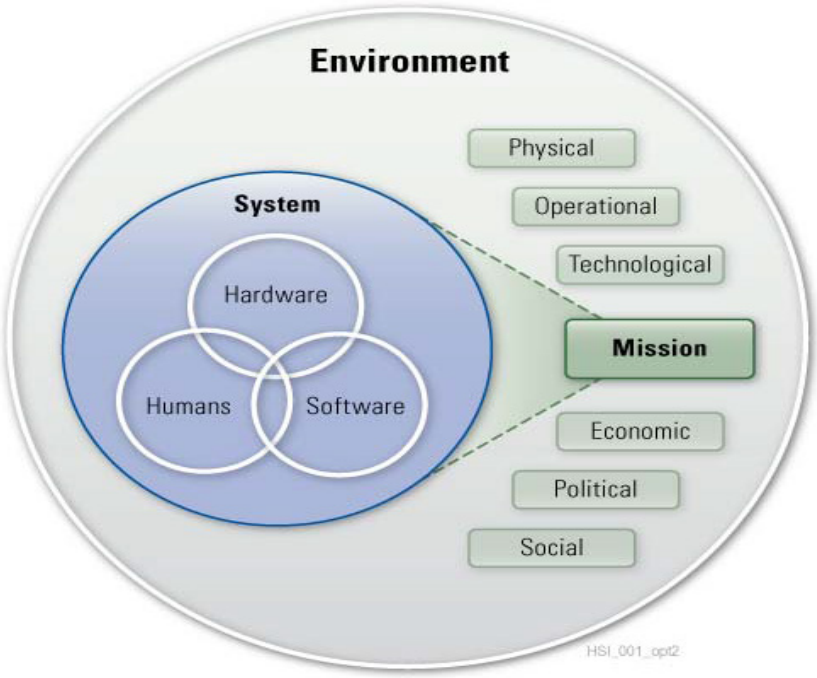

Figure 2-1: Elements of HIS.

This figure makes evident that systems comprise hardware, software, and people, all of which operate within a surrounding environment (physical, operational, technological, social, political, economic, etc.).

There are several conclusions that can be inferred from the above definitions and components of HSI. First of all, when designing a new system, it is essential to carry out a comprehensive study of the context in which this system is going to operate, to account for all possible elements of the surrounding environment. In addition, it is very important to consider human capacity or requirements as a central part of the system because this can help optimize task allocation between hardware, software, and the users. To promote ideal task allocation, it is critical that the human factor is considered early enough in the system design and development process. Finally, it is equally important to focus on the implementation of effective strategies for organizational processes improvement with the purpose of optimizing overall mission performance.

Briefly, the goals of HSI are to ensure that systems, equipment, and facilities:

1) Incorporate effective human-system interfaces;
2) Achieve the required levels of human performance;
3) Make economic demands upon personnel resources, skills, and training;
4) Minimise life-cycle costs, and
5) Manage the risk of loss or injury of personnel, equipment, or the environment [7].

Table 2-2 summarises the definitions of the main HSI domains.

Table 2-2: Human Systems Integration Domains [8], p. 9.

Human Systems Integration Domains	Definitions of the Domains
Manpower	Determination of the total number of personnel required to operate, maintain and sustain a system in order to achieve full operational capabilities.
Personnel	Determination of the combination of the whole spectrum of human characteristics and skill requirements for a system to support capabilities necessary to fully operate, maintain and support a system.
Training	Use of analyses, methods, and tools to ensure systems training requirements are fully addressed and documented by systems designers and developers. This is necessary to achieve the level of individual and team proficiency required to successfully accomplish tasks and missions.
Human Factors Engineering	Consideration and application of human capabilities and limitations throughout system definition, design and development to ensure effective human and machine integration for optimal total system performance.
Environment	Consideration of environmental factors, such as water, air and land and the interrelations between a system and these factors.
Safety	Consideration and application of system design characteristics that serve to minimise the potential for mishaps that could cause death or injury of operators and maintainers or threaten the system's survival and/or operation.
Occupational Health	The factors in system design features that minimise the risk of injury, acute or chronic illness, or disability and/or that reduce job performance of personnel who operate, maintain or support the system.
Habitability	Consideration of system-related working conditions and accommodations necessary to sustain the morale, safety, health and comfort of all personnel.
Survivability	Consideration and application of system design features that reduce the risk of fratricide (the death of one's own forces), the probability of detection, the risk of attack if detected and damage if attacked.

The definitions of the HSI domains, presented in Table 2-2, are focused on the implementation of a successful defence acquisition process. As it was mentioned before, the main goal of HSI is to optimize this process, i.e., to reduce the total ownership cost and to enhance overall mission performance.

How can we apply HSI approach to achieve our goals in the study of cyber security, and the role of the human in the system in particular?

The focus of our study is to explore the complex phenomenon of cyber security as a socio-technical system. This means applying the human-centred approach to analysing the interdependencies between technology and software developments, concepts, strategies and doctrines, organizational processes improvement and human performance. In this regard, the most important HSI domains of interest in our study are Manpower, Personnel, Training, Human Factors Engineering, Safety and Survivability. They should be integrated to perform effective HSI through trade-offs and collaboration. It is essential to avoid stovepipe approach or to take notice of either technological factors or human factors.

2.2 HUMAN SYSTEMS INTEGRATION DOMAINS FOR CYBER SECURITY

For the purposes of NATO STO HFM-259 Research Task Group, Human Systems Integration Approach to Cyber Security, we made an adaptation of the definitions of the main HSI domains. They are presented in Table 2-2. The revised definitions of the six domains that we consider adequate and applicable to study cyber security as a socio-technical system are presented in Table 2-3.

Table 2-3: Human Systems Integration Domains for Cyber Security.

Human Systems Integration Domains	Definitions of the Domains
Manpower	The determination of the total number of IT personnel, human factors experts, cyber security managers, scientists, educators and trainers, support staff, etc., required to operate, maintain and sustain cyber security as a socio-technical system in order to achieve full operational capabilities in both peacetime installations/structures and NATO operations. The goal is to bridge the gap between the cyber force, the operational community and other actors involved in terms of perceptions of cyber threat, procedures, and practices for prevention.
Personnel	The determination of the whole spectrum of individual characteristics and knowledge, skills and abilities of different actors (experts and users) required to fully operate, maintain and support cyber security as a socio-technical system. The focus is on the behavioural aspects of cyber security and the role of the social and personal competencies as strength to prevent cyber attacks.

Human Systems Integration Domains	Definitions of the Domains
Education and Training (E&T)	Identification of cyber security E&T requirements, planning and implementation of targeted E&T of IT personnel, cyber security managers, military leaders and users for raising cyber awareness and creating cyber security culture at individual, team and organization level in order to successfully accomplish tasks and missions; re-targeting the education from knowledge transfer to the development of mental models and mind-set change to account for the substantial role of human factors issues in cyber security.
Human Factors Engineering	Consideration and application of human capabilities and limitations throughout cyber security system definition, design and development to ensure effective human-machine interfaces; reduction of the complexity of security systems and workload, to improve attention, motivation, communication, and to build trust in security policies for optimal total system performance.
Safety	Consideration and application of a variety of methods and tools for identification of vulnerabilities due to the humans in cyber security as a socio-technical system; identification of the spectrum of knowledge, attitudes, and abilities to build safety culture and achieve mitigation of potential cyber threats in the defence organizations; securing against the insider threat; consideration of the operational side of cyber defence and possible consequences in NATO operations.
Survivability	Consideration and application of comprehensive policies, procedures and methods to reduce cyber security risks and to guarantee integrity, confidentiality and availability of information. These include building capabilities to monitor and respond to critical events, anticipate future threats, learn lessons from past experiences, enhanced decision making, increased situational awareness, etc. Furthermore, implementation of constant and effective strategies for organizational processes and procedures improvement is needed to boost cyber security organizational resilience. Finally, it is critical to integrate cyber defence in the military operational planning process.

2.3 CONCLUSION

The challenge for both collective and national security is to minimise the risks of cyber as a threat [9]; [10]. For that reason, we need a common research perspective to study cyber security that focuses on the interrelatedness of technology and software developments, concepts, strategies and doctrines, organizational processes improvement and human performance. A proper solution to respond to the complex phenomenon of cyber security is to implement HSI philosophy and methodology. This means to apply a human-centred approach, which provides comprehensive foundations to analyse cyber security as a socio-technical system covering diverse dimensions such as psychosocial, cultural, organizational processes, technological and software developments.

To achieve this goal, the HFM-259 RTG team developed and tested a framework, knowledge base and software tool that can be used to study the role of human factors in cyber defence processes. The framework includes the above-defined Human Systems Integration Domains, i.e., Manpower, Personnel, Training,

Human Factors Engineering, Safety and Survivability. The framework and the knowledge base are presented and discussed in Chapter 3. Furthermore, several chapters focus particularly on human behaviour and cyber security, organization factors and processes in cyber security, equipment, selection, retention and training of cyber warriors education and training for improved cyber security.

2.4 REFERENCES

[1] Booher, H.R. (Ed.). (2003). Handbook of Human Systems Integration. Hoboken, NJ: Wiley.

[2] Waterson, P., Kolose, S.L. (2010). Exploring the social and organisational aspects of human factors integration: A framework and case study. Safety Science. Amsterdam, Netherlands: Elsevier.

[3] INCOSE. INCOSE Systems Engineering Handbook. (2007). v. 3.1. Appendix C: Terms and Definitions. San Diego, CA: INCOSE.

[4] U.S. Air Force. U.S. Air Force Instruction 10-601, 12 July 2010, Air Force Materiel Command Supplement, 14 June 2011, Operations Operational Capability Requirements Development. Washington, DC: U.S. Air Force.

[5] Defense Acquisition Guidebook. (2005). Available at http://contractingacademy.gatech.edu/wp-content/uploads/2014/06/Defense-Acquisition-Guidebook-%E2%0%93-Feb.-26-2017.pdf. Accessed on 26 March 2020.

[6] U.S. Air Force. (2009). Air Force Human Systems Integration Handbook. Brooks City-Base, TX: Directorate of Human Performance Integration. Available at http://www.acqnotes.com/Attachments/Air%20Force%20Human%20System%20Integration%20Handbook.pdf. Accessed on 26 March 2020.

[7] Department of Defense. Standard Practice: Human Engineering Requirements for Military Systems, Equipment, and Facilities, Washington, DC, USA, 24 May 2011.

[8] Endsley, M.R. (2016). Building resilient systems via strong human systems integration. Defense AT&L, January – February 2016.

[9] NATO. (2011). Defending the Networks: The NATO Policy on Cyber Defence. NATO Policy on Cyber Defence, endorsed by Allied Defence Ministers, June 2014. Brussels, Belgium: NATO.

[10] European Commission. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. (2013). Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, p. 20. Brussels, Belgium: European Commission, High Representative of the European Union for Foreign Affairs and Security Policy.

Chapter 3 – HUMAN BEHAVIOUR IN CYBER SECURITY: A KNOWLEDGE BASE PERSPECTIVE

Dr. A. van Vliet
TNO Unit Defence Safety and Security
NETHERLANDS

During the last decades, a grand development and use of new communication and information technology has taken place. The ubiquitous availability of communication and information technology such as smartphones, tablets, PCs and other devices (Internet of Things), the worldwide adoption of social networking, and the fact that these interactions are stored allows for legal and illegal tracking and manipulation of individual and organizational behaviours. In our current world, people and organizations (in)voluntarily provide data that captures their behaviours, which offers diverse observations on both the physical world (e.g., location) and the online world (e.g., events) of people and organizations. This large amount of data provides insights that were not available on this scale and with this level of detail via traditional methods, and it is being used to influence people's behaviour, their devices' behaviour and their organizations' behaviour.

We expect that based on our initial problem analysis, armed forces (friend, foe or neutral) will target, design and execute more targeted and effective cyber interventions which impedes the cyber security of the intended target. To enable defence against such interventions, there is a growing need for methodologies and tools that enable sense making in this highly evolving field of digital (behavioural) influencing. In this chapter, we describe how these threats can be analysed, what can be done to impede these threats and what still needs to be done.

3.1 ONTOLOGY

Using social scientific insights (a human factors approach) and theory as a guideline, we provide a framework that can be used to analyse (the effectiveness of) these cyber influence processes. To this end, a structured registry of articles (peer-reviewed, journalistic, webpages, etc.) was developed and recorded in a knowledge base. This knowledge base enables analyses to be done on this body of articles in a systematic and replicable manner.

The first step was to develop an ontology to categorize the collected sources (articles, chapters, papers, etc.) so that appraisal, analysis and dissemination can be done in a systematic and replicable manner. And, for each data point the reference source is available for the user to deepen his knowledge. This ontology is used as framework for the knowledge base. We have loosely adopted Lasswell's model of communication as the basis for the ontology design, which he proposed in his 1948 article "The Structure and Function of Communication in Society". We extended this framework with specific attributes to enable a more sophisticated analysis. This extension of Lasswell's model came about by identifying concepts which needed a more detailed resolution.

Table 3-1 shows the first level of our ontology.

The ontology was further refined and extended[1], to be used one level deeper and to help formalize relationships between the different concepts within the ontology. Figure 3-1 represents this final version of the ontology.

[1] This was done in a series of interactive sessions with subject matter experts, based on their expertise with influence and interaction (NGOs, defence and social media experts).

Table 3-1: Top Level of Concepts Developed for the Ontology.

Concept	Definition Used
attacker.resource	The type of attacker
threat.source	Is the threat an insider or an outsider?
threat.motivation	What is the intent of the attacker?
threat.vectors	An attack vector is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element
influencing.techniques	Ways or methods to produce effects on the actions, behaviour, opinions of others
vector.complexity	The complexity of the threat vector (simple, complex)
red.behavior	Type of behaviour attackers show
affected.users	The type of user affected by the problem / the type of user targeted or affected by an attack
interaction.point	The device or system (including human) through which an attack is delivered/initialized or where it is targeted / the opponent's device or system (including the human) through which an offender tries to initiate its attack
information.assurance	NISTIR 7298 (US National Institute of Standards and Technology Internal Report)
impact.on.target	What the psychological impact is on the target of the attack in broad terms
mitigation.mechanism.supercategory	How threats are mitigated; highest level of (human factors) mitigation mechanisms
mitigation.mechanism	How threats are mitigated; detailed level of (human factors) mitigation mechanisms
mitigation.effectivness	Is the mitigation mentioned in the article presumed by the authors to be effective?
mitigation.target	The type of user who a mitigation is targeted at
performance.shaping.factors	A factor that influences human performance and human error probabilities (as used in Human Reliability Analysis)
situational.context	Aspects of the situation in which the target uses cyber means
organizational.factors	Aspects of the organization that can directly or indirectly impact cyber security

Concept	Definition Used
task.factors	Aspects of the task that can directly or indirectly impact cyber security
blue.behavior	Type of behaviour of target that is affected
attack.outcome.consequence	What was the ultimate consequence of the attack?
human.error.taxonomy	Based on the Reason categories
system.outcome	The (end) state of the system, either positively or negatively affected
source.methodology	The quality of the report (anecdotal, theoretical, empirical)
consequences.for.instruments.of.power	Based on comprehensive approach
sme.appreciation	Our SME appreciation of the report

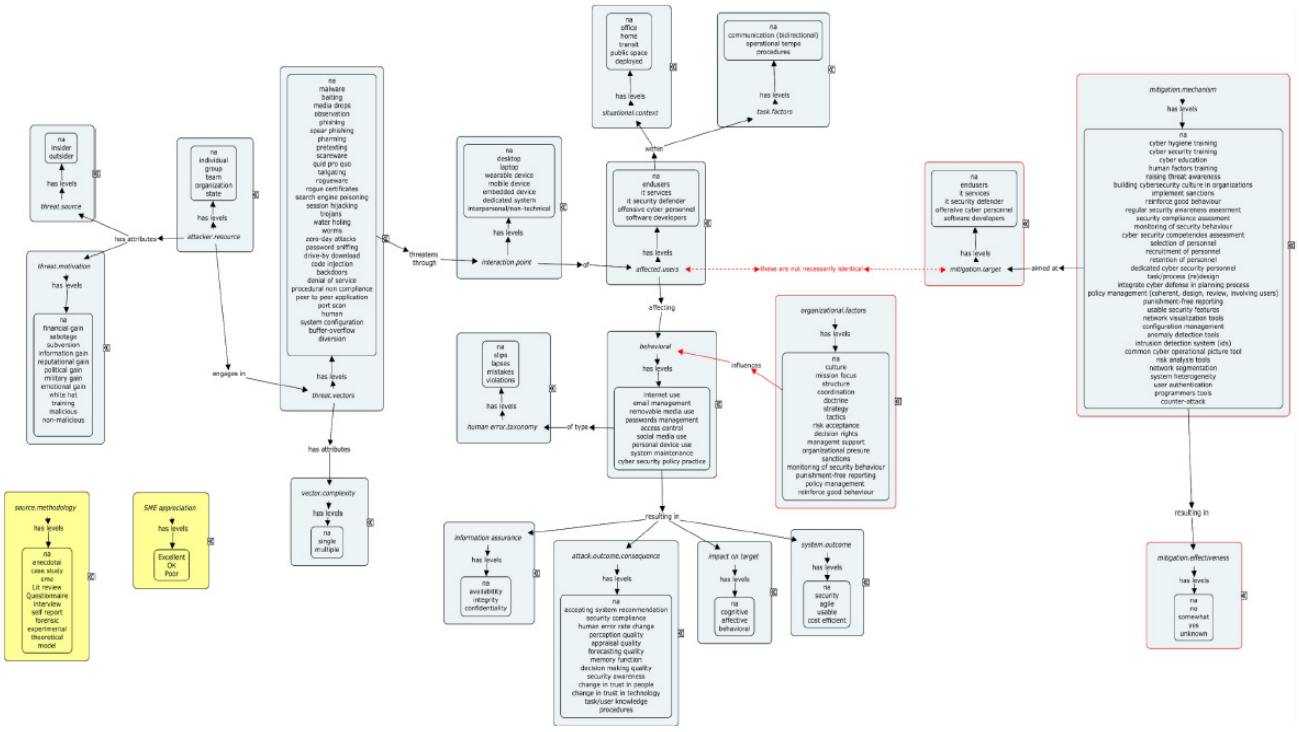

Figure 3-1: Thumbnail of Complete Ontology. See Annex A, Figure A-1 for full-size image.

3.2 POPULATING THE KNOWLEDGE BASE

Based on the ontology, the knowledge base was populated with the collected sources. At the time of writing, the database contains coded records based on 230 articles that have been selected over the course of three years by the members of the NATO HFM-259 group. The selection of articles was based on a set of selection criteria agreed beforehand. An important element of this selection process was the fact that the technology or influence process described in an article, could be 'operationally relevant for a military end user'. After the selection of articles, (see provided file: HFM 259 framework_Sources coded.xlsx) the team filled the knowledge base based on the ontology as described in Section 3.1. The basic procedure was to ascertain whether the paper (source document) has mentioned one or more of the concepts we defined in our ontology. This meant that for each paper multiple coding lines were possible due to the content of the paper. This practically means that for each paper more coding lines were possible. Coding of articles into database records was based on jointly agreed coding instructions.

3.3 ANALYSIS OPTIONS

The populated database allows for a multitude of analyses. The first being straightforward descriptive such as frequency tables of singular concepts. The second level of analyses are cross tabulations of two or more concepts. Finally, the most sophisticated analyses will be done based on a network approach. To that end the database was transformed in an edge list (see attached file) whereby for each edge (relationship between two connected concepts in a document) was connected to a set of qualifiers, such as the appreciation of the paper [sme.appreciation] or the methodology used in the paper [source.methodology].

3.4 DESCRIPTIVES

Let's start with the overall descriptives of the data points found in the database. For the generation of graphs, we used Gephi (a network representation tool, which can be downloaded here: https://gephi.org/).

In Figure 3-2 all the data points [elements] in the database are represented and with each label the number of occurrences is noted with - N, for example the element human and organizational factors - 2 occurs twice which belongs to the concept "mitigation mechanism super category". Furthermore, for the facilitation of a quick visual appreciation of the concepts the diameter of the element that has many occurrences is larger than the diameter of concepts occurring infrequent. Each element belongs to a concept [18 concepts in total], which is coloured according to the legend provided in the graph.

This is a straightforward descriptive representation of all the concepts in the database.

3.5 NETWORK

Now let us take this one step further and see how these elements [data points] and concepts [colour] are related within our database structure, which we have defined on the basis of our ontology represented in Figure 3-1.

In Figure 3-3 the whole network is represented. This is a directional network [implying causality which we defined in our ontology] and the representation form used is "forced Atlas". The connections between the elements are represented as arrows of which the thickness corresponds with the number of occurrences of this relationship in the database.

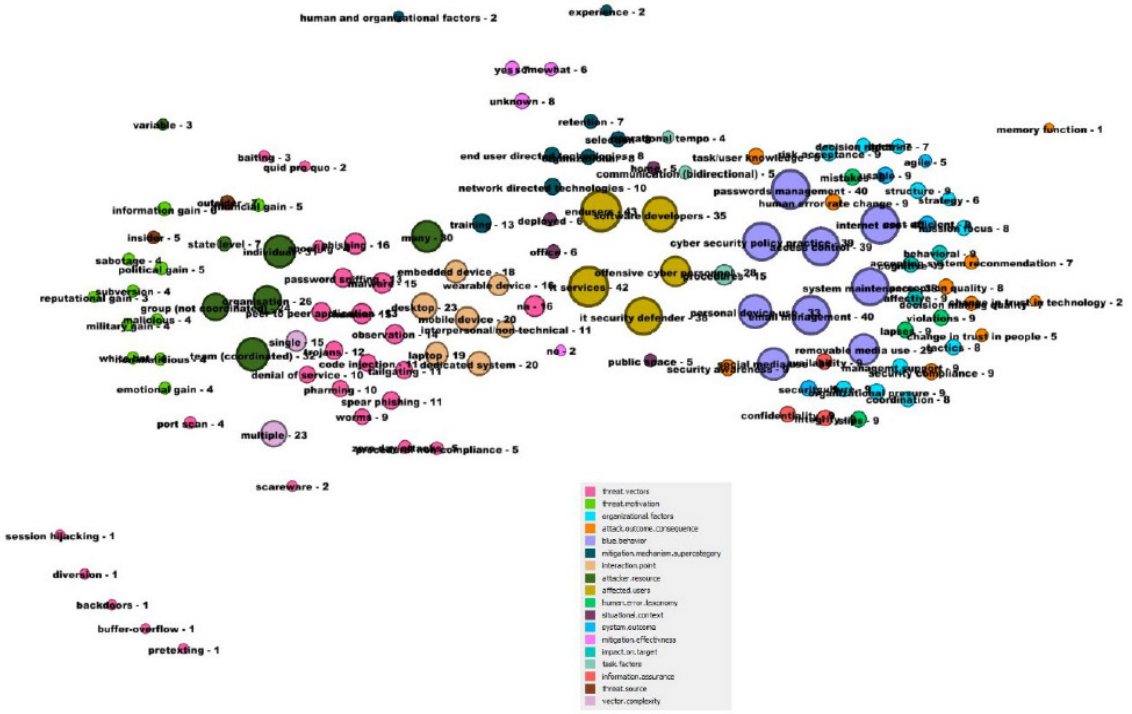

Figure 3-2: Thumbnail of Concepts and Their Occurrence in the Database. See Annex A, Figure A-2 for full-size image.

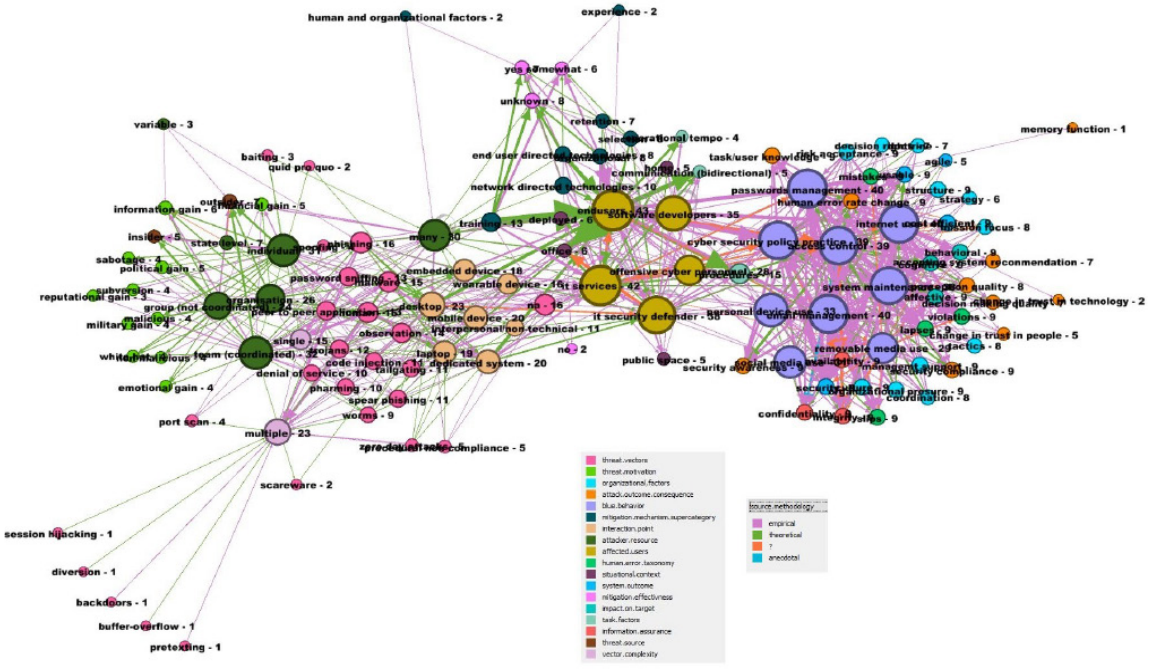

Figure 3-3: Thumbnail of Total Network. See Annex A, Figure A-3 for full-size image.

Furthermore, the relationships, which we found in our sources can have one of four qualities. The relationship can be based on empirical data described in the paper. The relationship can be a theoretical relationship, meaning to say that it is part of a coherent structure of relationships but with no empirical evidence in that particular paper. The relationship is an anecdotal relationship; a linkage mentioned by an author but not imbedded in a theoretical framework. And lastly, we were not able to classify the relationship and it was coded as [?].

These relationships are colour coded as described in the legend [source.methodology].

With this network structure, all sorts of analyses can be done to facilitate sense making.

How does this work?

3.6 QUERIES

3.6.1 Denial of Service

One particular [threat vector], the "denial of service" could be of interest and the query could be:

- Who are the attackers [attacker.resource]?
- Is the threat a single action or combined with other actions? or
- Which type of devices are threatened by "denial of service"?

In Figure 3-4, we can see that in our database, the element "denial of service" occurs ten times and is associated twice with an "individual" [attacker.resource], once with an "organization" and twice with a "coordinated team".

Furthermore, "denial of service" is associated once with "single" attack and twice with a "multiple" attack.

Finally, "denial of service" is associated with embedded devices (1), desktops (2), mobile devices (1), laptops (2) and dedicated systems (2). The nature of these relationships is empirical.

What you as reader need to keep in mind is that this is not a representation of what happens in the world, but what we have found in our set of articles and furthermore, for each relationship the link to the respective articles is available and thus to the author(s) and abstracts and other metadata.

3.6.2 Source Methodology

For an appreciation of the methodological quality of the relationships found in the database, separating out the connections based on the concept [source.methodology] can reveal how the database is populated.

76% of the relationships are based on empirical evidence, 28% are based on a theoretical notion, 4% of the relationships we could not categorize, and less than 1% of the relationships are of an anecdotal nature.

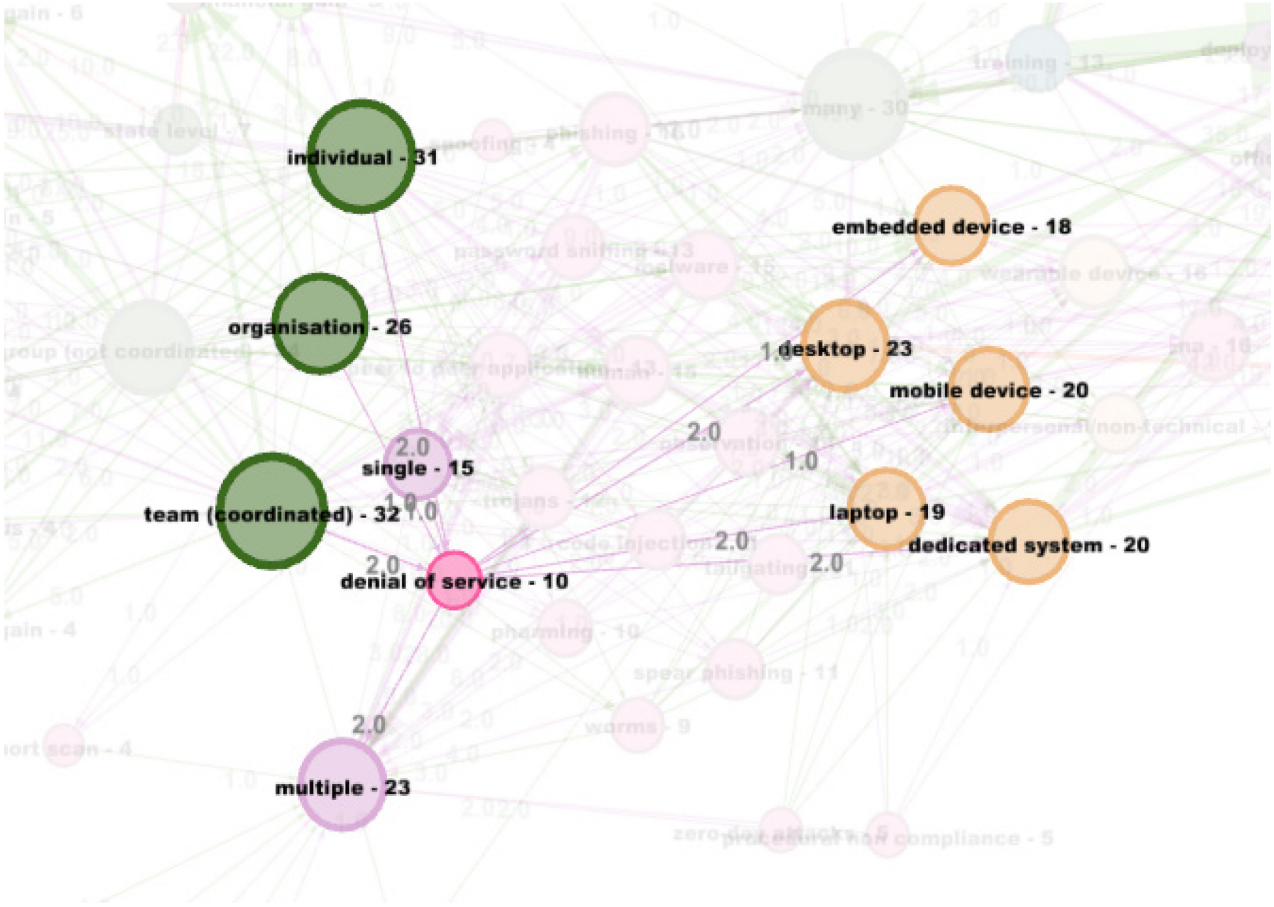

Figure 3-4: Denial of Service.

3.7 CONCLUSIONS

The essence of this approach is linking theoretical sound concepts in a database which can be accessed by users (login and password-protected, to be cyber secure) which will make available the empirical and theoretical insights and their sources in an insightful manner (e.g., Figure 3-5, Figure 3-6, Figure 3-7, and Figure 3-8). The demonstration of this approach shows that this is feasible, although in our case, because we are limited to paper, we lack the sophistication of an interactive demonstrator.

This approach is not restricted to human factors and cyber security, all sorts of other issues and phenomena can be made available in this manner. With the advancement of natural language processing, the manual work, which was considerable, can be automated.

If the NATO Science and Technology Organization would want the sharing and advancement of science and technology to be enhanced, we would advise the STO organization to start setting up server facilities that would allow for this sophisticated approach.

For online examples of this perspective, see:

- https://www.gdeltproject.org/.
- https://www.gapminder.org/tools/#$chart-type=bubbles.
- https://www.ted.com/talks/eric_berlow_and_sean_gourley_mapping_ideas_worth_spreading??utm_medium=social&source=email&utm_source=email&utm_campaign=ios-share.

3.8 ADDITIONAL RESOURCES

The complete database used for this chapter is made available with the file:

- "HFM 259 framework_Sources coded.xlsx"

For the network representations, the Gephi file used is also made available:

- "hfm 259 network data.gephi"

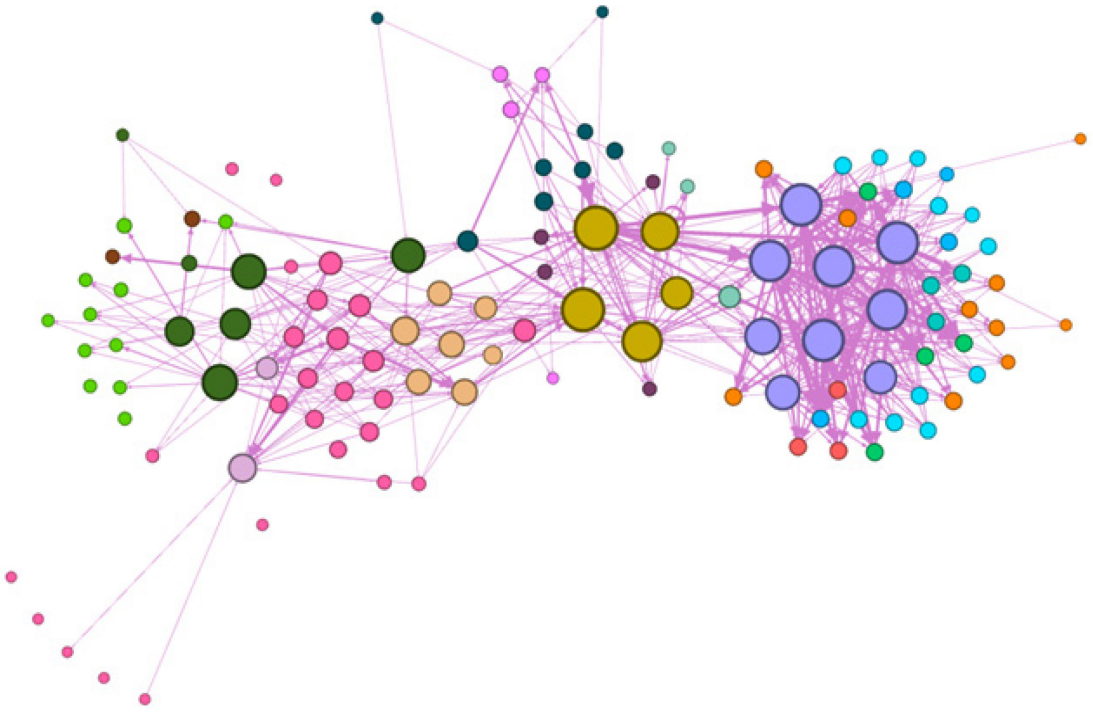

Figure 3-5: Empirical Relationships.

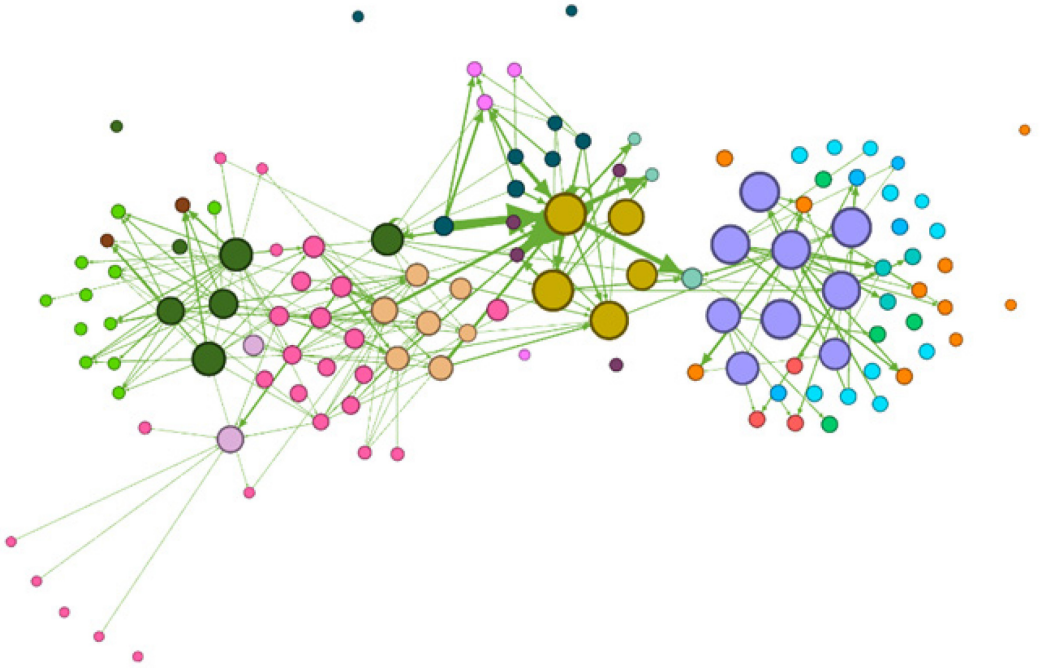

Figure 3-6: Theoretical Relationships.

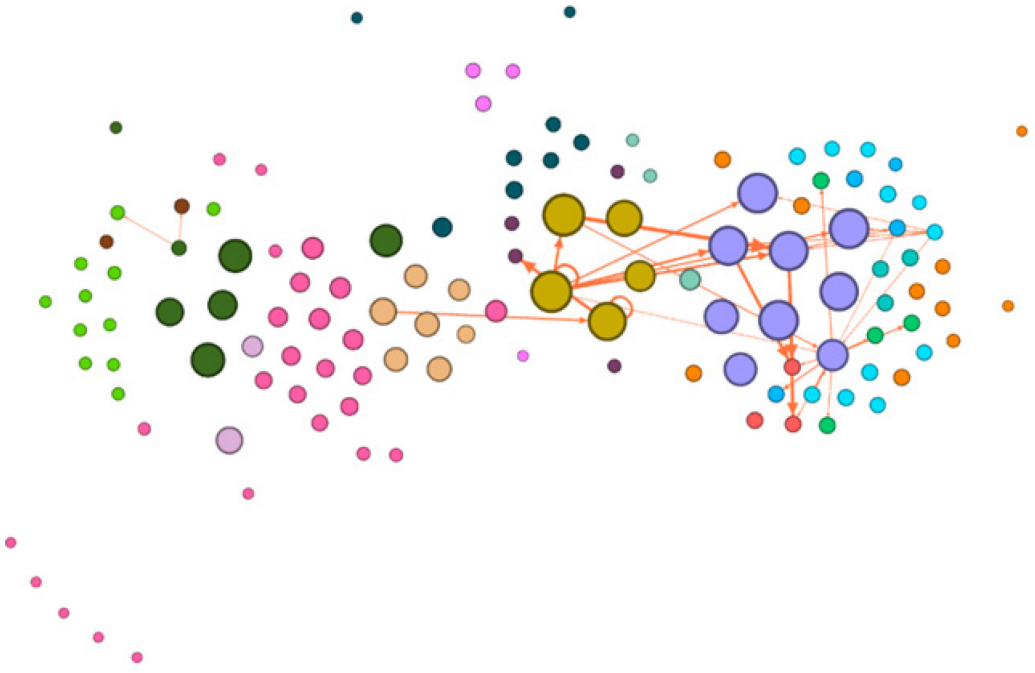

Figure 3-7: Unknown Methodology Relationships.

Figure 3-8: Anecdotal Relationships.

Chapter 4 – HUMAN BEHAVIOUR, COGNITION AND DECISION MAKING: AN INDIVIDUAL PERSPECTIVE

J. Marble, PhD
Johns Hopkins University
UNITED STATES

'If you want to keep your computer system secure, leave it in the box and never let anyone use it,' is the apocryphal security guidance. However, this warning does illustrate a key security concern: User actions, witting or unwitting, lead to the greatest vulnerabilities. Social engineering, such as phishing and spear-phishing, are well-researched techniques that adversaries use to extract information about cyber systems. Less well researched is the extent to which a human user can increase or decrease the security of the system. In this chapter, we will explore the questions that centre on human behaviour as it affects cyber security. They include:

- What kinds of errors do users make?
  - What tools exist to capture information about user errors?
- How can incorporating an understanding of user behaviour, cognition and decision making improve cyber system security?
- Do personality factors affect cyber security behaviours?
- Is awareness of a cyber threat sufficient to change users' behaviours?
  - How does perception of risk influence users' behaviour?
  - What do we know about risk awareness and personality with respect to social media?
- What do we know about insider threats, how to detect them and how to prevent them?

4.1 WHAT KINDS OF ERRORS DO USERS MAKE? WHAT TOOLS EXIST TO CAPTURE INFORMATION ABOUT USER ERRORS?

Cyber system vulnerabilities caused by human error have been attributed to poor situational awareness, lack of training, boredom, and lack of risk perception; in addition, poor human-system interfaces can exacerbate human error and limit situational awareness of the effect of potential human actions. Further, the nature of cyber attack is such that a good attack is not obvious to the users (unless the adversary wishes it to be, potentially to influence user actions). Therefore, users may never become aware of how their actions and choices to neglect cyber security controls can increase system vulnerability. Human error is categorized on the basis of intention or attention, where the incorrect execution of a plan is classified as a slip, a failure of attention yielding an error is classified is called a lapse, and errors caused by correctly following a flawed or inadequate plan is a mistake.

Regardless of the intent of the user, human actions can yield security breaches, leading to the perception that humans are the weakest link in the security process. With respect to cyber security, human error can lead to vulnerabilities both in use of the system, and in the deployment and use of systems designed to keep networks secure, because security systems are also managed by humans. Adversaries exploit human fallibility to gain unauthorized entry into computer systems. Pollock [1] argues that lack of awareness or knowledge of the purpose of a policy will lead to neglect, misuse or misadministration of the system. The reactive nature of cyber

security limits corporate ability to limit information security loss. Pollock adapted the Human Factors Analysis and Classification System (HFACS) to assess human error in cyber security settings. HFACS was originally developed to classify latent organizational factors and human error in aviation accidents. His goal was to analyse historical data to find common trends and identify areas that need to be addressed in an organization to the goal of reducing the frequency of human errors. Pollock notes that while human error is common in many industries and professions, frequently error is treated as an inevitability rather than something that can be studied, predicted or prevented. Vulnerabilities are not due to just user errors, as administrators of systems may also err or violate security policies.

Liginlal, Sim and Khansa [2] also classified human errors yielding privacy breaches into slips, lapses, and mistakes for events. They propose a defence-in-depth strategy founded on error avoidance, interception, and correction. They argue that mistakes (correct action but wrong plan) in the information processing stage is the basis for the majority of errors resulting in privacy breaches. They argue that changes to policies and policy enforcement in organizations are the most effective solution to this problem.

Kraemer and Carayon [3] describe human errors and violations of end users and network administration in computer and information security. They used the same generic error modelling taxonomy of human error as Liginlal et al. [2] to classify types of human error and identify human factors that contribute to security vulnerabilities and breaches. They conducted a series of 16 interviews with network administrators and security specialists. Network administrators tended to view errors by end users as intentional, while errors by themselves or other network administrators tended to be seen as unintentional. This is an example of the fundamental attribution error; people will attribute the cause of their own behaviours to context or circumstances but attribute the behaviour of others to behavioural or personality flaws. This example of a basic human cognitive bias influencing cyber operator performance leads to the next question we might ask about the interaction of human behaviour and cyber security that we can explore through the database.

4.2 HOW CAN UNDERSTANDING USER BEHAVIOUR, COGNITION AND DECISION MAKING IMPROVE CYBER SECURITY?

The effects of user actions, inactions, training, and decision making are illustrated throughout the database. Four example articles addressing user behaviour and human cognition culled from the database are discussed. Pfleeger and Caputo [4] argue that a key to improved cyber security is the incorporation and understanding of user behaviour into the design of the security systems and policy deployment. Pfleeger and Caputo [4] found that users did not have an awareness of how cyber security affected their job functions, and that when security interfered with what they perceived as their primary job function, users would ignore or even subvert the security measure. They concluded perception of security technology and policies as obstacles to the user increases users' resistance to those security policies. However, a focus on the cognitive load and cognitive biases of the users reduced this resistance and increased policy compliance and improvements in security. To support this line of reasoning, the authors cite Sasse, Brostoff, and Weirich [5] finding that frequent password changes result in more frequent login failures than do less frequent changes. This is not surprising as research on human memory demonstrates interference by newly formed memories on recall of older information. Therefore, development of cyber security systems that consider the strengths and weakness of human cognition should result in greater security and compliance.

When systems are designed without understanding the cognitive work or the goals of the operators, the resulting technology may not be useful to the intended users. Lathrop, Trent, and Hoffman [6] conducted focused research on human factors in cyber operations, and included recommendations on how to incorporate cognitive

engineering and experimental psychology practices into research and development projects. While operations in cyberspace are dependent upon highly sophisticated technologies, most technologies were not designed to support user decision making. Lathrop et al. recommend considering a sense-making and team sense-making in cyber operations approach in the design of tools for cyber operators, in order to develop appropriate visualizations to support the user in understanding cyber environment. They conclude with the following recommendations:

1) Sustained Experimentation and Cognitive Work Analyses. They recommend using a series of 'fail fast' experiments to explore the cognitive work process of users, to better under what information users need, how and when they use it, and with what other information is it used.

2) Operationally Grounded Measures and Metrics. Lathrop et al. [6] believe that a major flaw in research to that point has been that assessment measures and metrics are often misunderstood, misapplied or overlooked.

3) Realistic Environments for Training, Testing, Experimentation and Operations. Realistic operations simulation environments that afford data collection are necessary to support the needed research into cyber operator decision making.

Similarly, Gutzwiller, Fugate, Sawyer, and Hancock [7] argued that cyber security, operations and defence held significant research opportunities for the human factors engineering community. They point out that human situational awareness of cyberspace operations significantly differs from situational awareness for other environments. As Lathrop et al. [6] note, agreement on how and what aspects of operator behaviour to measure to define situational awareness in cyber environments is minimal in cyber operations because the definition would require predetermined understanding of operators' goals and potential actions to achieve those goals. Few robust task analyses have been conducted. Further, these analyses often lack sufficient measures of situational awareness, or validation in actual cyber environments. Gutzwiller et al. [7] state that task analysis, definition of goals and potential actions are a critical issues underlying the development of tools for cyber operators. Gutzwiller et al. [7] found that many existing cyber defence tools do not connect presented information with the operators' goals or information needs (e.g., threat determination), making these tools and visualizations unlikely to enhance cyber defender situational awareness or performance. Gutzwiller et al. [7] provide the argument that a "cyber common operating picture" is not sufficient to create situational awareness just because it presents potentially relevant information to the operator or the cyber team. They rightly point out that shared awareness of a datapoint or set of datapoints does not mean that a set of decision makers will draw the same conclusion from the information.

In general, the research available appears to indicate that using realistic simulation environments, which allow for testing of well-defined hypotheses can provide a milieu for research on human behaviour and cognition and their interaction with cyber security and policies; however, existing research is limited in scope and granularity. However, consideration of human cognitive limitations, strengths, and biases in the development of tools for cyber operators does appear to increase the efficacy of the tools and compliance with security policies.

4.3 DO PERSONALITY FACTORS AFFECT CYBER SECURITY BEHAVIOURS?

The second question we proposed that could be asked from the data base is the degree to which personality or individual characteristics interact with cyber security. Within the articles reviewed in the database, we found three that explored the interaction between personality factors and cyber vulnerabilities. Parrish, Bailey and

Courtney [8] explored the 'big five' personality traits on susceptibility to phishing. The 'big five' personality traits consist of Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism. Parrish et al. [8] theorized that variation in these traits could affect users' susceptibility to phishing. Hackers and cyber adversaries rely on "phishing" and other forms of influence to gain access to system information, which can be as simple as passwords or as complex as network infrastructure. Techniques used by adversaries to gain information from users seek to make the user believe that the request for information comes from a trusted source. Parrish et al. [8] created a model of the proposed interaction, but no experimental testing of the model was performed.

Continuing exploration of user personality characteristics on susceptibility to phishing, Butavicius, Parsons, Pattinson, and McCormac [9] examined the influence of authority, scarcity and social proof on users' judgments of how safe it was to click on a link in an email. The emails were either genuine, phishing, or spear-phishing tailored to the recipient. (In spear-phishing, the lure is crafted to be of specific interest to the recipient, such as referring to a hobby or organization the recipient is a member of.) With respect to personality factors, users who scored lower for impulsivity on measures of personality were less likely to judge a link as safe in the fraudulent emails. Of the social engineering techniques used in the phishing and spear-phishing emails, the researchers found that reference to authority had the greatest influence on whether or not users clicked on the email link. Recipients were best at detecting phishing emails when social proof was present. However, recipients were not very capable at distinguishing genuine from spear-phishing emails.

In a real world exploration of personality and susceptibility to social engineering, Halevi, Memon, and Nov [10] studied what causes people to be deceived by phishing attacks. As noted in the previous discussion, spear-phishing target specific individuals and represent a more difficult detection decision. Halevi et al. [10] explored how users' personality, attitudes, and perceived efficacy affected their detection of spear-phishing in an industrial setting. Participants were assessed on the Big 5 personality factors. The researchers asked whether people who score highly for Conscientiousness would be more easily persuaded to respond to a phony email than people who scored lower. The authors hypothesized that:

1) Highly conscientious people would show greater vulnerability to phishing when the social engineering appeal was to efficiency and order;
2) Greater internet use would yield greater awareness of phishing risks and thus lower vulnerability;
3) Users would have an inaccurate perception of their risk for being a target of phishing;
4) Lower perception of risk would increase vulnerability; and
5) Greater computer mediated communications competence would reduce susceptibility to phishing.

The experiment was performed on employees working for 'a large Indian company.' Prior to the email targeting employees, participants filled out a survey that assessed their awareness and perception of risk from phishing and spear-phishing. Two weeks later, an email which claimed to be from the IT manager was sent through the company email warning of missing time sheet information with a link that when clicked, brought users to a screen with a button to install a 'missing' plug-in. The address of this website in the link was external to the company website, which should have been a warning to the users. The study found that 62.5% of participants clicked the link, and of those, 30% downloaded the plug-in. Conscientiousness score was most highly correlated to clicking the link and downloading the plug-in. There appeared to be a negative correlation between the participants' estimate of their vulnerability to phishing attacks and the probability that they were phished; that is, participants with lower estimates of their probability of being phished were more likely to follow the links. Based on these findings, the authors argue that vulnerability to phishing is partially due to

users' personality, and that lack of awareness of phishing risks has less of an effect on vulnerability. Therefore, they conclude that design of security systems should account for users' personalities.

Frequently, companies have attempted to deter intentional misuse of resources through sanctions or reprimands. However, D'Arcy and Devaraj [11] found that the employees' need for social approval and their moral beliefs were key predictors of resource misuses. By applying deterrence via formal and informal sanctions they developed a framework to predict technology misuse intention. In general, they found that teleworking or remote employees were more likely to misuse their organization's technology resources.

4.4 WHAT DO WE KNOW ABOUT RISK AWARENESS AND PERSONALITY WITH RESPECT TO SOCIAL MEDIA?

Jeske, Briggs, and Coventry [12] also explored this interaction of remote work on misuse of technology, and their correlation to measures of individual impulsivity and social media use. As noted in the previous study, telework and remote work tend to blur the boundary between work and leisure tasks. Jeske et al. [12] note that this boundary is even less distinct when users are on mobile devices, users of mobile devices may not sufficiently attend to security issues when they are multitasking and users who score high for impulsivity may be more vulnerable distraction. In their study, Jeske et al. [12] asked 104 users to select a wireless network when responding to work demands while out of the office. Eye tracking was used with 40 of the participants to assess the interaction of impulsivity and attention during the task. Higher impulsivity scores were correlated with higher probability of accessing social media, and use of public networks. In addition, more highly impulsive people appeared to process less information before clicking links or taking other actions. The authors make suggestions for designs to support increased deliberation and reduce impulsive actions.

While social media and networking sites are frequently harvested by adversaries seeking information about users in order to gain access to their systems because the users of social media tend not to recognize the value and use of information that they share. The sites themselves have increased in reach and quantity of information, but the reliability of information in not assessed by providers nor by acquirers. Silic and Back [13] explored deception and victimization on social networking sites with respect to information security. They conducted a set of field experiments design on users to assess how credibility, persuasion and motivation theories predicted access to organizational data. The field study was followed by a qualitative study of employees who used social networking sites and interviews with Chief Information Security Officers (CISOs). The most critical findings of these two studies were:

1) Social networking sites provide contextual elements, which allow adversaries to define effective psychological vectors to deceive employees.
2) Organizations do not have tools or techniques that can effectively block SNS online security threats.
3) Social networking sites should be considered security holes that allow manipulation of employee behaviours through social engineering techniques, facilitating malicious attacks.
4) The authors recommend that companies strengthen their information security policies related to social networking and to require stronger employee identification and authentication.

Awareness of risk and concerns about online privacy, though, does not prevent people from sharing their personal information in online relationships according to Lips and Eppel [14]. In their New Zealand-based study of online information-sharing behaviours (as compared to attitudes towards online sharing), Lips and Eppel [14] explored motivation for information sharing, the degree to which information was shared, and conditions under

which individuals shared their personal information, including to whom the information was shared (e.g., commercial entities, government, or with social networking sites). All the participants in the study were strongly aware of risks to sharing personal information online, and were seen to make very deliberate choices about what information to share and when. Based on their findings the authors developed a taxonomy of online information-sharing behaviours that included four classifications of people's online information-sharing behaviours. These categories were privacy pragmatists, privacy victims, privacy optimists, and privacy fatalists. Privacy pragmatists were defined as those who were privacy aware but willing to trade off their personal information for perceived benefits, such as efficiency or convenience. Privacy victims, in comparison, believed that they had no choice but to hand over their personal information in order to use an online service. They tend to cease using the service when information demands are too high. Privacy optimists continue to perform behaviour that they acknowledge to be risky until they have a consequence. Finally, privacy fatalists believe that a major breach of their privacy is unavoidable, and that most personal information is already accessible. (These final two groups were the least common.)

Information vulnerability does not always come directly from the users of the social network. In some instances, vulnerability or access to information can come from the network of friends of the user. Aware of this potential, Ma, Teng, Lin, and Huang [15] explored how to make users aware of who among their networks are most likely to share the user's personal information. They defined these nodes as "vulnerable friends". They defined a Fuzzy Analytical Hierarchy Process (FAHP) assessing multiple factors (e.g., gender, birthday, hometown, mobile phone, high school, college, etc.) to predict propagation of privacy information by vulnerable friends. The FAHP was based on an initial calculation of users' influence, which was then used to predict the probability that a user would propagate another person's information. Using the model, they created a method to detect a user's vulnerable friends, and then provide this insight back to the user, with the idea that users could then decide with whom to share information based on the vulnerability of their friends.

Vidyalakshmi, Wong, and Chi [16] assessed users' desire for privacy to propose a method for control of information sharing, to allow the user to determine what information is seen by whom. In their method, the authors proposed shifting visibility information from assignment to groups (how visibility is traditionally allowed) to category of information. The authors argue that allowing users to determine whether to share or not share categories of information would allow users intuitive and hassle-free control over sensitive information.

4.5 IS AWARENESS OF A CYBER THREAT SUFFICIENT TO CHANGE USERS' BEHAVIOURS? HOW DOES PERCEPTION OF RISK INFLUENCE USERS' BEHAVIOUR?

Increasing information security awareness through training was the focus of 254 of the articles reviewed. With the exception of sabotage, users do not knowingly expose the systems they use to cyber attack. Rather, they take actions that they perceive to have little or no risk, but which allow them to (more efficiently) accomplish their goals. Parsons, Calic, Pattinson, Butavicius, McCormac, and Zwaans [17] developed the Human Aspects of Information Security Questionnaire (HAIS-Q), to measure information security awareness in university students. They found that students who scored higher on the HAIS-Q were less susceptible to phishing attempts. Therefore, accurate perception of the sources of risk does influence user behaviours. This builds on work by Parsons et al. (2015) who demonstrated that the cues used by most users to differentiate phishing email from real email (e.g., presence of legal disclaimers, quality of visual presentation) are not reliable cues. The question of whether awareness of potential threats reduces vulnerability to the threat is predicated on whether or not users can identify threats and security features of the workplace. So, while awareness reduces risk behaviour, users may not be well informed or properly aware of sources of risk. In general, there was an assumption that

increasing awareness will decrease network vulnerability. Dang-Pham, Pittayachawan, and Bruno [18] performed a case study in Vietnam to model the degree to which employees were aware of security priorities and performed security behaviours proactively. The greatest predictors of security policy awareness were periodic audit and monitoring, security policies, and co-workers' attitudes toward security policies and security prioritization.

Corporate security policies are designed to guide the behaviour of employees, and thus policy compliance is a key driver of security. Cox [19] described the knowing-doing gap, in which users fail to follow security policies, even when they are aware of them. Conversely, Rajivan and Cooke [20] point out that network and system complexity has increased to the point where the expanse of cyber security space exceeds the ability of the analyst to comprehend or perceive significant events in the network. As Shepherd, Archibald, and Ferguson [21] point out, risky security behaviour is not necessarily obvious to users. When the consequence of the behaviour is not understood, it is possible for adversaries to then manipulate the users. Shepherd et al. [21] explored methods to provide automatic, instant warning of potential risky actions by users, and feedback regarding the outcome of the actions they took. Ben-Asher and Gonzalez [22] demonstrated that feedback during training improves users' classification of network events; however, they agreed that if the source of the risk is not clear to users, behaviour may not change.

Sommestad and Halberg [23] explored the extent to which awareness of security policies affects cyber security behaviour in a meta-analysis of 16 studies on compliance with security policy. Their theory states that attitude toward behaviour, subjective norms, and perceived behavioural control together shape an individual's behavioural intentions and drive chosen actions. The authors applied the theory of planned action to explain information security policy compliance and violation. They concluded that intention, as defined by the theory, predicts information security policy compliance and violation. However, a significant limitation of the study was that it did not explore how to influence users' intention to comply with policy.

Gerber, McDermott, Volkamer, and Vogt [24] reasoned that since organizational information security policies can only improve security if employees comply with them, understanding the factors that affect employee security compliance is crucial for strengthening information security. They performed a survey of 200 German employees to explore factors that increased compliance with security policies. Gerber et al. [24] found that when employees were rewarded for production achievement, security compliance was lower than when they were rewarded for other work characteristics (e.g., product or work quality). Similarly, when the company culture emphasized avoiding errors (which lead to covering up of errors rather than prevention of errors), security compliance was reduced because employees were discouraged from discussing errors or the cause of errors. Finally, there was no improvement in security compliance as a function of "affective commitment" (loyalty) towards the organization, or the quality of the security policy information or the security goal setting process. Intriguingly and contradictory to Sommestad and Halberg [23], Gerber et al. [24] found that intention to comply with security policies was a poor predictor of actual security compliance. Gerber et al. argue that only measured behaviour (objectively measurable actions), rather than intention is the only reliable indicator of performance.

Pahnila, Siponen, and Mahmood [25] studied compliance of Finnish employees with security policy. Their results suggest that the quality of information about the rationale for the policy had a significant effect on actual security policy compliance. Employees' attitude, normative beliefs and habits significantly influenced report intent to comply with information system security policy. They further found that sanctions had an insignificant effect on intention to comply with IS security policy nor did rewards have a significant effect on actual compliance with security policy. Sommestad, Karlzén, and Hallberg [26] proposed Protection Motivation Theory, arguing that compliance with security policies are better when:

1) The behaviour is voluntary;
2) The threat and coping method are concrete or specific; or
3) The information security threat is directed to the person itself.

4.6 WHAT DO WE KNOW ABOUT INSIDER THREAT?

Because insiders have access to facilities and information, knowledge of the organization and the location of valuable assets, they pose the greatest threat when they choose to act against the organization. In addition, organizations may not have employed effective risk management strategies to deal with change, such as outsourcing which can break up protection barriers. At the same time, outsourcing can reduce controls and increase the number of people with full system access. The nature of outsourcing can lead to abnormal behaviour in long-term employees and managers because they are not traditional employees. There are essentially two forms of insider threat: Unintentional and intentional. An assessment of Unintentional Insider Threats (UITs) are outlined in the US CERT Insider Threat Team [27] report, which collected and analysed publicly reported phishing cases involving malware and performed an initial analysis of the industry sectors impacted by this type of incident. The report provides an analysis of the types of industries affected by UIT, case examples of UITs, and recommendations to lessen UITs stemming from phishing and other social engineering incidents. In addition, the report explores the utility of tracking near misses of insider threat, as is done for health care and critical systems.

Derbentseva, Fraser, Gibbon, and Hawton [28] surveyed open academic and practitioner information security literature on non-malicious user threat behaviours with the purposes of:

1) Identifying possible non-malicious user threat behaviours;
2) Understanding the reasons for these behaviours; and
3) Identifying mitigation strategies to minimise non-malicious user threat behaviours proposed in the literature.

They provide the key perspective that people have a significant role in information security, because these systems are designed to provide tools for the users and assist them to achieve their individual and organizational goals. However, even legitimate systems users are likely not aware of the most up-to-date security threats and protection mechanisms, or even of their organization's Information Systems Security Policies (ISSPs).

With respect to intentional insider threat, Greitzer and Frincke [29] attempted to develop a technique to detect insider threats. They combined traditional cyber security audit data with psychosocial data to define a usable set of predictive indicators, and a framework to integrate organizational and cyber security data to make predictions about insider threats. The psychosocial indicators of insider threat they identified included disgruntlement, difficulty accepting feedback, anger management issues, disengagement, confrontational behaviour, and stress, among others. They acknowledge, however, the need to verify and validate their model, and the difficulty of doing so.

Colwill [30] explored how to mitigate intentional insider threat. Their approach considered the nature of loyalty and betrayal in the context of organizational and cultural factors and changing economic and social factors. The author describes the approaches used by his company to assess and address insider threats and risks to mitigate against insider attacks rather than react after an event. From this perspective, technological measures alone are insufficient because controls are not designed with people's behaviour in mind.

4.7 CONCLUSION

As shown by this review, the HFM database can provide useful insights into how different aspects of user behaviour and cognition increase and decrease cyber security. Assessment of human behaviour can give insight into unexpected source of vulnerabilities, such as vulnerability, and the efficacy of different mitigation strategies such as training and rewards. Humans are the purveyors, operators, users, and exploiters of these systems. To ignore human behaviour in the system is to leave large vulnerabilities. Therefore, systems should be designed and deployed with consideration for who will use them, their purposes, and use contexts.

4.8 REFERENCES

[1] Pollock, T. (2017). Reducing human error in cyber security using the Human Factors Analysis Classification System. In: KSU Proceedings on Cybersecurity Education, Research and Practice. Available at: http://digitalcommons.kennesaw.edu/ccerp/2017/research/2.

[2] Liginlal, D., Sim, I., and Khansa, L. (2008). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. Computers & Security 28(3-4) (May-June 2009):215-228.

[3] Kraemer, S., and Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. Applied Ergonomics 38:12.

[4] Pfleeger, S., and Caputo, D. (2012). Leveraging behavioral science to mitigate cyber security risk. Computers & Security, doi: 10.1016/j.cose.2011.12.010.

[5] Sasse, M., Brostoff, S., and Weirich, D. (2002). Transforming the 'weakest link' – A human/computer interaction approach to usable and effective security. BT Technology Journal 19:122-131.

[6] Lathrop, S.D., Trent, S., and Hoffman, R. (2016). Applying human factors research towards cyberspace operations: A Practitioner's Perspective. In: D. Nicholson (Ed.), Advances in Human Factors in Cybersecurity. Advances in Intelligent Systems and Computing, vol. 501. Cham, Switzerland: Springer.

[7] Gutzwiller, R., Fugate, S., Sawyer, B., and Hancock, P. (2015). The human factors of cyber network defense. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting 59:322-326.

[8] Parrish, J.L., Jr., Bailey, J.L., and Courtney, J.F. (2009). A personality-based model for determining susceptibility to phishing attacks. In: Proceedings of the Southwest Decision Sciences Institute (SWDSI) Annual Meeting, July 2015. pp 285-296.

[9] Butavicius, M., Parsons, K., Pattinson, M., and McCormac, A. (2015). Breaching the human firewall: Social engineering in phishing and spear-phishing emails. In: Proceedings of the Australasian Conference on Information Systems.

[10] Halevi, T., Memon, N., and Nov, O. (2015). Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. Available at SSRN: https://ssrn.com/abstract=2544742 or http://dx.doi.org/10.2139/ssrn.2544742.

[11] D'Arcy, J., and Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. Decision Sciences 43(6):1091-1124.

[12] Jeske, D., Briggs, P., and Coventry, L. (2015). Exploring the relationship between impulsivity and decision-making on mobile devices. Pers Ubiquit Comput 20, 545–557 (2016). https://doi.org/10.1007/s00779-016-0938-4.

[13] Silic, M., and Back, A. (2016). The dark side of social networking sites: Understanding phishing risks. Computers in Human Behavior 60:35-43.

[14] Lips, A., and Eppel, E. (2016). Understanding and explaining online personal information-sharing behaviours of New Zealanders: A new taxonomy. Information, Communication, & Society, 20(3) 428-443 (2017). https://doi.org/10.1080/1369118X.2016.1184697.

[15] Ma, T., Teng, Y., Lin, L., and Huang, Z. (2015). Identifying vulnerable friends on a social networking site. In: Proceedings of the12th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 94-101.

[16] Vidyalakshmi, B., Wong, R., and Chi, C.-H. (2016). Privacy-preserving information dispersal in social networks based on disposition to privacy. In: Proceedings of SmartCity 2015, 372-377.

[17] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., and Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security 66:40-51.

[18] Dang-Pham, D., Pittayachawan, S., and Bruno, V. (2015). Factors of people-centric security climate: Conceptual model and exploratory study in Vietnam. Computers & Security 68:1-15.

[19] Cox, J. (2012). Information systems user security: A structured model of the knowing-doing gap. Computers in Human Behavior 28:1849-1858.

[20] Rajivan, P., and Cooke, N. (2018). Impact of team collaboration on cybersecurity situational awareness. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Available at: https://link.springer.com/chapter/10.1007%2F978-3-319-61152-5_8#citeas.

[21] Shepherd, L.A., Archibald, J., and Ferguson, R.I. (2013). Perception of risky security behaviour by users: Survey of current approaches. In: L. Marinos and I. Askoxylakis (Eds.), HAS/HCII 2013. Heidelberg, Germany: Springer-Verlag Berlin, LNCS 8030, 176-185.

[22] Ben-Asher, N., and Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. Computers in Human Behavior 48:51-61.

[23] Sommestad, T., and Halberg, J. (2012). A review of the theory of planned behaviour in the context of information security policy compliance. In: Proceedings of the 17th Nordic Conference on Secure IT Systems, 47-60.

[24] Gerber, N., McDermott, R., Volkamer, M., and Vogt, J. (2016). Understanding information security compliance – Why goal setting and rewards might be a bad idea. HAISA, 145-155. Available on www.cscan.org. Accessed on 14 April 2020.

[25] Pahnila, S., Siponen, M., and Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In: Proceedings of the HICSS 40th Annual Hawaii International Conference on System Sciences, 156b-166b. IEEE.

[26] Sommestad, T., Karlzén, H., and Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. International Journal of Information Security and Privacy (IJISP) 9(1):26-46.

[27] US CERT Insider Threat Team. (2014). Unintentional Insider Threats: A Review of Phishing and Malware Incidents by Economic Sector. Technical Note CMU/SEI-2014-TN-007, Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=297771. Accessed on 14 April 2020.

[28] Derbentseva, N., Fraser, B., Gibbon, S., and Hawton, A. (2015). What do we know about threats from well-intentioned users? A literature review. Available at http://cradpdf.drdc-rddc.gc.ca/PDFS/unc234/p804195_A1b.pdf.

[29] Greitzer, F., and Frincke, D. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. In: C.W. Probst, J. Hunker, D. Gollmann, and M. Bishop (Eds.), Insider Threats in Cyber Security. Springer, Boston, MA.

[30] Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? Information Security Technical Report 14(4):186-196.

Chapter 5 – CYBER SECURITY: AN ORGANIZATIONAL PERSPECTIVE

N. Derbentseva
Defence Research and Development Canada (DRDC)
CANADA

S. Träber-Burdin
Fraunhofer Institute for Communication
GERMANY

5.1 ORGANIZATIONAL MECHANISMS

Cyber security is a multilevel problem affecting individuals, organizations and nations. As organizational operations become increasingly dependent on networks and Information Technology (IT), Information Systems (IS) security becomes an important concern, especially when information protection is imperative be it for client/user privacy considerations, protection of intellectual property or national security.

Organizational factors play a significant role in shaping personnel behaviour and determining an organization's overall cyber security posture. For example, such organizational considerations as security policies and procedures, security culture in the organization, organizational structure, coordination mechanisms, managerial support for information security practices and policies, organizational pressure, risk acceptance, compliance monitoring, enforcement/sanctions, personnel selection, recruitment, retention and education and training have been discussed in relation to information systems security.

Over 89% of the sources coded in the current version of the knowledge base (206 out of 230) considered at least one of the above organizational factors in their analysis of information security, and Figure 5-1 shows the frequency distribution with which these factors were discussed in the analysed sources. About a quarter of the coded sources (56) in the dataset discussed one or more organizational mitigation mechanism. Figure 5-2 shows a further break down of the Organizational mitigation mechanisms in the coded dataset. This chapter discusses the role of organizational factors in cyber security.

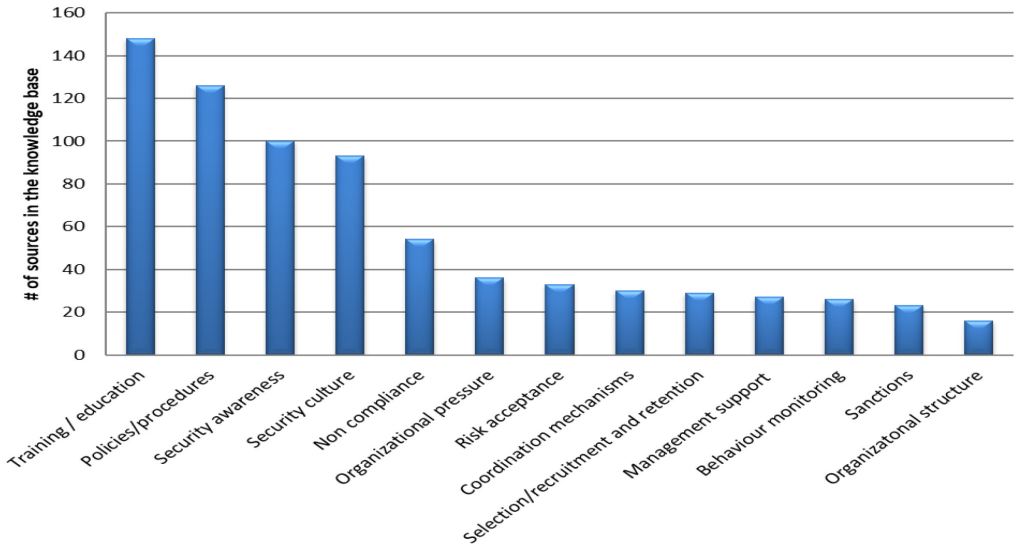

Figure 5-1: Distribution of Organizational Factors in the Knowledge Base.

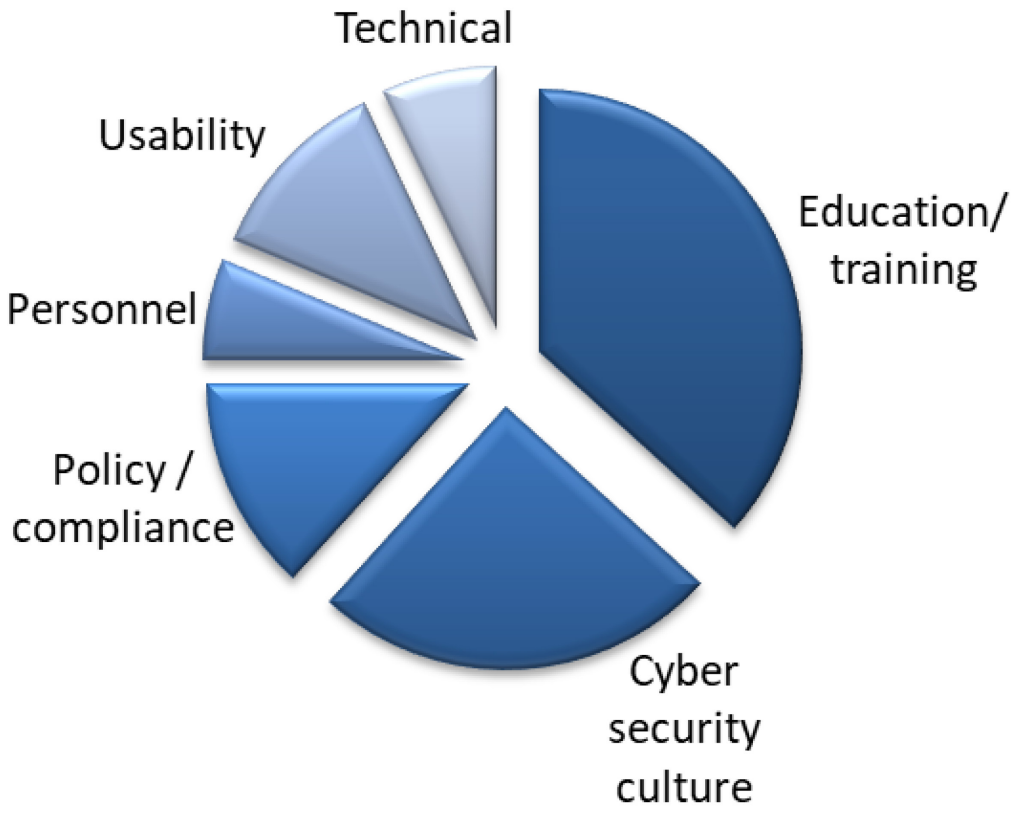

Figure 5-2: Distribution of "Organizational" Mitigation Mechanisms in the Dataset.

5.2 ORGANIZATIONAL POLICIES AND COMPLIANCE

Western governments and their armed forces are increasingly (and critically) dependent on Information Systems (IS) and networks for their operations. Such dependence, while being a great enabling power, on the other hand creates vulnerability to potential threats to systems, networks and information compromise. Thus, Information Security Management and protection of information resources has become of critical importance for virtually all organizations.

In most cases, information systems cannot be protected from compromise exclusively by technological means. People within the organizations play a key role in safeguarding organizations' systems and information. For example, IT personnel are responsible for proper installation and configuration of technological defences (e.g., someone needs to properly configure firewall settings). Employees require access to the organization's systems and information to perform their duties and achieve organizational goals and can take steps to protect IT resources or jeopardise them. As such, human behaviour is one of the major contributors to organizational information security, both as a vital safeguard and as one of the major threats (e.g., Ref. [1]).

To protect their IS and information, organizations employ a variety of security controls, which in addition to technical controls include procedural and managerial controls (e.g., NIST 800-053, ITSG-33). IS-related Security Policies and Procedures (ISSPs) are examples of procedural and managerial security controls that are put in place to protect organization's systems and/or information (e.g., Refs. [1], [2], [3]).

Recognising the role of policies and procedures in information security, various aspects of these mechanisms were captured and reflected throughout the ontology as shown in Figure 5-3 with red ovals circling the relevant concepts. For example, one of the threat vectors in the ontology is policy and procedural non-compliance and one of the mitigation mechanisms is policy management.

This sub-section summarises various factors related to information systems security policy from the knowledge base and provides an overview of the relevant literature.

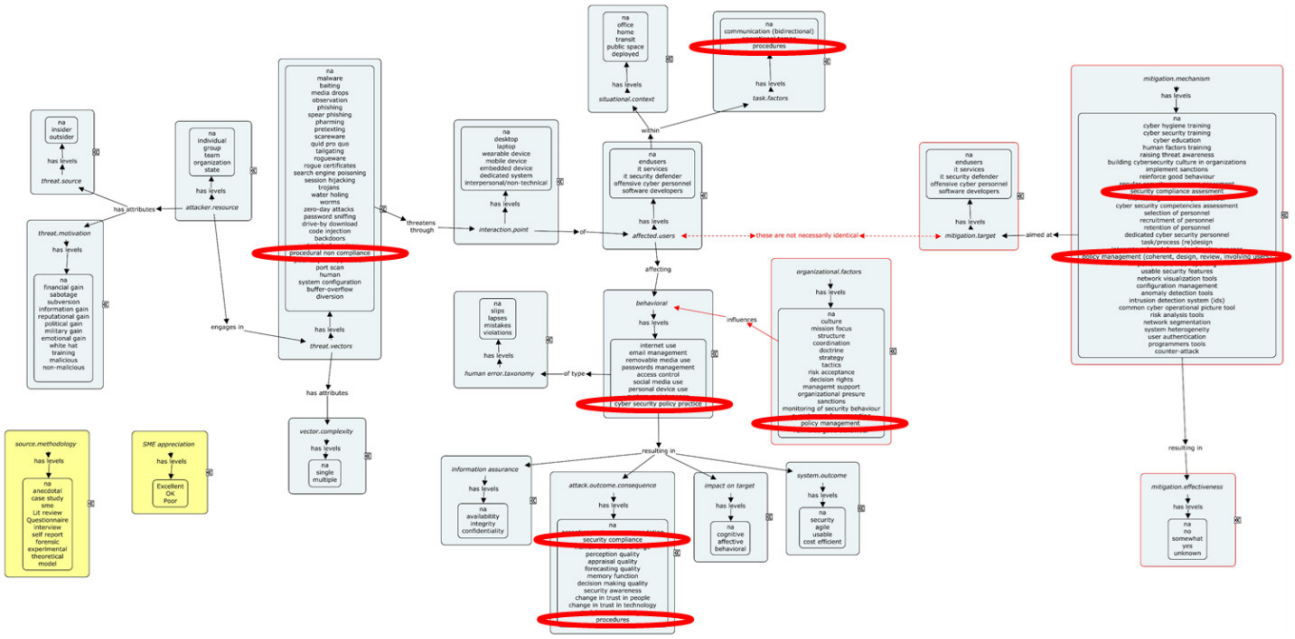

Figure 5-3: Policies and Procedures Captured in the Framework. See Annex A, Figure A-1, for full-size non-annotated image.

5.3 INFORMATION SECURITY POLICIES AND PROCEDURES

ISSPs are seen as an essential driving component of effective security management in organizations (e.g., Refs. [4], [5], [6], [7]). Security policies "are designed to inform the members of an organization of their obligatory responsibilities for protecting the information systems of their organization. Policies are adopted by a company as a statement of purpose, objectives, and roles and responsibilities" [5], p. 63. Depending on the size and technological climate of an organization, it may have a set of ISSPs organized in a hierarchical manner with lower level policies providing greater level of detail for specific technologies while supporting the higher-level policy [5], [8]. Procedures, in turn, provide specific step-by-step instructions on how to implement various policies [9], [5]. As such, ISSPs and procedures are organizational measures designed to regulate and guide personnel's security behaviour (e.g., Ref. [10]). Unlike technical security mechanisms, implementation and execution of policies and procedures rely on people behaving in a prescribed manner, and their effectiveness significantly depends on human behaviour, which could be influenced by many factors (e.g., Refs. [11], [12]).

Given the significant role that ISSPs play in the overall organizational information security, a great deal of attention has been devoted to understanding factors that contribute to ISSP effectiveness. Some of the factors

discussed in the literature include characteristics of the policies themselves, their development process, various organizational and individual factors that could influence employee security behaviour (e.g., Refs. [3], [5], [7], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], etc.). Below, we first discuss policy characteristics and policy development process, followed by a discussion of individual and organizational factors that contribute to policy compliance as captured in the knowledge base.

5.3.1 Policy Characteristics

A number of information security management standards and recommendations have been developed that can provide guidance for the development of information security management programs and security policies, including their content and structure (e.g., ISO 27000, 2013 series; NIST 800 series; [23]; [6]). For example, Höne and Eloff [7], Cappelli et al. [6], Karlsson et al. [24], and Stahl et al. [10] provided a general set of desirable ISSP characteristics and supporting processes, which are summarised below. Policies should be:

- Concise and easy to read;
- Clear and comprehensive;
- Coherent, and supported by explicit reasoning;
- Have clear target groups;
- Be relevant and important to users;
- Contain specific practical guidelines for actions;
- Practically implementable and enforceable;
- Reflect organizational culture to ensure acceptance;
- Fair for all employees;
- Not introduce goal conflicts;
- Adapted to the specific needs of the organization if based on any external guidelines;
- Distributed throughout the organization;
- Consistently enforced;
- Periodically reviewed to ensure policy currency; and
- Supported by periodic training.

There is some empirical evidence linking the above policy characteristics to employees' compliance with them. For example, Bulgurcu et al. [25] found that perceived ISSP fairness, a quality in the Cappelli et al. [6] list, was associated with employees' intention to comply with the policy. Bulgurcu et al. [25] also found that ISSP quality, operationalized as a combination of policy clarity, completeness and consistency, qualities found in both Höne and Eloff [23] and Cappelli et al. [6] lists, was also associated with employees' intention to comply with the policy. Son [26] found that perceived policy legitimacy (similar to being supported by explicit reasoning) was associated with self-reported policy compliance.

5.3.2 Policy Development

Organizations can use the standards and general guidelines, however for the information security programs and policies to be effective they need to be tailored to fit specific organizational context. Following general

guidelines and using policy templates without customizing them to the specific organizational environment may result in policies that are not aligned with organizational priorities, not supported by organization members, mostly ignored, and, thus, ineffective (e.g., Refs. [5], [24], [2], [3]). Although, various authors seem to agree on the importance of such customization of policies, there is an apparent scarcity of specific recommendations for information security managers on how to achieve that (e.g., Refs. [27], [24], [2]). Below we review common themes in the literature on ISSP development.

5.3.2.1 Identifying and Resolving Potential Conflicting Objectives

Conflicting objectives within an organization could interfere with employees' ISSP compliance and these need to be considered during the policy design and implementation process (e.g., Ref. [24]). Kirlappos et al. [3] argued that potentially conflicting organizational goals can be balanced through the context-aware policy design, communication of the value of security, and the development of desirable security norms and trust between the organization and employees, with less emphasis on monitoring and sanctions. Kolkowska et al. [27] developed a nine-step approach to facilitate the identification and analysis of differing objectives within an organization based on the values framework. This approach focuses on analysing both policy design rationale and policy use rationale and values associated with policy design and use. An important step in Kolkowska et al. [27] approach is collecting data about actual actions, and Kolkowska et al. [27] suggested techniques for collecting the actual compliance behaviour data, which is an important contribution in this field, especially given the scarcity of such information.

5.3.2.2 Participatory Design

Some authors argue that policies that are designed primarily by managers and policy makers without involving the end-users have a great chance to be ineffective [2], [28], [3], [29], [30]. Beautement et al. [17] argued that policy design needs to take into account the impact that compliance with the policy will have on mental and physical workload of the end-users and that policy design is one of the most effective ways to reduce these impacts. Kirlappos et al. [3] argued that considering employees' attitudes and beliefs when formulating policies is critical to achieving alignment between information security and business plan. User involvement in the ISSP development could improve usability of the security measures and user awareness, which in turn could provide additional motivation for the users to comply [30]. In their discussion of the ISSP life cycle, Flowerday and Tuyikeze [2] emphasised the importance of user involvement throughout all stages of the ISSP life cycle.

Generally, there is an agreement that engaging users in the policy design process and ensuring that their constraints and demands are taken into account in the final policy product will have an impact on policy compliance [31], [3], [30], [14].

5.3.2.3 ISSP Life Cycle Process

Several process models of ISSP design and development have been proposed (e.g., Refs. [8], [13], [2], [9]). Although different proposed frameworks vary to some extent in their emphasis, articulation and granularity of the stages, general common phases are shown in Figure 5-4.

The ISSP life cycle begins with the risk assessment, which informs policy development and leads to policy implementation. Knapp et al. [13] also added two extra stages between policy development and implementation – policy approval and policy awareness and training. Policy awareness plays one of the central roles in the overall effectiveness of a security program (e.g., Ref. [32]) and it will be discussed in more detail later in this chapter. The policy monitoring phase is common among various models; however, authors differ in their

treatment of the scope of this stage. For example, Flowerday and Tuyikeze [2] included policy review as a subcomponent of policy monitoring, but other models consider it as a separate stage (e.g., Refs. [13], [9]). Multiple authors emphasised the importance of periodic policy review, update and cancellation of obsolete policies (e.g., Refs. [5], [13], [23]).

Different process models, while include similar stages, make emphasis on different influencing factors. For example, Knapp et al. [13] emphasised the influence of the internal factors (e.g., senior management, culture) and external factors (e.g., economic sector, industry standards) on the policy process model. Flowerday and Tuyikeze's [2] model emphasised the importance of management and employee engagement throughout all stages of the process.

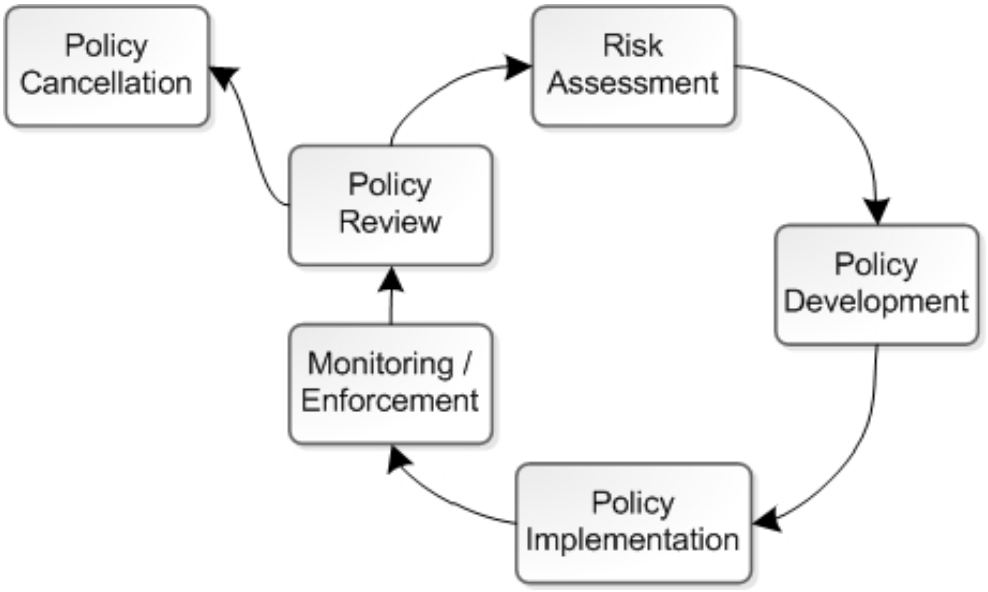

Figure 5-4: General Stages of the ISSP Life Cycle.

Overall, despite of the significant role that ISSPs play in information security management, there is still a scarcity of comprehensive work in this area [24]. Policy design, development and lifecycle management processes remain largely ad hoc in practice and understudied in the literature [2], [24], [27]. Very few specific techniques have been developed and validated in the literature, with a few notable exceptions (e.g., Ref. [27]).

5.4 COMPLIANCE WITH POLICY

Having a policy in place, however, does not guarantee IS and information protection. For the policies to be effective they need to be comprehensive to cover all aspects of information security and organization's members have to comply with them. Although, ISSPs have a great potential to safeguard organization's information security, they often are not as effective as they could be. Policy non-compliance, whether intentional or unintentional is a persistent issue in the workplace and remains a serious concern for organizational information security (e.g., Refs. [33], [34], [35], [36], [37], [38], [39], [40], [41]). As we discussed above, quality of the ISSPs themselves contribute to compliance or intention to comply [10], [16]. Lack of usability of security mechanisms also contributes to workarounds and errors [42], [43], [14].

5.4.1 Theories Used to Explain and Mitigate ISSP (Non-)Compliance

Several theories developed in social sciences have been applied in an effort to explain and mitigate ISSP non-compliance. Below is a list of most commonly used theories (in alphabetical order):

- **General deterrence theory** [44] emphasises the severity and certainty of sanctions in preventing unwanted behaviour.
- **Neutralization theory** [45] argues that people use different cognitive mechanisms to reduce psychological discomfort caused by their policy violation.
- **Protection motivation theory** [46], explains an individual's motivation to act as a function of threat appraisal (i.e., perceived vulnerability and severity of harm) and coping appraisal (self-efficacy – perceived ability to carry out the response action and response efficacy – perceived effectiveness of the response).
- **Situational crime prevention** [47] focuses on reducing the opportunities to commit undesirable behaviour by modifying the environment. It relies on five principles:
  - Increase effort necessary for the behaviour;
  - Increase risks;
  - Reduce rewards;
  - Reduce provocation; and
  - Remove excuses.
- **Social bond theory or social control theory** [48], [49] emphasises the role of various social bonds an individual has (e.g., social attachment, commitment to socially accepted goals, belief in social values, involvement in socially accepted activities) on conformity to rules and norms.
- **Social learning theory** [50] argues that individuals learn new behaviours by observing and imitating others and adjust their behaviours by observing which behaviours incur penalties.
- **Technology acceptance model** [51] is based on the theory of reasoned action and argues that perceived ease of use and perceived usefulness of technology (e.g., an application) influence the intention to use it.
- **Theory of planned behaviour** [52] states that an individual's behaviour depends on his/her intention to perform the behaviour, which in turn depends on the actor's attitude towards the behaviour, subjective norm and perceived behavioural control.

The database does not contain coding for specific theories, and therefore the frequency of each theory's occurrence in the database is not provided.

In their meta-analysis, Sommestad et al. [15] could not identify an unequivocally best theory to explain non-compliance; but they found that some theories performed worse than others – general deterrence theory and social control theory performed the worst in predicting compliance in the set of quantitative studies reviewed by Sommestad et al. [15].

5.4.2 Factors Associated with ISSP (Non-)Compliance

A large number of variables have been explored in relation to ISSP compliance; however, there is no consensus in the literature regarding its main contributing factors. For example, in their review of 29 quantitative studies

published on this topic, Sommestad et al. [15] identified over 60 different variables derived from seven different theories that were investigated in relation to compliance. Two thirds of these variables were included in a single study each, thus not allowing for effect size comparison/validation. When the same variable was included in several studies, Sommestad et al. [15] often found considerable variation across studies.

Our framework incorporates even more variables, some of which have been investigated with respect to policy compliance. Figure 5-5 shows the distribution of individual and organizational Performance-Shaping Factors (PSFs) associated with (non-)compliance within the database.

At the time of writing, approximately 23% of papers in the database discuss non-compliance as a threat vector (54 out of 230). Within this subset, 98% discuss individual performance-shaping factors and 85% discuss organizational factors.

The bars in Figure 5-5 show the percentage of papers that addressed certain factors in conjunction with non-compliance. Among the individual factors, "personal norms and values" have been discussed the most (69%), followed by "risk perception / risk appetite" (48%), "workload/stress" (43%), "Information Security Awareness" (39%) and "Information Security self-efficacy" (37%). Fewer sources explored the impact of personal characteristics (17%), cognitive dissonance neutralizations (9%) and no sources were associated with Human-Machine Interface (HMI) ergonomics/complexity issues with respect to (non-)compliance.

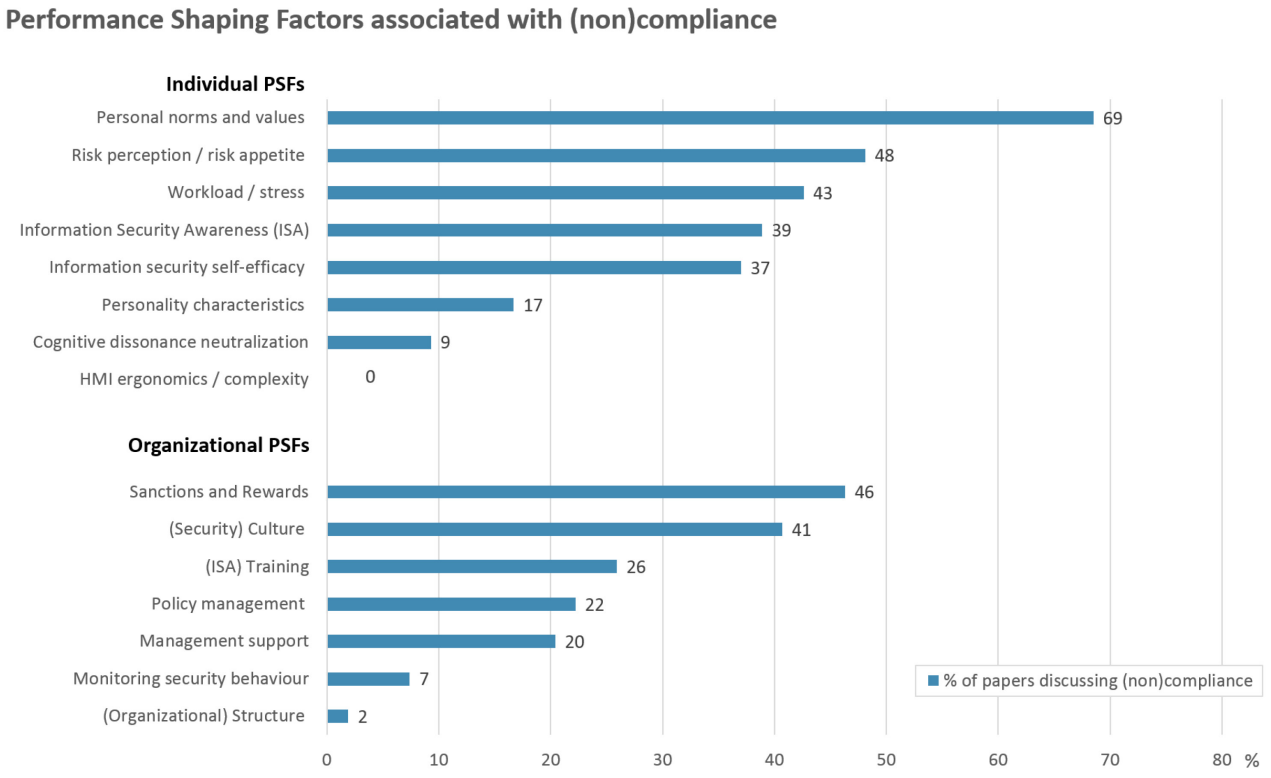

Figure 5-5: Distribution of Papers Addressing Specific Individual and Organizational Factors.

Among the organizational factors, the impact of "sanctions and rewards" and "(security) culture" on (non-)compliance has been discussed the most (46/41%), followed by "Information Security Awareness (ISA)

Training" (26%), "Policy management" (22%), "Management support" (20%) and "Monitoring security behaviour" (17%). And only 2% of the sources that dealt with (non-)compliance addressed the impact of organizational structure.

Below, we discuss these individual and organizational factors in more detail, except for policy management, which was already addressed above.

5.4.2.1 Individual Factors

Personal Norms and Values

Some authors argue that in order to be effective policies have to be aligned not only with the current organizational practices but also with employees' internal value systems and beliefs. People are more likely to comply with a policy that supports their values and are more likely to violate a policy that contradicts them (e.g., Refs. [53], [26], [31], [35]). Similarly, employees are more likely to comply with policies that they perceive to be legitimate, i.e., appropriate, desirable and just [26] and are more likely to violate policies and security measures that they perceive as excessive or unnecessary [17], [3].

Achieving closer alignment of policy with employees' values and legitimacy perceptions will likely require a combination of methods, including security awareness education and training (e.g., Ref. [54]), cultural initiatives (e.g., Ref. [6]), and will also require employees' involvement in the policy design process (e.g., Refs. [2], [3], [29], [30]) As we mentioned above, authors generally agree that customized policies adapted to the specific organizational environment and its employees are more likely to be effective (e.g., Ref. [5]).

Employees' organizational commitment, which is defined as the strength of employees' overall attachment to and identification with the organization has also been investigated with respect to ISSP compliance (e.g., Ref. [55]). Organizational commitment manifests itself in employees' motivation to behave in a way that meets organizational interests and goals (i.e., the stronger the commitment, the stronger the motivation). Not surprisingly, employees' organizational commitment has also been shown to have a positive relationship with their intention to comply with ISSPs [55], [56], [57]. Organizational commitment is related to and influenced by the overall organizational culture.

Risk Perception

One of the factors that has been linked to individuals' lax approach to information security that can also lead to policy non-compliance is people's risk perception [58], [59]. Liu et al. [59] argued that users often do not have clear information about the risks associated with policy-violating behaviour, which makes it difficult for them to adequately estimate risk. Users generally underestimate risk to themselves, their vulnerability and the probability of security breaches stemming from their actions or their possible adverse impacts [60], [55], [61]. Most commonly prescribed mitigation mechanism to address the overly optimistic perception of information security risks is information security training and awareness interventions (e.g., Ref. [61]) including contextual risk communication and awareness [59]. Risk perception and how it affects information security risky behaviours is discussed in greater detail in Chapter 4.

Workload and Stress

Quite often, security policies and procedures are not aligned well with current work practices, which either facilitates non-compliance (e.g., Refs. [29], [57]) or reduces productivity and results in opportunity loss

(e.g., Ref. [62]). Policies and procedures that require extra effort from the users increase users' workload and are perceived as costly work impediments [17], [31], [63], [16]. A potential mitigation of the increased workload due to security mechanisms could be to redesign the associated work tasks and processes. Unfortunately, not many authors addressed this issue. One of the exceptions, Bulgurcu et al. [16], suggested that to avoid this conflict, organizations should allocate a certain amount of employees' time to be used for fulfilling the ISSP requirements so that compliance efforts do not compete with daily job-related activities. However, the effectiveness of such mitigation is unclear. In addition, incentive systems that reward production goal achievement (over security) negatively impact security compliance [31], [19], [3], [29].

To avoid creating additional workload from security measures, Kirlappos et al. [29] argued that after deploying a security mechanism, organizations need to monitor and measure its impact on employees and business processes and adjust when necessary. This approach implies an iterative process to security measures' design and greatly depends on users' involvement in security effectiveness assessment.

Information Security Self-Efficacy

Self-efficacy refers to individual's beliefs about their own ability to complete tasks and achieve goals, and in the context of ISSP it translates to people's beliefs that they are able to perform the actions necessary to comply with the policy. Self-efficacy has been associated with employees' ISSP compliance or their intention to comply (e.g., Refs. [64], [55], [16]). Most common mitigation mechanisms discussed in relation to self-efficacy are education and training initiatives aimed at improving users' information security awareness, which is discussed below.

Security Awareness: Policy Awareness

One of the key prerequisites to policy compliance is policy awareness, which is also an integral aspect of the overall information security awareness. It is not surprising that awareness and understanding of policy has been shown to have a strong relationship with compliance, i.e., employees cannot be expected to intentionally comply with a policy if they are not aware of its existence or do not understand its content and what is required of them (e.g., Refs. [65], [32], [66], [67], [68], [1], [69]). According to Knapp and Ferrante [32], policy awareness construct includes not only employees' understanding of policies and consequences of violating them, but also continuous training and education initiatives. Knapp and Ferrante [32] showed that policy awareness had a significant relationship to the overall information security program effectiveness. In addition to dissemination initiatives, policy awareness and clear understanding of expectations arising from the policy depends on the clarity of the policy documents themselves. In their discourse analysis of a collection of information security policy documents, Stahl et al. [10] found a significant amount of ambiguity with respect to the content of the policy, often obscured in overly technical language, and delineation of responsibility and accountability for policy implementation. Consequently, Stahl et al. [10] recommended that policies should be written using accessible language and terminology to facilitate employees' policy understanding.

Even though policy awareness is a necessary precondition to compliance, quite often ISSP compliance studies do not account for participants' policy awareness. Pahnila et al. [69] argued that failure to control for the level of employees' knowledge of ISSPs may explain the inconsistency of research findings on non-compliance.

Security Awareness: Information Security Awareness (ISA)

Information Security Awareness (ISA) refers to individuals' awareness of potential information security risks and their understanding of information security best practices. ISA programs can cover a variety of different

topics, for example phishing, safe internet use, social engineering and password security in addition to disseminating information about the current ISSPs. ISA provides a foundation for employees' understanding of the rationale behind the ISSPs and it plays an important role in employees' security behaviour and their ISSP compliance [1], [34], [70], [71]. For example, Bulgurcu et al. [16] showed that ISA has a significant influence on attitude towards compliance and negatively influences the perceived work impediment of security controls, thus highlighting the importance of creating appropriate training and security awareness for organizations. Information security threat environment is constantly changing, and therefore ongoing long-term ISA interventions are more likely to be successful [13], [1]. We discuss ISA education and training in more detail in Section 5.4.2.2 (Organizational Factors).

Personality Traits

Individuals' personality traits have also been investigated in relation to ISSP compliance as well. For example, Johnston [20] found that the two meta-traits – stability and plasticity – formed from the big five personality traits model, had an impact on participants' intention to comply with the policies. The stability meta-trait, consisting of conscientiousness, agreeableness and emotional stability traits from the big five model, had a positive association with intention to comply, while plasticity meta-trait, consisting of openness and extraversion from the big five model, had a negative association with the intention to comply. These findings are consistent with other research in the information security field. For example, although not studying the ISSP compliance directly, McCormac et al. [72] also found that conscientiousness and agreeableness explained some of the differences in individuals' information security awareness scores. Shropshire et al. [73] found that the same two traits – conscientiousness and agreeableness – moderated the relationship between the individuals' behavioural intentions and their actual behaviour.

Age and Gender

The effect of age and gender on ISSP compliance generated somewhat mixed results. For example, Chua et al. [65] did not find a significant relationship between gender and compliance, but in Hovav and D'Arcy [74] study while gender did not show a significant effect in the US sample, it did in the Korean sample. McCormac et al. [72] found that female participants had a higher information security awareness score than males.

Chua et al., in 2018, found that age was positively associated with compliance, i.e., compliance increased with age; however, Hovav and D'Arcy [74] found the opposite relationship between age and compliance in their Korean sample. Hovav and D'Arcy [74] explained the observed differences between their US and Korean samples by cultural differences, and in McCormac et al. [72] study, the increase of individuals' information security awareness with age were partially explained by their risk-taking propensity.

Cognitive Dissonance Neutralization

Past research has suggested that formal and informal sanction as consequence of ISSP violations are less effective because people use neutralization techniques to rationalize their non-compliant behaviour [75].

Originally, neutralization techniques have been investigated in crime research to explain why people engage in criminal behaviours [45]. Sykes and Matza [45] defined different types of neutralization techniques that people use to rationalize their deviant behaviours: "the denial of responsibility", "the denial of injury", "the denial of the victim", "condemning the condemners", "appealing to higher loyalties". Over the time additional neutralization techniques have been proposed. For example, "the metaphor of the ledger" [76], "the defence of necessity" [77], "the claim of normalcy" and "the claim of entitlement" [78].

In Information Security literature, Siponen and Vance [75] proposed that "defence of necessity", "denial of injury" and "metaphor of the ledger" have a significant effect on employees' intention of ISSP violations whereas formal sanctions have no significant effect.

Barlow et al. [33] confirmed these findings only partially. Within the context of password sharing policies the authors found a significant effect regarding the "defence of necessity" but neither for the "denial of injury" nor the "metaphor of the ledger".

However, based on these finding Barlow et al. [33] postulated that security education, training and awareness programs should also focus on the mitigation of neutralization. Their work supported their assumption. Training approaches that focus on convincing employees not to use neutralization techniques have been found as strong as training approaches that focus on the communication of deterrent sanctions.

HMI Ergonomics and Complexity

At the time of writing, no sources in the database were associated with Human-Machine Interface (HMI) ergonomics/complexity with ISSP (non-)compliance. This could be the result of unintentional omission of this literature from the database or the lack of such literature, i.e., lack of attention to HMI ergonomics and complexity in addressing ISSP non-compliance issues. In any case, an explicit search for research papers addressing these factors is required.

5.4.2.2 Organizational Factors

Sanctions and Rewards

Sanctions and rewards are common mechanisms of behaviour influence, however their effectiveness in influencing ISSP compliance has accumulated mixed evidence. While some authors showed that sanctions have a significant effect on actual compliance (e.g., Ref. [79]) or intention to comply (e.g., Ref. [16]), others showed the opposite (e.g., Refs. [80], [81]).

Guo and Yuan [82] differentiated sanctions into organizational (formal, external) sanctions, workgroup (informal, external) and personal self-sanctions (internal) and analysed their effect on ISSP violations. Their findings suggested that group and personal self-sanctions have a negative effect on employees' intention to violate ISSPs. Additionally, workgroup sanction had a significant impact on personal self-sanction. In contrast, organizational sanctions have no direct effect on employees' intention to violate ISSPs. This effect is consistent with other studies in IS literature [83], [75], [84]. However, the findings suggested an indirect effect on employees' intention to violate ISSPs through workgroup sanctions and personal self-sanction. Regarding information security education and training the authors propose that an "influencing" strategy may be more effective than an "enforcing" strategy.

Regarding the influence of rewards on information security behaviour, the evidence is also contradictory. For example, in their laboratory study, Liu et al. [59] showed that monetary incentives were effective in encouraging risk-avoiding behaviours in freshmen students; however, the generalizability of these results to workplace behaviour in the real world remains to be shown. On the other hand, Parsons et al. [85] found that rewards did not contribute to effective information security decision making, and Pahnila et al. [79] and Pahnila et al. [80] showed that rewards did not have a significant effect on compliance with ISSPs. In their review, Sommestad et al. [15] concluded that sanctions and rewards were poor predictors of compliance.

Security Culture

Many researchers in the information security domain emphasised the importance of security culture for the overall information security (e.g., Refs. [86], [87], [85]). In their CERT guide to insider threats, Cappelli et al. [6] argued that training programs can create a security culture in organizations, which in turn will foster security behaviour and D'Arcy and Greene [21] showed the link between security culture and ISSP compliance. Da Veiga and Martins [88] also showed a link between security culture and compliance; however, in their model compliance contributes to security culture, as opposed to being its product (see also Ref. [89]). Therefore, there seems to be a feedback loop between security culture and compliance with one reinforcing the other.

Security culture refers to a subculture of a more general organizational culture [90], [27] and consists of shared assumptions and beliefs within the organization that are traded over time and affect information security [91]. Furthermore, Da Veiga, and Martins [92] argued that security culture is not necessarily uniform throughout the organization, and that there could be different security subcultures in different offices (geographical locations) or employee groups, e.g., different ethnic or age groups of employees could have different security-related assumptions and beliefs.

There is no agreement in the literature on the dimensions of security culture – Nasir et al. [93] identified 26 different dimensions among the models they reviewed, few of which were shared among the models. Security policy was the most common dimension identified by Nasir et al. [93], followed by change management, leadership and governance, user security management, information asset management and trust.

Building an organization's security culture has been often suggested as one of the mechanisms to facilitate overall security within the organization (e.g., Ref. [94]). Although the notion of security culture has received considerable attention in the information security literature, the field of information security culture research still lacks theoretical and methodological maturity (see Refs. [91], [93] for reviews and critique).

ISA Education and Training

Many different ISA training approaches have been proposed (e.g., see Refs. [1], [95] for a review). For example, to replace the commonly used top-down rote mode of training, Albrechtsen and Hovden [54] developed and tested a participatory approach to ISA training, in which participants are engaged in peer group discussions on the topics of security. Game-based (e.g., Refs. [96], [97]) and video-based (e.g., Ref. [97]) approached to ISA training delivery have also been explored. Security exercises, such as an unannounced phishing exercise, have been used to raise awareness about some aspects of security (e.g., Ref. [98]). Comparing different delivery methods, Abawajy [97] concluded that a mixed methods approach to ISA training could be more effective.

Drawing on cognitive and cultural biases literature, Tsohou et al. [99] made a set of recommendations for planning, developing, and implementing ISA programs that take into consideration potential cognitive and cultural biases of the target audience. For example, Tsohou et al. [99] recommended taking the time and effort to identify their own and audiences' individual cultural biases, taking this information into account when forming separate target groups, and designing bespoke communication strategies for different audiences that take into account both cultural biases and characteristics of human information processing. However, the effectiveness of these recommendations remains to be empirically validated. Bauer et al. [1] reviewed different structural and communication design recommendations for ISA programs, including media richness, intervention customization both to the organizational environment and individual needs of participants, ISA program quality control, and user involvement. Based on the comparative case study of three organizations, Bauer et al. [1] argued that context-sensitive ISA designs that use a comprehensive mix of delivery strategies and that are custom-tailored to different target audiences within the same organization are more likely to be effective. In

addition, Karjalainen et al. [100] showed that effectiveness of training and awareness interventions is context-dependant and it is contingent on their fit with the cultural learning paradigms of the organization.

Overall, even though there is a number of different recommendations for ISA training design and delivery, there is no commonly accepted agreement about how to effectively design ISA programs coupled with little validation of the proposed methods [1], [100]. One consistent theme that emerges from the literature is that ISA programs need to be custom-designed for the specific organization context and audience.

Management Support

Another critical aspect of the overall security culture and ISSP development and implementation that has been emphasised repeatedly is the support and involvement of the organization's top-level management in the security initiatives and policy (e.g., Refs. [2], [101], [102], [13], [87], [21], [86]). Flowerday and Tuyikeze [2] surveyed information security professionals in the USA and the UK on the importance of different ISSP lifecycle processes and found that management support was the second most important process after risk assessment. According to Kraemer et al. [103] findings, management plays an important role in many aspects of information security within an organizations, including determining which assets will be protected, how ISSPs are developed, resource allocation to information security initiatives and the overall priority given to these initiatives within the organization. Top-management participation in security initiatives is a crucial factor not only for policy development and implementation, but also for the development of a security culture within the organization [13], [21], [87]. For example, Hu et al. [87] found that the top-level management participation in security initiatives influences employees' attitude towards ISSPs and their intention to comply with them directly and indirectly, i.e., through the overall organizational culture, on which management has a significant influence.

Compliance Monitoring and Assessment

As we discussed in the policy management section above, policy compliance monitoring is one of the key processes in the overall ISSP lifecycle (e.g., Ref. [13]). Effective security management requires assessment of the impact of ISSP on employees' behaviour [28]. Such assessment depends on the ability of the organization to monitor the behaviour of the employees to determine if they are following the policy, and it should be coupled with enforcement [13]. Organizations often rely on technical means for behaviour monitoring, e.g., using system logs and transaction records. However, not all aspects of ISSP could be effectively monitored [94]. Beautement et al. [17] pointed out that the lack of continuous policy compliance monitoring leaves room for employees to choose to whether comply with the policies or not depending on their individual goals, perceptions and attitudes. Furthermore, Beautement et al. [17] argued that expanding more effort into monitoring can increase the likelihood of compliance decision on the part of the employees, but this influence is limited by the organization's ability to monitor the behaviour, can become quite expensive quite fast, and it needs to be coupled with formal sanctions, which, as we discussed above, are often not reliable mechanisms for changing behaviour (e.g., Refs. [80], [81]).

In addition, continuous monitoring may be seen by some employees as objectionable, implying a presumption that everyone is "potentially guilty", which can lead to counterproductive behaviours, such as absenteeism [104] and can negatively impact the overall organizational culture. Workman [104] found that a number of factors could improve employees' attitude towards monitoring, such as perception of higher vulnerability to security threats, higher self-efficacy, greater perceptions of organization security efficacy, and greater levels of trust.

The role of monitoring in ensuring compliance is not clear-cut. For example, in their survey of security professionals, Flowerday and Tuyikeze [2] found that although policy compliance was seen as one the most

important aspects of policy development and implementation, policy monitoring was seen as the least important among other ISSP lifecycle processes. Several authors advocated for a different approach to encouraging and ensuring compliance, one that relies less on monitoring and sanctions and more on building a security culture within the organization, formal and informal norms that motivate employees to behave securely (e.g., Refs. [3], [94]). Organizations may still choose to implement some degree of monitoring, such as identifying malicious behaviour (e.g., Ref. [105]); however, not as a main motivator for non-malicious employees [3], [94].

Organizational Structure

Very few papers directly evaluated the impact of organizational structure on policy compliance. Connolly et al. [71] is one of the few exceptions, they found that flat organizational structure tends to facilitate information security through its increased accessibility and approachability of management, which improves visibility for information security and increases likelihood of employees expressing their concerns to management. This provides a user perspective to managers and policy makers and can facilitate improvement of current processes and rules.

5.5 EFFECTIVENESS OF MITIGATION MECHANISMS

Within the subset of papers dealing with (non-)compliance, almost all of them (96%) suggested (and, in some cases, evaluated) potentially relevant mitigation mechanism(s). Figure 5-6 shows the percentage of papers discussing a particular mitigation mechanism (blue bars) together with the assessment of its effectiveness shown with different colours in the bar underneath the blue bar: green – effective, orange – somewhat effective, yellow – effectiveness is unknown.

The two most frequently mentioned mitigation mechanisms in the (non-)compliance subset are “cyber security training/education” (50%) and “compliance assessment” (48%), while the least frequently mentioned mechanisms were “task/process redesign” (7%) and “ISA/competency assessment” (13%).

Examining the effectiveness of various mitigation mechanisms discussed with respect to (non-)compliance, the striking observation is that the majority of sources (67% – 100%) did not report on the actual effectiveness of the proposed mechanisms (see Figure 5-6) with less than 20% of the papers in each category reporting that the mitigation mechanism was effective. This observation implies that recommendations are made in the literature, however they are often not evaluated, or the evaluation is inconclusive. These findings leave a high degree of uncertainty regarding the actual effectiveness of mitigation mechanisms. Thus, more work to test and evaluate various mitigation mechanisms is needed.

5.6 CONCLUSION

Information security policies are procedural and managerial controls that organizations use to enhance their computer and information security. In this chapter we reviewed the most frequently discussed individual and organizational factors associated with policy management and its effectiveness in the literature, i.e., compliance. Based on the information collected in our knowledge base at the time of writing, when investigating ISSPs and compliance the most frequently discussed individual factors include individual norms and values of the employees, their risk perception, workload, and information security awareness. The most frequently discussed organizational factors with respect to non-compliance are organizational sanctions and rewards, security culture, information security training and policy management.

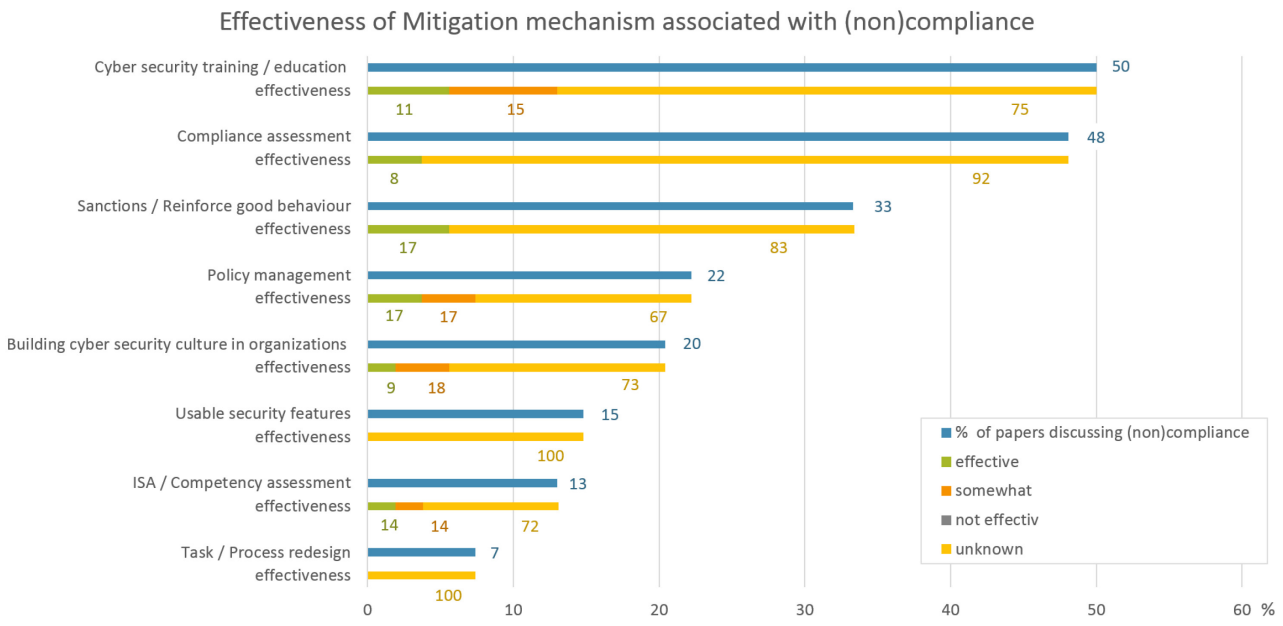

Figure 5-6: Distribution of Papers Addressing Specific Mitigation Mechanisms and Their Effectiveness with Respect to (Non-)Compliance.

Overall, there is a growing body of research addressing various aspects of ISSP management and compliance. While some of these factors have received considerable attention in the literature, others have not. For example, at the time of writing, the knowledge base contains no or very limited sources discussing the following:

- Technical mitigation mechanisms to address compliance issues;
- HMI ergonomics and HMI complexity issues with respect to ISSP compliance;
- Cognitive neutralization strategies that people use to justify non-compliance;
- The impact of organizational structure;
- Mitigating non-compliance with task and process redesign; and
- Assessment of information security competency.

More research in these areas would undoubtedly improve our knowledge and understanding of effective ISSP design and management.

Another significant gap in the current version of the knowledge base is the lack of information regarding effectiveness of various mitigation mechanisms. And, therefore, more research is required to investigate effectiveness of various mitigation mechanisms.

5.6.1 Methodological Challenges in the Literature

A significant number of studies on ISSP compliance focused on assessing behavioural intention rather than measuring the actual behaviour (e.g., Ref. [21]). Even though there is considerable evidence that supports the

link between intention and behaviour (e.g., Refs. [79], [106], [15]), there has been some contradictory evidence, e.g., Gerber et al. [19] found that intention to comply was a poor predictor of actual security compliance. While acknowledging the challenges in measuring the actual compliance behaviour, Crossler et al. [107] argued against relying on measuring intentions instead of the actual behaviour pointing out that intentions do not always lead to actions and that intention without action can lead to a security breach.

Actual compliance with ISSPs is rarely studied directly [15], and when it is studied it is most often done through a self-reported survey method where participants are asked to indicate their degree of agreement with statements like "I comply with information security policies". The degree of correspondence between individuals' responses to questions like this and their actual behaviour is not entirely clear. On the one hand, there are usually a number of different policies that employees are required to follow, and they may comply with some but not the others; and on the other hand, participants' might not be aware of all the policies and their specific behavioural expectations. However, developing and collecting behavioural measures of compliance is a challenging task. Some researchers used in-depth interview method to identify specific non-compliance behaviours and the reasons behind them (e.g., Refs. [3], [29], [27]). In addition to interviews, Kolkowska et al. [27] used the observation method to collect data about non-compliant behaviours. Crossler et al. [107] argued that measuring the actual behaviour remains to be one of the biggest challenges in the field; it should be the ultimate goal for information security research. The behavioural information security field needs to continue developing behavioural measures of actual compliance.

5.6.2 Knowledge Base Limitations

It is worth noting that the knowledge base created and used for this analysis is not exhaustive. We acknowledge that some relevant sources might have been not included in the knowledge base. The results reported here are based on the state of the knowledge base at the time of writing, and therefore do not include more recent scientific findings. New research is produced constantly, and for the knowledge base to remain current a continuous effort is required to keep it up to date.

5.7 REFERENCES

[1] Bauer, S., Bernroider, E.W., and Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. Computers & Security 68:145-159.

[2] Flowerday, S.V., and Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. Computers & Security 61:169-183.

[3] Kirlappos, I., Beautement, A., and Sasse, M.A. (2013). "Comply or die" is dead: Long live security-aware principal agents. In: A. Adams, M. Brenner, and M. Smith (Eds.), Financial Cryptography and Data Security: FC 2013 Workshops, 70-82. Berlin and Heidelberg: Springer.

[4] Doherty, N.F., and Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: An exploratory analysis. Information Resources Management Journal 18(4):21.

[5] Andress, J., and Leary, M. (2017). Chapter 4 – Why information security policies? In: J. Andress and M. Leary (Eds.), Building a Practical Information Security Program, 63-75. Syngress: Cambridge, MA, USA.

[6] Cappelli, D., Moore, A., and Trzeciak, R. (2012). The CERT Guide to Insider Threat. Toronto, Canada: Addison-Wesley.

[7] Höne, K., and Eloff, J.H.P. (2002). What makes an effective information security policy? Network Security 2002(6):3.

[8] Baskerville, R., and Siponen, M. (2002). An information security meta-policy for emergent organizations. Logistics Information Management 15(5/6):337-346.

[9] Rees, J., Bandyopadhyay, S., and Spafford, E.H. (2003). PFIRES: A policy framework for information security. Communications of the ACM 46(7):101-106.

[10] Stahl, B.C., Doherty, N.F., and Shaw, M. (2012). Information security policies in the UK healthcare sector: A critical evaluation. Information Systems Journal 22(1):77-94.

[11] Vieane, A.F.G., Gutzwiller, R., Mancuso, V., Sawyer, B., and Wickens, C. (2016). Addressing human factors gaps in cyber defense. In: Proceedings of the Human Factors and Ergonomics Society 2016 Annual Meeting.

[12] Pfleeger, S.L., and Caputo, D.D. (2012). Leveraging behavioral science to mitigate cyber security risk. Computers & Security 31(4):597-611.

[13] Knapp, K.J., Morris, R.F., Marshall, T. E., and Byrd, T.A. (2009). Information security policy: An organizational-level process model. Computers & Security 28(7):493-508.

[14] Adams, A., and Sasse, M.A. (1999). Users are not the enemy. Communications of the ACM 42(2):40-46.

[15] Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. (2014). Variables influencing information security policy compliance. Information Management & Computer Security 22(1):42-75.

[16] Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly 34(3):33.

[17] Beautement, A., Sasse, M.A., and Wonham, M. (2008). The compliance budget: Managing security behaviour in organizations. In: Proceedings of the 2008 New Security Paradigms Workshop. ACM.

[18] Coles-Kemp, L., and Theoharidou, M. (2010). Insider threat and information security management. In: C. Probst, J. Hunker, M. Bishop and D. Gollmann (Eds.), Insider Threats in Cyber Security, 45-71, Springer: New York, NY, USA.

[19] Gerber, N., McDermott, R., Volkamer, M., and Vogt, J. (2016). Understanding information security compliance – Why goal setting and rewards might be a bad idea. In: Proceedings of the 10th International Symposium on Human Aspects of Information Security & Assurance.

[20] Johnston, A.C.W.M., McBride, M., and Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. European Journal of Information Systems 25(3):231-251.

[21] D'Arcy, J., and Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. Information Management & Computer Security 22(5):474-489.

[22] Safa, N.S., Maple, C., Watson, T., and Von Solms, R. (2018). Motivation and opportunity-based model to reduce information security insider threats in organisations. Journal of Information Security and Applications 40:247-257.

[23] Höne, K., and Eloff, J. (2002). Information security policy – What do international information security standards say? Computers & Security 21(5):402-409.

[24] Karlsson, F., Hedström, K., and Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. Computers & Security 67:267-279.

[25] Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Quality and fairness of an information security policy as antecedents of employees' security engagement in the workplace: An empirical investigation. In: Proceedings of the 43rd Hawaii International Conference on System Sciences, Honolulu, HI. IEEE.

[26] Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Information & Management 48:7.

[27] Kolkowska, E., Karlsson, F., and Hedström, K. (2017). Towards analysing the rationale of information security non-compliance: Devising a value-based compliance analysis method. The Journal of Strategic Information Systems 26(1):39-57.

[28] Beautement, A.; Becker, I.; Parkin, S.; Krol, K.; and Sasse, M.A. (2016). Productive security: A scalable methodology for analysing employee security behaviours. In: Proceedings of the 12th Symposium on Usable Privacy and Security, Denver, CO.

[29] Kirlappos, I., Parkin, S., and Sasse, M.A. (2014). Learning from "shadow security": Why understanding non-compliance provides the basis for effective security. In: Proceedings of Workshop on Usable Security 2014, U.o.C., London, Editor.

[30] Kirlappos, I., and Sasse, M.A. (2014). What usable security really means: Trusting and engaging users. In: T. Tryfonas and I. Askoxylakis (Eds.), Human Aspects of Information Security, Privacy, and Trust, 69-78. Springer International Publishing: Switzerland.

[31] Albrechtsen, E. (2007). A qualitative study of users' view on information security. Computers & Security 26:14.

[32] Knapp, K.J., and Ferrante, C.J. (2012). Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organizations. Journal of Management Policy and Practice 13(5):16.

[33] Barlow, J.B., Warkentin, M., Ormond, D., and Dennis, A.R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. Computers & Security (in press).

[34] Bauer, S., and Bernroider, E.W. (2017). From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. The DATA BASE for Advances in Information Systems 48(3):44-68.

[35] Cox, J. (2012). Information systems user security: A structured model of the knowing-doing gap. Computers in Human Behavior 28:10.

[36] Herath, T., and Rao, H.R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems 47:12.

[37] Matthews, G., Davies, D.R., Westerman, S.J., and Stammers, R.B. (2000). Human Performance: Cognition, Stress and Individual Differences. Hove, UK: Psychology Press.

[38] Nash, K.S., and Greenwood, D. (2008). The global state of information security. CIO Magazine, 6 December 2008.

[39] Siponen, M., Mahmood, M.A., and Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & Management 51(2):217-224.

[40] Williams, P.A.H. (2008). In a 'trusting' environment, everyone is responsible for information security. Information Security Technical Report 13(4):9.

[41] Willison, R., and Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. MIS Quarterly 37(1):21.

[42] Molin, E., Meeuwisse, K., Pieters, W., and Chorus, C. (2018). Secure or usable computers? Revealing employees' perceptions and trade-offs by means of a discrete choice experiment. Computers & Security 77:65-78.

[43] Bartsch, S., and Sasse, M.A. (2013). How users bypass access control and why: The impact of authorization problems on individuals and organization. In: Proceedings of the 21st European Conference on Information Systems, Utrecht, the Netherlands.

[44] Straub, D.W., and Welke, R.J. (1998). Coping with systems risk: Security planning models for management decision making. MIS Quarterly 22(2):441-469.

[45] Sykes, G., and Matza, D. (1957). Techniques of neutralization: A theory of delinquency. American Sociological Review 22:664-670.

[46] Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. Journal of Psychology 91(1):93-114.

[47] Clarke, R. (1980). Situational crime prevention: Theory and practice. British Journal of Criminology 20:136-137

[48] Nye, F.I. (1958). Family Relationships and Delinquent Behavior. Oxford, UK: Wiley.

[49] Hirschi, T. (1969). Causes of Delinquency. Berkeley, CA: University of California Press.

[50] Bandura, A. (1977). Social Learning Theory. Oxford, UK: Prentice-Hall.

[51] Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MISQ 13(3):319-339.

[52] Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes 50(2):179-211.

[53] Hedström, K., Kolkowska, E., Karlsson, F., and Allen, J.P. (2011). Value conflicts for information security management. Journal of Strategic Information Systems 20:12.

[54] Albrechtsen, E., and Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection: An intervention study. Computers & Security 29:14.

[55] Herath, T., and Rao, H.R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems 18:21.

[56] Safa, N.S., and Von Solms, R. (2016). An information security knowledge sharing model in organizations. Computers in Human Behavior 57:442-451.

[57] Sharma, S., and Warkentin, M. (2019). Do I really belong? Impact of employment status on information security policy compliance. Computers & Security, 87, 1-12.

[58] Ostowan, B. (2006). Towards a framework to measure user compliance with computer security practices. Department of Computer and Systems Sciences, Stockholm University, Sweden.

[59] Liu, D., Wang, X., and Camp, L.J. (2009). Mitigating inadvertent insider threats with incentives. In: R. Dingledine and P. Golle (Eds.), Financial Cryptography and Data Security: 13th International Conference, 1-16. Berlin, Germany: Springer.

[60] Albrechtsen, E., and Hovden, J. (2009). The information security digital divide between information security managers and users. Computers & Security 28:15.

[61] Rhee, H.-S., Ryu, Y.U., and Kim, C.-T. (2012). Unrealistic optimism on information security management. Computers & Security 31:12.

[62] Sasse, M.A. (2014). "Technology should be smarter than this!" A vision for overcoming the great authentication fatigue. In: W. Jonker and M. Petković (Eds.), Secure Data Management, 33-36. Springer International Publishing: Switzerland.

[63] Adams, A., and Sasse, M.A. (1999). Users are not the enemy. Communications of the ACM 42(12): 40-46.

[64] Chen, X., Wu, D., Chen, L., and Teng, J.K.L. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. Information & Management 55(8):1049-1060.

[65] Chua, H.N., Wong, S.F., Low, Y.C., and Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. Telematics and Informatics, 35(6), 1770-1780.

[66] Dinev, T., and Hu, Q. (2007). The centrality of awareness in the formation of user behavioral technologies. Journal of the Association for Information Systems 8(7):386-408.

[67] D'Arcy, J., Hovav, A., and Galletta, D. (2008). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, Articles in Advance, 2008, p. 20, https://pubsonline.informs.org/doi/10.1287/isre.1070.0160.

[68] Al-Omari, A., El-Gayar, O., and Deokar, A. (2012). Security policy compliance: User acceptance perspective. In: Proceedings of the 45th Hawaii International Conference on System Sciences, Maui, HI.

[69] Pahnila, S., Karjalainen, M., and Siponen, M. (2013). Information security behavior: Towards multi-stage models. In: Proceedings of the Pacific Asia Conference on Information Systems (PACIS) 2013, Jeju Island, Korea.

[70] Bauer, S., and Bernroider, E.W. (2015). The effects of awareness programs on information security in banks: The roles of protection motivation and monitoring. In: Proceedings of the 3rd. International Conference on Human Aspects of Information Security, Privacy, and Trust (HAS 2015).

[71] Connolly, L.Y., Lang, M., Gathegi, J., and Tygar, D.J. (2017). Organisational culture, procedural countermeasures, and employee security behaviour. Information and Computer Security 25(2):118-136.

[72] McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., and Pattinson, M. (2017). Individual differences and information security awareness. Computers in Human Behavior 69:151-156.

[73] Shropshire, J., Warkentin, M., and Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. Computers & Security 49:177-191.

[74] Hovav, A., and D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. Information & Management 49(2):99-110.

[75] Siponen, M., and Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly 34(3):29.

[76] Klockars, C. (1974). The Professional Fence. New York, NY: Free Press.

[77] Minor, W. (1981). Techniques of neutralization: A reconceptualization and empirical examination. Journal of Research in Crime and Delinquency 2:295-318.

[78] Coleman, J.W. (1985). The Criminal Elite: The Sociology of White-Collar Crime. New York, NY: St. Martin's Press.

[79] Pahnila, S., Siponen, M., and Mahmood, A. (2007). Which factors explain employees' adherence to information security policies? An empirical study. In: Proceedings of the Pacific Asia Conference on Information Systems (PACIS) 2007.

[80] Pahnila, S., Siponen, M., and Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In: Proceedings of the 40th Hawaii International Conference on System Sciences.

[81] Hu, Q., Xu, Z., Dinev, T., and Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? Communications of the ACM 54(6):7.

[82] Guo, K.H., and Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. Information & Management 49:7.

[83] D'Arcy, J., and Hovav, A. (2009). Does one size fit all? Examining the differential effects of is security countermeasures. Journal of Business Ethics 89:15.

[84] Guo, K.H., Yuan, Y., Archer, N.P., and Connelly, C. (2011). Understanding non-malicious security violations in the workplace: A composite behavior model. Journal of Management Information Systems 28(2):35.

[85] Parsons, K.M., Young, E., Butavicius, M.A., McCormac, A., Pattinson, M.R., and Jerram, C. (2015). The influence of organizational information security culture on information security decision making. Journal of Cognitive Engineering and Decision Making 9(2):117-129.

[86] Kraemer, S., and Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. Applied Ergonomics 38:12.

[87] Hu, Q., Dinev, T., Hart, P., and Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences Journal 43(4):45.

[88] Da Veiga, A., and Martins, N. (2015). An information security culture model validated with structural equation modelling. In: Proceedings of the 9th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015).

[89] Da Veiga, A., and Eloff, J.H.P. (2010). A framework and assessment instrument for information security culture. Computers & Security 29(2):196-207.

[90] Schein, E.H. (1996). Defining organizational culture. In: J.M. Shafritz and J.S. Ott (Eds.), Classics of Organizational Theory, New York, N.Y.: Harcourt Brace College Publishers.

[91] Karlsson, F., Astrom, J., and Karlsson, M. (2015). Information security culture – State-of-the-art review between 2000 and 2013. Information and Computer Security 23(3):246-285.

[92] Da Veiga, A., and Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. Computers & Security 70:72-94.

[93] Nasir, A., Arshah, R.A., Hamid, M.R.A., and Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. Journal of Information Security and Applications 44:12-22.

[94] Vroom, C., and Von Solms, R. (2004). Towards information security behavioural compliance. Computers & Security 23(3):191-198.

[95] Karjalainen, M., and Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. Journal of the Association for Information 12(8):39.

[96] Cone, B.D., Irvine, C.E., Thompson, M.F., and Nguyen, T.D. (2007). A video game for cyber security training and awareness. Computers & Security 26:10.

[97] Abawajy, J. (2012). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 237-248.

[98] Dodge, R.C., Carver, C., and Ferguson, A.J. (2007). Phishing for user security awareness. Computers & Security 26:8.

[99] Tsohou, A., Karyda, M., and Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. Computers & Security 52:128-141.

[100] Karjalainen, M., Siponen, M., Puhakainen, P., and Sarker, S. (2013). One size does not fit all: Different cultures require different information systems security interventions. In: Proceedings of the Pacific Asia Conference on Information Systems (PACIS) 2013.

[101] Kadam, A.W. (2007). Information security policy development and implementation. Information Systems Security 16(5):246-256.

[102] Knapp, K.J., Marshall, T.E., Rainer, R.K. Jr., and Ford, F.N. (2006). Information security: Management's effect on culture and policy. Information Management & Computer Security 14(1):24-36.

[103] Kraemer, S., Carayon, P., and Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & Security 28(7):12.

[104] Workman, M. (2009). A field study of corporate employee monitoring: Attitudes, absenteeism, and the moderating influences of procedural justice perceptions. Information and Organization 19(4): 218-232.

[105] Caputo, D.D., and Stephens, G.D. (2009). Detecting insider theft of trade secrets. IEEE Security and Privacy 7(6):14-21.

[106] Siponen, M., Pahnila, S., and Mahmood, M.A. (2010). Compliance with information security policies: An empirical investigation. Computer 43(2):64-71.

[107] Crossler, R.E., Johnston, A.C., Lowry, P.B., and Hu, Q. Warkentin, M.; Baskerville, R. (2013). Future directions for behavioral information security research. Computers & Security 32:12.

Chapter 6 – RECRUITMENT, SELECTION AND TRAINING OF IT/CYBER PERSONNEL

Peter Svenmarck
FOI
SWEDEN

6.1 INTRODUCTION

A large number of skilled cyber security personnel is required to meet the increasing demands for cyber security. Cyber security personnel perform a diverse set of roles, such as system administrator, information security specialist, intrusion detection analyst, and Computer Emergency Response Team (CERT). All these personnel categories contribute to configuration and management of information systems to assure information confidentiality, integrity, and availability. Figure 6-1 shows how the framework captures recruitment, selection, training and retention of IT/Cyber personnel for mitigation of cyber threats. The following sections describe studies that investigate the best ways to recruit, select, train, and retain IT personnel for cyber security.

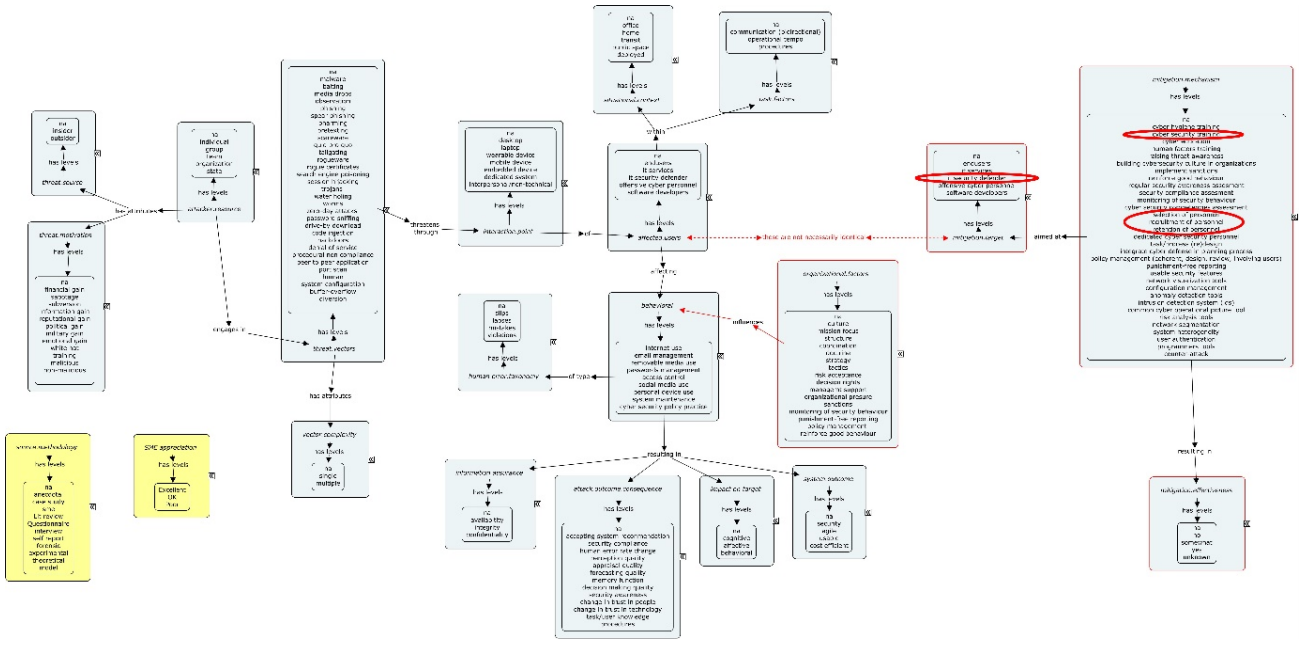

Figure 6-1: Recruitment, Selection, Training and Retention of IT/Cyber Personnel Is Captured in the Framework. See Annex A, Figure A-1 for full-size non-annotated image.

6.2 RECRUITMENT AND SELECTION

Cyber security competitions are one way to increase interest for cyber security. Participants in these competitions commonly form teams that attack or defend a preconfigured IT system. Since some personality traits are especially important for cyber security personnel, cyber security competitions should try to encourage

these personality traits. For example, Bashir, Wee, Memon, and Guo [1] investigated participants' personality traits, vocational interests, cultural orientation, as well as decision-making and attachment style during the competition Cybersecurity Awareness Week. Personality traits that had a positive effect on participants' interest to seek future employment within cyber security were investigative interests, rational decision-making style, and higher self-efficacy. Cyber security competitions should therefore encourage these personality traits.

While all cyber security personnel should ideally have a computer science education, the demand for cyber security personnel currently exceed the number of students that graduate in computer science. Several studies therefore investigate general aptitude assessment for cyber security personnel that is independent of educational background to increase the recruitment base. Morris and Waage [2] describe some options for aptitude assessment, such as:

- **Armed Services Vocational Aptitude Battery – Cyber Test (CT)** (formerly the Information/Communication Technology Literacy (ICTL) test) measures abilities in verbal, non-verbal, and mathematical reasoning, problem identification, creativity, oral and written comprehension, as well as perception [3].
- **Cyber Aptitude and Talent Assessment (CATA)** that classifies cyber work roles in the draft framework from the National Initiative for Cybersecurity Education (NICE) [4]. CATA categorize the NICE work roles along two dimensions of cognitive demand [5], [6]. The first dimension ranges from operations in real-time to exhaustive operations where completeness is more important than time constraints. The second dimension ranges from initiating actions in anticipation of potential vulnerabilities to responding to others' actions. Saner et al. [6] describe 43 questions for assessing work role requirements. CATA is still in development, but some important cyber work roles mostly correspond to the two cognitive dimensions [7].
- **Cyber Talent Targeting Methodology (CTI)** focuses on identifying and locating talented personnel. Selected candidates participate in a one-week program that includes psychological tests, problem solving, cyber competitions, and interviews. A review board approves suitable candidates.
- **Defence Cyber Aptitude Test (DCAT)** focuses on identifying applicants' ability rather than existing skills [8]. Keeley, Parkes, and Pons [9] describe how major role requirements for cyber security personnel are intellectual skills, resiliency, tenaciousness, independency, self-confidence, communication skills, and proactivity, while applicants may obtain IT knowledge later. DCAT consists of several scales for personality traits, such as adaptability and stress tolerance, as well as abilities in problem solving, numerical and verbal reasoning, logical reasoning, and error detection in highly detailed information.

CT/ICTL is the only one of these options for aptitude assessment that has been used extensively [2]. CT/ICTL is a good predictor of training success in many cyber work roles [10]. However, Morris and Waage [2] consider CATA as the best future option for aptitude assessment.

6.3 EDUCATION AND TRAINING

Cyber security personnel need adequate education and training for their work roles. However, there is currently a lack of systematic scientific research on how to perform such education and training. Studies may report course programs in cyber security and students' reactions, but seldom any empirical results of how acquired knowledge corresponds to actual requirements. A good example of more systematic research is Martini and Choo [11] that describe how the course program relates to crime prevention theories based on deterrence and required skills for

cyber security personnel. Deterrence against crime may increase perceived effort and risk, decrease rewards and crime inducing factors, and stimulate correct behaviour [12]. The authors describe that sixteen of thirty-one competency areas in the NICE framework by Newhouse et al. [4] relate to crime prevention. A cyber security exercise was useful for transferring theoretical knowledge to practical skills in crime prevention.

Intrusion detection is an important part of cyber security to detect malicious activity. Intrusion detection requires significant skill due to large volumes of network traffic, many information sources, that it is difficult to distinguish malicious activity from legitimate activity, incomplete information about attackers' actions, continuously evolving situation, and reluctance to disturb the network [13]. Goodall, Lutters, and Komlodi [14] describe how intrusion detection requires both foundational knowledge and situated expertise about the specific network. Foundational knowledge includes network architectures, protocols, security, and typical attack patterns that can be attained during education and training. The situated expertise, on the other hand, is based on deep knowledge of normal network traffic and develops over time when working as a cyber security analyst. The importance of situated expertise means that expertise in network analysis is specific for a particular network that may not generalize to other networks.

The level of feedback that cyber security analysts receive during training affects the learning of attack patterns. Ben-Asher and Gonzales [15] found that detailed feedback improves analysts' detection of attacks throughout the training compared to aggregated feedback that has limited effect on analysts' performance. The detailed feedback showed analysts' performance for each event during a trial as correct detection and rejection of attacks, false alarms, and missed attacks. The aggregated feedback showed similar information, but only summarized for the whole trial and not for specific events. The detailed feedback increases analysts' correct detection of attacks from about 40% to 80% during training. The benefits of detailed feedback transfer to new scenarios not used during training.

Cyber security analysts use both general-purpose software tools and specialized cyber security software applications for intrusion detection. Some examples of general-purpose software tools are web browsers, text editors, and spreadsheets. Some examples of cyber security software applications are monitors for network traffic and hex editors. McClain et al. [16] describe that more experienced cyber security analysts were better at using general-purpose software tools and combining them with specialized cyber security software applications during a cyber security exercise. Further, Silva et al. [17] describe that successful participants during the exercise tend to work for longer blocks of time using a few specific software tools compared to less successful participants. These findings suggest that training in intrusion detection should provide explicit instructions on how to use available software tools.

Most intrusions that cyber security analysts detect and respond to are of routine nature that they manage by themselves without involving other personnel. Larger incidents, on the other hand, often require a team of analysts to work together, while severe incidents may require collaboration with other teams, such as investigation teams, human resources personnel, legal teams, internal audit staff, desktop support, or systems experts [18]. Cyber security analysts need collective information-sharing skills, collaboration skills, and preference for working with others to manage such major incidents [18]. Only investigative skills and problem-solving skills are not enough since a lack of teamwork skills reduce team performance. For example, team members may duplicate efforts due lack of communication or focus on their individual performance instead of the joint team performance [19]. Some suggestions for improving team performance are encourage team members to work as a team and measure team performance on the team level [20].

There is currently no standard set of roles for team members, neither between nor within organizations [19]. However, Buchler et al. [21] describe how high performing teams have a functional role specialization with both breadth and depth in skills. The functional role specialization evolves over time as the team matures according to Tuckman's [22] stage model of team development. Teams initially focus on understanding one another's skills and develop a shared collaborative approach over time. Mature teams have both defined roles for some team members and the flexibility to respond effectively to the task. High performing teams have an open communication where team members find ways to update each other about ongoing tasks and help each other when necessary [23]. Buchler et al. [21] describe how mature teams with both breadth and depth of skills can successfully perform common task for intrusion detection, maintaining network services, incident response, and administrative duties, such as creation of policy documents. Some important skills are threat analysis and data triage analysis for intrusion detection, incident escalation for maintaining network services, forensic analysis for incident response, and risk analysis for administrative duties. Finally, team leadership may improve team performance when task complexity is too high or the situation evolves too rapidly for the team's maturity level. Several team leaders may share the leadership for complex incidents [23].

6.4 RETENTION AND PERSONAL DEVELOPMENT

Many Security Operations Centres (SOCs) experience high burnout rate of cyber security analysts, which results in frequent personnel turnovers. Cyber security analysts often only have one to three years of employment before switching jobs [24]. Sundaramurthy et al. [25] describe an anthropological study to investigate underlying issues that contribute to the high burnout rate. The results show that burnouts are a human capital management problem from a cyclic interaction between human, managerial, and technical factors. The human capital refers to the cyber security analysts' knowledge, skills, and experience. The human capital should ideally grow in a positive cycle of using existing skills in challenging tasks that stimulate learning of new skills. Burnout occur when analysts become stuck in a vicious cycle where there is no learning of new skills. For example, entry-level analysts may be less expensive to hire than senior analysts, but since the management does not trust their abilities, they are only given tasks that provide limited opportunities for growth. Breaking a vicious cycle requires more trust in analysts' abilities and opportunities to work on challenging tasks.

6.5 CONCLUSIONS

Available studies provide some initial recommendations for how to recruit, select, train, and retain cyber security personnel. For example, recruitment should encourage investigative interests, rational decision-making style, and higher self-efficacy. Further, for selection of cyber security personnel, applicants' general abilities are more important than their IT knowledge. Cyber security personnel perform a wide range of roles that require many abilities, such as problem identification, communication, and resilience that are more difficult to obtain during training than IT knowledge.

Course programs for training of cyber security personnel needs to be more explicit of how acquired knowledge corresponds to actual requirements. Positive responses by students is not enough to guarantee necessary knowledge requirements. One option is to base the training on deterrence from crime prevention theories. Such training may increase attackers' perceived effort and risk, decrease rewards and crime inducing factors, and stimulate correct behaviour.

Intrusion detection is an important part of cyber security where detailed feedback during training improves analysts' detection of attacks. The detailed feedback should include whether analysts correctly detect and reject attacks, give false alarms, and miss attacks. Further, analysts need training in how experienced analysts use

available software tools. Additionally, while most intrusions are of routine nature that analysts manage by themselves, larger incidents require analysts to work as a team. Training in role specialization and teamwork processes are important for improving analysts' ability to manage such larger incidents.

The high burnout rate of some cyber security analysts may be due to entry-level analysts having limited opportunities to learn new skills when the management does not trust their abilities. Breaking such a vicious cycle and instead grow the human capital requires more trust in analysts' abilities and more opportunities to work on challenging tasks.

Finally, while research about how to recruit, select, train, and retain cyber security personnel continues to mature, further studies are necessary for definite recommendations about how to create a coherent and sustainable profession of cyber security personnel. Further studies should focus on:

- Specification of work requirements for cyber security personnel;
- Validation of selection instruments;
- Training of teamwork skills; and
- How to grow the human capital of all roles for cyber security personnel.

6.6 REFERENCES

[1] Bashir, M., Wee, C., Memon, N., and Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. Computers & Security 65:153-165.

[2] Morris, J.D., and Waage, E. (2015). Cyber Aptitude Assessment: Finding the Next Generation of Enlisted Cyber Soldiers. West Point, NY: The Army Cyber Institute at West Point.

[3] Trippe, D.M., Moriarty, K.O., Russell, T.L., Carretta, T.R., and Beatty, A.S. (2014). Development of a cyber/information technology knowledge test for military enlisted technical training qualification. Military Psychology 26(3):182-198.

[4] Newhouse, B., Keith, S., Scribner, B., and Witte, G. (2016). NICE Cybersecurity Workforce Framework (NCWF). NIST Special Publication 800-181, National Institute of Standards and Technology. National Institute of Standards and Technology: Gaithersburg, MD.

[5] Campbell, S.G., O'Rourke, P., and Bunting, M.F. (2015, September). Identifying dimensions of cyber aptitude: The design of the cyber aptitude and talent assessment. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting 59(1):721-725. Los Angeles, CA: SAGE Publications.

[6] Saner, L.D., Campbell, S., Bradley, P., Michael, E., Pandza, N., and Bunting, M. (2016). Assessing aptitude and talent for cyber operations. In: D. Nicholson (Ed.), Advances in Human Factors in Cybersecurity, 431-437. Advances in Intelligent Systems and Computing, Vol. 501, Springer International Publishing: Cham, Switzerland.

[7] Campbell, S.G., and Bradley, P. (2018). What shape peg are you? Different cyber jobs require different cognitive skills. In: Proceedings of the USENIX Symposium on Usable Privacy and Security (SOUPS). August 12 – 14, 2018, Baltimore, MD.

[8] IBM. (2018). IBM Cybersecurity Aptitude Assessments. Retrieved from https://www.ibm.com/talent-management/hr-solutions/cyber-security-skills-assessment.

[9] Keeley, S., Parkes, J., and Pons, T. (2017). Searching for cyber aptitude from within the armed forces. In: Division of Occupational Psychology Annual Conference 2017 Abstracts. The British Psychological Society: Leicester, United Kingdom.

[10] Trippe, D.M. Reeder, M.C., Brown, D. Jose, I.J., Heffner, T.S., Wind, A.P., Canali, K.G., and Thomas, K.I. (2015). Validation of the information/communications technology literacy (ICTL) test. Washington, DC: US Army Research Institute.

[11] Martini, B., and Choo, K.K.R. (2014). Building the next generation of cyber security professionals. In: Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel, June 9 – 11, 2014.

[12] Cornish, D.B., and Clarke, R.V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. Crime Prevention Studies 16:41-96.

[13] Branlat, M., Morison, A., and Woods, D.D. (2011). Challenges in managing uncertainty during cyber events: Lessons from the staged-world study of a large-scale adversarial cyber security exercise. In: Proceedings of the Human Systems Integration Symposium 2011, 10-25. American Society of Naval Engineers: Alexandria, VA.

[14] Goodall, J.R., Lutters, W.G., and Komlodi, A. (2009). Developing expertise for network intrusion detection. Information Technology & People 22(2):92-108.

[15] Ben-Asher, N., and Gonzalez, C. (2015). Training for the unknown: The role of feedback and similarity in detecting zero-day attacks. Procedia Manufacturing 3:1088-1095.

[16] McClain, J., Silva, A., Emmanuel, G., Anderson, B., Nauer, K., Abbott, R., and Forsythe, C. (2015). Human performance factors in cyber security forensic analysis. Procedia Manufacturing 3:5301-5307.

[17] Silva, A., McClain, J., Reed, T., Anderson, B., Nauer, K., Abbott, R., and Forsythe, C. (2014). Factors impacting performance in competitive cyber exercises. In: Proceedings of the Interservice/Interagency Training, Simulation and Education Conference, Orlando, FL. National Training and Simulation Association: Arlington, VA.

[18] Chen, T.R., Shore, D.B., Zaccaro, S.J., Dalal, R.S., Tetrick, L.E., and Gorab, A.K. (2014). An organizational psychology perspective to examining computer security incident response teams. IEEE Security & Privacy 5(12):61-67.

[19] Cooke, N.J., Champion, M., Rajivan, P., and Jariwala, S. (2013). Cyber situation awareness and teamwork. EAI Endorsed Transactions on Security and Safety 1(2):1-6.

[20] Rajivan, P., Champion, M., Cooke, N.J., Jariwala, S., Dube, G., and Buchanan, V. (2013). Effects of teamwork versus group work on signal detection in cyber defense teams. In: Proceedings of the International Conference on Augmented Cognition, 172-180. Springer: Cham, Switzerland.

[21] Buchler, N., La Fleur, C.G., Hoffman, B., Rajivan, P., Marusich, L., and Lightner, L. (2018). Cyber teaming and role specialization in a cyber security defense competition. Frontiers in Psychology 9:2133.

[22] Tuckman, B.W. (1965). Developmental sequence in small groups. Psychological Bulletin 63(6):384-399.

[23] Jariwala, S., Champion, M., Rajivan, P., and Cooke, N.J. (2012). Influence of team communication and coordination on the performance of teams at the iCTF competition. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting 56(1):458-462. SAGE Publications: Washington, DC.

[24] Hewlett-Packard. (2011). Building a successful security operations center. Retrieved from http://h71028.www7.hp.com/enterprise/downloads/software/ESP-BWP014-052809-09.pdf.

[25] Sundaramurthy, S.C., Bardas, A.G., Case, J., Ou, X., Wesch, M., McHugh, J., and Rajagopalan, S.R. (2015). A human capital model for mitigating security analyst burnout. In: Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS) 2015, 347-359. Usenix Association: Berkeley, CA.

Chapter 7 – CYBER SYSTEMS: A POTENTIAL PROTECTIVE AND ORGANIZATIONAL MEANS PERSPECTIVE

Oleksandr Burov
Institute of Information Technologies and Learning Tools
UKRAINE

At present, our lives are being built more and more around digital networks. Interventions to these networks pose a real threat to humans and to the country [1]. In this context, humans should be considered as not only military (including cyber) specialists, but everybody, because the cyberspace becomes the general environment of a human life and activity. For example, Internet of Things (IoT) entered our life practically in each house (computers, laptops and smartphones, routers, IP cameras, digital video recorders, etc.). In 2018, more than 30 billion IoT devices around the world were connected to the Internet.

In order to keep abreast with the rapidly changing threat landscape and maintain a robust cyber defence, civilian and military organizations at the national and international levels try to adopt their new enhanced policy accounting for new challenges [2]. The policy establishes that cyber defence is a part of the core task of government and collective defence, confirms that international law applies in cyberspace and intensifies military cooperation with industry [3].

The top priority is the protection of the communications systems owned and operated by them. Cyberspace is and will continue to be a very important part of the battlefield of ideas and civilizations [4]. Lesson learned from Ukraine-Russia conflict allows to argue that most future operations will (at least) start in cyberspace and operations will most probably be conducted within it during the conflict, increasing the importance of its control [5], [6].

While technical/technological solutions are being developed in response to cyber attacks, there is increasing awareness that the role of human performance and decision making in cyber security is critical to increase the effectiveness of responses to developing threats [7]. Especially it is significant from viewpoint of future manpower, because young people are especially sensitive to external influence and are the most active part of "network population", and "Cognitive space is the goal of any information war, both in peace, for example, during elections and in military situations. In fact, the transmission of information over which everyone is fighting is a secondary goal, since the primary purpose is to change the model of the world in the human brain. You can perfectly transmit messages that do not lead anywhere" [6].

New challenges of time and new directions of society development – Society 4.0, Education 4.0, penetration of the latest technologies into all spheres of life [8], "hybrid" warfare – require understanding of the key and safety issues of the educational process in digital space, in particular the security of all direct participants, the organizers of education, the state, as well as the safety of the content of learning [9]. Accordingly, the significance of cyber security has reached the level of competence in human life safety, has become an integral part of digital competence, first and foremost, all participants in the educational process. These trends in the paradigm shift in teaching impose additional requirements both on subjects of learning (both teachers and students) and on learning resources, especially in synthetic learning environments. Training with the use of technical means, primarily electronic, is becoming more and more usual for modern work, during which external and internal factors affecting person cognitive capabilities, and can suffer because of external vulnerabilities coming from networks. As a result, the training of cyber security specialists has rapidly increased, as their global deficit in the world by 2020 is estimated at 1.5 million workers.

Training of specialists in cyber security is being conducted in hundreds of universities worldwide. Typically, future specialists receive theoretical knowledge and practical skills in programming, developing and managing databases, developing information security models and security policies, technical and cryptographic information security, building secured digital TCP/IP networks and maintenance of public key certificates, testing of penetration protection systems, administration of secure information and communication systems, monitoring and auditing, etc. [10]. However, five years after the adoption of the ISO standard [11], the vision of the cyber security problem has changed significantly, as a person ceases to be the sole subject of cybercrime, turning into an object by itself, and not just its financial and economic interests and opportunities [12]. So, according to the analytical company RAND Corporation, the structure of cyber risk has changed in recent years. More and more analysts pay attention to the fact that the main causes of incidents in Internet resources in 2017 were related to the effect of the human factor, the massive fragmentation of IoT devices and cloud services [13]. Particularly this problem is getting worse by the growing role of social networks in human life in general and in education, in particular, as well as the understanding of the need to transition to education throughout lifespan.

Over the past three years, educational reform has been developed in many economically developed countries by educators, among them developed and presented in the EU. Digital Competence Framework for Citizens 2.0-2.1 [14]. Information and communication competence was defined as one of the key competencies. Cyber security issues were important components of this competence and reflect the common approaches formulated in the Digital Competences Framework for EU citizens [14].

7.1 THEORETICAL AND METHODOLOGICAL QUESTIONS OF THE CYBER SECURITY IN EDUCATION

The human factor may be a system's weakest link, but at the same time it may also be a powerful resource to detect and mitigate emerging threats. Several areas of most critical and urgent needs as well as the knowledge gaps to address in cyber research agendas of NATO and the nations can be defined as psychosocial, cultural, conceptual and organizational dimensions of cyber security.

Cyber objects (humans) can be decision makers, key defence specialists, financial managers, key industry managers, creators of knowledge, and general population (including future military and defence manpower).

Successful cyber security involves accounting for all groups of remedies. Ignoring any of them can lead to loss of government control, military control, financial control, industry control, manpower control, and data.

Taking into account last years' trend in hybrid war, the cognitive war needs a special attention, because its goal is not a prompt military operation and fight for territorial or economic resources, but for people [6]. Moreover, not only the highest level's decision makers, but also the entire population of the target country, since it must perceive and support state leaders controlled by the aggressor (e.g., via mass media), as events in Ukraine and other countries demonstrated over last years. In such a context, cyber security is a way of countering and neutralizing cognitive weapons.

Cognitive weapon is a control of the intellectual environment of the country of the enemy by false scientific theories, paradigms, concepts, strategies, influencing its governance towards weakening the defence of significant national capacities [15]. Main features of the cognitive war are as follows:

- *Military strategy* is suppressed and subordinated the consciousness of the enemy. Opponent is programmed cognitively to self-destruction.

- *Goal* is implanting to the enemy a thought that the struggle itself does not exist.
- *Result* consists in enemy's cognitive damage which features can be characterized as:
  - Represented false theory affects national science, relevant scientific schools and generations;
  - Corresponding defective frames are programmed to misconceptions about the most important management paradigms, development of the country;
  - This reproduce generations of students and graduate students of the corresponding grade; and
  - They saturate the relevant reference structures of government and decision makers, accordingly, there is an erroneous destructive state management policy.

To date, there is a gap between the traditional approach to cyber security (the solution of technical and information tasks) and the need to take into account the human factor in the cognitive dimension. Understanding of this leads to changes in the training of specialists in cyber security : in their training programs, more and more skills and abilities are added with focus "on the social, economic, and behavioural aspects of cyberspace, which are largely missing from the general discourse on cybersecurity" [16], p. viii, that needs to take into account the human features and his/her functional state as well as cognitive resilience, because of increasing role of the cognitive warfare [17].

The closing of such a gap needs to expand the number of key Cyber Security (CS) questions: Who, Why, What, Where, When, In What Way?

Besides, selection of appropriate CS means should take into account their time perspective:

1) *Short-term* (cyber attacks, battle operations);
2) *Middle-term* (cyber staff training); or
3) *Long-term* (cognitive weapon).

The issues of cyber security are acute from the time that computer technology has ceased to be just the prerogative of major research centres. With the advent and spread of local and global networks, the understanding of cyber security, relevant trends, problems and challenges has changed. Let's consider them taking into account the transformation of education in the direction of digital education, Education 4.0.

7.2 INFORMATION AND COMMUNICATION TOOLS AS THE BASIS FOR THE EMERGENCE OF A CYBER SECURITY PERSPECTIVE

To date, our lives are building more and more around digital networks, and virtual media is becoming a new social environment [18]. Interference with these networks poses a real threat to security in education and the country as a whole. The constituents (factors) of the network can be represented in this simplified form (see Figure 7-1).

Network agents can act as nodes – people (resource creators and their content, resource administrators, regular or random users), technical (terminal stations, computers, networked gadgets, communicators) and information (databases, databases knowledge, control systems, etc.) means. All agents, depending on their nature, have their own interfaces and types of communication with other agents.

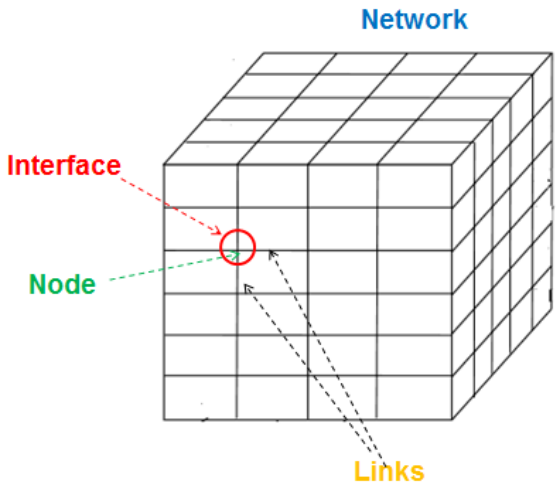

Figure 7-1: Simplified Model of Cyberspace.

However, it should be noted that the network ceased to be merely an intermediary between users (means of communication in time of the development of technologies for building networks), their complication, the use of artificial intelligence, the emergence of cloud and foggy technologies, the growth of the power of Databases (DB) and Knowledge Bases (KB). Since the information in the global network exists outside the defined space and time, the network itself becomes an active agent of human influence [12], first of all, while maintaining large amounts of data available to the public [19]. Any user can log on to the network (legally or illegally) and access the necessary nodes (when using cloud-based means, specific nodes may not be known to the common user), including changing their content (for example, a Wiki-object) for permitted rules.

However, information in DBs and KBs under the allowed rules can be changed or introduced in order to distort the representation of users about the data they are looking for. Certain users are able to use it to influence the broad or target audience, “distorting” the nodes (technical or informational) or influencing them by means of social engineering (if the node is a person). Since the network is a system of connected nodes, a damaged (“distorted”) node may already effect on its secondary nodes. In addition, distorted information begins to exist on the network, even independent on the person (“aggressor”), who introduced it (Figure 7-2).

Thus, the network acquires the features of an independent component (factor), which affects its properties, functioning and users, as well as the System “Human-Technology-Environment” (SHTE) as a whole. All four network performance parameters (see Figure 7-1) have certain common critical properties from the point of view of efficiency and impact on the user – initiative, efficiency, stability, flexibility and performance (Table 7-1). Their manifestation in relation to each factor can be characterized by certain indicators, characteristic for the corresponding parameter, and a set of indicators allows estimating the overall influence of the factor on the network as a system “human-technology-environment”.

Any consideration of cyber security as an independent factor in SHTEs is limited and only partially effective, since it does not take into account the changes that occur with SHTE agents, not only in time but also in space, and this effect expands with the development of technologies from local to global ones. Corresponding changes occur in relation to the learning environment.

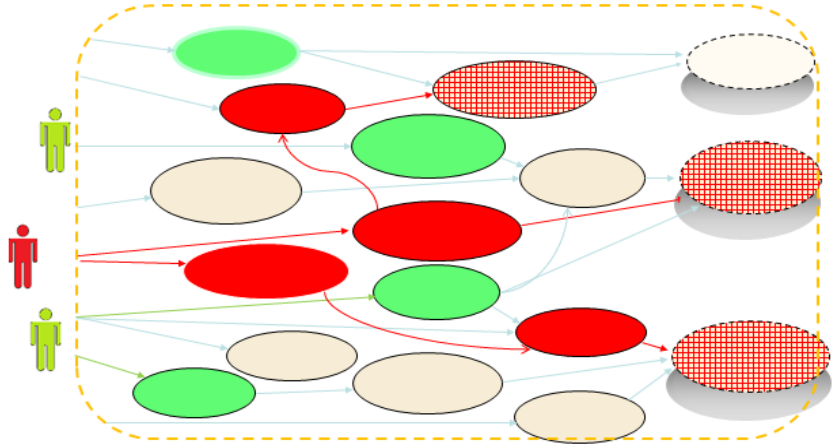

Figure 7-2: Example of an Active Fragment of the Network and External Users (Green – Normal, Red – "Aggressor") Connected to Nodes (Red – the Node with "Distorted" Information).

Table 7-1: Network Elements and Their Features.

HSI Features	Node	Interface	Link	Network
Initiative	Situation awareness	Situation information	Routing	Intent
Efficiency	Performance	Usability	Packet loss	Quality of service
Stability	Response to stress	Consistency	Reliability	Resilience
Agility	Capability	Display modes	Redundancy	Reconfigure
Capacity	Workload	Clutter	Bandwidth	Density

7.3 LEARNING ENVIRONMENT AND CYBERSPACE

The Educational Environment (EE) is one of the cornerstones of education. There are many different definitions and classifications of the EE. It has a multifactorial influence on subjects of the educational process, changing both in time and in space. And this is true both for the traditional learning environment and for the synthetic one. One can note that the learning environment in the content plan always arises as a dynamic process of forming a network of relations in the subject of learning, to which (not always consciously) selectively involve the various elements of the external and/or internal environment, and this dynamic process is characteristic of any learning environment, but in immersive and virtual EE, it becomes even more acute due to a more profound immersion of the student into the learning process.

Different authors distinguish natural and artificial, subject and informational dynamic, adaptive and other educational environments, using different criteria of their typology; for example, the style of interaction within the environment, the nature of the attitude to social experience and its transfer, the degree of creative activity, and by nature interaction with the external environment. However, at present, the digital space or cyberspace is the main attraction due to the exacerbation of the human security problem in it, first of all, the young person whose formation takes place only in the personal and competent dimensions.

Attention is drawn to the fact that cyberspace is determined by the diversity of compounds, which simultaneously translates it into a category of risk area. All increasing dimensions, coverage and functions increase the capacity of both law-abiding citizens and hostile players. An opponent only needs to attack the weak link of the network in order to win a new bridgehead and gain advantages [7]. Local issues can grow and spread rapidly, creating threats and systemic risks. The vulnerability in the cyberspace is real, serious and it is growing rapidly. Facilities of special importance infrastructure, intelligence, communications, command and control, trade and financial operations, logistics, mitigation and emergency preparedness are entirely dependent on IT systems integrated in the network. Violations of cyber security, theft of data and intellectual property do not know the boundaries. They affect everything from personal information to state secrets.

Cyberspace can be considered as a triad, which includes:

1) Information in its digital representation: static (files recorded on the storage medium) and dynamic (packets, threads, commands, queries, etc.);
2) Technical infrastructure: Information and communication technologies, software, databases and knowledge bases; and
3) Information interaction of entities using received (transmitted) information and processing through technical infrastructure.

This notion is bound with the notion of cyber security as the protection of the vital interests of man and citizen, society and state when using cyberspace. At the international level, a number of definitions of this concept are used, but accounting the fact that learning is a type of activity, one can agree with the approach that cyber security is considered as “any networking, digital activity, including the content of information and activities that are carried out through digital networks” [20]. Keeping in mind that today’s students are born in a digital age, grow, study and develop to a large extent precisely in cyberspace, one can argue that cyberspace is and will remain a very important part of the battlefield of ideas and civilizations. Accordingly, before education there are new tasks connected not only with the formation of the necessary knowledge and social awareness of the learner, but also his/her understanding of his/her own integration into the world community already in the early stages of learning, practically unlimited possibilities of the influence of cyberspace on personality, responsibility to him/herself and society for their own behaviour and its (possible) global implications, knowledge and understanding of the dangers of cyberspace.

7.4 THREATS TO PARTICIPANTS IN EDUCATIONAL PROCESS FROM CYBERSPACE

The threats’ spectrum from open cyberspace is constantly expanding. If ten years ago the hazard to schoolchildren could be reduced to a relatively small number of groups (viral attacks, cybercrime, threats of Internet surfing), at present, the diversity of threats and hazards is constantly increasing, affecting all possible human actions in the network. The greatest danger to students is hidden active threats [21].

To protect young humans from cyber threats especially their cognition, it is useful to understand modern trends in education (digitalization of education) and potential specific targets of attackers in educational domain. Recognizing the role of education subjects and their specific role in society, various aspects of the education domain were captured and reflected throughout the ontology as shown in Figure 7-3 with red ovals circling the relevant concepts. For example, one of the threat vectors in the ontology is policy and procedural non-compliance and one of the mitigation mechanisms is policy management.

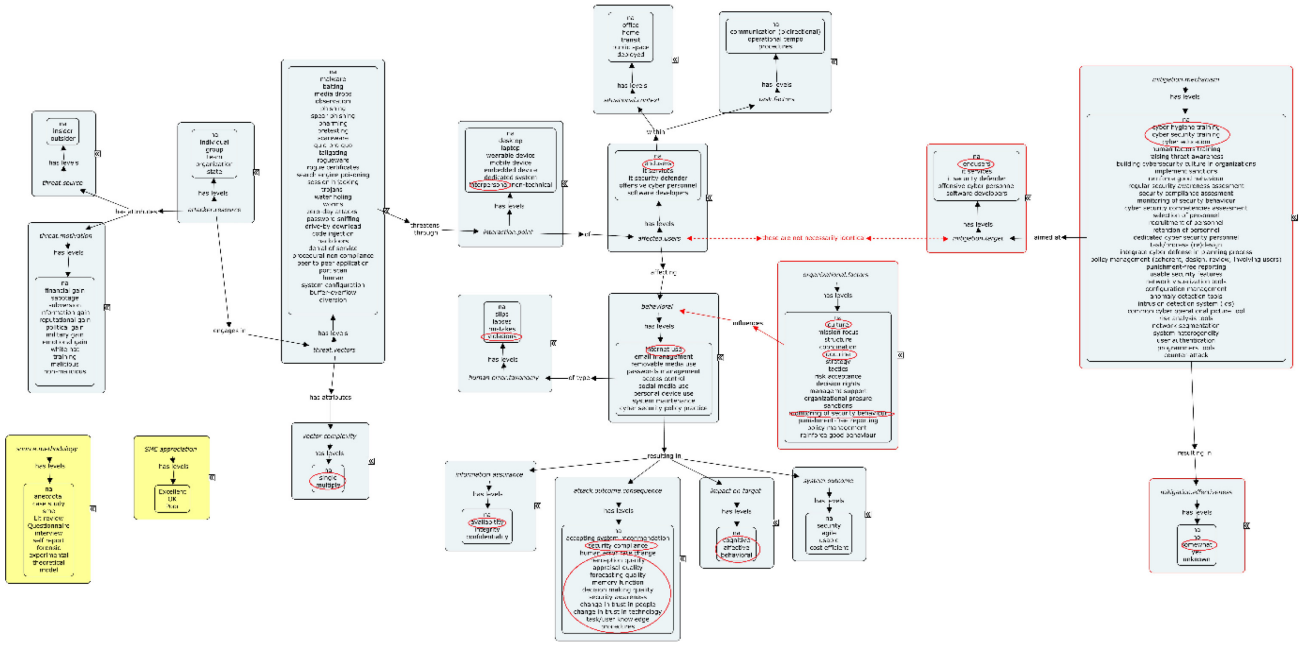

Figure 7-3: Education Aspects Captured in the Framework. See Annex A, Figure A-1 for full size non-annotated image.

Section 7.4 summarises general factors related to human-systems security related to education and provides an overview of the relevant literature.

7.4.1 Network Threats

The active use of networks, especially by children and young people, is accompanied by an increase in various types of threats coming from the Web. This problem is especially acute when developing and using social networks. The most active hidden threats (for children) originating from a computer network can be represented by the following classification [21]:

- Viral attacks;
- Cybercrime (spamming, carding, phishing, botnets, etc.); and
- Threats from network surfing (cyber bullying, "adult" content, illegal content, online violence, private disclosure, paid services, etc.).

The authors recommend to consider the interaction of students between them and students with the computer network as a system "human-technology-environment." In this system, the computer network acts as a machine, which allows us to consider the impact of the network on a person as a threat from the machine. Accordingly, the concept of "network effect" can be detected through the notion of "operator error and low quality of the operator", "the impact of computer games" and "Internet addiction."

The threats coming from networks can be divided into the following types: active and passive, open and hidden, current and deferred ([21], p.308).

Using the ergonomic approach and methodology, it is possible to evaluate active threats as a hierarchical set of indices:

- One *integrated* (complex) index: the level of hazard due to the operation of the computer network. The index is the dimensionless value included in the estimates of the system of the upper level.
- Three *group indicators*: the level of danger caused by viral attacks, cybercrime and internet surfing. Indices are dimensionless values and are associated with the average level of system evaluation.
- Set of particular indices of a group of one or a combination of threats. Indices are also dimensionless and correspond to the classification of lower-level systems.

Such an integrated index gives an opportunity to assess the influence of the set of weighted threats independently on their nature and ways of measurements, and to project it on a scale [0,1] that could be a scale of the general cyber risk. For example, 0 … 0.2 means lack of significant risk, 0.2 … 0.5 the presence of risk, 0.51 … 0.8 high risk, > 0.8 unacceptable risk.

7.4.2 Cyber Security (CS) Directions

As a rule, national legislations related to CS do not consider the sphere of education as the critical area for the protection of which they are aimed. However, today's pupils and students in the short term can work in those areas. Therefore, they already need protection and appropriate training as well as an understanding of the general possible target groups of cyber security. For example, by the following classification [12], [9]:

- Pupils/students;
- Teachers;
- Children/youth (in general); and
- Population (in general, as a social environment).

Depending on the means of action, the problems (and appropriate means) of cyber security can be classified into five groups:

- Legal;
- Technical;
- Information;
- Organizational; and
- Psychological.

The legal and technical issues of cyber security are handled by appropriate specialists and organizations, so they are not addressed in this article.

Information tools can be categorized according to the tasks solved by the users:

- Protection/Remedies;
- Informing;
- Content;

- Learn how to use;
- Security;
- Lifespan; and
- Avoiding threats.

In the broadest sense possible, *targets* for the impact of cyber security (in addition to critical infrastructure objects) can be:

- Databases;
- Personal data, including financial;
- Mass media;
- Social networks;
- Education/training; and
- Textbooks, historiographical editions.

The latter two points relate to the domain of cognitive safety, i.e., to the prompt human factors area.

Organizational tools for solving cyber security issues are:

- Informing;
- Learning the culture of cyber security, professional staff of CS and the general population;
- Creation of special means of the CS;
- Distribution of CS facilities; and
- Control of use.

Psychological means can be grouped depending on the personal and interpersonal level:

- National;
- Public;
- Group;
- Individual;
- Cultural;
- Cognitive;
- Intellectual; and
- Habits.

Although technological solutions are developed in response to cyber attacks, awareness is growing that the role of human activity and decision making in the field of cyber security is crucial for increasing the effectiveness of responding to emerging threats. This is especially important in terms of future workforce, since young people are particularly sensitive to external influences and are the most active part of the “network population.”

The human factor may be a systemic weak link but can also be a powerful resource for identifying and mitigating emerging threats. Several areas of the most critical and urgent needs and gaps in knowledge that are considered in cyber research programs in NATO and other countries can be identified as: psychosocial, cultural, conceptual, and organizational aspects of cyber security.

7.5 POSSIBILITIES AND WAYS OF PROVIDING CYBER SECURITY PROFESSIONAL EDUCATIONAL PROCESS

Recent studies on cyber security show that information technology in this area is constantly being improved and hacker attacks are reoriented not to technology, but to humans (see, for example, https://www.computerweekly.com/news/252448101/People-top-target-for-cyber-attackers-report-confirms). It is especially important to take into account the acuteness of the issue of its personal security and the results of its activities. When a human is "opening" during the work (connecting his/her own information models with the information flow), the information environment becomes not only a subject, but an object and a tool of the activity of other participants in the information space. The information can affect the target human from outside, because the human openness is a result of the goal of work: using information as an instrument, a person has to "touch" it, contact it. At this moment, the human becomes open to information and vulnerable to it.

7.6 SOCIAL ENGINEERING AND CYBER SECURITY

The shifting of the goals of cybercrime from technical (information) to the human link of the SHTE led to the emergence of Social Engineering (SE) as methods and technologies for obtaining the necessary access to information based on the peculiarities of the psychology of people, in particular, the manipulation of human fears, interest, or trust [22].

The main types of social engineering at the time can be considered in relation to education as follows: pretexting, phishing, Trojan horse, *Quid pro quo*, road apple, biting, reverse social engineering, friendly letters, whishing, contacts [23].

Social engineering tools have been widely used in recent years to influence decision makers in politics and business. Recommendations, methods and means of counteracting them are developed and improved (https://lab.deiteriy.com/#service). However, there is virtually no discussion of action and countermeasures in the SE on the educational field, despite the fact that children and teenagers are increasingly exposed to attacks via the Internet, and the use of countermeasures for adults can be extended to pupils/students, but taking into account peculiarities – age and spheres of activity. A lot of tools for SE are proposed for everybody in the Internet (e.g., http://www.spy-soft.net/social-engineering-toolkit/).

7.7 LEARNING SUBJECTS AND SECURE INTERNET

The main way of protecting from the methods of social engineering is to teach Subjects of the Educational Process (SEP). All of them (students, educators, and trainers) should be warned about the risk of disclosure of personal information and confidential information, as well as ways to prevent data leakage. In addition, each SEP, depending on the place and function in the educational process, should have instructions on how and on what topics it is possible to communicate with third parties regarding personal characteristics, which information can be provided to the technical support, as well as what information can notify the learner to third parties and media In addition, you can select nine typical rules of resistance to the SE (https://efsol.ru/articles/social-engineering.html).

Intended user credentials are the property of an educational institution. All employees on the day of recruitment should be told that those logos and passwords that they have been given (if any) cannot be used for other purposes (on websites, for personal mail, etc.), to transfer to the third person or other employees who do not have this right. For example, very often on leave, an employee can transfer his authorized data to his colleague in order to be able to perform some work or look at certain data at the time of his absence. Personal data from the results of testing and performing psychological and medical examinations can be used by SE users; therefore, they require careful use.

Introductory and regular training of staff and students aimed at raising awareness of information security is required. Conducting such briefings will allow the SEP to have current data on existing methods of social engineering, and to not forget the basic rules of information security.

It is mandatory to have security regulations, as well as instructions that the user must always have access to. Instructions should describe the actions of the SEP in the event of a situation. For example, in the regulation you can prescribe what you need to do and where to contact when you try to invite third parties to receive confidential information or credentials.

The computer users should always have current antivirus software, and also install a firewall.

7.8 "COGNITIVE VACCINATION"

On December 20, 2002, the General Assembly of the United Nations adopted Resolution 57/239 Elements for Creating a Global Cybersecurity Culture, which identified nine fundamental complementary elements that form the global cyber security culture [24]:

1) Awareness;
2) Responsibility;
3) Response;
4) Ethics;
5) Democracy;
6) Risk assessment;
7) Design and implementation of security measures;
8) Security control; and
9) Revaluation.

These elements relate to all five groups of means specified in Section 7.4.2 – information (numbers 1, 6 and 9), technical (3 and 7), organizational (5 and 8) and psychological (2 and 4). At the same time, it can be noted that psychological means (which directly relate to each individual) provide only behavioural aspects – responsibility and ethics, that is, manifestation of a person's social attitude towards cyber security. However, in the cognitive aspect, which is shaping in relation to human behaviour, attention is not focused, that is, a person is seen as a relatively passive element of the cyber security system. At the same time, since no means guarantee 100% protection of the person, it is expedient to determine the range of possibilities of the person himself to the formation of personal protection, except for the above.

The analysis of the programs of educational institutions in many countries showed that in studying the teaching methods of learners enough attention to the question of the formation of critical thinking students in connection with the use of the Internet is not always paid [25].

At the same time, solving the problem of the safety of students online in the developed world, where the Internet is widely used in educational and scientific activities, is characterized by an integrated approach and the security problem is closely linked with questions of forming the student's own responsibility for their actions or inactivity on the network to avoid and/or risk reduction. For example, students from the United States, Germany, Canada, Finland and other countries, together with parents and school representatives, sign special agreements on safe and responsible use of the Internet. In such agreements, bonds of safe and responsible use of social networks by all participants in the educational process are defined and prescribed.

The most effective way to deal with the problems of cyber threats is to understand their essence and change their behaviour. Safety rules are simple and well known; they need to be applied. First of all, it's worth looking into actions and understanding what dangerous actions you and other SEPs do. For example, click on the links, relying on the fact that antivirus protection will provide cyber security? Unfortunately, no technical equipment from the cyber security arsenal is a guarantee, especially if the target of the hazardous action is a person as such.

In a cyber-threatening world, an important part of the training of all networking participants should be taken on the possible impact of the cyber environment. General and specific information about cyber threats and possible consequences of their impact on life and human activities should be supported by simulation of certain situations that may occur to the user of the Internet. Effective means of educating teachers and students of safe and responsible behaviour when using Internet resources is to conduct special training sessions on the critical assessment of the reliability of sources and the reliability of data published on the network.

The most effective approach is to use computer simulation of cyber threats in relatively closed systems: corporate and educational ones. As recommended by professionals, if you are dealing with security issues, "training" attacks, in fact, is a useful way. "But it should be used correctly. Not just divide employees into those who felt the trick and those who got caught. It is imperative to convey to others the essence of their mistakes and how not to make them in the future. You can also find out exactly how dangerous the testers have been identified. Perhaps from this you will be able to glean useful ideas" (accessed 03/28/2020 https://legal-it.club/kiberbezopasnost-chelovecheskij-faktor/). Examples include simulation of unauthorized distribution of private information about a particular person in a modelling environment (using real information from social networks, which many do not randomly place there); phishing modelling, etc.

As it is virtually impossible to provide full protection, it is important to train the users' resilience to cyber threats, that is, learning "cyber survival", which consists of the ability to recognize the threat or possible dangerous effect of the network and rational compensation for this action – both psychological and behavioural (including the appeal to the relevant specialists, because of the impossibility of self-restored actions at the initial stage of training). To some extent, such training is similar to the training of first aid measures in the event of damage to health.

Integrated training in these areas can be considered "cognitive vaccination", that is, the formation of a conscious sensory experience of staying under the influence of cyber threat and counteraction to it. In general, the following levels or "layers" of cyber security can be identified:

- Legal;
- Technical;

- Information;
- Organizational; and
- Psychological, with special regards to cognitive means and responsible behaviour.

It is possible to effectively solve the issue of cyber security only if system resources are used at all structural levels, considering the specific weight of each of them for a specific target group and/or the scope of application of the corresponding anthropocentric system.

7.9 CONCLUSIONS AND PERSPECTIVES FOR FURTHER STUDIES

1) The problems of cyber security are not limited to the technical aspects of the protection of information resources; they must include in their entirety the following types of protection: legal, technical, informational, organizational and psychological.

2) At the same time, among psychological means of securing cyber security it is expedient to distinguish cognitive, since the population in general, and especially children and youth, are increasingly becoming targets of cyber attacks, first of all, their cognitive sphere, becoming the most vulnerable (weak) link in the network.

3) The network itself acquires new properties, acting as an independent vector (in addition to factors such as the network node, interface and nodes) in human-centric networks, which make up an ever-increasing share among common networks.

4) Threats to participants in the educational/training process on the part of cyberspace should be considered as passive and active, developing adequate means of protection and viability of the system “subject of educational process – learning – environment”.

5) The most significant for the participants among cyber threats of the educational process are methods of social engineering, whose knowledge and opposition can be most effective in providing cyber security.

6) As part of the training of participants in the educational process on cyber security, it is proposed to use “cyber vaccination”, that is, the formation of a conscious cognitive experience of staying under the influence of a cyber threat and counteracting it as a system of training activities that include, in addition to traditional methods, training “cyber attacks”, as well as the formation of knowledge and skills of sustainability (recovery) in relation to cyber threats.

7) Further research of the problem should focus on the detailed development of types of threats to the participants in the educational process, as well as methods of counteraction. A special point should be the issue of resistance to cyber hazards, which can use the experience of training operators of the emergent industries, primarily diagnosing the current state of the person and necessary adjustments in order to optimize its activities.

7.10 REFERENCES

[1] Nemchynova, K. (2015). Cyber security and cyber weapons as a challenge to the State of Ukraine. https://www.liga.net/economics/opinion/kiberbezopasnost-i-kiberoruzhie-kak-vyzov-gosudarstvu-ukraina-3999533. Accessed 28 March 2020 (in Russian).

[2] Glaspie, H.W., and Karwowski, W. (2018). Human factors in information security culture: A literature review. In: D. Nicholson (Ed.), Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity. Advances in Intelligent Systems and Computing, Vol. 593. Cham, Switzerland: Springer.

[3] Schmitt, M.N. (2015). The law of cyber targeting. The NATO CCDCOE Tallinn Papers. Tallinn Paper No. 7. Tallinn, Estonia: CCDCOE.

[4] Snegovaya, M. Putin's information warfare in Ukraine: Soviet origins of Russia's hybrid warfare. www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf. Accessed 28 March 2020.

[5] Gery, W.R., Lee, S., and Ninas, J. (2017). Information warfare in an information age. Joint Force Quarterly. I. 85.

[6] Pocheptsov, G. (2017). The war in cognitive space. Retrieved from https://nesterdennez.blogspot.com/2017/08/global-permanent-war_39.html (in Ukrainian).

[7] Yan, Z., Robertson, T., Yan, R., Park, S.Y., Bordoff, S., Chen, Q., and Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cyber security judgment? Computers in Human Behavior 84:375-382, ISSN: 0747-5632.

[8] Bykov, V.Yu. (2018). Knowledge society and education. Retrieved from https://www.youtube.com/watch?v=cDIytlESUz4.

[9] Bykov, V.Yu., Burov, O.Yu., and Dementievska, N.P. (2019). Cybersecurity in digital educational environment. Information Technologies and Learning Tools 70(2):313-331.

[10] Bystrova, B. (2017). Comparative analysis of curricula for bachelor's degree in cyber security in the USA and Ukraine. Comparative Professional Pedagogy 7(4):114-119.

[11] ISO/IEC 27032:2012. (2012). Information technology – Security techniques – Guidelines for cyber security.

[12] Burov, O. (2016). Educational networking: Human view to cyber defence. Information Technologies and Learning Tools 52:144-156.

[13] SecurityLab. Retrieved from https://www.securitylab.ru/news/492191.php. Accessed 28 March 2020.

[14] Digital Competences Framework for EU citizens. Retrieved from https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digcomp-21-digital-competence-framework-citizens-eight-proficiency-levels-and-examples-use. Accessed 28 March 2020.

[15] Bagdasaryan, V. (2016). "Cognitive weapons" as a tool for desuverization. Retrieved from https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/.

[16] Ahram, T., and Karwowsky, W. (2019). Advances in human factors in cybersecurity. In: Proceedings of the AHFE 2019 International Conference on Human Factors in Cybersecurity, July 24 – 28, 2019, Washington DC.

[17] Bienvenue, E., Rogers, Z., and Troath, S. (2018). Cognitive warfare. Retrieved from https://cove.army.gov.au/article/cognitive-warfare.

[18] Burov, O. (2014). Virtual life and activity: New challenges for human factors/ergonomics. In: Symposium Beyond Time and Space STO-MP-HFM-231, STO NATO, 8-1 to 8-8.

[19] Mansour, R.F. (2016). Understanding how big data leads to social networking vulnerability. Computers in Human Behavior 57:348-351, Elsevier Ltd.

[20] Klimburg, A. (2012, December). National Cyber Security Framework Manual. NATO CCD COE Publications. Retrieved from https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/. Accessed 28 March 2020.

[21] Burov, O.Yu., Kamyshin, V.V., Polikhun, N.I., and Asherov, A.T. (2012). Technologies of network resources' use for young people training for research activity. Monograph. Burov, O.Yu. (Ed.), Kyiv: TOV «Informatsiini Systemy» (in Ukrainian).

[22] A powerful tool for social engineering. The WordPress Security Learning Center: Understanding Social Engineering Attacks. Retrieved from https://www.wordfence.com/learn/understanding-social-engineering-attacks/. Accessed 28 March 2020.

[23] Savchuk, T. (2018). Social engineering: How fraudsters use human psychology on the Internet. Accessed 30 August 2018. Retrieved from https://www.radiosvoboda.org/a/socialna-inzhenerija-shaxrajstvo/29460139.html (in Ukrainian).

[24] Elements for creating a global cybersecurity culture. UN document. Retrieved from http://www.un.org/ru/documents/decl_conv/conventions/elements.shtml. Accessed 28 March 2020.

[25] Dementiievska, N.P. (2015). Formation of the skills of critical evaluation of web resources and the problem of student safety on the Internet. Kompiuter u shkoli ta simi 7:46-51 (in Ukrainian).

Chapter 8 – DISSEMINATION AND INTERACTION

Yantsislav Yanakiev
Bulgarian Defence Institute "Prof. Tsvetan Lazarov"
BULGARIA

Over the process of the work, the HFM-259 RTG team organized several international scientific events and participated in other activities for dissemination of the results and obtaining feedback from other recognized experts in the field. And finally reported on the results of the collaboration in this report.

8.1 INTERNATIONAL CONFERENCE ORGANIZED IN COOPERATION WITH ARMED FORCES COMMUNICATIONS AND ELECTRONICS ASSOCIATION (AFCEA) SOFIA CHAPTER

The first important milestone in the PoW was an international conference on Human Systems Integration Approach to Cyber Security, organized in cooperation with Armed Forces Communications and Electronics Association (AFCEA) Sofia Chapter on 28 – 29 September 2015, in Sofia, Bulgaria. The output of the conference was the book *Human Systems Integration Approach to Cyber Security: Proceedings of International Conference,* published in 2016 [1]. The papers in the book cover a broad range of issues related to NATO, EU and national experiences in the research in cyber security domain. Among the most important topics are NATO cyber defence and Human Factors (HF), cyber attacks in NATO military operations, conceptual and organizational dimensions of cyber security, development of a vision for cyber defence in the context of the national cyber security strategy, testing vulnerability of organization's cyber security of social engineering attacks, systems thinking and modelling for HF in cyber security, developing HF framework for cyber vulnerabilities investigations, security issues in mobile banking, the significance of cognitive user profiles for improving usability of computer systems' interfaces, increasing cyber security competencies through mission-based learning, etc. Scientists and practitioners in cyber security from NATO HQ, NATO STO, NATO Joint Warfare Centre, European Defence Agency, the ministries of defence and various educational and research institutions from Canada, Germany, the Netherlands, Sweden, the UK, Ukraine and the USA presented their findings at the conference.

There were two keynote speakers that shaped the discussions. The first keynote speaker, Mr. Alan Shaffer, Director of NATO STO Collaboration Support Office (CSO), presented NATO Science and Technology Organization research activities in the area of cyber security. The key message of Mr. Shaffer was that NATO STO focus is on defensive cyber. He presented the main topics of the STO Cyber Programme of research which include Detection, Mitigation and Attribution of Cyber Threat. Currently, ten activities of different STO Panels are implemented, among them one Exploratory Team, four Research Task Groups and five Research Symposia and Workshops. They cover a broad spectrum of issues, including Military Strategic-Level Decision Making within a (Future) Framework of Cyber Resilience, Cyber Security of Military Platforms, Secure Future Internet Architecture for Military Applications, Predictive Analysis of Adversarial Cyber Operations, Human Systems Integration Approach to Cyber Security, Modelling and Simulation in Support of Cyber Defence, etc. Mr. Shaffer concluded that cyber is more than a computer network. He presented some gaps in NATO cyber research programme, among which are vulnerabilities of platforms / standalone systems; the need of developing an agreed set of parameters to measure cyber performance and of procedures for cyber (test) range operations, to mention just a few.

The second keynote speaker, Mr. Marc Scheir, Deputy Director of NATO HQ C3 Staff, focused his presentation on NATO cyber defence and the role of human factors. First of all, he restated the three cornerstones of NATO Cyber Defence Policy, approved at the 2014 Wales Summit. First, re-calibrating and enhancing the cyber defence paradigm within NATO: cyber defence is part of collective defence; NATO is responsible to protect its own networks; international law applies in cyberspace. Second, re-enforcing capability development and capacity-building: continued improvement of NATO's cyber defence capabilities; integration of cyber defence into operations planning; enhanced cyber defence education, training and exercises; multinational development of smart defence projects on cyber defence. Third, re-shaping the way NATO does business: enhanced information sharing; increased emphasis on partnerships with partner countries, international organizations and the industry. Mr. Scheir emphasized that NATO is a target of state-sponsored advanced-threat actors, criminal organizations, hacktivists, fame-seeking hackers, witting/unwitting personnel actions, etc. Human factor becomes the greatest challenge to prevent, mitigate and respond to these attacks. What are the most significant attributes of people as a threat vector? Top issues comprise bad practice due to lack of awareness; tendency to shortcut processes; mistakes/human errors; being tricked into compromise; being forced into compromise; intentional malicious behaviour, to mention just a few. What is NATO doing in this regard? Among the most important measures are improved technical countermeasures, e.g., introducing strong authentication; creating and introducing NATO-wide cyber awareness programme; renewed focus on cyber defence education, training and exercise activities; introducing new and improved cyber defence courses at the NATO Communication and Information Systems School and NATO Cooperative Cyber Defence Centre of Excellence. The most important message of Mr Scheir was that we should always remember that all systems are used, operated, administered and managed by people. In addition, it is essential to consider human factor throughout the lifecycle of any security system/service. Moreover, it is critical to simplify and rationalise security processes to increase their adoption by the users. Finally, yet importantly, we have to 'train as we fight' by injecting challenging cyber scenarios into military exercises. In conclusion, Mr Scheir put forward some ideas on how scientific research can help prevent and mitigate cyber threat. The most important recommendations include to develop methods to measure cyber awareness; to investigate options to increase users' appetite for good security practice; to develop techniques to detect anomalous/suspicious user behaviour both online and offline, and to balance 'need-to-know' and 'need-to-share'.

8.2 NATO STO RESEARCH WORKSHOP (RWS) ON INTEGRATED APPROACH TO CYBER DEFENCE

The second important milestone in the PoW of HFM-259 RTG was the NATO STO RWS HFM-288 Research Workshop (RWS) on Integrated Approach to Cyber Defence: Human in the Loop organized at the final stage of the work of the team on 16 – 18 April 2018 in Sofia, Bulgaria.

During the workshop, thirty-seven authors from nine NATO and PfP nations submitted twenty-eight presentations in three days of sessions. Four keynote presentations in two sessions were delivered the first day, followed by seven topic sessions in the next two days of the workshop.

The general concept for an Integrated Approach to Cyber Defence, centered on human behaviour in the cyber domain, has been recognized as a missing block in building and sustaining cyber security systems in the rapidly growing and dynamic cyberspace.

Recognizing the value of this research domain, HFM-288 RWS was organized to achieve the following goals:

- To promote cyber security system thinking including the Human Factors in defence domain;
- To explore and address the range of Human Factors topics/ issues relevant to cyber security; and

- To summarize conclusions and recommendations for how Human Factors can enhance cyber defence in national and allied formats.

The three-day workshop was designed to identify various aspects of the key role and responsibilities of the human factor in building resilient cyber security and cyber defence systems. Bringing together civilian policy makers, military leaders at strategic and operational level, cyber security experts, academia, IT industry and non-governmental organizations, the workshop organizers created a collaborative environment for intensive discussion and sharing of ideas on the enhanced role of the human factor in fighting cybercrimes and cyber attacks. A challenge to all participants was to provide a solid research basis for developing concepts and approaches to keep humans in the loop in building and sustaining a resilient cyber defence in military and non-military organizations.

The first session included two keynote presentations under the general theme of the workshop. The initial presentation was the keynote address by Mr Alan R. Shaffer, Director of Collaboration Support Office at NATO STO, who stressed the changing character of the cyber warfare in terms both the networks and human factors. A key point he made was that all modern platforms are networks of computers, which are vulnerable to cyber attacks. He also defined the future warfare, compared to the contemporary one, as different, computer and network assisted, and combined with cyber campaigns against the population and critical infrastructure of the target nation. Mr Shaffer outlined the mission and activities of NATO STO and the CSO, defining latter as a collaborative production engine of the STO. He also outlined the mission of HFM Panel and the collaborative program of work in cyber domain and the current HFM-288 RWS. His conclusions about the human factor in building a robust cyber security and defence system were training humans to detect the anomalous behaviour and develop better training measures; implement more robust cyber hygiene; evaluate cyber architecture; and incorporate/develop artificial intelligence tools to detect / turn off attacks. The key message of Mr. Shaffer was that any collection of computers in a network is vulnerable and needs a robust protection with humans in the loop. His presentation generated great interest and many questions.

Professor Alan Brill highlighted in his keynote address that cyber offensive operations, if not confronted, have a potential to kick humans out of the loop in cyber security. He discussed the sensitive issue of judicial aspects of cybercrimes, insisting that only humans can be committed to such crimes. He also stressed the requirement for using cyber defence automation and even Artificial Intelligence (AI) cyber security tools under human control in successfully protecting against fast automated and sophisticated cyber attacks. Professor Brill claims that the human control must prevent the violation of laws, so “humans have to be in the loop”. His understanding is that different categories of people, working for the offensive or the defensive side of the cyberspace, can be the part of the loop and the lines are often blurring. He left three important messages: automated response to cyber attacks will be required but under human control; a formal process for security evaluation of all Internet of Things (IoT) devices need to be established and applied when we buy them; and apply the knowledge of this workshop to our organizations.

The second session of the workshop began with two additional keynote presentations. Professor Max Kilger has an extensive experience in the area of information security, especially on the social and psychological factors motivating malicious online actors, hacking groups and cyber terrorists. His presentation highlighted some theoretical work and empirical research into the social processes that shape significantly the threats in cyberspace. He presented some examples of these social processes at the individual, group and global community levels. Professor Kilger also emphasized the importance of developing a more comprehensive understanding of the relationship between individuals and digital technology as a method for developing future threat scenarios to inform policy makers and defence strategists. His recommendations in this respect, including the incorporation in the scenarios of psychological and social factors, can be considered as a valuable activity for

researches and professionals in this area. He underlined the reactive nature of current cyber defence strategies and the necessity for shift to more proactive and preventive strategies. His special emphasis on psychological roots of terrorists' use of cyberspace is of particular value in understanding their motivations and the emergence of cyber terror community. He stressed that the motivations are "the most traditional cause for terrorism and cyber terrorism". A special interest provoked his views on the evolution of cyber communities in the digital world, from hacking through cybercrime to cyber terror community.

Professor Corrado Jiustozzi addressed the issue of the cyber threats in perspective. From historical perspective he stressed the tremendous expansion of Internet with 3 billion users in 2015, and the prediction is to reach 4 billion users in 2019. He presented data of what happened in Internet for 1 minute in 2017: 156 million emails sent, 16 million text messages, 4.1 million videos viewed, 3.5 million Google search queries, 900,000 Facebook logins, etc. He also stressed that in 2019 network-connected devices will number more than three-and-a-half times that of the Earth's population. To his understanding, this unmanageable internet complexity created "cultural, behavioural and legal problems in the human society". Professor Jiustozzi believes that exploiting technical, complexity and human/behavioural weaknesses of the cyberspace, cyber attackers will always put at risk and compromise cyber security systems. His key message was that in a highly populated cyberspace the threats are rapidly growing, as well as the cyber attack surface.

In addition, the workshop covered the following topics: Cyber resilience: individual and organizational aspects; Cyber situation awareness; Innovative Human Systems integration approaches to cope with cyber threats; Cyber Security Education and Training; Cyber Security: How to improve human machine interface; Vulnerabilities with respect to the role of human factors and organizational processes in cyber defence and Lessons learned and future research perspectives.

During the workshop, NATO STO HFM-259 RTG team presented the intermediate results from the process of development of the conceptual framework to study human factors in cyber security, data collection, analysis and relational database (MySQL) with a web-based interface application to support data exploration.

The output of the workshop is to be a publication of selected papers in *Information & Security: An International Journal* in 2019.

Finally, yet importantly, the HFM-259 RTG team presented the findings during the IST-143 Lecture Series on Cyber Security Science and Engineering in Sofia, Bulgaria, 7 – 8 November 2017 and collaborated with IST-108 RTG and SAS-116 RTG on Cyber Security Awareness.

8.3 REFERENCES

[1] Yanakiev, Y. (Ed.). Human Systems Integration Approach to Cyber Security: Proceedings of International Conference, 28 – 29 September 2015, Sofia, Bulgaria. ISBN 978-954-9348-77-4.

Chapter 9 – DISCUSSION AND CONCLUSION

Dr. A. van Vliet
TNO Unit Defence Safety and Security
NETHERLANDS

1.1 DISCUSSION

In Chapter 1 we illustrate that the challenge for both collective and national security is to minimise the risks of cyber threats. For that reason, we need a common research perspective to study cyber security that focuses on the interrelatedness of technology and software developments, concepts, strategies and doctrines, organizational processes improvement and human performance.

A proper solution to respond to the complex phenomenon of cyber security is to implement HSI philosophy and methodology, as is discussed in Chapter 2. This means to apply a human-centred approach, which provides comprehensive foundations to analyse cyber security as a socio-technical system covering diverse dimensions such as psychosocial, cultural, organizational processes, technological and software developments.

To achieve this goal, the HFM-259 RTG team developed and tested a framework, knowledge base and used sophisticated software tooling (Gephi) that can be used to analyse what is known about human factors in cyber security.

In Chapter 3 we described the essence of our approach by linking theoretical sound concepts in a database which could be accessed by users and made available the empirical and theoretical insights and their sources in an insightful manner. The demonstration of this approach shows that this is feasible, although in our case, because we are limited to paper, we lack the sophistication of an interactive demonstrator.

This approach is not restricted to human factors and cyber security, all sorts of other issues and phenomena can be made available in this manner. With the advancement of natural language processing, the manual work, which was considerable, can be automated.

If the NATO.STO organization would want the sharing and advancement of science and technology to be enhanced, we would advise the STO organization to start setting up server facilities that would allow for this kind of knowledge sharing and sophisticated tooling.

In Chapter 4, as shown by this review, the HFM database can provide useful insights into how different aspects of user behaviour and cognition increase and decrease cyber security. Assessment of human behaviour can give insight into unexpected source of vulnerabilities, such as vulnerability, and the efficacy of different mitigation strategies such as training and rewards. Humans are the purveyors, operators, users, and exploiters of these systems. To ignore human behaviour in the system is to leave large vulnerabilities. Therefore, systems should be designed and deployed with consideration for who will use them, their purposes, and use contexts.

Information security policies are procedural and managerial controls that organizations use to enhance their computer and information security. In Chapter 5 we reviewed the most frequently discussed in the literature individual and organizational factors associated with policy management and its effectiveness, i.e., compliance. Based on the information collected in our knowledge base at the time of writing, when investigating ISSPs and

compliance the most frequently discussed individual factors include individual norms and values of the employees, their risk perception, workload, and information security awareness. The most frequently discussed organizational factors with respect to non-compliance are organizational sanctions and rewards, security culture, information security training and policy management.

Overall, there is a growing body of research addressing various aspects of ISSP management and compliance. While some of these factors have received considerable attention in the literature, others have not. For example, at the time of writing, the knowledge base contains no or very limited sources discussing the following:

- Technical mitigation mechanisms to address compliance issues;
- HMI ergonomics and HMI complexity issues with respect to ISSP compliance;
- Cognitive neutralization strategies that people use to justify non-compliance;
- The impact of organizational structure;
- Mitigating non-compliance with task and process re-design; and
- Assessment of information security competency.

More research in these areas would undoubtedly improve our knowledge and understanding of effective ISSP design and management.

Another significant gap in the current version of the knowledge base is the lack of information regarding effectiveness of various mitigation mechanisms. And, therefore, more research is required to investigate effectiveness of various mitigation mechanisms.

Chapter 6 shows that available studies provide some initial recommendations for how to recruit, select, train, and retain cyber security personnel. For example, recruitment should encourage investigative interests, rational decision-making style, and higher self-efficacy. Further, for selection of cyber security personnel, applicants' general abilities are more important than their IT knowledge. Cyber security personnel perform a wide range of roles that require many abilities, such as problem identification, communication, and resilience that are more difficult to obtain during training than IT knowledge.

Course programs for training of cyber security personnel needs to be more explicit of how acquired knowledge corresponds to actual requirements. Positive responses by students is not enough to guarantee necessary knowledge requirements. One option is to base the training on deterrence from crime prevention theories. Such training may increase attackers' perceived effort and risk, decrease rewards and crime inducing factors, and stimulate correct behaviour.

Intrusion detection is an important part of cyber security where detailed feedback during training improves analysts' detection of attacks. The detailed feedback should include whether analysts correctly detect and reject attacks, give false alarms, and miss attacks. Further, analysts need training in how experienced analysts use available software tools. Additionally, while most intrusions are of routine nature that analysts manage by themselves, larger incidents require analysts to work as a team. Training in role specialisation and teamwork processes are important for improving analysts' ability to manage such larger incidents.

The high burnout rate of some cyber security analysts may be due to entry-level analysts having limited opportunities to learn new skills when the management does not trust their abilities. Breaking such a vicious circle and instead grow the human capital requires more trust in analysts' abilities and more opportunities to work on challenging tasks.

While research about how to recruit, select, train, and retain cyber security personnel continues to mature, further studies are necessary for definite recommendations about how to create a coherent and sustainable profession of cyber security personnel.

In Chapter 7 we show that the problems of cyber security are not limited to the technical aspects of the protection of information resources; they must include in their entirety the following types of protection: legal, technical, informational, organizational and psychological.

As part of the training of participants in the educational process on cyber security, it is proposed to use "cyber vaccination", that is, the formation of a conscious cognitive experience of staying under the influence of a cyber threat and counteracting it as a system of training activities that include, in addition to traditional methods, training "cyber attacks", as well as the formation of knowledge and skills of sustainability (recovery) in relation to cyber threats. A special point should be the issue of resistance to cyber hazards, which can use the experience of training operators of the emergent industries, primarily diagnosing the current state of the person and necessary adjustments in order to optimize its activities.

Finally, by means of workshops the NATO STO HFM-259 RTG team presented the intermediate results from the process of development of the conceptual framework to study human factors in cyber security and used the feedback to update and enhance our collaborative effort.

1.2 CONCLUSIONS

The NATO STO HFM-259 RTG team has made clear based on theory and evidence that human factors are of major importance in enhancing cyber security. The cyber system consists of "machine entities" that act but also human entities that act and therefore both machines and humans can enhance or debilitate the security of cyber systems or parts thereof, whether these entities are attackers or targets.

We have proposed a framework to make sense of actors and actions involved and collected data from open sources to support our sense making effort.

We have highlighted various points of view to illustrate in more detail the importance of human factors. We are aware that other perspectives are also possible but lack the resources within the scope of this RTG to explore these and their utility.

We also understand that more open source information is available, and this body of knowledge is growing, perhaps even exponentially. We think it would be worthwhile to take our approach to the next level by making use of the advancements in the field of data science. This would allow for a more comprehensive and evolving collection of insights that could be made available to some or all stakeholders involved within a NATO setting.

Finally, comprehending how cyber security can be enhanced, identifying mechanisms that are instrumental, also poses a danger for misuse of these insights. This is an observation that the HFM panel can ponder on.

Annex A – FRAMEWORK

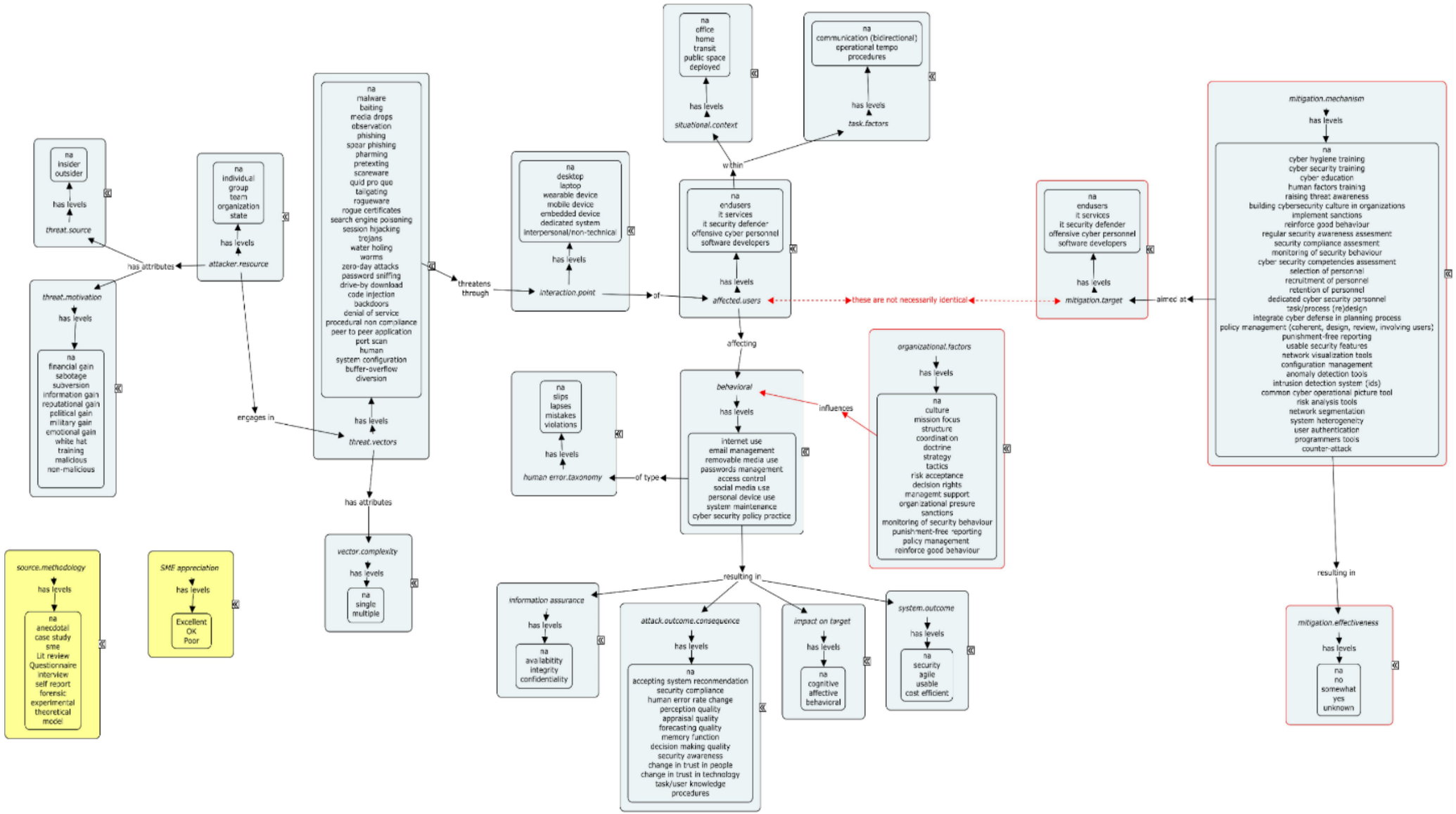

Figure A-1: Complete Ontology.

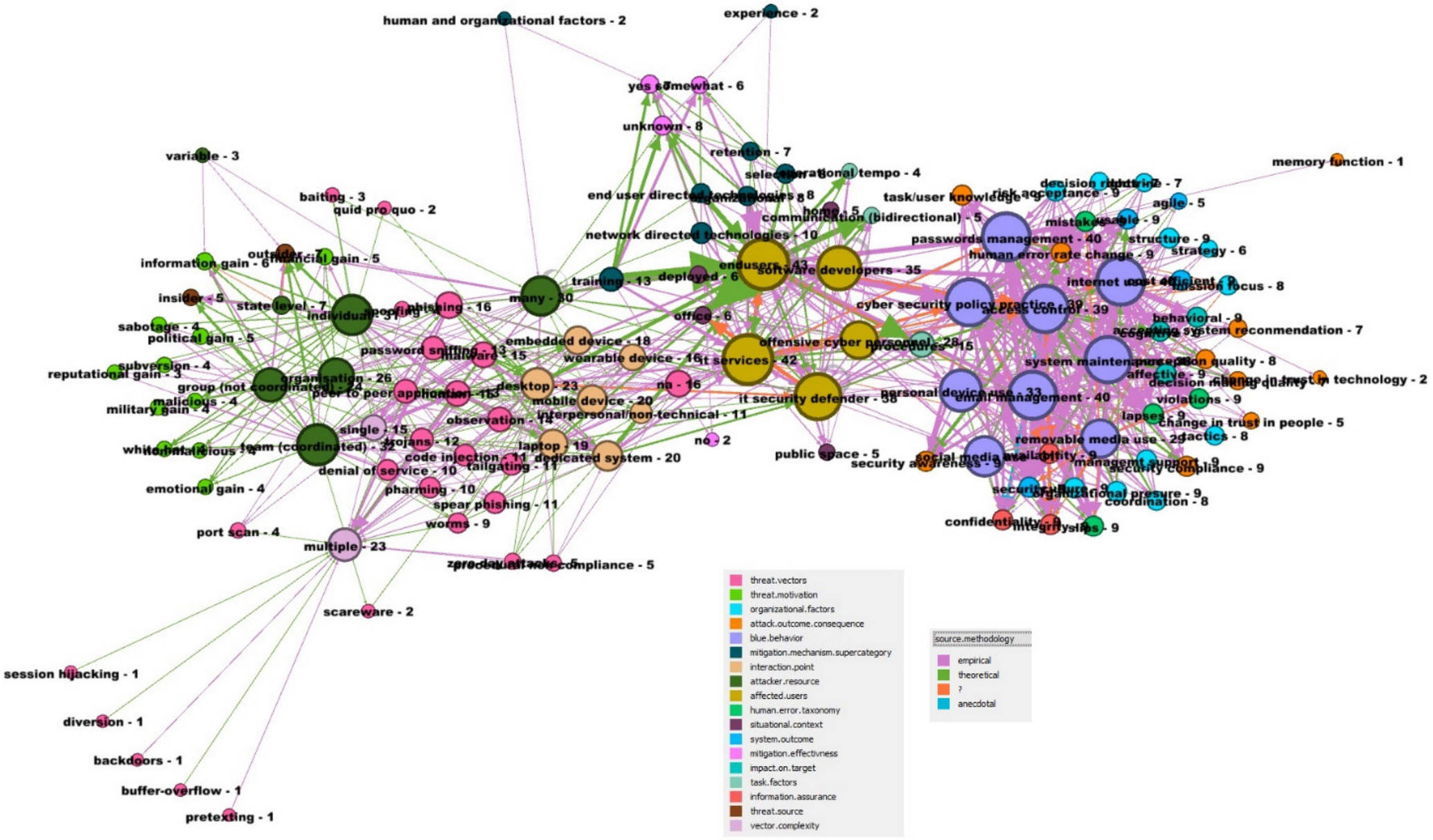

Figure A-2: Total Network.

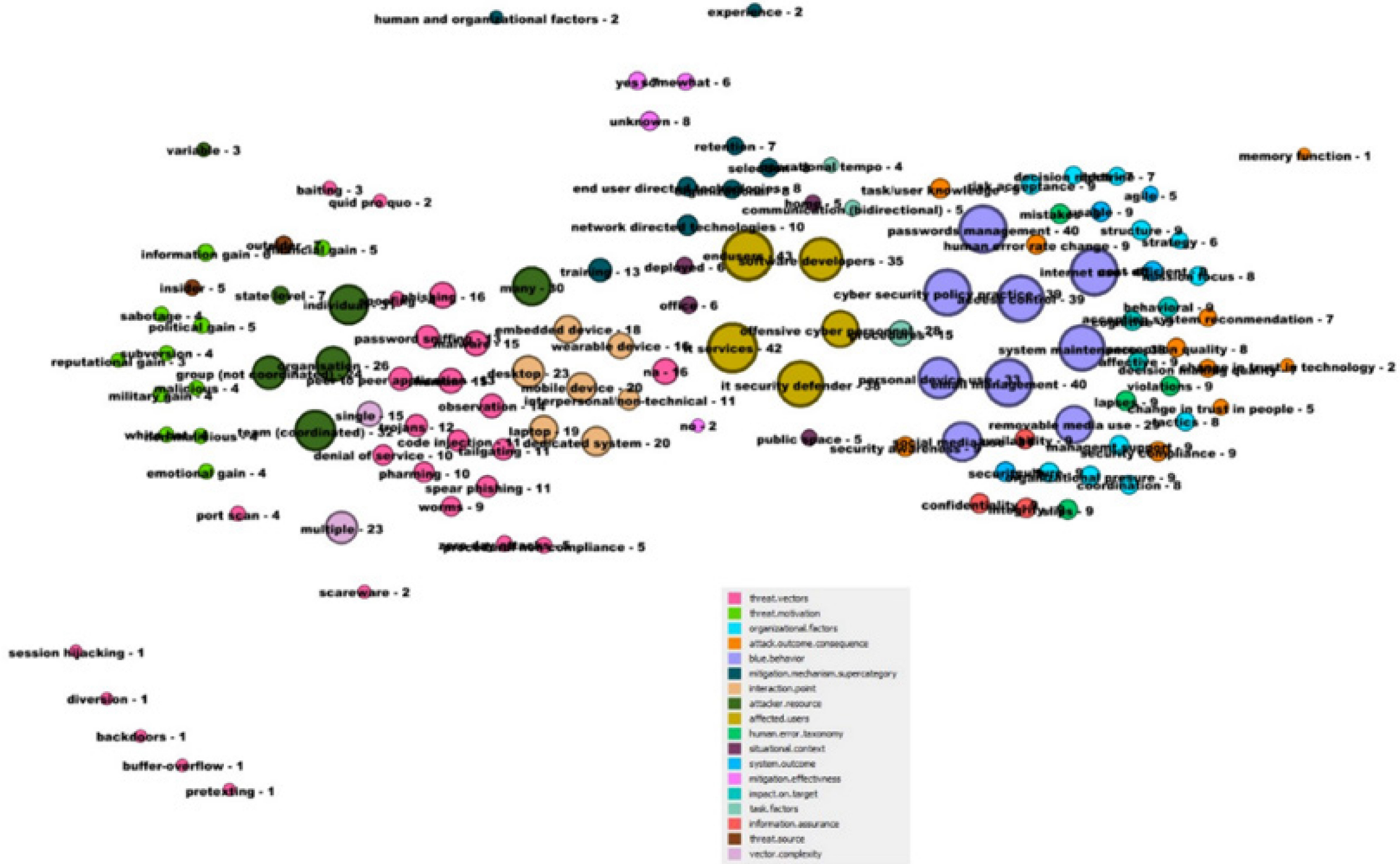

Figure A-3: Concepts and Their Occurrence in the Database.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-HFM-259 AC/323(HFM-259)TP/948	ISBN 978-92-837-2272-4	PUBLIC RELEASE

5. Originator

Science and Technology Organization
North Atlantic Treaty Organization
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

6. Title

Human Systems Integration Approach to Cyber Security

7. Presented at/Sponsored by

Final Report of Research Task Group HFM-259.

8. Author(s)/Editor(s)	9. Date
Multiple	June 2020
10. Author's/Editor's Address	**11. Pages**
Multiple	112

12. Distribution Statement

There are no restrictions on the distribution of this document. Information about the availability of this and other STO unclassified publications is given on the back cover.

13. Keywords/Descriptors

Cyber resilience; Cyber security; Human factors; Human Systems Integration; Human-machine interfaces; Insiders threat; Mitigation of non-compliance; Non-compliance; Ontology; Socio-technical system

14. Abstract

This report describes the efforts of the NATO STO HFM 259 RTG team to make sense of how human factors contribute to the enhancement of cyber security. In a systematic approach, a framework for the understanding of actors and factors involved in cyber systems was developed by the contributing nations. The framework was used as an architecture for a database which was then manually populated with open source information, extracted from articles. Various perspectives on this knowledge base were reported and these generate insights in mechanisms that are or could be instrumental in the enhancement of security of cyber systems.

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DIFFUSION DES PUBLICATIONS
STO NON CLASSIFIEES

Les publications de l'AGARD, de la RTO et de la STO peuvent parfois être obtenues auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la STO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

Les publications de la STO, de la RTO et de l'AGARD sont également en vente auprès des agences de vente indiquées ci-dessous.

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivi du numéro de série. Des informations analogues, telles que le titre est la date de publication sont souhaitables.

Si vous souhaitez recevoir une notification électronique de la disponibilité des rapports de la STO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (http://www.sto.nato.int/) et vous abonner à ce service.

CENTRES DE DIFFUSION NATIONAUX

ALLEMAGNE
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7, D-53229 Bonn

BELGIQUE
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research
for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Bruxelles

BULGARIE
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DGSIST 2
Recherche et développement pour la défense Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

DANEMARK
Danish Acquisition and Logistics Organization
(DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESPAGNE
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

ESTONIE
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

ETATS-UNIS
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72
92322 Châtillon Cedex

GRECE (Correspondant)
Defence Industry & Research General
Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HONGRIE
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALIE
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG
Voir Belgique

NORVEGE
Norwegian Defence Research
Establishment
Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

PAYS-BAS
Royal Netherlands Military
Academy Library
P.O. Box 90.002
4800 PA Breda

POLOGNE
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

REPUBLIQUE TCHEQUE
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

ROUMANIE
Romanian National Distribution
Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

ROYAUME-UNI
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down
Salisbury SP4 0JQ

SLOVAQUIE
Akadémia ozbrojených síl gen.
M.R. Štefánika, Distribučné a
informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

SLOVENIE
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

TURQUIE
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi
Başkanlığı
06650 Bakanliklar – Ankara

AGENCES DE VENTE

The British Library Document
Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
ROYAUME-UNI

Canada Institute for Scientific and
Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications STO, RTO et AGARD figurent dans le « NTIS Publications Database » (http://www.ntis.gov).

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DISTRIBUTION OF UNCLASSIFIED STO PUBLICATIONS

AGARD, RTO & STO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all STO reports, or just those relating to one or more specific STO Panels, they may be willing to include you (or your Organisation) in their distribution.

STO, RTO and AGARD reports may also be purchased from the Sales Agencies listed below.

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number. Collateral information such as title and publication date is desirable.

If you wish to receive electronic notification of STO reports as they are published, please visit our website (http://www.sto.nato.int/) from where you can register for this service.

NATIONAL DISTRIBUTION CENTRES

BELGIUM
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30
1000 Brussels

BULGARIA
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DSTKIM 2
Defence Research and Development Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

CZECH REPUBLIC
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

DENMARK
Danish Acquisition and Logistics Organization (DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESTONIA
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc – BP 72
92322 Châtillon Cedex

GERMANY
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7
D-53229 Bonn

GREECE (Point of Contact)
Defence Industry & Research General Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HUNGARY
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALY
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG
See Belgium

NETHERLANDS
Royal Netherlands Military Academy Library
P.O. Box 90.002
4800 PA Breda

NORWAY
Norwegian Defence Research Establishment, Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

POLAND
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

ROMANIA
Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

SLOVAKIA
Akadémia ozbrojených síl gen M.R. Štefánika, Distribučné a informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

SLOVENIA
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

SPAIN
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

TURKEY
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar – Ankara

UNITED KINGDOM
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down, Salisbury SP4 0JQ

UNITED STATES
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

SALES AGENCIES

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
UNITED KINGDOM

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of STO, RTO and AGARD publications are given in "NTIS Publications Database" (http://www.ntis.gov).

ISBN 978-92-837-2272-4