CENTER FOR
CYBER DEFENCE AND
INFORMATION SECURITY

KTH
VETENSKAP
OCH KONST

Reflections on Cyber Situation Awareness

Henrik Artman, KTH

CDIS Spring Conference 2022

KTH Royal Institute of Technology

Tuesday, May 24, 2022

Project: Cyber Situation Awareness

Doctoral Student:

Annika Andreasson

Supervisors:

Henrik Artman

Joel Brynielsson

Ulrik Franke

The overall aim of the project is to:

“conduct research in support of developing the CSA capability”

What is Situation Awareness?

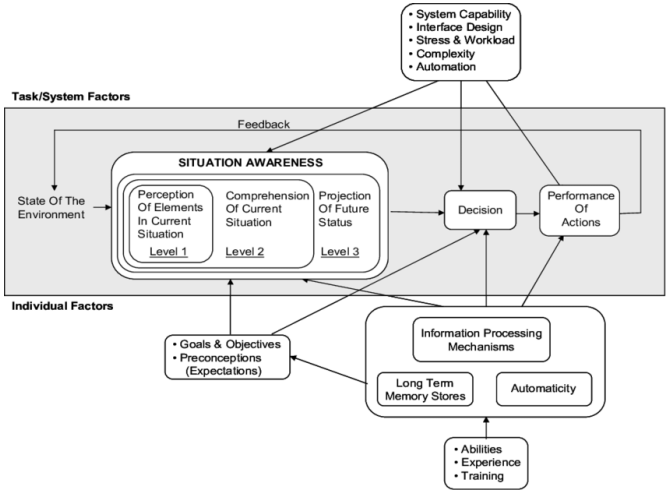
Situation Awareness

*"the **perception** of the elements in the environment within a volume of time and space, the **comprehension** of their meaning, and the **projection** of their status in the near future"*

Endsley, M. (1995) Toward a theory of situation awareness in dynamic systems, *Human Factors*, 37 (1), 32-64

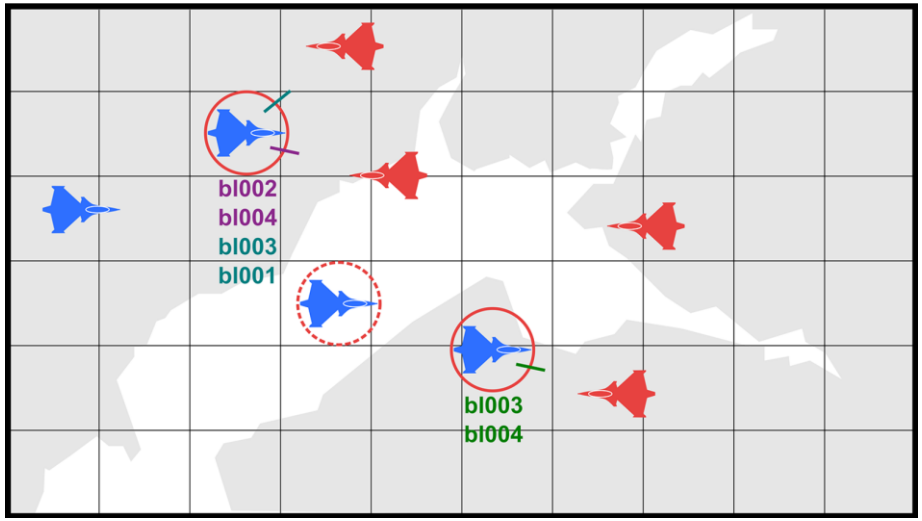
Criticism of Situation Awareness

- **Mentalistic** – does not account for external aids
- **Individualistic** – focus on the individual, not collaboration (negotiation; interpretations; task alignment etc.)
- **Not a strong explanation** – loss of Situation Awareness…
- Cyber is something different from Aviation



Situation Awareness in fighter pilot aviation

- Geographical position
  - Projection (speed/time/space)
- Known adversary
  - Relatively known capacity
  - Tactics relatively known
- Haptics and partly visual view
- Highly cooperative
- Perception and radar-driven



Cyber Situation Awareness

- Time and Geography different
- Unknown threat (initially)
- Adversary known, not known
- Meaning with attack is not easily understood
- Erasable trails
- Data-driven approach / reactive

Common operation picture

COP & SA

Common Operational Picture
(*Lägesbild*)

Situational Awareness
(*Lägesförståelse*)

Foton: SAAB, Försvarsmakten

Current research question

What factors do decision-makers consider important for making relevant decisions regarding the cyber environment?

or

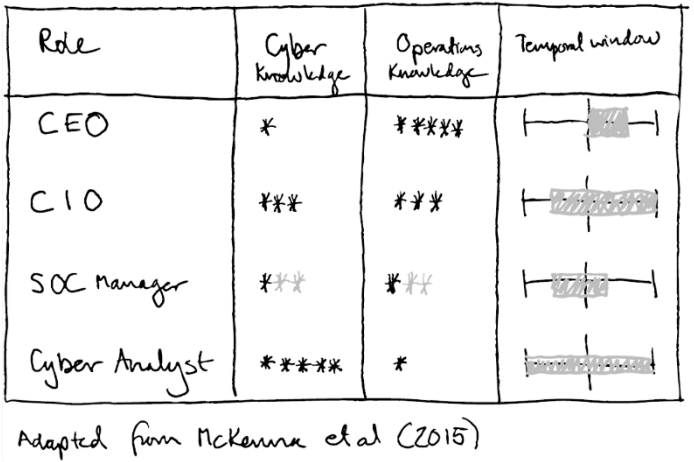
What CSA do decision-makers (think that they) need?

What factors are there?

Perception
- Network factors
  - > Network infrastructure state (normal)
  - > Firewall
  - > IDS

Comprehension
- Intelligence factors
  - > Threat intelligence
  - > Threat actors
  - > *Modus operandi*

Projection
- Organization/Mission factors
  - > Organizational dependencies
  - > Organizational goals



2022 Research plan

1. **Administrative Authority Employee CSA**
   Interviews transcribed and undergoing analysis
   Write-up Spring 2022
2. **Semi-autonomous Cyber Command and Control System (SAC3)**
   Demonstrator project
   Planned project start: 15 January 2022
   Project duration: 1 year
3. **Planned surveys with Bredband2**

Future research ideas

- **GDTA within an organization**
  - Perform a GDTA within an organization to understand CSA requirements for successful job performance
- **Case study of an organization**
  - Examine if/how CSA requirements differ between decision-makers at different levels within the organization

Questions?

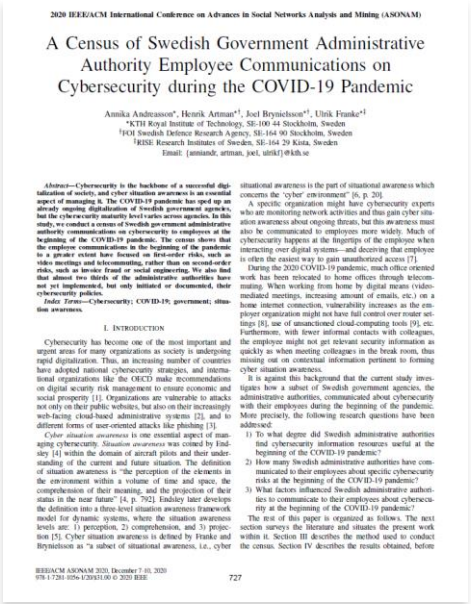
Publications

1. A. Andreasson, H. Artman, J. Brynielsson, and U. Franke, “A census of Swedish government administrative authority employee communications on cybersecurity during the COVID-19 pandemic,” in *Proceedings of the 2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2020)*. IEEE, 2020, pp. 727-733.
2. A. Andreasson, H. Artman, J. Brynielsson and U. Franke, “A census of Swedish public sector employee communication on cybersecurity during the COVID-19 pandemic,” *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 2021, pp. 1-8.
3. U. Franke, A. Andreasson, H. Artman, J. Brynielsson, S. Varga, and N. Vilhelm. “Cyber situational awareness issues and challenges”, in M. Ahmed (Ed.), *Cybersecurity and Cognitive Science,* Elsevier, forthcoming.

Paper 1

“A census of Swedish government administrative authority employee communications on cybersecurity during the COVID-19 pandemic”

- 64% of administrative authorities are not yet at the implemented systematic cybersecurity maturity level
- 89% of administrative authorities found information from MSB useful
- Stronger focus on first-order risks (telecommuting, video meetings) than second order risks (phishing, invoice fraud)



2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)

A Census of Swedish Government Administrative Authority Employee Communications on Cybersecurity during the COVID-19 Pandemic

Annika Andreasson*, Henrik Artman*†, Joel Brynielsson*†, Ulrik Franke*‡
*KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
†FOI Swedish Defence Research Agency, SE-164 90 Stockholm, Sweden
‡RISE Research Institutes of Sweden, SE-164 29 Kista, Sweden
Email: {anniandr, artman, joel, ulrikf}@kth.se

***Abstract*—Cybersecurity is the backbone of a successful digitalization of society, and cyber situation awareness is an essential aspect of managing it. The COVID-19 pandemic has sped up an already ongoing digitalization of Swedish government agencies, but the cybersecurity maturity level varies across agencies. In this study, we conduct a census of Swedish government administrative authority communications on cybersecurity to employees at the beginning of the COVID-19 pandemic. The census shows that the employee communications in the beginning of the pandemic to a greater extent have focused on first-order risks, such as video meetings and telecommuting, rather than on second-order risks, such as invoice fraud or social engineering. We also find that almost two thirds of the administrative authorities have not yet implemented, but only initiated or documented, their cybersecurity policies.**

***Index Terms*—Cybersecurity; COVID-19; government; situation awareness.**

I. Introduction

Cybersecurity has become one of the most important and urgent areas for many organizations as society is undergoing rapid digitalization. Thus, an increasing number of countries have adopted national cybersecurity strategies, and international organizations like the OECD make recommendations on digital security risk management to ensure economic and social prosperity [1]. Organizations are vulnerable to attacks not only on their public websites, but also on their increasingly web-facing cloud-based administrative systems [2], and to different forms of user-oriented attacks like phishing [3].

Cyber situation awareness is one essential aspect of managing cybersecurity. *Situation awareness* was coined by Endsley [4] within the domain of aircraft pilots and their understanding of the current and future situation. The definition of situation awareness is “the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future” [4, p. 792]. Endsley later develops the definition into a three-level situation awareness framework model for dynamic systems, where the situation awareness levels are: 1) perception, 2) comprehension, and 3) projection [5]. Cyber situation awareness is defined by Franke and Brynielsson as “a subset of situational awareness, i.e., cyber situational awareness is the part of situational awareness which concerns the ‘cyber’ environment” [6, p. 20].

A specific organization might have cybersecurity experts who are monitoring network activities and thus gain cyber situation awareness about ongoing threats, but this awareness must also be communicated to employees more widely. Much of cybersecurity happens at the fingertips of the employee when interacting over digital systems—and deceiving that employee is often the easiest way to gain unauthorized access [7].

During the 2020 COVID-19 pandemic, much office oriented work has been relocated to home offices through telecommuting. When working from home by digital means (video-mediated meetings, increasing amount of emails, etc.) on a home internet connection, vulnerability increases as the employer organization might not have full control over router settings [8], use of unsanctioned cloud-computing tools [9], etc. Furthermore, with fewer informal contacts with colleagues, the employee might not get relevant security information as quickly as when meeting colleagues in the break room, thus missing out on contextual information pertinent to forming cyber situation awareness.

It is against this background that the current study investigates how a subset of Swedish government agencies, the administrative authorities, communicated about cybersecurity with their employees during the beginning of the pandemic. More precisely, the following research questions have been addressed:

1) To what degree did Swedish administrative authorities find cybersecurity information resources useful at the beginning of the COVID-19 pandemic?
2) How many Swedish administrative authorities have communicated to their employees about specific cybersecurity risks at the beginning of the COVID-19 pandemic?
3) What factors influenced Swedish administrative authorities to communicate to their employees about cybersecurity at the beginning of the COVID-19 pandemic?

The rest of this paper is organized as follows. The next section surveys the literature and situates the present work within it. Section III describes the method used to conduct the census. Section IV describes the results obtained, before

IEEE/ACM ASONAM 2020, December 7-10, 2020
978-1-7281-1056-1/20/$31.00 © 2020 IEEE

Paper 2

“A census of Swedish public sector employee communication on cybersecurity during the COVID-19 pandemic”

- Same sources of information were deemed useful across public sector
- 73% of county councils self-assess as having implemented systematic cybersecurity
- 71% of municipalities do not have full time cyber-/information security staff

A Census of Swedish Public Sector Employee Communication on Cybersecurity during the COVID-19 Pandemic

Annika Andreasson*, Henrik Artman*†, Joel Brynielsson*‡, Ulrik Franke*‡
*KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
†FOI Swedish Defence Research Agency, SE-164 90 Stockholm, Sweden
‡RISE Research Institutes of Sweden, SE-164 29 Kista, Sweden
Email: {anniandr, artman, joel, ulrikf}@kth.se

***Abstract*—The COVID-19 pandemic has accelerated the digitalization of the Swedish public sector, and to ensure the success of this ongoing process cybersecurity plays an integral part. While Sweden has come far in digitalization, the maturity of cybersecurity work across entities covers a wide range. One way of improving cybersecurity is through communication, thereby enhancing employee cyber situation awareness. In this paper, we conduct a census of Swedish public sector employee communication on cybersecurity at the beginning of the COVID-19 pandemic using questionnaires. The study shows that public sector entities find the same sources of information useful for their cybersecurity work. We find that nearly two thirds of administrative authorities and almost three quarters of municipalities are not yet at the implemented cybersecurity level. We also find that 71 % of municipalities have less than one dedicated staff for cybersecurity.**

***Index Terms*—Cybersecurity; COVID-19; public sector; situation awareness.**

I. Introduction

The COVID-19 pandemic has taken its toll on society all over the world; first and foremost in terms of human life and suffering in the wake of illness, but also through the secondary effects disrupting everyday life and the economy. Among those secondary effects is the impact on cybersecurity. As people and organizations have struggled to adapt to the “new normal,” changing their patterns of work, social interaction, consumption, education, commuting, travel, etc., new cyber risks have emerged. Some risks are non-adversarial: when processes and procedures change rapidly, the risks of human errors, untested software, and improvised processes can easily entail service outages and data being lost or exposed to the wrong eyes. Other risks are adversarial: people working from home under stressful conditions and outside corporate networks offer new attack vectors that cybercriminals can take advantage of.

In this paper, we study such COVID-19 effects on cybersecurity by investigating how the Swedish public sector reacted to the new threat landscape. In particular, we study how government administrative authorities, county councils, and municipalities gathered information to uphold cyber situation awareness [1] and how they chose to communicate to their employees about cybersecurity.

This study was supported by the Swedish Armed Forces.

More precisely, we address three research questions:

1) To what degree did Swedish public sector entities find cybersecurity information resources useful at the beginning of the COVID-19 pandemic?
2) How many Swedish public sector entities have communicated to their employees about specific cybersecurity risks at the beginning of the COVID-19 pandemic?
3) What factors influenced Swedish public sector entities to communicate to their employees about cybersecurity at the beginning of the COVID-19 pandemic?

This paper extends our previous work [2]. Whereas the previous paper covered government administrative authorities only, we now present a fuller picture of the Swedish public sector: government administrative authorities, county councils, and municipalities. This broader material allows us to draw more profound conclusions compared to our previous work. Municipalities and regions are autonomous units as compared to the administrative authorities, which are part of the central government. This makes it interesting to compare how they handled cybersecurity during the pandemic.

Sweden is an interesting case to study, since the country regularly scores high in terms of digitalization. For example, in the European Commission’s Digital Economy and Society Index (DESI) 2020 [3], Sweden ranked second among all the EU countries. Indeed, the top four EU countries in the index (Finland, Sweden, Denmark, and the Netherlands) are considered among the global leaders in digitalization. However, Sweden often scores worse in international rankings on cybersecurity. For example, Sweden ranked only 17th in the ITU Global Cybersecurity Index (GCI) in 2017 [4] (and only 32nd in the 2018 edition, but this is a less valid measure since Sweden did not actively participate in the ranking exercise that year). This tension between being a forerunner in digitalization but somewhat lagging behind in cybersecurity makes Sweden an interesting object of study.

The rest of the paper is structured as follows. Section II discusses some related work, followed by a description of the undertaken methodology in Section III. Section IV contains the results obtained. The findings are discussed in Section V, before Section VI concludes.

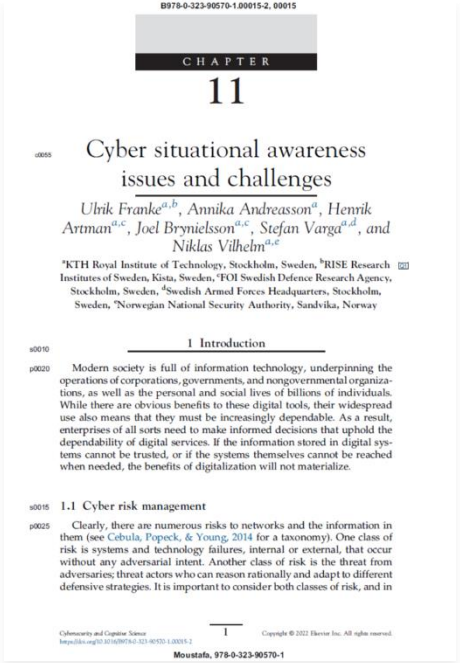
2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) | 978-1-6654-3259-2/20$31.00 ©2021 IEEE | DOI: 10.1109/CyberSA52016.2021.9478241

Paper 3

“Cyber situational awareness issues and challenges”

Exploring perspectives on CSA:

- Technological perspective
- Socio-cognitive perspective
- Organizational perspective
- Adversarial perspective



B978-0-323-90570-1.00015-2, 00015

CHAPTER

11

Cyber situational awareness issues and challenges

Ulrik Franke[a,b], Annika Andreasson[a], Henrik Artman[a,c], Joel Brynielsson[a,c], Stefan Varga[a,d], and Niklas Vilhelm[a,e]

[a]KTH Royal Institute of Technology, Stockholm, Sweden, [b]RISE Research Institutes of Sweden, Kista, Sweden, [c]FOI Swedish Defence Research Agency, Stockholm, Sweden, [d]Swedish Armed Forces Headquarters, Stockholm, Sweden, [e]Norwegian National Security Authority, Sandvika, Norway

1 Introduction

Modern society is full of information technology, underpinning the operations of corporations, governments, and nongovernmental organizations, as well as the personal and social lives of billions of individuals. While there are obvious benefits to these digital tools, their widespread use also means that they must be increasingly dependable. As a result, enterprises of all sorts need to make informed decisions that uphold the dependability of digital services. If the information stored in digital systems cannot be trusted, or if the systems themselves cannot be reached when needed, the benefits of digitalization will not materialize.

1.1 Cyber risk management

Clearly, there are numerous risks to networks and the information in them (see Cebula, Popeck, & Young, 2014 for a taxonomy). One class of risk is systems and technology failures, internal or external, that occur without any adversarial intent. Another class of risk is the threat from adversaries; threat actors who can reason rationally and adapt to different defensive strategies. It is important to consider both classes of risk, and in

Moustafa, 978-0-323-90570-1

What factors have we studied?

- Paper 1 and 2
  - Network factors
    - > What observed cyber incidents prompted communication?
  - Intelligence factors
    - > What sources of information were deemed trustworthy and useful for communication
- Paper 3
  - ”All factors”
    - > Reasoning about how factors focusing on different areas fit in CSA and how CSA is best understood by combining technological, socio-cognitive, organizational, and adversarial perspectives.