Volume 16, Issue 4 • Fall 2017

ISSN 1445-3312 (Print)

ISSN 1445-3347 (Online)

JOURNAL OF INFORMATION WARFARE

Journal of Information Warfare

Volume 16 Issue 4 Fall 2017

Journal of Information Warfare

Volume 16, Issue 4
Fall 2017

Contents

Authors

Robert Bird is a Senior Lecturer at Coventry University and the course director for a number of programs, including the master's program in Forensic Computing. Prior to joining Coventry, he was a superintendent with the West Midlands Police.

Frans Hendrik Botes is a postgraduate student at Cape Peninsula University of Technology. He is a hobbyist hacker and has research interests in artificial intelligence and cyber security.

Dr. Retha De La Harpe is the acting Head of the IT Department in the Faculty of Informatics and Design at Cape Peninsula University of Technology. She earned both a bachelor's degree in Informatics and a master's degree from Rand Afrikaans University. She earned D.Tech (IT) qualification at Cape Peninsula University of Technology in 2009. She is the South African Coordinator of the Informatics Development for Health in Africa (INDEHELA) international research network and was a National Research Fund grant holder for four years. She is author and co-author of several research funding proposals—including the South Africa Finland Partnership. Her main research interest concerns data quality implications in both business and healthcare contexts.

Dr. Roger Green is Emeritus Professor of Electronic Communication Systems at the University of Warwick. He earned a bachelor's degree in Electronics from the University of Manchester in 1973, and a doctorate in Video Communications from Bradford University in 1976. After graduation, he worked for GEC Electro-Optical Systems in Essex until 1978 when he rejoined academic life at Bradford University, serving there from 1978 to 1999. He was appointed to the Chair in Electronic Communication Systems at Warwick University in September 1999 and led a research group there in optical communications. For five years during his time at Warwick he served as Head of the Division of Electrical and Electronic Engineering. He continues to be active in the area of optical wireless communications. In 2009, he was awarded the D.Sc. in Photonic Communications, Systems, and Devices by Warwick University for his research. He was appointed to fellowship with the Institution of Engineering and Technology, and the Institute of Physics, and became a Senior Member of the Institute of Electrical and Electronics Engineers. He is also a member of the European Society for Engineering and Medicine. He oversaw the successful completion of 66 research students—mainly at the doctoral level—during his career. He has published widely, with around 300 refereed research papers published and presented internationally. He holds several patents.

Dominik Grüdl is a graduate student at Coburg University of Applied Sciences and Arts, where he serves on Dr. Dieter Landes' research team investigating Intrusion Detection Systems (IDSs). He completed undergraduate studies in Informatics at Coburg.

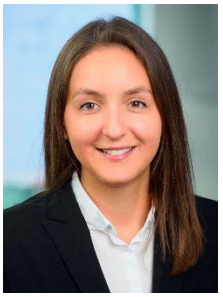
Dr. Diana Hintea is a Lecturer in Computer Science at Coventry University. There, she leads a series of modules on advanced programming, algorithms, and digital forensics. She earned a bachelor's degree in Engineering in 2010 from the Technical University of Cluj-Napoca and a doctorate from Coventry University in 2014. Her research interests focus on digital forensics, machine learning, and reinforcement learning-based applications.

Dr. Andreas Hotho is a Professor at the University of Würzburg. He earned a doctorate from the University of Karlsruhe, where he worked from 1999 to 2004 at the Institute of Applied Informatics and Formal Description Methods (AIFB) in the areas of text, data, and web mining; semantic web; and information retrieval. From 2004 to 2009 he was a Senior Researcher at the University of Kassel. In 2011, he joined the L3S. Since 2005, he has been leading the development of BibSonomy, the social bookmark and publication-sharing platform. He has published more than 100 articles in journals and at conferences, has co-edited several special issues and books, and has co-chaired several workshops. He has worked as a reviewer for journals and has been a member of international conferences and workshop program committees. His research focuses on Data Science—in particular, on the combination of data mining, information retrieval, and the semantic web.

Dr. Dieter Landes is a Professor of Software Engineering and Database Systems at Coburg University of Applied Sciences and Arts. He holds a diploma in Informatics from the University of Erlangen-Nuremberg, and a doctorate in Knowledge-Based Systems from the University of Karlsruhe. After several years working in industry—including time with Daimler Research—he joined Coburg in 1999. He has published 70 papers in journals, books, and at conferences. His research interests include requirements engineering, software-engineering education, learning analytics, and data mining.

Dr. Louise Leenen is a Principal Scientist in the Cyber Defence Research Group at the Council for Scientific and Industrial Research. She earned a doctorate in Computer Science from the University of Wollongong. She is the Chair of the International Federation for Information Processing's Working Group on ICT in War and Peace. Her research focuses on artificial-intelligence applications in cyber defence.

Dr. Mark S. Leeson is a Reader in Communication Systems in the School of Engineering at the University of Warwick. He earned bachelor's degrees in Electrical and Electronic Engineering from the University of Nottingham in 1986. He earned a doctorate in Engineering from the University of Cambridge in 1990. He worked as a Network Analyst for National Westminster Bank in London prior to taking academic posts in London and Manchester. In 2000 he joined the School of Engineering at Warwick. He has more than 250 publications and has supervised seventeen successful research students. He is a Senior Member of the Institute of Electrical and Electronics Engineers, and a Fellow of both the UK Institute of Physics and the UK Higher Education Academy. His major research interests are optical-communication systems, molecular communications, and machine learning.



Dr. Maria Leitner is a Scientist in the Center for Digital Safety & Security at AIT Austrian Institute of Technology. She earned a doctorate in Computer Science in 2015 from the University of Vienna. Her thesis focused on the integration and life-cycle management of security policies in process-aware information systems in order to ensure holistic security-policy management in organisations. Prior to joining AIT, she was a Researcher at SBA Research and a Research Assistant in the Workflow Systems and Technology Group in the Faculty of Computer Science at the University of Vienna. She is currently coordinating and working on national and international research projects in the areas of situational awareness, cyber defence, ICS security and identity management. She is representing AIT in the European Cyber Security Organisation (ECSO) Working Group 5 (Education, training, awareness, exercise) and in the Cyber Security Platform Austria. She is a member of the ACM and has published more than 25 refereed articles, conference papers, and workshop papers.

James Moss is a Senior Penetration Tester who has been involved in leading engagements against UK government systems and commercial clients.

Timea Pahi is a Junior Scientist at the Austrian Institute of Technology and is working on several research projects focusing on national cyber security, the protection of critical infrastructures, and cyber situational awareness.

Markus Ring is a Research Associate at Coburg University of Applied Sciences and Arts where he is working on his doctoral thesis. He previously studied Informatics at Coburg. He has previously worked as a Network Administrator at T-Systems Enterprise GmbH. His research interests include the generation of realistic flow-based network data and the application of data-mining methods for cyber-security intrusion detection.

Dr. Mari Ristolainen is a Researcher at the Finnish Defence Research Agency. She has studied psychology at the Moscow State University and she earned a doctorate in Russian Language and Cultural Studies from the University of Joensuu in 2008. She has been conducting postdoctoral research in the field of Russian and Border Studies in several Academy of Finland- and EU-funded projects at the University of Eastern Finland and at the University of Tromso. Her current research interests include cyber warfare as a phenomenon, Russian digital sovereignty, and the governance of cyber/information space.

Keith Scott is Programme Leader for English Language at De Montfort University, where he is also a member of the Cyber Security Centre. His research is concerned with human factors in cyber security, with a particular interest in the fields of influence and perception management.

Dr. Florian Skopik is a Senior Scientist at the ICT Security Research Team at the Austrian Institute of Technology (AIT), where he is responsible for national and European research projects focusing on smart grid security, the security of critical infrastructures, and national cyber security and cyber defence. Before joining AIT, he worked with the Distributed Systems Group at the Vienna University of Technology as a Research Assistant and Postdoctoral Research Scientist from 2007 to 2011, where he was involved in a number of international research projects dealing with cross-organisational collaboration over the Web. In the context of these projects, he finished his doctoral studies. He also spent a sabbatical at IBM Research India in Bangalore for several months. In addition, he has worked for numerous small- and medium-sized enterprises as a Firmware Developer for microcontroller systems for about 15 years. He has published more than 100 scientific conference papers and journal articles, and is a member of various conference program committees and editorial boards, as well as standardisation groups, such as ETSI TC Cyber and OASIS CTI. He holds 20 industry-relevant security certifications, including Trusted Security Auditor, ISA/IEC 62443 Security Specialist, CCNA Security, and ISO27001 Information Security Manager. In 2017, he finished a professional degree in Advanced Computer Security at Stanford University. He is an Institute of Electrical and Electronics Engineers Senior Member and Member of the Association for Computing Machinery (ACM).

Sharifuddin Sulaman is the International Engagement Executive at CyberSecurity Malaysia, an agency under the Ministry of Science, Technology, and Innovation, Malaysia. He earned a bachelor's degree in Information Systems Management from Universiti Teknologi MARA (UiTM).

Dr. Chrysanthi Taramonli is a Lecturer in Cyber Security and Forensics at Coventry University. She earned a bachelor's degree in Computer Science and a master's degree in Networks Security. She earned a doctorate in Engineering from the University of Warwick. Her research is focused on the use of stochastic methods in low-energy encryption and adaptive security, as well as on network forensics and stochastic log-file analysis.

Sarah Wunderlich is a Research Associate at the Coburg University of Applied Sciences and Arts. She earned a master's degree in Computer Science from Coburg in 2016. She has also worked as a Lecturer in Data Mining at Coburg. Her research interests include the generation of realistic flow-based network data and the application of data-mining methods for cyber-security intrusion detection.

Dr. Zahri Yunos is the Chief Operating Officer of CyberSecurity Malaysia, an agency under the Ministry of Science, Technology, and Innovation, Malaysia. He earned a doctorate in Information Security from the Universiti Teknikal Malaysia Melaka (UTeM). He has contributed to various publications related to cyber security. He also has been appointed as Adjunct Professor at UTeM.

Preparation, Modelling, and Visualisation of Cyber Common Operating Pictures for National Cyber Security Centres

T Pahi, M Leitner, F Skopik

Center for Digital Safety & Security
AIT Austrian Institute of Technology
Vienna, Austria

E-mail: timea.pahi@ait.ac.at; maria.leitner@ait.ac.at; florian.skopik@ait.ac.at

Abstract: *Common Operating Pictures (COPs) have long been a common denominator of effective cyber defence operations (for example, in law enforcement and the military). COPs are widely used to represent, visualise, and assess situations. In recent years, Cyber COPs (CCOPs) have become important in establishing cyber situational awareness. This paper describes the information types and sources required for an efficient information management process supporting CCOPs. Following an initial description of CCOPs, the paper next discusses potential decisions supported by them. Finally, it provides an example of the entire process—from the application of the information management process to national decision-making.*

Keywords: *Cyber Common Operating Picture (CCOP), Information Management (IM), Cyber Security, Cyber Situational Awareness (CSA), Decision-Making Processes*

Introduction

As the number of complex cyber attacks (such as ransomware, phishing, Distributed Denial of Service [DDoS], and Chief Executive Officer [CEO] fraud) has risen rapidly in recent years, it is becoming increasingly challenging for organisations and government agencies to adequately prepare for these incidents and to provide adequate cyber crisis management (Uma & Padmavathi 2013; Mansfield-Devine 2016). Moreover, recent conflicts and incidents have shown that no future conflict is likely to be fought without a cyber element, and establishing effective defensive measures is a difficult and resource-consuming task (for example, the cyber attack on Estonia described in Lesk [2007] or in Ottis [2008] or the cyber hacktivists described by Danitz & Strobel [2001]). However, a common denominator has always been the application of Common Operating Pictures (COPs), for example, in law enforcement and in the military. COPs are widely used to represent, display, and assess situations. Typically, they consist of objectively measured events, gathered from both internal and external sources, as well as the subsequent rating of these sources and enrichment with contextual information to facilitate the interpretation of measured events. In recent years, Cyber COPs (CCOPs) have become a key factor in the establishment and analysis of Cyber Situational Awareness (CSA) as well as decision-making processes (Conti, Nelson & Raymond 2013). CCOPs can be established with a variety of information depending on the purpose. For example, a CCOP for an organisation might display anomalous network traces in local network traffic or might identify potential malware that transmits data to external servers (such as with a security information and event management system). At the national level,

however, CCOPs become more challenging as potential incidents do not only occur in governmental agencies or institutions, but also within organisations (public and private) such as Critical Infrastructures (CIs) or small- and medium-sized enterprises. Instead, only shared incident information can be processed and evaluated at the national level.

This paper proposes an information management process to derive CCOPs at the national level. It consists of several steps (from defining the aim of the CCOP and selecting data types and sources, to preparing CCOPs for target groups). In addition, the authors elaborate each step and provide visualisation examples as well as potential considerations for decisions that are made based on the CCOPs. The information management process can be used as a reference for further developments and reconfigurations of CCOPs which contribute to strengthening the organisation's situational awareness. Moreover, the authors demonstrate these findings with an illustrative application scenario about a National Cyber Security Centre (NCSC) that is focusing on the prevention of common cyber attacks. The scenario shows that building a CCOP can become very complex, especially with regard to the selection of relevant information and sources.

This paper is organised as follows: The first section provides an introduction in the form of background information. The second section describes an information management process that can be used to generate CCOPs. The section titled "Core Data and Context Information for CCOPs" investigates diverse types of information, forming the foundation for establishing adequate CCOPs. The section titled "Information Sources for CCOPs" provides a classification of information sources and further investigates how they can contribute to CCOPs. The next sections describe methods of visualising the CCOPs and potential decisions at the national level. The last section provides an example demonstrating the findings from the previous sections.

Background

Establishing Situational Awareness (SA) at the national level has become a key factor for national governments. While first defined in the mid-1980s, most literature has adopted the definition for situation awareness proposed by Endsley (1995): "Situation awareness is the perception of the element 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". Recent SA models have extended the concept of SA to cyberspace and introduced CSA, as described by Pahi and Skopik (2016), and Pahi, Leitner, and Skopik (2017a). One example is to create a national CCOP that provides the current state on major national incidents and responses at the national level. Typically, CCOPs aim to support the decision making in operational environments by providing a comprehensive representation about the present situation (Conti, Nelson & Raymond 2013). CCOPs established at NCSCs, for example, can serve as a basis for establishing effective CSA. CSA is a required capability of national stakeholders and governments to effectively perform their operations, thereby also relying on the knowledge about the technical status of CIs and available cyber-security incident information. In recent years, research has investigated, for example, the technical data gathering and processing within organisations (Skopik *et al.* 2012) or strategies for CSA (ENISA 2012).

In this paper, the authors assume that NCSCs are gathering and collecting information, for example, on incidents; and, thus, they prepare the information for decision makers in the national government. As shown in **Figure 1**, below, the CIs serve as a primary information basis for the

NCSCs. Received and gathered input is processed with the Information Management (IM) process that is further outlined in the next section. The results of the IM processes within the NCSC are, for instance, the CCOPs that can be further used to establish CSA. This CSA can be used by decision makers to provide strategies and actions to protect the safety and security of their citizens.

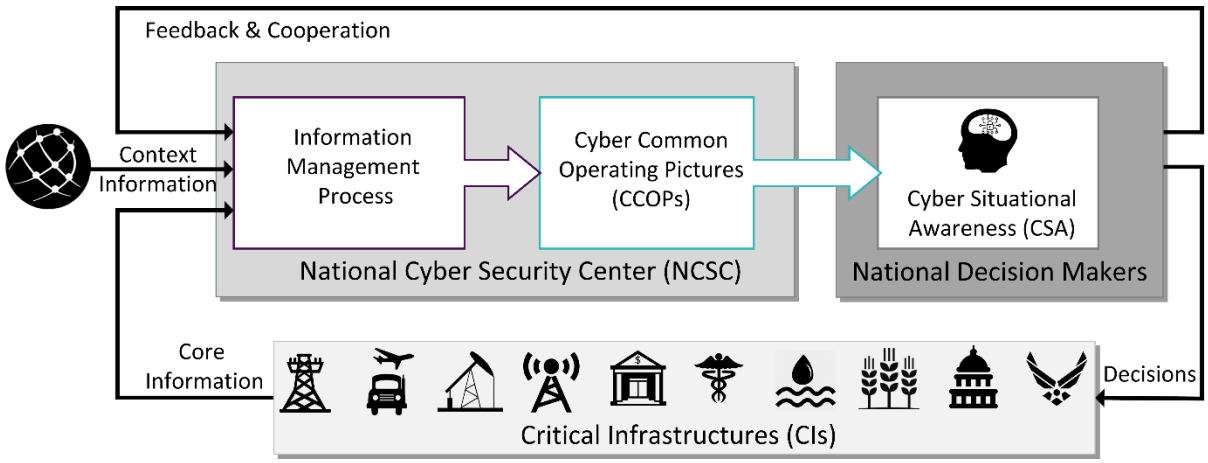


Figure 1: Information cycle between NCSCs and national stakeholders

Information Management Process for CCOPs

This section describes an IM process that is used to establish CCOPs for NCSCs. The process is divided into eight steps and is an example set of steps to establish CSA with CCOPs. These steps are not exhaustive and can be adapted according to the specific needs for NCSCs. A detailed description of each step is given in the following.

Step 1 is to define the purpose of the CCOPs (**Figure 2**, below). The purpose of CCOPs is to capture and visualise incidents in relevant systems. Such systems could range from a classified network system (for instance, government or military systems) to nationwide critical infrastructures. In order to be aware of the current status of the critical infrastructures, their local data need to be collected and analysed as a basis for the core CCOP (such as log files). In Step 2, a selection of relevant data types is required for the creation of tailored CCOPs. Therefore, the information management process will focus on the selected data types, such as security alerts, vulnerabilities, malware, and Indicators of Compromise (IoC) related to governmental institutions. Step 3 is about the identification of the core CCOP sources of the required data, for instance databases and log files to analyse network traffic. The creation of CCOPs requires the combination and correlation of various information sources. The next section further examines which sources can be potentially useful for CCOPs. In Step 4, an evaluation of the Information Quality (IQ) of core CCOP data is conducted. The selection of core data can be difficult due to the myriad information types, for example logs or security alerts. However, a balance of the required and negligible data must be found. The required quality criteria for the evaluation of data and information sources can be, for example, reliability, relevance, reputation, verifiability, price, accuracy, availability, and interpretability (Naumann & Rolker 2000). Numerous IQ assessment methodologies exist such as in Lee *et al.* (2002).

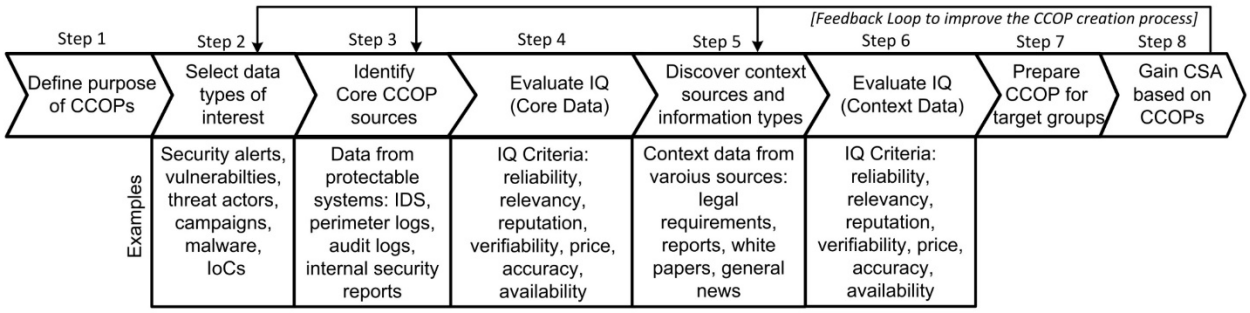


Figure 2: Information management process for CCOPs

In Step 5, context sources and information types for contextual data are investigated. This information covers, for instance, contextual information, such as reports about security incidents at CIs or, in specific domains, global-incident trends or legal requirements. In Step 6, an evaluation of the IQ of context data is performed to maintain a certain quality level for context data. This leads to a CCOP. In Step 7, a CCOP is adapted to target groups (for example, CIs, public administrations, or decision makers). As CCOPs contain, aggregate, and summarise various information types, different domains such as energy, CIs, finance, or transportation might require different key indicators from the CCOPs (for example, potential threats or detected malicious activities).

The derived CCOP enables CSA-gaining for decision makers (Step 8). Decision makers such as CIs or national governments can make security-related decisions and effectively implement (counter) measurements in cyber-crisis situations by relying on the contemporary knowledge on the security status of CIs at the national level.

Ideally, the CSA gaining process contains a feedback loop between the IM process and the decision makers (**Figure 2**). The feedback loop enables the integration of reactions, adaptations, and policies to the changing threat landscape by modifying the CCOP creation process.

Core Data and Context Information for CCOPs

Based on the wide range and large amount of information available to create CCOPs, it is challenging to select and filter the most relevant information. Based on the IM process defined above, this section focuses on the description of the elements (Steps 2-6) displayed in **Figure 2**; core CCOP data collected for protection (Steps 2-4); and related context information for CCOPs (Steps 5-6).

Core information for CCOPs

Core information (or data) consists of essential incident information that might have a higher impact (for example, on national security). The core data of CCOPs consists of objectively measured events, gathered from both internal and external sources, as well as the subsequent rating of these sources and enrichment with contextual information to facilitate the interpretation of measured events. For this analysis, the authors considered ongoing activities that included standards and best practices that have evolved within the past years. For example, Structured Threat Information Expression (STIX) is a structured language for specifying cyber incident

information (Barnum 2014). This standard was developed by many international experts and is meant to convey the full range of cyber-threat information; it strives to be fully expressive, extensible, automatable, flexible, and as human-readable as possible (for example, modelled with XML and JSON). In this paper, the authors used STIX as the basis to represent core CCOP data.

STIX 1.1 contains eight basic elements outlined by Barnum (2014):

- 'Observables' are stateful properties or measurable events (for example, HTTP requests and information about files);
- 'Indicators' convey specific observable patterns. Incidents consist of data such as time-related information, parties involved, assets affected, impact assessment, related Indicators, and related Observables;
- 'Tactics, Techniques, and Procedures' (TTP) are representations of the behaviour or *modus operandi* of cyber adversaries;
- 'ThreatActors' are characterisations of malicious actors (or adversaries) representing presumed intent and historically observed behaviour;
- 'Campaigns' are instances of 'ThreatActors' pursuing intent, as observed through sets of 'Incidents' and/or 'TTP', potentially across organisations;
- 'ExploitTargets' are vulnerabilities or weaknesses in software, systems, networks, or configurations that are targeted for exploitation by the 'TTP' of a 'ThreatActor';
- 'Courses of Action' are specific measures to be taken to address threats, whether they are corrective or preventative, to address 'ExploitTargets', or to counter or to mitigate the potential impacts of 'Incidents';
- 'Incidents' capture information about events.

The recently presented STIX 2 (OASIS Cyber Threat Intelligence Technical Committee 2017) format introduces twelve STIX Domain Objects (SDOs) in order to extend or to replace the eight elements listed above. With STIX 2, cyber-threat intelligence can be even more precisely defined and interlinked using further relational objects between these SDOs. The details of STIX 2, however, go far beyond the scope of this paper.

Context information for CCOPs

Context information serves as a complementary component of the core data for gaining CSA. It provides additional information to understand, interpret, or evaluate some core CCOP data. Context can be a single piece of information or the combination of more information from various sources having different dates (Ntanos *et al.* 2014). Context information can cover a wide range of topics from political news to technical reports. Each piece of information can be crucial to identify connections between apparently unimportant details and major incidents. In this paper, the context information is organised by the focal points shown in **Figure 3**, below. This list does not claim to be exhaustive and can be adapted depending on, for example, the target group or the aim of the CCOP. One of the main challenges is to filter, select, and aggregate the relevant information from the context in order to enrich the core CCOP information adequately and to avoid packing it with unnecessary information. In the following, each category of context information is described and examples are given to demonstrate its applicability.

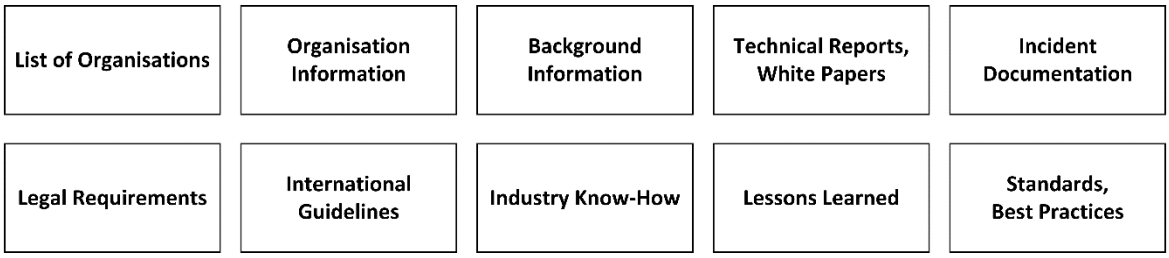


Figure 3: Context information for CCOPs

In **Figure 3**, 'List of organisations' is a critical assessment of organisations that are relevant for the nationwide operation of reliable business processes. These lists cover not just the CI providers but also other essential organisations for the nation-state, such as sole component vendors or research institutes. Furthermore, it would be beneficial to accumulate more detailed 'organisation information'. Particularly for the sharing of incident information, the organisational information can include company contacts, documentations about the assets, or IP ranges used by an organisation. 'Background information' consists of relevant and related information about trends, for instance in the economic, political, or technical developments, and trends that can lead to security problems. 'Technical reports' delivered by partner organisations about their incidents can be used as a primary source to analyse current trends and techniques of cyber attacks and incidents. Moreover, 'white papers' elaborate technical procedures and details and are often published by IT vendors or public authorities (for example, the report on the cyber espionage case at RUAG by GovCERT.ch [2016]). 'Incident documentation' describes the course of actions within past incidents, usually from the perspective of the victim organisation. The experience gathered during an incident may save another potential victim organisation from falling prey to the same or similar cyber attack. 'Legal requirements' and 'international guidelines' form the underlying legal framework for dealing with incidents. For example, within the European Union (EU), the directive on security of network and information systems (NIS Directive) was adopted by the European Parliament to ensure a high common level of network and information security across the EU (European Union 2016). Additionally, national law also defines various legal requirements such as privacy or the use of data preservation. Further guidelines have been published by technical organisations such as NIST or ENISA (such as a technical guideline on security measures by ENISA [2014]). 'Industry know-how' is essential in a crisis and for deploying sector-specific preventive and responsive measures. 'Lessons learned' is an experience gained from a cyber incident that should be considered for future occasions. 'Standards' and 'best practices' are successful methods derived from lessons learned and may serve as reference guides to organisations. Organisations can develop their own best practices and/or use standards on information security and incident management such as ISO 17799, ISO 27000, ITIL, CobiT, and NIST 800 series.

Information Sources for CCOPs

Information can be derived, gathered, and collected from different sources. Thorough analysis and correlation of this information contributes to the generation of new knowledge and insights. Information sources for cyber-incident information are typically electronic sources and can be categorised in various ways. In this paper, four categories to classify information sources for CCOPs are identified: accessibility, recording type, information owner, and information modelling

(**Figure 4**, below). The following discussion provides a brief description and examples of each of these categories.

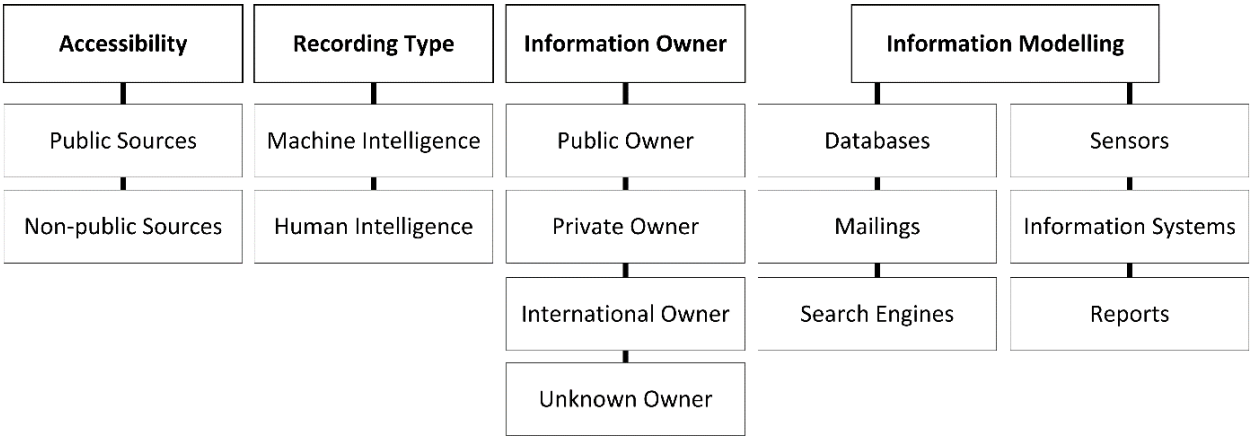


Figure 4: Categorisation of information sources

In **Figure 4**, the categorisation by 'accessibility' divides information sources into public sources and non-public sources. Public information sources typically provide Open Source Intelligence (OSINT) and can cover, for example, national and international news, reports, professional journals, whitepapers of IT security vendors (such as FireEye, Kaspersky), professional blog entries and forums, mailing lists and subscriptions, public databases of vulnerabilities and exploits, such as Common Vulnerabilities and Exposures (CVE) (MITRE 2017) or the National Vulnerability Database (NVD) (NIST 2017). Non-public sources have restricted access and may only allow members with special permissions or may allow access only to certain search engines. For example, non-public sources may include special forums on the Deep Web or closed mailing lists.

The category 'recording type' is based on the method through which the information is gathered. Here, a distinction is made between artificial intelligence and human intelligence that can collect data. Artificial intelligence gathers the data with sensors or software solutions, such as Intrusion Detection Systems (IDSs) in networks. Information collected and provided by human sources can be classified as human intelligence. This intelligence is particularly popular (for example, in police work or in cases of espionage). However, nowadays the lines between machine and human intelligence are blurred, and hybrid approaches emerge. For example, an officer can use a machine to derive information but can only connect the missing links by using human intelligence.

The categorisation of an information source as 'information owner' is a relevant aspect because the owner might influence the attributes of the information such as its credibility and confidentiality. While public ownership and private ownership are fairly simple to distinguish, other information sources, where the origin of data is often unclear or unknown, can be classified as having unknown ownership (for example, information from the Deep Web and Dark Web [Bergman 2001]).

Finally, the category 'information modelling' in **Figure 4** uses models to formulate a concept by a set of entity types, properties, relationships, and operations for a certain domain. Furthermore, mappings of these models are called data models, regardless of whether they are object models, entity relationship models, or XML schemas. The content that can be stored within these data models can be either human-readable or machine-readable. For example, news, blogs, incident reports, and white papers are typically human-readable, while source codes, log entries, and STIX records are mainly machine-readable sources, although they might be human-understandable.

Visualisation of CCOP Contents

A challenging task is to design CCOPs in such a way that they present the most relevant information to the target group. The target audience in this article is national decision makers in NCSCs. The multifaceted information of CCOPs can be visualised in various ways—for example, through different diagrams, such as box plots, bubble charts, bullet charts, chord diagrams, coordinates, tree maps, sunbursts, or dependency wheels. CCOPs can be presented dynamically on interactive dashboards or statically at regular intervals—monthly, quarterly, or annually—in reports. The degree of detail and visualisation methods of CCOPs can vary according to changing requirements from NCSC to NCSC, within an NCSC related to the purpose of the CCOP (as described above in Step 1 in the IM process in **Figure 2**), and based on the application domain, such as for short-term operative support or long-term strategic-political decision making.

Figure 5, below, shows two CCOP mock-ups for a dashboard for NCSCs. The design is a mix of common security visualisation techniques for organisations (such as can be found in Security Information and Event Management [SIEM] solutions) and visualisations based on requirements specifically for public decision makers (for example, evaluations concerning national security).

Figure 5: CCOP mock-ups

Based on the mock-ups in **Figure 5**, a CCOP may cover various content in accordance with the outputs of the analysis and the requirements on the national level. However, other content may be included for other application scenarios and NCSCs. In the mock-up examples, the primary aim is to give an overview of the cyber security status at the national level. This includes overviews of each level in the sectors of the critical infrastructure with a pre-defined threshold, such as the number of affected companies in the banking sector.

Based on a requirements analysis, it was derived that a CCOP should visualise cyber security incident reports sent by critical infrastructures, the number of reports per domain, and a list of obligatory and voluntary notifications. Furthermore, the NCSC can aggregate the information and categorise the reports and incidents by vulnerability, attack vector, or other aspects.

The CCOPs visualise and aggregate relevant aspects of the cyber incidents such as by threat vector, by magnitude of impact, by geographic location, and by potential subsequent events. Common and important content are the attack types including their TTPs. This type of CCOP covers statistics about different attack types and trends (for example, "12 percent more ransomware attacks in the last three months").

Rankings provide a quick overview about the situation, for instance, the top five attack vectors or most affected sectors, newest threats, or countermeasures. The tool CAESAIR, for example, provides such insight (CAESAIR 2017).

An overview of the security and readiness levels is essential for effective CCOPs. This information covers, among other things, whether the organisations have adequate information security policies, business continuity plans, change management policies and procedures, and reliable back-up solutions. The essential part of CCOPs is the representation of connections and interdependencies among the information particles. For example, the assessment of the security and readiness level may vary based on the policies, standards, and guidelines implemented per branch. This information builds the basis to predict emerging threat indicators and to derive the probability of future events. For instance, if 30 percent of the critical infrastructures have no processes for effective patch management, and there is a recently discovered exploit in a specific server version used by 50 percent of the organisations in their perimeter network, then how likely is it that the related server version will be exploited in these organisations?

Supporting Decision Making at National Level

The gained CSA (Step 8 in the IM process in **Figure 2**) supports decision making at the national level. The decisions made based on the information level and quality of CCOPs can vary. The more adequately and relevantly information is outlined in CCOPs, the faster CSA can be established and decisions can be made.

Based on the reaction and implementation time, potential decisions can be divided into three categories. The first category covers decisions with reaction and implementation time within the most recent 24-hour period. Decisions within this short period could cover operative assistance in recovery or incident response processes, early warning of potential victims, forced information sharing and exchange among providers of critical services and the NCSC, coordination of

emergency forces, or ensuring that citizens are properly informed about the situation and measures taken.

The second category contains decisions having an implementation time of days or months. For example, these could cover creating ad-hoc working groups in the NCSC to cope with the impact of a cyber incident, notifying relevant international first responders and organisations, contacting affected manufacturers (for instance in the case of a released product's vulnerability), assisting in disaster recovery, and providing documents about best practices, technical descriptions, and white papers.

The last category of decisions based on CCOPs focuses on long-term decisions with reaction and implementation time of months to years, such as raising cyber-security awareness with training courses for CI or citizens, providing financial support for organisations for enhancing their security level, instructing periodic external and internal audits, constantly reviewing cyber-security readiness in private and public organisations, providing consultancy, and adapting related legislations.

Although this list of decisions is indicative and not necessarily exhaustive, it nevertheless presents a wide range of decision types that call for different CCOPs to support national decision makers in cases of cyber incidents.

Illustrative Application Scenario

The following illustrative application scenario aims to provide insight into the IM process and the need for CCOPs and CSA. In the fictional example, a NCSC is focusing on the protection of governmental institutions, and its aim is to prevent three common cyber attacks: phishing emails, ransomware, and DDoS attacks (Step 1). The data used within each of the following steps is described in **Table 1**, below, and is based on the process in **Figure 2**. To detect these threats and attacks, adequate data types must be selected in Step 2. The identification of the suspicious emails is, for instance, the primary task to prevent phishing attacks. First, the suspicious addresses with malicious attachments (from known threats and unknown senders) can be blocked. The delivered malware and ransomware can be identified by their payloads if they are already in anti-virus databases. Another option is the monitoring of typical malware activities, such as creating, reading, writing, executing, or deleting files; creating hard-links, or modifying attributes in relevant directories. For example, the Cryptolocker ransomware uses create, execute, and write operations, and it is designed to block any random .exe file at the root and any subdirectory of a folder named AppData anywhere on the C drive. These activities are stored in log files on local hosts within the governmental institutions. Secondly, DDoS attacks can be recognised by monitoring the network traffic. Both forms of attack can be detected with monitoring systems, and this information can be selected for use in the core data of CCOPs: namely security alerts, malware, and IoCs.

Step	Illustrative application scenario–Sample data
Step 1	Focus on the protection of governmental institutions against phishing emails, ransomware, and DDoS attacks
Step 2	Identify suspicious incoming emails and attachments, malicious activity, anti-virus databases, network traffic
Step 3	Monitor network traffic, various internal log files (such as audit, firewall, traffic, and DNS log files) on the hosts and network nodes
Step 4	Focus on potential sources of error and mistakes (remediate false positive alerts, for example) for implementing security or monitoring solutions, check criteria (such as price, reliability)
Step 5	Reach out to official information sources, such as national law enforcement agencies, to request international cooperation, such as cooperation with other national CERTs, press releases, and other OSINT information
Step 6	Create statistics of ransomware incidents using cryptocurrency created by the FBI (highly reliable), national and partner CERTs reports about increased phishing and ransomware activity (highly reliable), press releases about dissemination of cryptocurrency and its criminal usage (limited reliability)
Step 7	Prepare CCOPs for national government with focus on economic and political reasons and effects as well as graphics of emerging trends for CIs, with a focus on technical IoCs and solutions
Step 8	Decide about early warnings of potential victim organisations, enhance information sharing with the NCSCs, prepare preventive measurements

Table 1: Application scenario data example

In Step 3, the identification of core CCOP sources is performed based on the selected data types. In the example, the sources deliver information about already existing or implementable security and monitoring solutions for devices and network nodes. Collected information contains, for instance, detailed network traffic information and various internal log files (such as information from audit logs, firewall, traffic, and Domain Name Server [DNS] log files).

Then, Step 4 evaluates the Information Quality (IQ) of the core data. Since the core data contain mainly internally collected data, the reliability is assured. The IQ evaluation focuses on the potential sources of errors and mistakes. The applied monitoring solutions may produce actual false positive alerts. The aim of the evaluation is to remediate the source of these kinds of errors. In case new security or monitoring tools need to be installed, the evaluation is required according to, for example, its price and the usability of the system. The core CCOPs give an overview about the security status of the ICT systems; hence, they are based on the internal core data. In the example, the core data shows increased phishing and ransomware activity within the governmental sector.

To understand the core CCOP of the protected domain and to be able to foresee future trends, the core data needs to be merged with the relevant context information in Step 5. The selected context information contains official information sources (such as national law enforcement agencies), reliable international information sources (for example, cooperation with national CERTs), and OSINT.

The IQ of the context information is evaluated in Step 6, like core data in Step 4. The U.S. Federal Bureau of Investigation (FBI) is a highly reliable official information source in the application scenario. The report of the FBI shows a clear increase in the number of ransomware incidents using Bitcoin for payment nationwide. Other highly reliable information sources confirm this statement. In our fictional example, the national CERT and partner CERTs also report a 25 percent increase in phishing and ransomware activity. The analysis of OSINT information contains information sources with limited reliability, such as press releases about the rapid dissemination of cryptocurrency that worry about its criminal usage and support investigation of the emergence of the ransomware threat.

After these steps, the CCOPs are prepared in Step 7. In this scenario, the target groups for the CCOP preparation are the national government and CIs. The decision makers of the national government receive, for instance, CCOPs focusing on economic and political aspects, future impact and emerging trends of phishing, ransomware, and DDoS activities. The analysis shows that the existence of bitcoins made the use of ransomware more popular for cyber criminals. By collecting additional context information, the results show that 40 percent of the fictional governmental institutions have no sufficient backup systems. The growing number of successful ransomware incidents targeting public institutions, such as the attack waves against the European and American healthcare facilities (Mansfield-Devine 2016), will likely result in even more attack waves against the government sector. The CCOPs also provide a rough estimate of the possible monetary and reputation losses based on the past attacks on healthcare facilities. Unlike the political decision makers, the CIs receive CCOPs focusing on emerging cyber threats and IoCs, as well as possible technical solutions. The CCOPs may also contain the possible financial and reputation losses, possible mitigation methods and their costs, as well as relevant technical details.

In Step 8, the decision makers gain CSA based on the received CCOPs created by the NCSC. With CSA, decision-makers can decide on cyber-security-related topics and an effective implementation of countermeasures. In addition, decision-makers of the national government decide on the early warnings of potential victim organisations by the NCSCs and on inviting the CIs to enhanced information sharing and exchange initiatives with the NCSCs. Moreover, the governmental institutions are increasing the communication with other CIs and raising their security measures according to the technical recommendations made by the NCSC (such as creating or upgrading their backup systems and security solutions against potential cyber attacks).

In summary, this scenario shows that CSA is an essential tool for national stakeholders and governments to protect citizens and to maintain collaboration with CIs at the national level. Therefore, the primary aim of the NCSCs is establishing suitable CCOPs relying on the knowledge about the technical status of CIs and available cyber-security incident information. Several processes can be automatized for creating CCOPS, but human capabilities still play a significant role, especially for gaining and applying CSA.

Conclusion

In this paper, the modelling and visualisation of CCOPs using an information process was presented. The process can potentially be applied by various organisations that aim to establish CSA. The process for establishing CCOPs can become complex and lengthy. One of the biggest challenges is to select adequate information from reliable sources. Various sources are used to obtain different types of information that is confidential, dynamic, up-to-date, and accurate. This paper presented a variety of sources and information that are useful for gaining CSA, ranging, for example, from public to non-public sources. Other challenges include how to manage dynamics, redundancy, and selection, as well as incident categorisation (such as when an incident is critical for national security), and decision support for complex cyber situations. After the selection of data sources, visualisation mock-ups for CCOPs are proposed that contain information such as rankings of top targets or common attack vectors. Finally, an illustrative example showed how sample data can be categorized in an information quality level as well, which identifies how CSA strategies could be developed. As this is a complex task, the selection, aggregation, and evaluation of information for CCOPs has to be uniquely adapted to each NCSC that may want to adopt the proposed process.

Acknowledgements

This work—an extended version of Pahi, Leitner and Skopik (2017b)—was partly funded by the Austrian FFG research program KIRAS in the course of the project Cyber Incident Situational Awareness (CISA) (850199).

References

Barnum, S 2014, *Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™)*, version 1.1, revision 1, viewed 25 August 2017, <http://www.standardscoordination.org/sites/default/files/docs/STIX_Whitepaper_v1.1.pdf>.

Bergman, MK 2001, 'White Paper: The deep web: surfacing hidden value', *Journal of Electronic Publishing*, vol. 7, no. 1.

CAESAIR 2017, *CAESAIR—Collaborative analysis engine for situational awareness and incident response*, viewed 25 August 2017, <http://caesair.ait.ac.at/>.

Conti, G, Nelson, J & Raymond, D 2013, 'Towards a cyber common operating picture', *Proceedings of the 5th International Conference on Cyber Conflict (CyCon)*, pp. 1-17.

Danitz, T & Strobel, WP 2001, Networking dissent: Cyber activists use the Internet to promote democracy in Burma, *Networks and netwars: The future of terror, crime, and militancy*, eds. John Arquilla & David Ronfeldt, pp. 129-69.

Endsley, MR 1995, 'Toward a theory of situation awareness in dynamic systems', *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 37, no. 1, pp. 32-64.

ENISA 2012, *National cyber security strategies: Practical guide on development and execution*, *ENISA*, viewed 25 August 2017, <https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport>.

ENISA 2014, *Technical guideline on security measures, Version 2.0*, viewed 17 January 2017, <https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf >.

European Union 2016, 'Concerning measures for a high common level of security of network and information systems across the Union', *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016*, OJ L 194.

GovCERT.ch 2016, *Technical report about the malware used in the cyberespionage against RUAG*, viewed 25 August 2017, <https://www.melani.admin.ch/melani/en/home/dokumentation/reports/technical-reports/technical-report_apt_case_ruag.html>.

Lee, YW, Strong, DM, Kahn, BK & Wang, RY 2002, 'AIMQ: A methodology for information quality assessment', *Information & Management*, vol. 40, no. 2, pp. 133-46.

Lesk, M 2007, 'The new front line: Estonia under cyberassault', *IEEE Security Privacy*, vol. 5, no. 4, pp. 76-9.

Mansfield-Devine, S 2016, 'Ransomware: Taking businesses hostage', *Network Security*, vol. 2016, no. 10, pp. 8-17.

MITRE 2017, *Common vulnerabilities and exposures (CVE): The standard for information security vulnerability names*, viewed 17 August 2017, <https://cve.mitre.org/>.

Naumann, F & Rolker, C 2000, 'Assessment methods for information quality criteria', *Proceedings of the Fifth Conference on Information Quality (IQ 2000)*, pp. 148-62.

NIST 2017, *National vulnerability database (NVD)*, viewed 25 August 2017, <https://nvd.nist.gov/>.

Ntanos, C, Botsikas, C, Rovis, G, Kakavas, P & Askounis, D 2014, 'A context awareness framework for cross-platform distributed applications', *Journal of Systems and Software*, vol. 88, pp. 138-46.

OASIS Cyber Threat Intelligence Technical Committee 2017, *About STIX*, viewed 12 September 2017, <https://oasis-open.github.io/cti-documentation/stix/about>.

Ottis, R 2008, 'Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective', *Proceedings of the 7th European Conference on Information Warfare. European Conference on Information Warfare*, p. 163.

Pahi, T & Skopik F 2016, 'A public-private-partnership model for national cyber situational awareness', *International Journal on Cyber Situational Awareness (IJCSA)*, vol. 1.

Pahi, T, Leitner, M & Skopik, F 2017a, 'Analysis and assessment of situational awareness models for national cyber security centers', *Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP)*, SCITEPRESS, pp. 334-45.

——2017b, 'Data exploitation at large: your way to adequate Cyber common operating pictures', *Proceedings of the 16th European Conference on Cyber Warfare and Security ECCWS 2017*, eds. Mark Scanlon & Niehn-An Le-Khac, pp. 308-15.

Skopik, F, Ma, Z, Smith, P & Bleier, T 2012, 'Designing a cyber attack information system for national situational awareness', *Future Security Proceedings*, Springer, pp. 277-88.

Uma, M & Padmavathi, G 2013, 'A survey on various cyber attacks and their classification', *International Journal of Network Security*, vol.15, no. 5, pp. 390-6.