Submission Topic: Cyber Security

Data Exploitation at Large: Your Way to Adequate Cyber Common Operating Pictures

Timea Pahi, Maria Leitner, Florian Skopik
AIT Austrian Institute of Technology, Vienna, Austria
firstname.lastname@ait.ac.at

Abstract: Recent conflicts and political incidents, such as Operation Orchard, have shown that no future conflict is likely to be fought without a cyber element. However, establishing effective defensive measures against cyber attacks is a difficult and resource-consuming task. A common denominator of an effective cyber defence has always been the application of Common Operating Pictures (COP) e.g. in law enforcement or the armed forces. COPs are widely used to represent, display and assess situations. In recent years, Cyber COPs (CCOPs) have become a key factor in the establishment and analysis of situational awareness as well as decision-making processes in the cyber domain. However, the process to establish an adequate CCOP is not trivial. The careful selection of data sources for the core CCOP, which 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, pose new challenges. This paper will therefore provide an information management process that aims at establishing cyber situational awareness (CSA) for stakeholders based on CCOPs. The process consists of several steps such as selecting data types, identifying core CCOP sources, evaluating the information quality, preparing CCOPs for target groups and gaining CSA based on CCOPs. Furthermore, we provide a qualitative survey of potentially usable information and related sources that are vital for CCOPs. We demonstrate our work by displaying the basic steps and grand picture to create a CCOP in an illustrative scenario. The example is set around a fictive national cyber security center (NCSC) that aims to decrease phishing, ransomware and DDoS attacks within the critical infrastructure. This CCOP example can then be used by numerous stakeholders to achieve situational awareness and thus facilitate decision making processes.

Keywords: cyber common operating picture, information management, cyber security, cyber situational awareness, decision-making processes;

1. Introduction

As the number of complex cyber attacks (such as ransomware, phishing, DDoS, CEO fraud) has risen rapidly in recent years (Uma & Padmavathi (2013), Mansfield-Devine (2016)), it is becoming increasingly challenging for organizations and government agencies to adequately prepare for these incidents and provide adequate cyber crisis management. Moreover, recent conflicts and incidents (for example the cyber attack on Estonia (Lesk, 2017) or cyber hacktivists (Danitz & Strobel, 2000)) 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. However, a common denominator has always been the application of Common Operating Pictures (COP) e.g. in law enforcement or the armed forces. 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) (Conti et al., 2013) have become a key factor in the establishment and analysis of cyber situational awareness (CSA) as well as decision-making processes. CCOPs can be established with a variety of information depending on the purpose. For example, a CCOP for an organization might include an analysis of the current local network traffic to study anomalous network traces or identify potential malware that transmits data to external servers. At national level, however it gets more challenging as potential incidents do not only occur in governmental agencies or institutions – they also occur at organizations (public and private) such as critical infrastructures (CI) or small- and medium-sized enterprises (SME). Hence, only shared incident information can be processed and evaluated at national level.

In this paper, an information management process to derive CCOPs is specified. The process can be used as a reference for further developments and reconfigurations of CCOPs. In addition, an investigation of current information and sources that can be used to create CCOPs is given. Organizations can use these results to further develop and adapt their CCOPs which contribute to strengthening CSA. Moreover, we demonstrate our findings with an illustrative application scenario about a national cyber security center (NSCS) that is focusing

on the prevention of common cyber attacks. It can be seen from the scenario that building a CCOP can be multifaceted and complex in particular by selecting relevant information and sources.
The paper is structured as follows. Section 2 motivates the topic of this paper by giving background information. Section 3 displays an information management process that can be used to generate CCOPs. Furthermore, Section 4 investigates different types of information and how they build the foundation to establish adequate CCOPs. Section 5 provides a classification of sources and further investigates how they can contribute to CCOPs. Section 6 provides an illustrative example to demonstrate the findings from the previous sections. Section 7 will conclude the paper.

2. Background

Establishing SA at 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) as: "*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*". Newer models have adapted this term to the cyber space to CSA models as described in Pahi et al. (2016, 2017). One way for example is to create a national CCOP that provides the current state on major national incidents and responses at national level. Typically, CCOPs aim to support the decision making in operational environment by providing a comprehensive representation about the present situation (Conti et al., 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 critical infrastructures (CIs) and occurring incident information. In recent years, research has investigated e.g., the technical data gathering and processing within organizations (Skopik et al., 2012) or strategies for CSA (ENISA, 2012). In this paper, we assume that NCSCs are gathering and collecting information e.g., on incidents and prepare the information for decision makers in the national government. As shown in Figure 1, the CIs serve as primary information basis for the NCSCs. Received and gathered input is processed with the information management (IM) process that is further outlined in Section 3. The results of the IM processes within the NSCS 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 (see Figure 1).

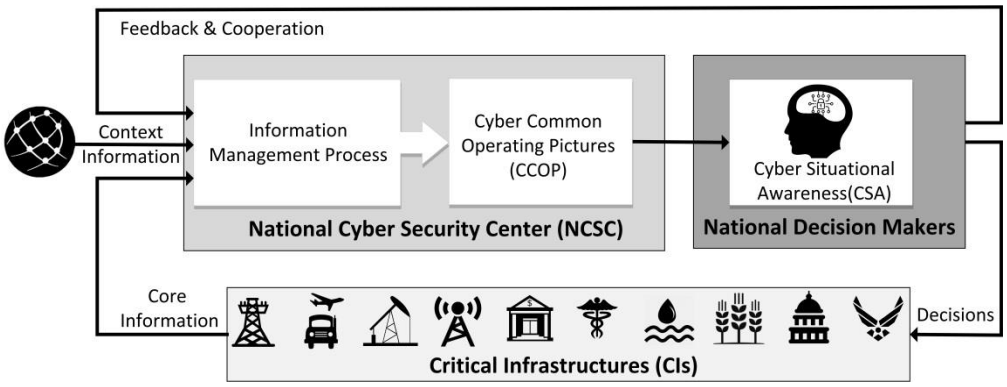

Figure 1: Information cycle between NCSCs and national stakeholders

3. Information Management Process for CCOPs

This section describes an information management (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 and the application cases (see Figure 2). The purpose of CCOPs is to capture and visualize incidents in relevant systems. Such systems could range from a classified network system (for instance government or military systems) to nation-wide critical infrastructures. In order to be aware of the current status of the critical institutions, local data need to be collected and analyzed as basis for the core CCOP (e.g., log files). Furthermore 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, indicators of compromise (IoCs) 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 analyze network traffic. The creation of CCOPs requires the combination and correlation of various information sources. Section 5 further examines which sources can be potentially useful for CCOPs. Moreover in **Step 4**, an evaluation of information quality (IQ) of core CCOP data is conducted. The selection of core data can be difficult due to the myriad of information types, e.g., logs or security alerts. However, a balance of the required and negligible data must be found (see Section 4.1). 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 et al., 2000).Numerous IQ assessment methodologies exist such as the AIMQ by Lee et al. (2002).

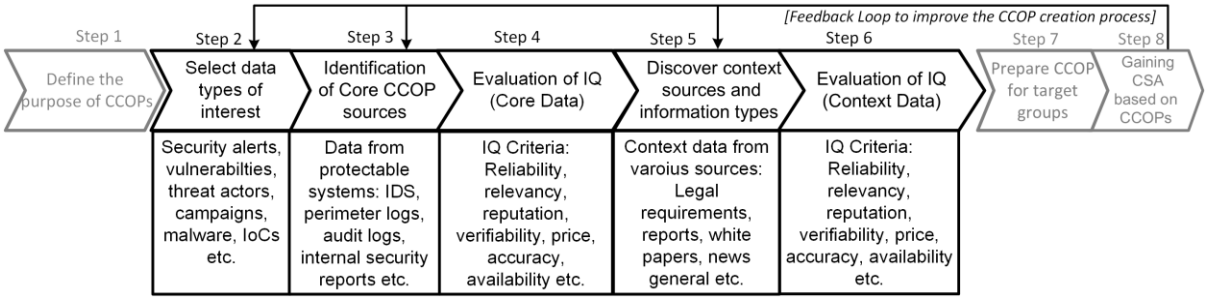

Figure 2: Information Management Process for CCOPs

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. Further explanation of context data for CCOPs is given in Section 4.2. In **Step 6**, an evaluation of 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 (e.g., CIs, public administrations, decision makers etc.). As CCOPs contain, aggregate and summarize various information types, different domains such as energy, finance or transportation might require different key indicators from the CCOPs (e.g., potential threats or detected malicious activities).
The derived CCOP enables CSA-gaining for decision makers (**Step 8**). The decision makers such as CI providers or national governments can make security related decisions and effectively implement (counter)measurements in cyber crisis situations relying on the contemporary knowledge on the security status of CI at national level. Ideally, the CSA gaining process contains a feedback loop between the IM System and the decision makers (see Figure 1). The feedback loop enables the integration of reactions, adaptations and policies to the changing threat landscape by modifying the CCOP creation process.

4. 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 in Section 3, this section focuses on the description of the elements (steps 2-6) displayed in Figure 2: (1) core CCOP data collected for protection and (2) related context information for CCOPs.

4.1 Core information for CCOPs

Core information (or data) consists of essential incident information that might have a higher impact (e.g., on national security). Core data of CCOPs 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. For this analysis, we consider ongoing activities that include 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). It is developed by many international experts and is meant to convey the full range of cyber threat information and strives to be fully expressive, extensible, automatable, flexible and as human-readable as possible (i.e., XML and JSON from version 2.1). In this paper, we will use STIX as our basis to represent core CCOP data.
STIX 1.1 contains of eight basic elements outlined in Figure 3. Observables are stateful properties or measurable events (e.g., 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, related Observables, leveraged TTP or attributed Threat Actors. Tactics, Techniques, and Procedures (TTP) are representations of the behavior or modus operandi of cyber adversaries. Campaigns are instances of Threat Actors pursuing intent, as observed through sets of Incidents and/or TTP, potentially across organizations. Threat Actors are characterizations of malicious actors (or adversaries) representing presumed intent and historically observed behavior. Exploit Targets are vulnerabilities or weaknesses in software, systems, networks or configurations that are targeted for exploitation by the TTP of a Threat Actor. Courses Of Action are specific measures to be taken to address threats whether they are corrective or preventative to address Exploit Targets, or responsive to counter or mitigate the potential impacts of Incidents (Barnum, 2014).

Figure 3: Basic elements of CCOPs (based on STIX)

4.2 Context Information for CCOPs

The 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 organized by the focal points shown in Figure 4. This list does not claim to be exhaustive and can be adapted depending on e.g., 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 not cram it with unnecessary information. In the following, we describe each category of context information and give examples to demonstrate its applicability.

Figure 4: Context information for CCOPs

Lists of Organizations contain a critical assessment of organizations that are relevant for the nation-wide operation of reliable business processes. These lists cover not just the CI providers but also other essential organizations for the nation state, such as sole component vendors or research institutes. Furthermore, it would be beneficiary to accumulate more detailed Organization Information. Particularly for the sharing of incident information, the organizational information can include company contacts, documentations about the assets or IP ranges used by an organization. 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 organizations about their incidents, can be used as a primary source to analyze current trends and techniques e.g., of cyber attacks and incidents. Moreover, White Papers elaborate the technical procedures and details and are often published by IT vendors or public authorities (e.g., 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

organization. The experience gathered during an incident may save another potential victim organization 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 EU, the NIS directive was adopted by the European Parliament to ensure a high common level of network and information security across the European Union (2016). In addition, national law also defines various legal requirements such as privacy or the use of data preservation. Furthermore, other guidelines have been published by technical organizations such as NIST or ENISA (e.g., a technical guideline on security measures by ENISA (2014)). Industry Know-How is essential in a crisis situation and for deploying sector-specific preventive and responsive measures. Lessons Learned is an experience gained from a cyber incident that should be taken into account for future occasions. Standards and Best Practices are successful methods derived from lessons learned and may serve as a reference guide to organizations. Organizations 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.

5. 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 categorized in various ways. In this paper, we identified four categories to classify information sources for CCOPs: accessibility, recording type, information owner, information modelling (Figure 5). In the following, a brief description and examples of these categories are given.

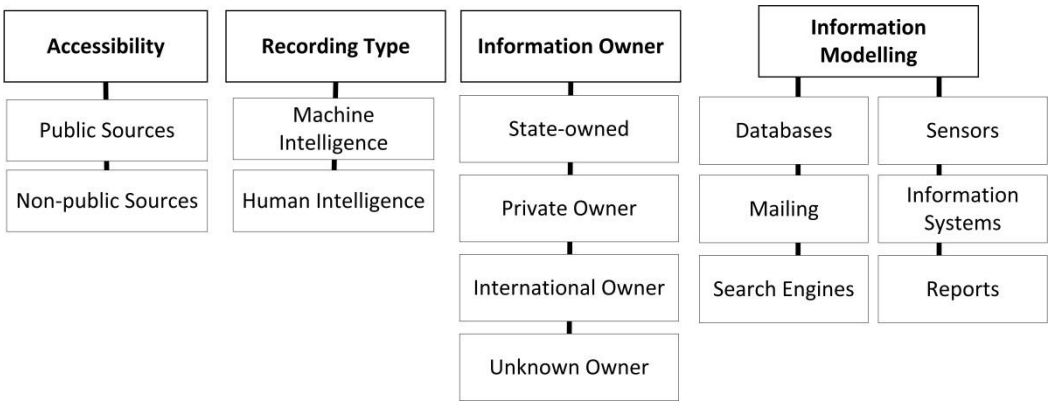

Figure 5: Categorization of information sources

The Categorization by accessibility divides information sources into public sources and non-public sources. Public information sources typically provide Open Source Intelligence (OSINT) and can cover e.g., national and international news, reports, professional journals, publications, 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 CVE (MITRE, 2017) or NVD (NIST, 2017). Non-public sources have restricted access and may allow only e.g., members with special permissions or may allow access to certain search engines. For example, non-public sources are special forums on the Deep Web or closed mailing lists.

The Categorization by recording type is based on the method the information is gathered. Here, we distinguish 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 (IDS) in networks. Information collected and provided by human sources can be classified as human intelligence. This intelligence is particularly popular e.g., in police work or in case 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 Categorization by information owner of the information source is a relevant aspect, because the owner might influence the attributes of the information such as credibility and, confidentiality. In this paper, information sources are divided into three categories. While state ownership and private ownership is fairly simple to distinguish, information sources where the origin of data is often unclear or unknown can be classified as unknown ownership (e.g. Deep Web, Dark Web (Bergman, 2001)).

The category information modeling 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, irrespective of whether they are e.g., object models (e.g. using UML), entity relationship models or XML schemas. The content that can be stored within these data models can be either human-readable and machine-readable. For example, news, blogs, incidents reports, white papers are typically human-readable, while source codes, log entries, STIX records are mainly machine-readable sources (but might be human-understandable).

6. 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 fictive example, a NCSC is focusing on the protection of governmental institutions and their aim is to prevent three common cyber attacks: phishing mails, ransomware and DDoS attacks (**Step 1**). The data used within each of the following steps is also described in Table 1. In order to detect these threats and attacks, adequate data types have to 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 payload, 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 recognized by monitoring the network traffic. Both forms of attacks can be detected with monitoring systems and this information can be selected for the use in the core data of CCOPs: namely security alerts, malware and IoCs.

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 (e.g., from audit logs, firewall, traffic and DNS log files).

Then, **Step 4** evaluates the IQ of the core data. Since the core data contain mainly internally collected data, the reliability is guaranteed. 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 this kind of errors. In case new security or monitoring tools need to be installed, the evaluation is required according to e.g., its price and usability of the system. The core CCOPs give an overview about the security status of the ICT systems hence it is based on the internal core data. In the example, the core data shows an increased phishing and ransomware activity within the governmental sector.

Table 1: IM Process Example Data

Step #	**Illustrative application scenario – Sample Data**
Step 1	Focus on the protection of governmental institutions against phishing mails, ransomware and DDoS attacks
Step 2	Suspicious incoming emails and attachments, malicious activity, anti-virus databases, network traffic
Step 3	Monitoring network traffic, various internal log files (e.g. 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 etc.) for implementing security or monitoring solutions, check criteria (e.g. price, reliability etc.)
Step 5	Official information sources, such as national law enforcement agencies, international cooperation, such as cooperation with other national CERTs, press releases and other OSINT information
Step 6	Statistic 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 reliable)
Step7	Prepared CCOPs for national government with focus on economic and political reasons and effects and graphics of emerging trends for Cis with focus on technical IoCs and solutions
Step 8	Decision about early warnings of potential victim organizations, enhanced information sharing with the NCSCs, preparing preventive measurements

In order 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 (e.g., national law enforcement agencies), reliable international information sources (e.g., cooperation with national CERTs) and OSINT.
The IQ of the context information is evaluated in **Step 6,** similar to core data in Step 4. The FBI is a highly reliably 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. The national CERT and partner CERTs report also about increased phishing and ransomware activity in our fictive use case by 25%. The analysis of OSINT information with limited reliability, such as press releases about the rapid dissemination of cryptocurrency and worries about its criminal usage support the investigation of the emergence of the ransomware threat.
The resulting CCOPs after these steps 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 usage of ransomware more popular for cyber criminals. By collecting additional context information, the results show that 40% of the fictive governmental institutions have no sufficient backup systems. The growing number of successful ransomware against 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 governmental sector. The CCOPs provide also a rough estimate of the possible monetary and reputation loss based on the past attacks on healthcare facilities. Contrary to the political decision makers, the CIs receive CCOPs focusing on emerging cyber threats and IoCs, and possible technical solutions. The CCOPs may also contain the possible financial and reputation lost, 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 are able to decide on cyber security-related topics and an effective implementation of (counter) measures. In addition, decision makers of the national government decide on the early warnings of potential victim organizations 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 (e.g., creating or upgrading their backup systems and security solutions against potential cyber attacks).
In summary, this scenario shows that CSA is a required capability of national stakeholders and governments to protect citizens and maintain collaboration with CIs at national level. Therefore the primary aim of the NCSCs is establishing suitable CCOPs relying on the knowledge about the technical status of CIs and occurring incident information. Several processes can be automatized for creating CCOPS, but human capabilities still play a significant role, especially for gaining and applying CSA.

7. Conclusion

In this paper, we presented an information process for CCOPs potentially applied by all kinds of organizations to gain CSA. The process for establishing CCOPs is challenging. One of the most critical issues is to select adequate information from reliable sources. Sources are used to obtain different types of information that is e.g., confidential, dynamic, up-to-date and/or accurate. Other challenges include how to cope with dynamics, redundancy or selection, as well as at which level an incident can be categorized as critical for national security and how systems can support the evaluation of complex cyber situations. This paper presented a variety of sources and information that is useful for gaining CSA. In addition, we presented an illustrative example that showed how sample data can be categorized in an information quality level as well which 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 study was partly funded by the Austrian FFG research program KIRAS in course of the project CISA (850199).

References

Barnum, S. (2014) Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™). Version 1.1, Revision 1. Available at: http://www.standardscoordination.org/sites/default/files/docs/STIX_Whitepaper_v1.1.pdf.

Bergman, M. K. (2001) 'White Paper: The Deep Web: Surfacing Hidden Value', Journal of Electronic Publishing, 7(1).

Conti, G., Nelson, J. and Raymond, D. (2013) 'Towards a cyber common operating picture', in 2013 5th International Conference on Cyber Conflict (CyCon), pp. 1–17.

Danitz, T. and Strobel, W. P. (2001) 'Networking dissent: Cyber activists use the internet to promote democracy in Burma', in Networks and Netwars. National Defense Research Institute RAND.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. Human Factors: The Journal of the Human Factors and Ergonomics Society, 37(1):32–64.

ENISA (2012) National cyber security strategies: practical guide on development and execution. ENISA, p. 45. Available at: 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. Available at: https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf (Accessed: 17 January 2017).

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

GovCERT.ch (2016) Technical Report about the Malware used in the Cyberespionage against RUAG. Technical Report. Available at: https://www.melani.admin.ch/melani/en/home/dokumentation/reports/technical-reports/technical-report_apt_case_ruag.html

Lee, Y. W., Strong, D. M., Kahn, B. K. and Wang, R. Y. (2002) 'AIMQ: a methodology for information quality assessment', Information & Management, 40(2), pp. 133–146.

Lesk, M. (2007) 'The New Front Line: Estonia under Cyberassault', IEEE Security Privacy, 5(4), pp. 76–79.

Mansfield-Devine, S. (2016) 'Ransomware: taking businesses hostage', Network Security, 2016(10), pp. 8–17.

MITRE (2017) Common Vulnerabilities and Exposures, CVE The Standard for Information Security Vulnerability Names. Available at: https://cve.mitre.org/

Naumann, F. and Rolker, C. (2000) 'Assessment methods for Information Quality Criteria', in Fifth Conference on Information Quality (IQ 2000). IQ, Cambridge, MA, USA, pp. 148–162.

NIST (2017) National Vulnerability Database (NVD), Available at: https://nvd.nist.gov/

Ntanos, C., Botsikas, C., Rovis, G., Kakavas, P. and Askounis, D. (2014) 'A context awareness framework for cross-platform distributed applications', Journal of Systems and Software, 88, pp. 138–146.

Ottis, R. (2008) 'Analysis of the 2007 cyber attacks against estonia from the information warfare perspective', in 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, November 2016, Article 2, C-MRIC.

Pahi, T., Leitner, M. and Skopik, F. (2017). Analysis and Assessment of Situational Awareness Models for National Cyber Security Centers. In Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP). SCITEPRESS.

Skopik, F., Ma, Z., Smith, P. and Bleier, T. (2012) 'Designing a Cyber Attack Information System for National Situational Awareness', in Future Security. Proceedings. Springer, pp. 277–288.

Uma, M. and Padmavathi, G. (2013) 'A Survey on Various Cyber Attacks and their Classification.', International Journal of Network Security, 15(5), pp. 390–396.