Bachelor Degree Project

UNIVERSITY OF SKÖVDE

COUNTERMEASURES AGAINST COORDINATED CYBER-ATTACKS TOWARDS POWER GRID SYSTEMS

A systematic literature study

Bachelor Degree Project in Information Technology with a Specialisation in Network and System Administration Level ECTS, 22.5 credits, IT610G Spring term 2019

Jonatan Johansson
f15jonjo@student.his.se

2019-09-15

Supervisor: Thomas Fischer
Examinator: Jianguo Ding

Table of Contents

Abstract

A study on countermeasures against coordinated cyber-attacks (CCA) towards power grid systems has been carried out. A coordinated cyber-attack is a cyber-based attack where multiple attackers use multiple attack-mechanisms towards multiple targets in a coordinated fashion. The coordination is based on that the different attack-mechanisms help each other in attacking the target. A CCA is made up of different stages where each stage consists of a number of attack-mechanisms and together have a certain purpose. The different stages are used to systematically advance towards its goal, which is to compromise the operation of internal systems or to steal confidential data. For example, the first stage may be used to locate entry points at the target system, and a second stage may be used to locate vulnerable hosts by sniffing ongoing network activity to further itself towards its attack goal.

Power grids that are used to generate, transmit, and distribute electricity over large geographical areas are connected to the Internet. Within these environments, commercial IT systems have been adopted to control their electrical equipment, which poses cybersecurity risks to the power grid.

Intrusion Detection Systems (IDS) are designed provide internal network protection in case of intruders. However, state-of-the-art IDSs has been found to have certain limitations in protecting against multi-stage and slow attacks. The inadequacy of state-of-the-art IDSs for protecting against CCAs motivates the need to identify alternate countermeasures that can mitigate CCAs, when the target is a power grid system. The method of choice to address this problem in this study is a systematic literature study where 48 countermeasures were identified and assessed to which extent they are suitable to mitigate CCAs. Results suggest to follow three approaches, namely to preemptively identify technical vulnerabilities in the local system, to distribute intrusion detection hosts across a larger network for better situational awareness, and to implement new types of IDS technologies. Countermeasures with references to specific publications are also provided. The study contributes to how security operators of power grids can fulfil the requirement on cybersecurity as demanded by the NIS directive of the European Union regarding protection against CCAs.

1 Introduction

Power grids are critical infrastructure for modern society. In recent years, existing power grid systems have been redesigned to make use of information technology and to become part of the Internet. Just the sole fact that such systems are connected to the Internet brings a number of security considerations regarding confidentiality, integrity and availability. Ukraine did undergo a series of cyber-attacks directed at one of their power grids that resulted in a power outage, which lasted for a few hours affecting ca 225,000 people (E-ISAC, 2016). This attack was executed in a sophisticated manner compared to regular cyber-attacks. Attacks similar to these are referred to as coordinated cyber-attacks (CCAs).

Power grids experience individual cyber-attacks as well. Based on reported incidents received by ICS-CERT (2016), in 2016 there were 59 known cyber incidents in the energy sector where spear-phishing and network scanning were some of the most common attack methods. These reports indicate that power grids are targets of malicious actors on the Internet. To put this into perspective, ICS-CERT (2016) collected cyber incident reports from all critical infrastructures in the United States and the number of received reports for all critical infrastructures that year was 290.

An Intrusion Detection System (IDS) is an existing protection mechanism against abnormal or malicious activity on a local network. However, Sun, Hahn, & Liu (2018) argue that IDSs cannot handle the malicious activity of CCAs because IDSs monitor a local area and that they might be deceived to waste protection resources on a decoy.

Given this context, this final year project conducts a literature study on relevant scientific literature to identify alternatives for better protection against CCAs towards power grid systems. The aim of this project is to provide information that could strengthen the protection against CCAs for power grid systems for the purpose of protecting the integrity of this critical infrastructure from being compromised. The motivation of this study is based on the assumption that IDSs are limited in protecting against CCAs. The contribution of this study is to provide guidance in fulfilling the NIS directive regarding how to protect against CCAs. The content of the NIS directive and its parts relevant to this study is explained in more detail as follows. ‘Directive (EU) 2016/1148’ on security of network and information systems (NIS directive) is a legislation on cybersecurity by the European Union (EU) and applies to digital service providers and operators of essential services in all EU member states. The NIS directive contains a set of requirements, where each member state should form their own national laws in some way in order to fulfill the requirements. The aim of the directive is to achieve a high common level of cybersecurity across the EU (European Commission, 2016). The goals of the NIS directive can be briefly summarized as international cooperation, nations adopting a cybersecurity strategy, national response teams handling computer security incidents, conducting risk management, prevent and minimize the impact of incidents, and operators being responsible for notifying response team directly about incidents. The NIS directive covers many areas and is currently being developed on a continuous basis. The requirements in this directive are defined with generally broad terms. Therefore, each specific requirement has the focus of an umbrella at the same time as there is leeway for implementation, hence the motivation to boost the *general* level of cybersecurity. This means that nations can follow this directive in various ways. It may be difficult to know how to deal with every single cybersecurity threat when the requirement is simply to protect against them. So, the contribution of this study is to provide guidance on the means for fulfilling the NIS directive requirement about cybersecurity risk management for operators of essential services, with special focus on the threat of CCAs toward power grid systems.

The most relevant section of the NIS directive is the first requirement (1) in Article 14 and is defined as follows.

> ***Article 14 Security requirements and incident notification***
> ***1.*** *"Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed."*
>
> (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, 2016).

This requirement is explained as follows by citing the requirement and describing within parentheses how it is related to this study. Member States (e.g. Sweden) shall ensure that operators of essential services (e.g. Vattenfall operating electricity) take appropriate (i.e. reasonable financial efforts) and proportionate (i.e. effective) technical (e.g. cybersecurity) and organisational (not related to this research project) measures to manage the risks (CCAs) posed to the security of network and information systems (e.g. power grids) which they use in their operations. Having regard to the state of the art (i.e. which this study includes), those measures shall ensure a level of security of network and information systems appropriate to the risk posed (i.e. solving the problem to some extent).

2 Background

This section describes IDSs, the role IDSs have in comparison to other cybersecurity measures, CCAs, power grids, limitations of state-of-the-art IDSs towards CCAs, why IDSs are even used, and how CCAs relate to national security. Lastly, how CCAs, the NIS directive, IDSs, and power grids relate to each other is explained.

2.1 What are Intrusion Detection Systems?

An IDS is a network device that monitors activity either at the border of or within a sub-network of an organization's internal computing system for malicious events. IDSs are usually able to detect some of the regular network attacks or unwanted events that even might be accidental. Once a such an event is detected, the IDS send alarms about a possible intrusion to an administrator or to another device. The IDS is considered a second line of defense because it is located behind the organization's perimeter controls, firewall, authentication mechanisms, and other access controls (Pfleeger, Pfleeger, & Margulies, 2015). There are several characteristics of an IDSs that make up for each specific IDS type, which are knowledge- or behavior-based, network- or host-based, and IDSs with the ability to deploy countermeasures on their own (Sun, Hahn, & Liu, 2018). Not all of these types are within the scope of this study.

This study focuses on network-based IDSs (NIDS) with either a knowledge- or behavior-based detection approach. The different types of IDSs are described below to motivate the relevance of the selected IDS types. A NIDS monitors and analyzes network activity within or between network segments for malicious events. The NIDS mainly inspect network packets, but also analyzes network traffic volumes, load-balance systems, and actions taken by administrators. In contrast to NIDSs, a

host-based IDS (HIDS) resides on a single machine and thus can only monitor and analyze activity of that particular host (Pfleeger, Pfleeger, & Margulies, 2015). Since a HIDS is focused on a single network host, it analyzes its data on operating system level (Pfleeger, Pfleeger, & Margulies, 2015) as well as files, memory, and network traffic sent from and to the local host (Sun, Hahn, & Liu, 2018).

A NIDS is more relevant to this study than a HIDS because a HIDS is limited from seeing the big picture of ongoing events in the network. HIDSs are less likely to detect attacks aimed towards multiple hosts where an individual host may only experience a small portion of malicious activity that is not enough for the HIDS to raise an alarm. As argued by Nicol (2018), a CCA may use different individual hosts in a system as stepping stones to achieve the goal of the attack. NIDSs that can analyze multiple network flows are more suitable to detect such distributed attacks, but in the context of CCAs, there are limitations in its protection.

A knowledge-based IDS, also called signature-based IDS, analyzes network and system activity such as packets, processes, packet segmentation, handshake relationships, and also creates statistics out of these. A knowledge-based NIDS can detect individual malware files based on its database if they are listed there. It can also detect certain sequences of network packets known to have been used by certain attacks. Monitored activity is compared against a database where a set of predetermined attack signatures are installed. A signature is a defined kind of pattern of an attack. The IDS raises an alarm when monitored activity matches one of these signatures. The main disadvantage of this approach is that the IDS only detects a malicious event if a signature has been installed into the database that describes that specific event. This means that different variants of the same type of attack might have to be accounted for in order for complete protection against that attack type. An advantage of this approach is a good level of protection if the target system is not attacked by a large variety of attacks. In contrast to a knowledge-based IDS, a behavior-based IDS, also referred to as heuristic intrusion detection, uses a defined network profile to determine what is considered normal and abnormal behavior on the local system. It differs from a knowledge-based IDS is by raising an alarm as soon as monitored activity matches bad activity to a certain degree (Pfleeger, Pfleeger, & Margulies, 2015). In other words, the IDS will tolerate ongoing network activity until its behavior exceeds a given boundary for network behavior. The group of boundaries that has been set by a behavior-based IDS is called a network profile.

Knowledge-based IDSs and behavior-based IDSs can also be differentiated as rule-driven versus suspicion-driven intrusion detection. The challenge of a knowledge-based IDS is to maintain a database of attack signatures that represent all attacks that is a risk to the local system, whereas the challenge for a behavior-based IDS is to specify an appropriate network profile to produce as little false-positives as possible and at the same time being able to detect real attacks (Sun, Hahn, & Liu, 2018). Both knowledge and behavior-based detection techniques are related to this study because they both have their own disadvantages of managing malicious activity.

An IDS should not be mistaken for an Intrusion Prevention System (IPS), which extend IDS technology with the ability to take security measures to block or stop harm. However, an IPS does not execute its security measures until something suspicious has been detected (Pfleeger, Pfleeger, & Margulies, 2015). Thus, IPSs are not within the scope of this study because execution of security measures depends on if attacks are detected in the first place, and state-of-the-art IDSs are not sufficient in the detection of CCAs.

2.2 General Ways of Protecting Against Cyber-Attacks

A general picture of network security measures being taken by organizations to protect against cyber-attacks is described in this section. The relevance of this section is that it provides insight to what different security measures an organization can protect itself with, but mainly providing context for the role of IDSs in a network. An important aspect of computer security is finding out if someone or something that wants to enter or make changes to a system really is rightful to do so (i.e. authentication). An identity and something that verifies that identity must be provided in order to be authenticated. Password use is widely used in computer systems, but their level of protection mainly depends on limitations at password creation, choice of password, and password management. Patching software that is in use from known vulnerabilities is also a common way for protection.

A vital part of network security is the use of cryptography. It is used to protect stored data or messages being sent across one or several networks by making them unintelligible to unauthorized users or applications in some aspect. One approach of protecting network traffic with cryptography is to fully encrypt each message that is being transmitted across the next communication link (i.e. link encryption at layer 1 or 2 in the OSI model). This particular approach of using cryptography is useful when the communication links between individual network hosts may be vulnerable to some attack. However, the disadvantage of this approach is that each message must be decrypted for each receiving host in order to forward the package in the right direction. All in all, the aim here is to encrypt messages on all links in a network. Another approach of protecting network traffic with cryptography is where the source host encrypts the data portion of each package with some application running on top of the operating system, transmits them across a communication link towards a destination, and not letting any intermediate host decrypt the message until it has reached the destination host (i.e. end-to-end encryption covering all 7 layers of the OSI model). The idea is to protect information being sent across a network from potentially unsecure and intermediate hosts. An advantage of end-to-end encryption is that nullifies session hijacking attacks at the network layer because the message is still encrypted. What end-to-end encryption does not protect against is what happens on the host before the encryption process is complete, which might be an intercepting and malicious software.

The Secure Sockets Layer (SSL) is another way of using cryptography. It encrypts the shared information between a user's browser and a web server. This is a vital part of protection if the information shared should remain confidential when providing login credentials to a Internet-connected web server for example. The information is no longer encrypted than until the server's firewall, making the information potentially vulnerable to the activity beyond that firewall.

A more hands-on cryptographic measure for network security is a Virtual Private Network (VPN) where a client establishes an encrypted session towards a server to access a remote network. Remotely accessing an organization's network is a common practice by workers for effectiveness and convenience. The idea of VPNs is to establish a logical link between two hosts across some network routes and also to keep the exchanged information secured. A VPN solution protects against all the identities that are not registered as legitimate users from accessing the network, via the VPN.

Network segmentation is an important aspect in the defense of cyber-attacks. It can act as a basis for the construction of multiple perimeters within a network, which might require an attacker to perform additional actions to achieve the goal. For example, an organization might want some services to be visible from the Internet while another part of the network stores some sensitive information that only should be visible to in-house workers. Segmenting the part of the network with

sensitive information together with additional security measures may not be such a bad idea.

A firewall is a measure for network security which filters all network traffic being sent in or out of the network. It can determine what kind of data, ports, users, or traffic based on source that is allowed to pass to name a few. This is accomplished with a set of rules configured in the operating system of the firewall. The challenge of using a firewall is knowing what rules to configure in order to block as much malicious traffic as possible and at the same time allow the legitimate traffic to pass. As with firewalls, edge routers can be configured to block some type of traffic as well.

Intrusion Detection Systems monitor traffic that has bypassed a firewall and an authentication mechanism to find out if it might be malicious, as described in section 2.1 (Pfleeger, Pfleeger, & Margulies, 2015).

2.3 Coordinated Cyber-Attacks (CCA)

What a CCA is and how it stands out from other attacks is described in this section. The concept of CCAs can be described and interpreted in many different ways. Therefore, this section presents a description of CCAs based on what a various set of researchers agree upon. These publications are Moya and Wang (2018), Sun, Hahn, and Liu (2018), Xiang, Wang, and Liu (2017), Sun, Hong, and Liu (2016), Wu, Ma, Javadi, and Jiang (2016), Sridhar (2015), Ashok, Hahn, and Govindarasu (2014), Rob, Tural, McLorn, Sheikh, and Hassan (2014), Sisneros, Rivera, Jeantete, and Le (2012), and Braynov and Jadiwala (2003).

CCAs are only executed in cyberspace and should not be confused with coordinated cyber-physical attacks where both cyber and physical attacks are combined to work towards a target. CCAs are typically characterized as coordinated, sophisticated, advanced, structured, and well-organized cyber-attacks. An aspect worth noting about CCAs is that different *stages* are defined in order to systematically advance towards the goal where each stage consists of the combination of all actions being performed concurrently.

A CCA, also referred to as Advanced Persistent Threat (APT) in the scientific domain of cybersecurity, generally consists of a large group of attack hosts targeting multiple targets by the utilization of many cyber-attack mechanisms. The large group of attack hosts allows for cyber-attacks with greater resources, where those resources can be shared in between or to provide extra resources for some of the attacks. A CCA can be designed to target multiple components in a system to increase the chances of stumbling upon or identifying a vulnerability. However, the aim is usually to target multiple components that either rely on or make use of each other in some way. A high number of cyber-attack mechanisms is utilized in order to execute attacks towards multiple system components and also to systematically help other attackers' actions (e.g. causing a vulnerability to be exploited by another attack, delaying a security measure from terminating another concurrent attack, or cover-up). Sometimes, some of these cyber-attack mechanisms are designed to act as non-stealthy decoys by trying to cause a minor abnormality in the target network. The intention here is to deceive the defenders from the real attack by making the victim waste their resources on the decoy.

Aside from non-stealthy decoys, a CCA is stealthy and hard to detect during its execution because the attacks are distributed in space and time. Delays are used between individual actions that may be identified as suspicious if issued too frequently (e.g. not exceeding an IDS's anomaly threshold by delaying individual probe packets for port scanning) and attacks are executed towards a number of individual but related administrative domains or simply many target hosts within a large network. Examples of individual cyber-attack mechanisms or cyber-attacks that have been used in previous CCA incidents are DoS, DDoS, spear-phishing over e-mail, documents with malicious macros over e-

mail, worms, infecting local workstations with availability disrupting malware.

Sridhar (2015) explain the concepts of spatial and temporal cyber-attacks, whose characteristics are similar to CCAs. A spatial cyber-attack is described as "*Spatial attack vectors are attack combinations where an adversary exploits locational dependencies in the power system topology to create maximum impact.*". As for a temporal cyber-attack, it is described as "*Temporal attack vectors are coordinated attack vectors wherein an attacker controls the timing of constituent attacks in an attempt to create maximum damage to the system*".

As compared to individual cyber-attacks, the idea of a CCA to increase its likelihood of being successful attack and also to maximize the damage by uniting numerous individual attacks into coordination. The goal of a CCA is compromising a computer or network system.

Since the contribution of this study is to provide guidance for countermeasures against CCAs on a national level, it must be argued why CCAs pose a threat to nations in the first place. A CCA could target a country (Nath & Mehtre, 2015) and an example of a CCA targeting a nation is where the U.S. Department of Defense did get their documents stolen on several weapon systems (Fortinet, 2013). Another example is the case of Government of Canada where confidential information was taken (Fortinet, 2013).

2.3.1 Defining CCA and its Attack Mechanisms

This section provides an answer to what a CCA is and the different attack mechanisms that can be involved in a CCA in more detail. Mehresh and Upadhyaya (2015) define the different stages of a CCA as listed below.

- *Initial compromise*: Social engineering, phishing, zero-day viruses, etc.
- *Establish foothold*: Install backdoors, Trojan horses, etc.
- *Escalate privileges*: Gain administrator privileges using exploits, password cracking, etc.
- *Internal reconnaissance*: Collect confidential infrastructure information.
- *Move laterally*: Compromise more internal systems.
- *Maintain presence*: Ensure continued control over channels and credentials without raising red flags.
- *Complete mission*: Steal data or compromise mission at an appropriate time.

In addition to already mentioned attack mechanisms in the bullet list above, Zhou, Leckie, and Karunasekera (2010) name some other specific attack mechanisms that are used by CCAs. Slow network scanning is used to locate vulnerable hosts. Worms such as SQL-Slammer, Code Red 2, W32 and Sasser are used to recruit DDoS zombies from one single host.

2.4 Power Grids

A description of power grids is provided in this section in order to understand what kind of systems that is aimed to apply countermeasures to regarding protection against CCAs. The focus of power grids instead of other critical infrastructures is motivated.

The power grid is a network of various types of electricity systems that provide electricity to

residents, commercial organizations, industries etc. The different components of electricity systems are electricity generation, electricity transmission, and electricity distribution. Electricity generation systems are facilities that use any sort of means to produce electric power such as nuclear plants, oil plants, gas plants, solar panels, wind turbines, and water turbines. Electricity transmission systems consist of control centers, substations, and power transmission lines for interconnection between these control centers, substations as well as the electricity generation and distribution systems. Electricity distribution systems consist of means to deliver power to consumers and transformers that adjusts voltage to appropriate levels per service location (Fang, Misra, Xue, & Yang, 2012).

The use of information technology (IT) and Internet has been adopted by modern power grids, which can expose power grid systems to new threats. IT systems being integrated into the power grid is not always tailored towards this type of industrial environment. In recent years, off-the-shelf IT solutions (i.e. standardized and commercial IT solutions) have been integrated into the power grid to a great extent, which means that the same kind of vulnerabilities that expose individual citizens' computers also might expose some system in a power grid (Ericsson, 2010). A certain system that plays an important role in monitoring and controlling a critical infrastructure, e.g. the power grid (Nazir, Patel, & Patel, 2017), is the supervisory control and data acquisition (SCADA) system. SCADA systems are sometimes accessed remotely over the Internet, where improper security management of remote access solutions might open an attack vector for possible attackers.

In comparison to other critical infrastructures, power grids are considered for this study due to reports indicating that it was one of the critical infrastructures in the United States that experienced the most cyber-incidents during 2015. The top five critical infrastructures, ranked in terms of reported cyber-incidents during 2015, were Critical Manufacturing with 97, Energy Sector with 46, unknown with 27, Water with 25, and Transportation Systems with 23 (NCICC, 2015). The real-world event of the successful coordinated cyber-attack against the Ukrainian power grid (E-ISAC, 2016) contributes to the focus on power grids as well. In general, stable electricity is required for other vital systems (e.g. public transport or IT services).

The consequences a CCA might have on critical infrastructure and power grids in particular are described as follows. The most commonly mentioned impact is severe physical impact to the power grid infrastructure as argued by Rob et al. (2014) and Sridhar (2015). Both Sun et al. (2016) and Sisneros et al. (2012) provide a bit more concrete description on this type of impact, which is mis-operation or damage to generation or transmission equipment. In contrast, power grid distribution equipment does not seem just as vulnerable to CCAs as it is never brought up in this aspect. The second most commonly mentioned impact is failure of two or more components in the power grid, which a power grid is not capable of recovering from since a power grid only has redundancy capability for one failed component at a time, as argued by Moya and Wang (2018) and Ashok et al. (2015). From a more abstract perspective, Moya and Wang (2018) state that CCAs could inflict catastrophic consequences and Sisneros et al. (2012) state that a CCA disables or impairs the integrity of multiple control systems.

2.5 Limitations of State-of-the-Art IDSs Towards CCAs

What limitations do state-of-the-art intrusion detection systems have towards CCAs? In a study by Akinrolabu, Agrafiotis, and Erola (2018), it is concluded that existing IDSs are inadequate in detecting multi-staged, low and slow attacks. Sun, Hahn, and Liu (2018) argue that IDSs are limited in handling CCAs because of their monitoring scope design and in most cases, IDSs focus on a local area. Cyber protection systems such as IDSs can be weakened by insiders performing abnormal actions due to

being disgruntled or misinformed by attackers (Sun, Hahn, & Liu, 2018). Most early IDSs focused on monitoring a single system or network for intrusions. The monitoring boundary at the edge of a single network makes detection for sophisticated and distributed attacks improbable since events outside of the local network are unknown of (Vasilomanolakis, Karuppayah, Mühlhäuser, & Fischer, 2015).

Aniello, Di Luna, Lodi and Baldoni (2011) state that single organizations use IDSs to protect against port scan attacks but that the modern attacker at the same time can perform port scan attacks that are distributed in both space and time, which can go undetected by the IDS. Such an attack is distributed in time by delaying individual probes and distributed in space by probing a small amount of ports towards different administrative domains of an organization, one at a time. This way of performing port scan attacks could exploit time window controls and set thresholds of an organization's IDS. Zhou, Leckie, and Karunasekera (2010) argue that it is less likely that an IDS located and focused on a single network domain would detect malicious probe packets because the quantity of such packets at that particular network may not exceed the anomaly packet threshold of the local IDS. An attacker could exploit this threshold in an effective way by sending each single probe packet directed at multiple network domains in random order, as long as the packets do not exceed the threshold of each IDS in each individual network domain.

Moya and Wang (2018) clearly express existing limitations in IDSs; "*they suffer from false alarms, fail to identify CCAs, and cannot estimate the attack consequences on the grid*". IDSs cannot protect against all kinds of at"tacks (Elshoush & Osman, 2011) and also have a hard time detecting unusual attacks (Moya & Wang, 2018). Another limitation of IDSs is that an attack might deploy some decoys to deceive the IDS to waste its protection resources on that, instead of focusing on the real attack (Sun, Hahn, & Liu, 2018).

2.6 Relationships Between IDS, CCA, and the NIS Directive

How CCA, IDS, and the NIS directive relate to each other from the perspective of this study is described in this section. A CCA is a kind of attack that mainly differs from conventional attacks because of it uses multiple individual attacks in a well-planned and coordinated way instead of single and independent attacks. Both the likelihood of being successful and impact of a CCA are considerably greater than conventional attacks.

IDSs play an important role in protecting internal networks of an organization where sensitive information may exist. Although initial security mechanisms of a network (e.g. authentication mechanisms) may hinder attacks, IDSs can prevent some attacks who succeed to surpass initial security mechanisms. Also, an IDS might be the only line of defense internally.

CCAs are stealthy and are capable of exploiting the limitations of IDSs. CCAs might then compromise the operation of internal systems or steal confidential information. CCAs thus become a relevant threat because of the inadequacy of protection from IDSs.

The NIS directive aims to achieve a higher common level of cybersecurity in the EU, where critical infrastructures are heavily focused on and are required to take appropriate actions to protect themselves from threats as posed from the Internet. Power grids, as the critical infrastructure that it is, have integrated information technology and off-the-shelf IT solutions to a great extent, including IDSs. The integration of information technology and connectivity towards the Internet makes power grids possible targets of cyber-attacks, just as any other host taking part of the Internet, and may even be seen as an exciting or challenging target for causing as much damage as possible.

CCAs have already shown its presence in attacking and successfully compromising power grids in

various ways. At the same time, the NIS directive requires power grids to protect itself from threats, such as the CCA. Guidance on how IDSs or other system components in power grids should be re-designed can allow security persons of power grids to know how the requirement from NIS can be fulfilled.

2.7 Related Research

Related research is where Singh, Sharma, Moon, Moon and Park (2016) conduct a literature study on the countermeasures against CCAs, and their result is that they categorize countermeasures based on what domain they are aimed to be applied to. In contrast, this study has primary focus on the application domain of power grids.

3 Problem

It is not expected that state-of-the-art IDSs should be able to prevent all types of cyber-attacks. They have the role of monitoring a network for malicious activity but have limitations in what they actually can detect, considering CCAs in particular. The main limitations are that IDSs are limited to the local network (Sun, Hahn, & Liu, 2018), probe packets may be allowed as long as they do not exceed the set packet number threshold (Zhou, Leckie, & Karunasekera, 2010), and fail to identify multi-stage attacks (Akinrolabu, Agrafiotis, & Erola, 2018). An attack such as a CCA might exploit these limitations and possibly compromise the integrity of an Internet-connected critical infrastructure such as the power grid. Sun, Hahn, and Liu (2018) argue that while IDSs have been heavily researched in terms of all-out IT systems, there are less IDS solutions that are designed for systems where cyber and physical systems are interconnected (e.g. power grids). If an IDS should be implemented to a power grid environment, it must be tailored in order to support the unique communication protocols and operations that is used by the physical components of the power grid. In this context, some IDS solutions that have been developed to meet these requirements. Yet, many of these solutions have not been tested enough to ensure their operability to real-life environments (Sun, Hahn, & Liu, 2018). The level of protection an IDS provides to a power grid system when implemented is therefore rather unknown currently, and when implemented, may make a power grid system vulnerable in some way.

Those considerations lead to the following research question:

Given the limitations of state-of-the-art intrusion detection systems towards coordinated cyber-attacks, which other countermeasures are available and which ones are most suitable to mitigate such attacks towards power grid systems?

Sun, Hahn, & Liu (2018) conducted a state-of-the-art survey of the most relevant cybersecurity studies in power grids, which present state-of-the-art technologies of power grids. The authors also discuss which unsolved cybersecurity problems there are. How CCAs towards power grids should be dealt with is one of them, emphasizing that further research on the topic is much needed.

It is important to address the formulated research question because the critical infrastructure of power grids must be protected to keep its operational integrity in control so that people in a potentially large geographical area does not lose the electricity they depend on. The problem is relevant in the context of network and system administration because network security, where coordinated cyber-attacks pose a threat, is one of the main responsibilities of a system administrator.

4 Methodology

A systematic literature study is the chosen method to provide answers to the research question. In a literature study, literature that are relevant to a certain research question is collected by searching in catalogues of scientific publications. The collected material can be used to summarize, show differences or similarities, and present other aspects about the field which can be learned from or provide answers to a certain research question. In this literature study, a qualitative approach is taken because this study is on a theoretical level due to the confidentiality of how power grid systems technically operate. The guidelines of how a systematic literature study should be performed as suggested by Kitchenham & Charters (2007) are followed but in a simplified way, since those guidelines are aimed above the academical level of this study. The guidelines of Kitchenham and Charters (2007) influence a number of steps in this thesis, namely the steps of selection of publications, data extraction, data analysis, and summarization. Kidwai (2012) describe different themes that can be used to focus the organization of a literature study in different ways, which are; *Do they present one or different solutions? Is there an aspect of the field that is missing? How well do they present the material and do they portray it according to an appropriate theory? Do they reveal a trend in the field? A raging debate?* The theme "*Do they present one or different solutions?"* has been chosen for this literature study because the idea of this literature study is mainly to find out which countermeasures are available in existing scientific publications to mitigate CCAs, regardless of any debate or currently missing pieces about the topic. Furthermore, identified countermeasures from the literature are categorized based on their characteristics for further analysis where they are compared to see which one seem to be the most suitable solution for mitigating the problem. A number of different searches are conducted with focus on different subjects. The search subjects are the following.

Search subject #1 – presented in section 2.3.1
What is a CCA and what different attack mechanisms can be involved in a CCA? Historic CCA incidents may be presented as an outcome of this search.

Search subject #2 – presented in section 2.5
What limitations do state-of-the-art intrusion detection systems have towards CCAs?

Search subject #3 (Research question regarding available countermeasures) – presented in Appendix B
Given the limitations of state-of-the-art intrusion detection systems towards coordinated cyber-attacks, which other countermeasures are available to mitigate coordinated cyber-attacks towards power grid systems?

Search subject #1 and #2 are used to provide background information to the research question. Only limited literature search has been conducted on answering these subjects, whereas a systematic literature study is conducted for search subject #3 as it is the main focus of this project.

4.1 Process of Selecting Literature

How literature is systematically selected is presented in this section. Before the process of selecting literature began, a pre-study was conducted to validate if the set of selected databases provide adequately relevant literature and also to see if the search queries need to be improved based on the

relevancy of the search results. The effects the pre-study had on the final process of selecting literature is described in results. The guidelines of Kitchenham and Charters (2007) are used to select which databases to search in, which are the academic databases ACM Digital Library, IEEE Xplore Digital Library, Science Direct, SpringerLink, and Citeseer. As mentioned by Kitchenham and Charters (2007), they make up for majority of the databases that software engineers should use for systematic literature studies.

The process of selecting literature has several steps which are described as follows. Each publication must be relevant to the research question in order to pass to the next step in this process. A number of steps are performed to select literature from each database, which are outlined below.

1. Based on the research question and experience from pre-study searches, relevant keywords for a database search are identified and categorized.
2. Based on the identified keywords, several relevant catalogues of scientific publications are queried with search requests customized with the catalogues' query syntax and accounting for known database limitations.
3. Search results are filtered from non-relevant titles
4. Search results are filtered from non-relevant abstracts
5. Remaining publications are read in full-text and filtered from ones that do not provide relevant information to the research question

4.2 Search Databases and Terms

This section presents databases where relevant literature is searched for and all search strings to search with in each database. The search terms have been chosen based on the research question itself, related words, synonyms, abbreviations, and common terms that are used in the publications as found during pre-study searches. A variety of terms are used along with the Boolean operators ‘AND’ and ‘OR’ in order to higher the chances of retrieving as many relevant search hits as possible from each database. An example of such a search string can be seen in Table 1.

Table 1. An example of how search terms can be combined

‘critical infrastructure’ ‘power grid’ ‘energy sector’ ‘smart grid’ ‘electric grid’ ‘electrical grid’ powerhouse ‘power plant’ ‘power station’ SCADA ‘control system’	‘coordinated cyber attack’ ‘coordinated attack’ ‘combination attack’ ‘multi-stage attack’ ‘heterogeneous attack’ ‘multi-step attack’

An OR-operator is used between every term or phrase inside each cell, and each split between two cells represents an AND-operator. Search results must therefore match at least one term or phrase from each cell and thus different matches can be made.

4.3 Selection Criteria

This section presents the inclusion criteria that aim to for relevant publications. Quality criteria that are used to avoid a biased selection for publications are also listed. The inclusion criteria are presented in the bullet list below.

- Date of publication is not earlier than 2014
- The number of pages is five or more
- Is a journal article or conference article
- Is a non-duplicate of another selected publication
- Provides a countermeasure towards some form of CCA
- CCAs are described as a cyber-attack consisting of multiple attackers, using multiple cyber-attack mechanisms, towards multiple related targets in a coordinated manner

The date of publication not being older than five years is motivated by the constantly evolving mechanisms of cyber-attacks. The year 2019 regarding date of publication is considered to include the latest research. The publications may not consist of four pages or fewer because they provide too little information and tend to have low quality. Only journal articles and conference articles are selected because they are assumed to be of higher quality.

Countermeasures that are designed to be applied to other domains than power grids (e.g. other critical infrastructures or enterprise networks) are also included. While some countermeasures may be too specifically designed towards another kind of system than power grids, others may have a somewhat generic design, which may allow for a possible implementation into a power grid system. The motivation behind this reasoning is that power grids have integrated off-the-shelf IT solutions to a great extent (Ericsson, 2010), which means that non-power grid systems may use the same kind of equipment and technology as power grid systems, except from the physical machinery directly related to the operation of power grids. However, since countermeasures that are designed to be applied to other domains than power grids are included in this study, it should be noted that not every countermeasure as presented in this study may be suitable for integration into a power grid environment without modification.

Literature studies are not included because they do not provide genuine new contributions to the subject of this study.

Regarding quality criteria, the assessment for the quality of each publication is based on subjective impression. This subjective impression takes a certain number of different aspects into consideration, which are grammar, tidiness of report structure, and orderliness of diagrams.

It should be clearly noted that there are no restrictions for what a countermeasure may be in order to be included for this study. The different kinds of countermeasures can thus be overall directional advices, or very situational with specific technical details. Publications that only focus on a certain aspect of a CCA instead of a CCA as a whole are also included.

4.3.1 Addressing the Problem of Publication Bias

Kitchenham and Charters (2007) refer to a problem among publications where positive results are more likely to be published than negative results. This applies to researchers in general but

researchers of experiments in particular. For example, a certain IDS software that successfully protects against a certain threat is more likely to be published than an IDS software that does not. In order to keep the study systematic, the problem is addressed by including relevant conference proceedings into the pool of literature. Kitchenham and Charters (2007) recommend to find relevant grey literature, conference proceedings, and getting hands on unpublished results to address the problem of publication bias. Only the measure of conference proceedings is taken into practice by this study because such literature material already exists in the search results from the databases. Searches for grey literature and unpublished results are not conducted because it is considered to be beyond the scope for a thesis on Bachelor level.

4.4 Data Extraction

Relevant information from each publication is extracted for being able to address the research question. As suggested by Kitchenham and Charters (2007), data extraction forms are used during this process to extract relevant information needed to answer the research question, but in a simplified way, and also to present all publications in a consistent way (see Table 2).

Table 2. Data extraction form to represent all selected publications

Authors, year of publication	***Title***	**Aspect of a CCA**	**Countermeasure**	**Application domain**

All elements presented in Table 2 are extracted in order for easier association between authors and their work. Countermeasures are extracted for summarization by descriptions of the CCA aspect to mitigate, methodology, and effect. Application domains are extracted to see which countermeasures that are applicable to power grids.

4.5 Data Analysis and Evaluation

Based on the data extraction and subjective interpretation of each publication, a data analysis is performed where all identified countermeasures are compared against each other to identify their differences. Such differences may be focused on the certain aspect of a CCA, applicability towards power grids, or pros and cons between approaches. Furthermore, identified countermeasures are categorized into classes after they have been analyzed to show what different types of approaches there are. The selected publications are also used to present how many publications there has been per year. According to Berndtsson, Hansson, Olsson, and Lundell (2008), making categorizations and detecting patterns are suggested means when analyzing literature. The outcome of this analysis is a categorization of studied publications, which is later used to draw conclusions regarding the most suitable countermeasure to mitigate CCAs towards power grids.

After the data analysis, a data evaluation is conducted primarily to present and discuss advantages and disadvantages or the different categories. At the end of the data evaluation, a comparison of the different categories is conducted to show what differences and similarities there are between the

categories and which parts of CCAs they mitigate. Also, possible gaps in research are identified as an outcome of the data evaluation.

4.6 Validity

The type of literature study that this study uses is systematic, as compared to descriptive literature studies where only a representative sample is collected to represent the population. For reproducibility purposes, the number of included publications for each step in the selection process is logged. Search strategies initially defined in the planning phase are tested during the pre-study of each database in order to improve the validity of its comprehensiveness of search results. Date of search, used search strategy, and the number of saved publications is documented for validity and reproducibility purposes.

4.7 Ethical Considerations

This study provides information on the main limitations of IDSs and how CCAs can exploit them overall, which may encourage hackers to begin executing attacks. However, the ethical aspect of this study is justified by the argument that all information is gathered from publicly available publications, and that no concrete vulnerabilities are revealed, nor how to exploit them, and this study is actually focused on how the threat of CCAs can be mitigated and seeing the importance of that. Ethical considerations on the results are justified through the idea of identifying countermeasures to mitigate a problem that can compromise the integrity of a critical infrastructure.

4.8 Alternative Methods

The method of choice is not a case study nor an experiment because the technical information about cybersecurity for power grids is often confidential or restricted to access due to the importance of protecting sensitive information for critical infrastructures. Instead, publicly accessible material is worked with.

5 Results

This section presents how the study was executed and the literature that was gathered. Data analysis, data evaluation, and findings from evaluating the literature are also presented.

5.1 Pre-Study

As previously mentioned, the pre-study was conducted to validate if databases contained relevant publications and if the created database queries retrieved comprehensive results. During pre-study searches, relevant publications were read to identify relevant keywords for retrieving as many relevant results as possible. When conducting the pre-study for the database Citeseer, the following search query was used to assess the relevancy of its publications (see Table 3).

Table 3. Database query for Citeseer

'critical infrastructure' 'power grid' 'control system' SCADA	'coordinated cyber attack' 'multi-stage attack' 'distributed attack' 'organized attack' 'heterogeneous attack'	countermeasure counteraction counteract counterstep mitigate mitigation prevent minimize avoid improve

Based on the titles of retrieved search results from Citeseer, this database indicated a low level of relevancy to the research question. Citeseer was therefore assessed of not being able to provide an adequate level of relevant publications. The search was executed on the April 29, 2019. As a result, Citeseer was excluded from the set of selected databases, keeping only IEEE Xplore, ACM Digital Library, SpringerLink and Science Direct. Removing Citeseer led to only using half of the databases that Kitchenham & Charters (2007) recommend. The other half of not used databases are Citeseer, Inspec, EI Compendex, and Google Scholar. Aside from what databases Kitchenham and Charters (2007) recommend, SpringerLink is also one of the selected databases where Berndtsson, Hansson, Olsson, and Lundell (2007) recommend to use it.

After each database query had been tested towards its designated database, each database query resulted in being different from each other (see section 5.2). Since the databases had different limitations regarding length of the query and allowed number of Boolean operators, different numbers of terms had to be excluded from each query in order to retrieve as many results as possible while only making use of a single query (i.e. terms had to be more prioritized for some database queries than others). Changes were also made to the database query if search results indicated a low level of relevance based on the retrieved titles. Terms to replace with in such cases were heavily influenced by the words used in relevant publications. Search queries used for the selected databases can be seen in the next section. Pre-study searches for the database ACM Digital Library resulted in a database query having the most amount of terms related to power grids compared to the other database queries. Initial pre-study searches for ACM Digital Library indicated few search results when not all of these terms relating to power grids were used. Terms inspired from publications during the pre-study searches were added to the database query, which later resulted in a higher number of search results.

5.2 Selected Literature

In order to select a set of literature, retrieved search results from databases went through a process for selecting only relevant publications. A number of publications was selected per database (see Figure 1). The selection process that was used for each database to select the publications is described in section 4 where the steps are search results, title, abstract, and lastly full-text.

All following databases in this section were used for search subject #3, being *Given the limitations of state-of-the-art intrusion detection systems towards coordinated cyber-attacks, which other countermeasures are available to mitigate coordinated cyber-attacks towards power grid systems?*. For ACM Digital Library, the following database query was used (see Table 4). The search was executed on the April 21, 2019.

Table 4. Database query for ACM Digital Library

'critical infrastructure' 'critical infrastructure' energy 'energy sector' 'power grid' 'smart grid' 'smart power grid' 'electric grid' 'smart electric grid' 'electrical grid' 'smart electrical grid' 'intelligent grid' intelligrid futuregrid intergrid intragrid 'power station' 'power plant' powerhouse 'generating station' 'generating plant' generation substation transmission distribution SCADA 'control system'	'coordinated cyber attack' 'coordinated attack' 'combination attack' 'multi-stage attack' 'cooperated attack' 'sophisticated attack' 'sophisticated cyber attack' 'advanced attack' 'advanced threat' 'structured attack' 'organized attack' 'synchronized attack' 'systematic attack' 'multi-attack' 'attack group' 'many cyber attacks' 'cyber mechanisms' 'heterogeneous attack' 'heterogeneous threat' 'simultaneous attack' 'spatial attack' 'temporal attack' 'multi-step attack' 'distributed attack'

As previously explained in section 4.2 regarding database queries, each term or phrase in each column is OR-combined and each column that makes up for the whole database query is AND-combined, which forms a search expression in conjunctive normal form. The database query was not affected by any limitation of the database searches. 'The ACM Full-Text Collection' is selected for the search in order to narrow down the results only to literature published or sponsored by ACM, in contrast to the alternative 'The ACM Guide to Computing Literature' that includes literature from other publishers.

In IEEE Xplore Digital Library, the following database query was used (see Table 5). The terms used in this query did not need to be adapted to retrieve more search results and was not affected by any limitation of the database searches. The search was executed on the April 29, 2019.

Table 5. Database query for IEEE Xplore Digital Library

'critical infrastructure' 'power grid' 'energy sector' 'smart grid' 'electric grid' 'electrical grid' powerhouse 'power plant' 'power station' SCADA 'control system'	'coordinated cyber attack' 'coordinated attack' 'combination attack' 'multi-stage attack' 'sophisticated attack' 'sophisticated cyber attack' 'advanced attack' 'advanced threat' 'structured attack' 'organized attack' 'synchronized attack' 'systematic attack' 'multi-attack' 'attack group' 'many cyber attacks' 'heterogeneous attack' 'temporal attack' 'simultaneous attack' 'multi-step attack' 'distributed attack'

In Science Direct, the following database query was used (see Table 6). This database query is very short in comparison to the other queries, and that is because Science Direct do not allow more than a few Boolean operators per search. The most important keywords were selected because of this matter. The search was executed on the May 1, 2019.

Table 6. Database query for Science Direct

'critical infrastructure' 'control system' grid SCADA	'coordinated attack' 'distributed attack' 'organized attack' 'multi-stage attack'

In SpringerLink, the following database query was used (see Table 7). This is the same database query that was used for IEEE Xplore (i.e. no change was needed in order to work well). The search was executed on the April 24, 2019.

Table 7. Database query for SpringerLink

'critical infrastructure' 'power grid' 'energy sector' 'smart grid' 'electric grid' 'electrical grid' powerhouse 'power plant' 'power station' SCADA 'control system'	'coordinated cyber attack' 'coordinated attack' 'combination attack' 'multi-stage attack' 'sophisticated attack' 'sophisticated cyber attack' 'advanced attack' 'advanced threat' 'structured attack' 'organized attack' 'synchronized attack' 'systematic attack' 'multi-attack' 'attack group' 'many cyber attacks' 'heterogeneous attack' 'temporal attack' 'simultaneous attack' 'multi-step attack' 'distributed attack'

The number of publications that was kept for each step of the process of selecting literature is shown below (see Figure 1).

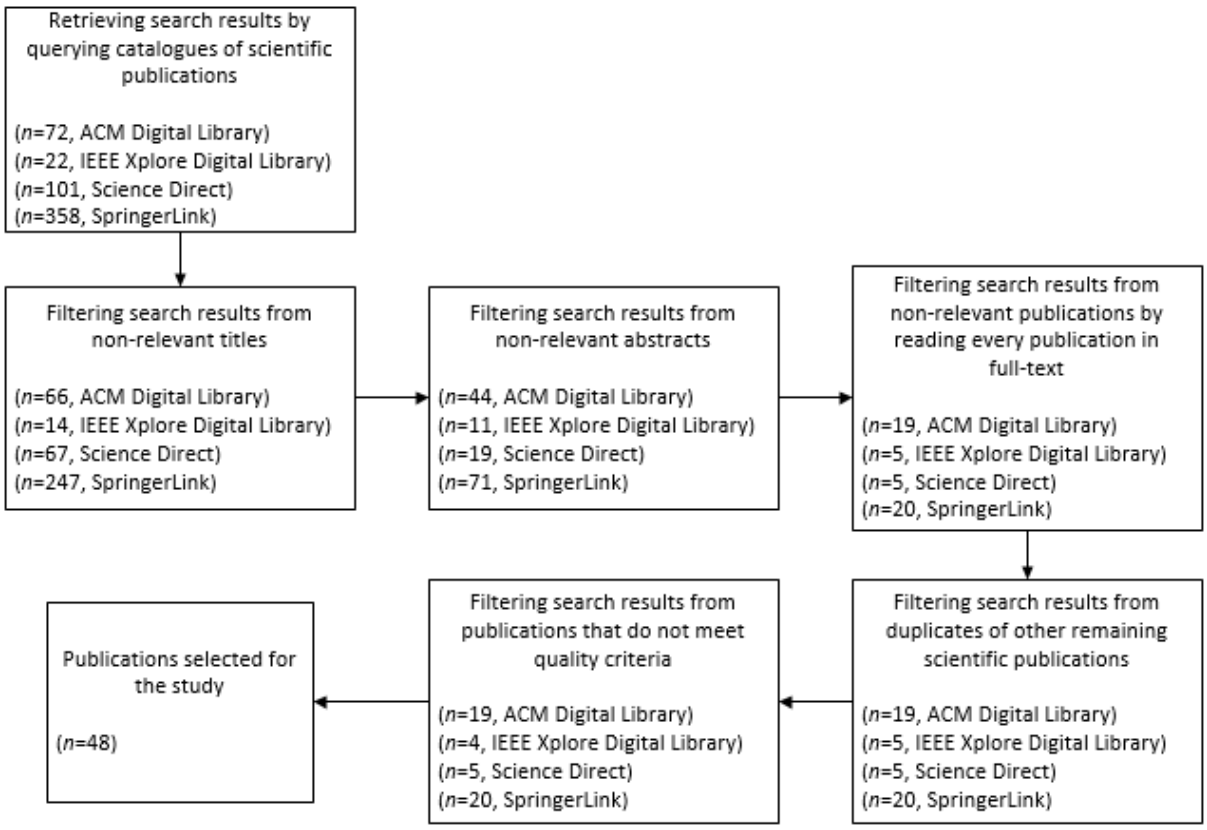

Figure 1. The number of publications for each database and selection process step

The process of selecting literature resulted in 48 scientific publications, without needing to exclude any duplicates. One publication did not meet quality criteria. Each publication that is subject to the study can be found in Appendix A. Extracted data to represent each publication can also be found in Appendix B.

5.3 Data Analysis

The annual rate of publications on the topic is shown in Figure 2.

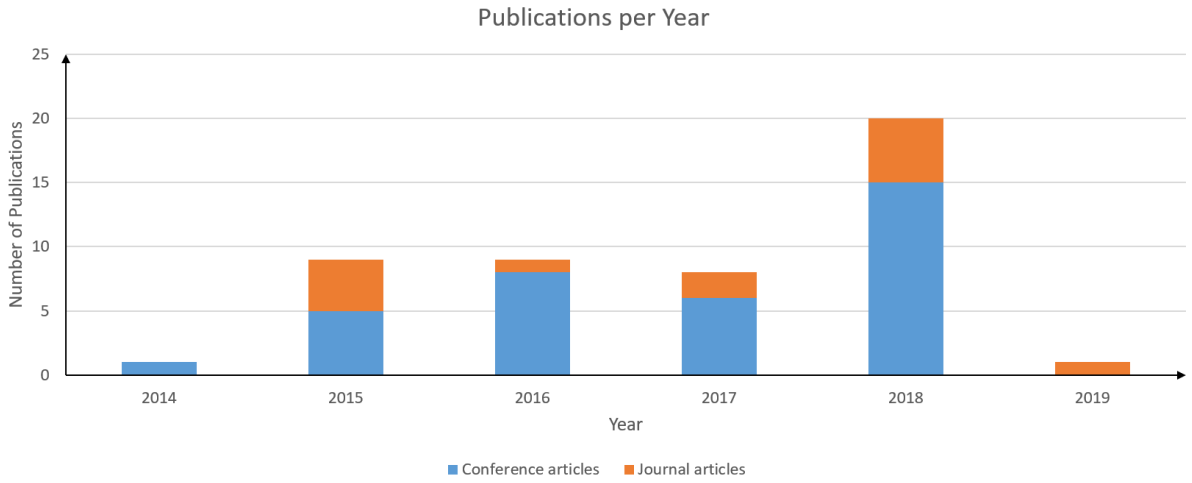

Figure 2. Illustration of scientific publications per year on the topic of countermeasures against CCAs

As can be seen in the diagram, the increase of publications suggests a general increase in attention and prioritization of the topic. There is almost no research made in 2014 which may depend on a lack of importance on the topic at the time. There is a considerable drop in research during the current year, 2019, which may depend on that effective countermeasures have been developed or that there has not been a full year yet. Regarding type of literature, 35 out of the 48 publications are conference articles and the remaining 13 are journal articles.

Eight categories have been created to represent different types of approaches for mitigating CCAs. A publication can be in multiple categories at the same time, which is due to some publications proposing multiple countermeasures. The created categories and each category's publication rate per year are shown in the table below (see Table 8). Each category in the table is ordered by the number of publications fitting into this category.

Table 8. Number of publications per year for each category

Category	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**Total**
New Analysis Process for the Individual IDS	0	2	2	1	7	1	13
System Vulnerability Analysis	0	4	2	1	4	0	11
Cooperative Intrusion Detection	0	1	1	3	2	0	7
Network Obfuscation	1	0	2	0	3	0	6
Investigate CCA Characteristics	0	1	1	1	3	0	6
Game Theoretical Guidance of Defense	0	0	1	1	2	0	4
Baiting the Attacker	0	1	0	0	1	0	2
Cybersecurity Information Sharing	0	0	0	1	0	0	1

Category *New Analysis Process for the Individual IDS* focuses on technical implementations to single IDSs which may be different from conventional IDS technology. Such implementations could redesign correlation between events, alarm techniques, and the type of information being analyzed by the IDS. Proposed countermeasures involve white-list-based IDSs, making the IDS consider relationships between local applications and devices, capturing information from a simulated power grid that experience attacks in order to learn what activity that is abnormal from experiments rather than real-world incidents, and integrating attack-graphs into an IDS's analysis process, where an attack-graph represents unsecured paths in the local network which an attacker can exploit by a combination of actions, whether it be malicious or legitimate actions. The majority of studied publications have been placed in this category. A possible reason for the higher number of publications focused on this type of countermeasure might be because of published research claiming that IDSs have limitations against multi-stage and sophisticated attack mechanisms (see section 2.5).

This approach is discussed by Angelini et al. (2018), Babu et al. (2017), Friedberg, Skopik, Settanni, and Fiedler (2015), Haas and Fischer (2019), Kiesling, Ekelhart, Grill, Strauss, and Stummer (2016), Kim, Choi, and Choi (2018), Kumar, Rensink, and Stoelinga (2018), Lanoe, Hurfin, and Totel (2018),

Luh, Schramm, Wagner, Janicke, and Schrittwieser (2018), Nath and Mehtre (2015), Rubio, Roman, Alcaraz, and Zhang (2018), Sun, Hong, and Liu (2016), and Zhao and Qiu (2018).

Category *System Vulnerability Analysis* mainly focuses on assessing the level of security for the local network to identify how the system is vulnerable in different ways and what threats there are. Proposed countermeasures involve generating attack-graphs (i.e. unveil possible attack paths that can be taken through the network by exploiting a combination of certain technical vulnerabilities), finding out if there are any non-monitored traffic flows in the network, simulating a network for assessing how it handles attacks or alternations, and an algorithm that generates attack-graphs based on online exploit databases and compares it to the local network.

This approach is discussed by Bodström and Hämäläinen (2018), Ekelhart, Kiesling, Grill, Strauss, and Stummer (2015), Ghosh et al. (2015), Gonzalez-Granadillo, Rubio-Hernan, and Garcia-Alfaro (2018), Han, Cheng, Zhang, and Feng (2015), Kumar, Ruijters, and Stoelinga (2015), Mediouni, Nouri, Bozga, Legay, and Bensalem (2018), Nicol (2018), Paul and Ni (2017), Potteiger, Martins, and Koutsoukos (2016), Rodríguez, Chang, Li, and Trivedi (2016).

Category *Cooperative Intrusion Detection* focuses on decentralization of intrusion detection techniques. The idea is to improve the awareness of threats through distributed monitoring and distribution of tasks. This defense approach is similar to how CCAs are performed, which put distributed resources and various techniques into use. When there are multiple hosts that analyze a larger network as a whole (e.g. multiple instances IDSs), they can compute different tasks for wide-spread coverage or they can cooperate to do a single task that may require a lot of resources (i.e. load balance). Proposed countermeasures involve deploying multiple agents that can prioritize more suspicious events over others.

This approach is discussed by Kendrick, Criado, Hussain, and Randles (2018) Nagar, Nanda, He, and Tan (2017), Paridari et al. (2016), Rubio, Alcaraz, and Lopez (2017), Settanni et al. (2017), Singh, Ozen, and Govindarasu (2018), Zulkefli, Singh, and Malim (2015).

Category *Network Obfuscation* focuses on making changes to the configuration of the local network and topology. This is either performed routinely or after an intruder has been detected to have surpassed initial security mechanisms. The aim of this approach is to obscure the attacker's view of the target network so that no vulnerable hosts can be identified through possible network reconnaissance. Proposed countermeasures involve sending fake messages internally to make it harder for an attacker to know what network traffic that is legitimate.

This approach is discussed by Chowdhary, Alshamrani, Huang, and Liang (2018), de Sá, da Costa Carmo, and Machado (2018), Jafarian, Al-Shaer, and Duan (2014), Jeon, Yun, and Kim (2016), Smith, Zincir-Heywood, Heywood, and Jacobs (2016), and Zimba, Wang, and Chen (2018).

Category *Investigate CCA characteristics* focuses on learning what CCAs are, how they behave, and how they are conducted, as a preemptive approach. Proposed countermeasures involve learning from historical events, reflect on theories such as improbable events, contradiction between the idea of a CCA and reality, the unknown duration of a CCA, and that duplicate information hinder learning.

This approach is discussed by Bodström and Hämäläinen (2018), Luh, Schrittwieser, and Marschalek (2016), Mehresh and Upadhyaya (2015), Paudel, Smith, and Zseby (2017), Pitropakis et al. (2018), and Wang, Kwon, Ma, Zhang, and Xu (2018).

Category *Game Theoretical Guidance of Defense* focuses on to influence the decision-making on what security measures to implement to tackle attacks, by using game-based ideas on the interplay between defenders and attackers. Games in this context refer to how a defender should play to win the game against the attacker. Proposed countermeasures involve a simulated environment where the defender has a set of security measures to choose from and learns over time which measures that are the most effective ones and can therefore develop a plan for real-life attack situations.

This approach is discussed by Fielder, Li, and Hankin (2016), He and de Meer (2017), Moothedath et al. (2018), Touhiduzzaman, Hahn, and Srivastava (2018).

Category *Baiting the Attacker* simply focuses on luring the attacker into targeting a specific piece of information in the local network, such as a file or host, where the attacker exposes himself by a hard-coded alarm being triggered if that information is accessed. Proposed countermeasures involve decoys, such as honeypots that are designed for this particular purpose.

This approach is discussed by Bodström and Hämäläinen (2018), and Gjermundrød and Dionysiou (2015).

Category *Cybersecurity Information Sharing* focuses on sharing and obtaining technical data on cybersecurity to raise awareness about current vulnerabilities and threats. The information is either obtained from online reports or from other organizations which share their experiences and incidents.

Only one publication discussed this kind of approach, where de Fuentes, González-Manzano, Tapiador, and Peris-Lopez (2017) presented a protocol that can aggregate thousands of online cybersecurity incident reports and an organization can share that information to others thereafter.

The process of creating these categories is explained as follows. The categories were created by first reading all publications in their entirety and identifying similarities and differences thereafter. The first factor that separates different countermeasures is whether the focus is on the attacker or a potential target system. This aspect was taken into account since all systems may not be able to make certain changes to the local system in the near future due to implementation costs or even reduced security for example. In such cases, the attacker can be focused on instead. For example, *Investigate CCA Characteristics* focus on the attacker while *System Vulnerability Analysis* mainly focus on the local system.

The second factor that was used for the categorization were if countermeasures are aimed towards some network component within a local network and towards which component if that is the case. The type of network component was taken into account for categorizing the countermeasures because each component can provide or be the cause of different strengths and weaknesses to the local system. Network components may differ in such an aspect since each component in a network may run its own software and network components may also differ in criticalness to the local system (i.e. some network components may be dependent on others). This factor was used to present for which components new technology has been developed. Proposed countermeasures aimed towards a certain network component can thereby be taken part of if that specific component is known to provide an insufficient level of security. An example of a category focusing on a specific network component is *New Analysis Process for the Individual IDS* for IDSs.

The last factor that was used for the categorization was if the publications present similar concepts and ideas on a general level. This aspect was used to show if authors make research with similar focus.

The name of each category has been influenced by the words used in the publications. Some of the publications propose multiple separate countermeasures and are therefore part of multiple categories. Such publications are also counted multiple times in the table below because of this. Some of the publications are part of multiple categories since they have proposed multiple countermeasures. In terms of publication frequency per category, the majority of research lies on *New Analysis Process for the Individual IDS* in total, with a special spike in 2018. *Cybersecurity Information Sharing* is discussed by the least amount of publications. Research on *System Vulnerability Analysis* has been made continuously throughout all years except for 2014. The oldest research lies on *Network Obfuscation*, which is the only category that has a publication from 2014. However, the topic still seems important as there are 2 publications from 2016 and three from 2018. The most amount of research in the latest year lies on *New Analysis Process for the Individual IDS* and stands out with seven publications, where *System Vulnerability Analysis* comes second with only four publications. A comparison that can be drawn from this is that research has generally shifted from obscuring the network to coming up with new technology for IDSs.

All of these approaches for countermeasures do indeed seem to focus on applying changes to the network. There is not a single countermeasure that aims at executing physical countermeasures, e.g. disconnecting the power grid from the Internet to only operate in an offline environment.

Regarding the aspect of a CCA that each publication focuses on to mitigate, almost all publications focus on CCAs in general and not any particular aspect (e.g. mid-stages or starting-stages). When publications focus on a particular aspect, the initial stage of a CCA is most focused on, where CCAs perform reconnaissance on the target or exploiting vulnerabilities to penetrate the network. It was surprising to see that few publications focus on the initial CCA stages because initial stages can be designed to provide something to later stages that is taken advantage of, thereby systematically advancing towards the attack goal. Apart from protecting against CCAs in general or the initial stage of a CCA, only one publication focused on a later stage of a CCA (Jeon, Yun, & Kim, 2016) where the aim is to prevent a CCA from sniffing valuable information within a SCADA system.

5.4 Data Evaluation

This section presents the data evaluation and discusses the advantages and disadvantages about each category followed by a comparison that aim to highlight the biggest differences between the categories. Each section about a category starts with background information about some of the proposed countermeasures for better understanding of good and bad aspects. Advantages and disadvantages that are given for each category are based on specific examples from publications, along with general advantages and disadvantages for that category.

5.4.1 New Analysis Process for the Individual IDS

Babu et al. (2017) present a framework that generates datasets of network activity from simulated power grid environments, which can be integrated into a knowledge-based IDS for improved awareness of abnormal activity. This is achieved by creating a virtual environment representing a local power grid system where ongoing network activity is captured during different treatments of normal operation and network attacks. The time in the virtual power grid environment is sped up to generate datasets quicker. The datasets are generated to build databases that either represent normal or abnormal activity in a power grid environment (i.e. configurations or conditions), which can be integrated into IDSs.

The main advantage of this countermeasure is being able to create information from a simulated

environment that is fully controlled instead of learning from real-world incidents or collecting network activity from a live power grid system slowly over time and providing information to IDSs.

Friedberg, Skopik, Settanni, and Fiedler (2015) present a whitelist-based IDS (i.e. only allowing behavior which is explicitly accepted) that learns about the local system, identifies dependencies between events, and is able to point out the most critical dependencies between local nodes by reading log-lines from the local nodes and systems, without knowledge of any syntax of the log-lines. Upon identification of critical dependencies, they can be prioritized and protected if they happen to be exposed in some way.

Advantages of this specific countermeasure are the following. This IDS is able to detect malicious actions that are typically used in the late stages of CCAs, which are "*direct access to database servers"* and *"copying large amounts of data*". Also, this IDS try to predict what is going to happen among different components in the network, based on these log-lines.

Disadvantages about this countermeasure are the following. The negative aspect about the fact that this IDS is able to detect a CCA's actions not earlier than its late stages, is that the intruder may already be in control to compromise the target without being stopped (see section 2.3.1). The operation of this IDS is not automatic and requires a lot of manual work. This IDS is not able to immediately identify abnormal behavior as it learns what is normal behavior over time, and the IDS is only yet a prototype. This specific IDS becomes useless if an important service in the local system does not report all its security-related events through logs or does not produce logs at all since this countermeasure is dependent on the information provided by log-lines. A disadvantage about whitelist-based IDSs in general is the difficulty of knowing if the IDS really has been configured to allow network activity that is necessary for normal operation, because if not, a false-positive alarm may be raised by the IDS.

There are a number of advantages with this category, such as that presented technical solutions (i.e. technical frameworks) are ready for implementation. Many of the proposed countermeasures argue that the detectability of malicious events has improved. For example, Luh, Schramm, Wagner, Janicke, and Schrittwieser (2018) state that their developed tool is able to accurately identify recurring network events that are malicious in an automatic manner. Another example of an advantage of this category is Lanoe, Hurfin, and Totel (2018) who present a correlation engine that tolerates hundreds of incoming alerts per second coming from other network components (e.g. other IDSs) in the local network. Lastly, Sun, Hong, and Liu (2016) has shown that their proposed countermeasure is capable of identifying some (i.e. not all) CCAs, and are limited to the number of relations that are identified in the local network during a cyber-attack.

General disadvantages for this category are the following. Correlation engines and other proposed solutions come with scalability challenges since many of them try to identify as many correlations between events as possible, which leads to excessive amounts of so-called correlation rules being generated. This type of countermeasure generally requires long periods of time in order to fully operate as intended since many of these IDSs learns about the local system over time. Overall, the focus is on single IDSs which means that each IDS may still not see the big picture of ongoing activity in order to detect attacks being performed across several networks. Because of how IDSs are designed to operate in terms of network security, countermeasures in this category only aim to improve the detection of CCAs and not deploying any security measure that has a direct effect to mitigate CCAs in some way.

5.4.2 System Vulnerability Analysis

The evaluation of category *System Vulnerability Analysis* is described as follows. Ekelhart, Kiesling, Grill, Strauss, and Stummer (2015) present a security analysis tool that analyzes and visualizes the resilience of the local system through simulated attacks using a penetration testing catalog that contains various sorts of attacks, combined with the use of legitimate and allowed actions (e.g. legitimately requesting information from a database after bypassing a security mechanism). In addition to the consideration of combining malicious and legitimate actions, different amounts of resources that different attackers may possess is taken into account as well to show what different impacts the same kind of attack with different resources may have on the local system. The tool also shows the impacts the local system may experience during system alterations. Finally, the tool identifies the most important nodes to protect (i.e. the tool assigns a security value for each node in the network) and also identifies different paths attackers possibly can take through the network with a certain amount of resources. Based on this design, the tool assesses the local system's resilience.

Advantages with this specific countermeasure are the following. Vulnerabilities identified from generated attack-graphs are visualized and presented directly the user of the security analysis tool, which the user can learn from and take appropriate actions for strengthening the protection. Taking attacks supported with different amounts of resources into account help to understand the impacts that a CCA may inflict since CCAs may possess a great amount of resources compared to stand-alone attacks. Another advantage of this countermeasure is that the tool takes internal attackers into account, which may make an administrator to ensure the principle of least privilege for all users.

Disadvantages of this specific countermeasure are the following. Ekelhart, Kiesling, Grill, Strauss, and Stummer (2015) explicitly state that zero-day vulnerabilities are not taken into consideration when the tool analyses the local system, which is problematic since CCAs are known to exploit such vulnerabilities. The tool does not analyze critical configuration files (i.e. misconfigurations etc.) on the local system. During penetration tests for generating attack-graphs for the local system, the tool requires considerable time before the process of generating attack-graph is complete because the tool tries to select the most effective attacks based on the local system (i.e. not performing all known attacks one after another).

General advantages of this category are the following. A typical advantage is that all nodes and connections in the local network are considered for identifying vulnerabilities. Some publications consider inside attackers who all have some level of access to operational systems. In case a network node is deployed into the local system and is overlooked in terms of security, an all-inclusive vulnerability analysis for the whole local network might identify such unnoticed vulnerabilities, and may thus be fixed. Bodström and Hämäläinen (2018) contribute to mitigating CCAs by identifying the most important factor that is needed in order for a CCA to be successful, which is communication. Gonzalez-Granadillo, Rubio-Hernan, and Garcia-Alfaro (2018) present a tool that identifies relations between different network events to compute potential collateral damage and coverage, based on suspicious events. The tool is able to detect some stages of a CCA, which is taken advantage of to deploy different countermeasures at each identified stage. The tool is also able to "*evaluate multiple and complex attacks and select the best mitigation strategy"*. Kumar, Ruijters, and Stoelinga (2015) present a solution for threat analysis that provides information on the most vulnerable parts of the system and resources that are necessary for a successful attacking towards the local system. Temporal dependencies in the local network are taken into consideration when identifying vulnerabilities in the local system.

General disadvantages for this category are the following. Vulnerabilities are identified and noted about to administrators, but no security measure is deployed that directly has an effect towards the identified problems. This means that the technologies in this category are primarily designed to produce network security-related information for preemptive use (i.e. used later on to mitigate security problems). A certain disadvantage of this category is that while multiple authors present attack-graphs as a prominent mitigation technique against CCAs, Nicol (2018) criticize its effectiveness due to an explosion of complexity in mitigating potential threats. Nicol (2018) suggests that heuristic based protection mechanisms is a better fit for large infrastructure networks (e.g. knowledge-based IDSs or focusing on patching vulnerabilities).

5.4.3 Cooperative Intrusion Detection

Kendrick, Criado, Hussain, and Randles (2018) present a decentralized agent-based system, where agents analyze one local software service each (i.e. ranging between network protocols to software applications). When suspicious activity is detected at the local network (e.g. port scan), the decentralized agents start to collect different pieces of information about the potential attacker before security measures are deployed for providing more context to the situation. The different pieces of information are then gathered into a single source of information for improving the detection of malicious attacks and also for decreasing the number of false alarms. During the process of collecting contextual information, each agent is aimed towards one specific piece of information. The agents of the system are able to operate across multiple networks, which allows for potential detection of attacks that enter networks with weak protection only to access another network that is interconnected with the first. The system aims to detect zero-day exploits by spreading agents across multiple networks where each agent focuses on a single service and communicates with other agents to see if there are any similarities.

The advantages of this specific countermeasure are the following. The process of collecting and analyzing data is automatic after a certain software service has been chosen for the agent. The detection rate of malicious attacks is increased by 20 percent when the detection is based on information gathered by multiple agents compared to a single agent making the decision on its own. When multiple agents are used together, the amount of processing for a security event is decreased by over 50 percent. An agent is able to assess the workload of its given task and is able also to request other agents for load balancing if needed. Agents can in some cases detect malicious insiders because agents take local user accounts into consideration, where alarms are more likely to be raised when users with low privileges are making suspicious actions and administrators do not have to worry as much for causing false alarms during maintenance for example.

A benefits of this countermeasures is that decentralization of agents across a greater number of networks has a positive effect on the analysis of identifying zero-day exploits, where a greater number of identified footprints left by such attacks provide more information.

Disadvantages of this countermeasure are that the countermeasure is heavily dependent on communication between agents, where network congestion or a denial of service incident would have a considerably negative impact on the operation of this solution. More communication also means a bigger burden for the network. Lastly, the system only raises alarms about potential attacks and do not deploy security measures on its own.

Regarding all countermeasures in this category, the general advantage is that comprehensive information often is provided to the user of the proposed solutions, where appropriate actions can

be taken quickly to counter suspected attacks. Other general advantages are accurate identification of abnormal network topology changes, reduced amounts of false alarms and computational costs, and effective risk analyses where tailored security measures can be developed.

A general disadvantage with these solutions is that agents are spread out and connected to a central coordinator which analyzes and makes decisions based on received information from agents. The disadvantage here is that a potential point of failure would stop the operation of detecting malicious events in the local network. Backup coordinators can be integrated, but solutions such as these may get bulky because of that.

5.4.4 Network Obfuscation

Chowdhary, Alshamrani, Huang, and Liang (2018) present a framework which cooperate with knowledge-based IDSs and deploys port hopping changes to the network configuration, where local service ports are frequently changed to make it harder for an intruder to identify and explore running services. The specific countermeasure as proposed by Chowdhary, Alshamrani, Huang, and Liang (2018) only deploys network changes when the local IDS raises an alarm or when manually selected by the administrator. Once deployed, service ports are changed between intervals of seconds.

Advantages of this countermeasure is that this technology benefits all networks which host 50 different services or more. Also, the technology is shown to be more prominent when it is implemented into networks that host around 200 services. A probable match in this aspect could be cloud networks that host many different services. In terms of CCAs, local service ports can be effectively hidden when the attacker performs internal reconnaissance to identify their target by making the attacker lose the identified service port due to port hopping.

A disadvantage of the proposed countermeasure by Chowdhary, Alshamrani, Huang, and Liang (2018) is that network packets such as ICMP requests are untouched by this countermeasure, which could be used by the attacker to explore the local network. Quality of Service (QoS) is not taken into consideration by the framework performing the network changes. Excluding QoS could potentially result in network changes being delayed due to network congestion or service latency. Regarding the cooperating IDS that should let the framework know when network changes are necessary, the framework is limited to knowledge-based IDSs (i.e. no behavior-based IDSs). Other disadvantages of these frequent network changes are, if implemented, that it takes up more bandwidth on local links, services must be able to adapt to its frequently changing service port. This countermeasure is aimed to protect internal systems, i.e. providing a level of protection after initial security measures fail to prevent intruders. Thus, this countermeasure does not have any preemptive qualities and only operates reactively.

de Sá, da Costa Carmo, and Machado (2018) present a solution that aim to prevent attackers who performs passive reconnaissance internally from modelling the local network by sending fake control function messages between an internal controller (i.e. digital control systems that control the dynamics of physical plants) and a plant's physical actuators. The aim is to disrupt a potential attacker's layout of the local system to make the attacker less confident in launching an attack that is meant to be precise and accurate to succeed.

Several advantages can be taken from this countermeasure. This technique is shown to mitigate a passive reconnaissance attack since it becomes harder to know how to launch an attack that simultaneously disrupts multiple controllers, which often is needed in order to compromise a physical plant. In addition, if the attacker would try to identify which messages that are fake, the rapid pace of switching between real and fake messages within seconds makes it considerably

difficult for the attacker.

Jafarian, Al-Shaer, and Duan (2014) present a frequently randomizing IP-addressing countermeasure towards hosts in a local network to invalidate attackers' assumptions about the network. This countermeasure which is found effective in countering CCAs. Also, this countermeasure is compatible with clients, routers, switches, DNS servers, DHCP servers, firewalls and IDSs.

A general advantage of this countermeasure is that these techniques, which are also referred to as Moving Target Defenses (MTD), make it harder for attackers who try to create a model of the target system. In such cases, attackers may possibly spend more time and resources which increases the chance of detecting such attacks.

A general disadvantages are increased overhead for the network (e.g. DNS overhead) and that the network must carry more traffic than it already does. This can also be referred to as a problem of scalability.

5.4.5 Investigate CCA Characteristics

Wang, Kwon, Ma, Zhang, and Xu (2018) present a system that searches for information relating to an identified attacker including attackers' origin as well as deriving network path for investigating in background information of CCAs. This system traces log-files of system calls in combination with library tracing. This solution is lightweight and do not cause any major network overhead. The system can also accurately identify the origin of malicious libraries when an attack is detected at the local network. Pitropakis et al. (2018) present a framework that tries to learn about the malicious actors behind CCAs, which make use of various types of information and practices to produce trustworthy information about CCAs. Network forensics one of these practices which is heavily used to provide evidence relating to malicious actors of CCAs. Finally, produced information should be used to improve the detection of CCAs. Bodström and Hämäläinen (2018) present theories which relate to the characteristics of CCAs, that should be taken into consideration that should influence the design of security for a network. These theories that should be taken into consideration are that "extreme improbable events" may occur, that a person should be aware of his or her limitation in what he or she currently understands about CCAs, and lastly that CCAs can happen during a very short period of time in matter of hours or simply as long as it takes for the CCA to succeed.

The proposed countermeasures in this category generally provides insight to how CCAs can be launched, background information, motivation, strategies and unveils different ways of combining attacks. These solutions are often able to collected, analyzed and synthesized a large selection of information of different types efficiently. Proposed countermeasures that are technical and ready for implementation into a system all has low overhead in terms of time and performance (i.e. light-weight solutions).

Although these solutions provide information based on large sets of data etc., a disadvantage is that the outcome often is long-term suggestions that has not a immediate effect for improving the security for a local network. This argument is justified by Mehresh and Upadhyaya (2015) who state "*although our framework does not directly improve the quality of the existing IDSs it allows them to operate with increased effectiveness*".

5.4.6 Game Theoretical Guidance of Defense

Fielder, Li, & Hankin (2016) present a game of defenders and attackers, which is run by the developed algorithm in a virtual ICS environment, where the defender has a set of security measures to choose from, and learns over time which measures that are the most effective and can thereby develop a plan for real-life attack situations. The outcome of this game tends to be that defense in-depth (i.e. security is applied evenly in a network) is more cost-effective than only protecting critical nodes in a network. This technical game also provides suggestions for what kind of security solutions to adopt. Moothedath et al. (2018) present a different kind of approach where a security mechanism operates after a CCA has been detected at the local network, where the design of the security mechanism is inspired by a game-driven approach with certain algorithms. A special advantage of this solution is that experiments shows that this countermeasure can detect CCAs successfully.

General advantages are identifying cost-effective defense techniques, and at which times (e.g. based on the amount of resources available and their effectiveness). Successfully detecting CCAs should be explicitly expressed here as well.

General disadvantages are that proposed solutions often provide some advice to the user, where the disadvantage is that these suggestions can be misinterpreted. Therefore, users must be absolutely certain that they interpret produced advices accurately in order not to make mistakes that could end up reducing the level of security. Some countermeasures are also limited in its flexibility of being compatible to operate in different kinds of systems, where it typically is tailored towards one specific type of system.

5.4.7 Baiting the Attacker

The two publications that are associated with this category are Bodström and Hämäläinen (2018) and Gjermundrød and Dionysiou (2015). Bodström and Hämäläinen (2018) argue that setting up a baiting the attacker via so-called honeypot can shift an attacker's focus from the initial target to the bait, which makes it more probable that the attacker is detected by the alarm that the honeypot can raise. Gjermundrød and Dionysiou (2015) discuss the practical usefulness of honeypots and also present a technical framework that can use several honeypot agents that send their data to the framework where attack signatures can be created. The design of this honeypot framework is that it baits the attacker by exposing itself as running several services which an attacker can probe and thereby exposing himself or herself.

A certain advantage of this category is that it is able to collect information that there is otherwise a lack of (i.e. new types of attack-signatures).

A disadvantage of these solutions is that they are only made to complement existing defense mechanisms and do not provide an adequate level of protection on their own.

5.4.8 Cybersecurity Information Sharing

de Fuentes, González-Manzano, Tapiador, and Peris-Lopez (2017) present a countermeasure that aim to encourage enterprises to share their own security related information with others without the risk of exposing sensitive information about their own network, where shared experience can improve security for other systems. The solution mainly consists of a central message broker and a set of participants that all can share encrypted information with each other. When a message is sent, the message broker is not able to view the content of incident reports, but is still able to forward the

message towards its desired destination. This leaves a publisher's sensitive information protected while being stored on the message broker and while being shared over the Internet.

An advantage of this countermeasure is that subscribers of a message broker can select a certain type of incident reports to receive, instead of searching manually by one self which helps to find relevant information to an organization's specific situation more easily. During exchanges of incident reports, publishers are identified through a Hash-based Message Authentication Code (HMAC), which lets subscribers know that the reports come from trusted publishers.

The main disadvantage here is that sensitive information may be shared over the Internet, where security practices of participants play a major role in how secure this countermeasure is. Before a message is sent to the message broker, it is only assumed that participant have established a secure TLS connection towards the receiving host. Since it is only assumed that subscribers are making secure TLS connection to the message broker, sensitive information could get stolen, thereby exposing possible vulnerabilities of large enterprise networks.

5.4.9 Comparison

This section presents identified differences and similarities between the categories. In the table below (see Table 9), each category is assessed in terms of technicality. Also, the different publications in a category has been analyzed in terms of research impact based on popularity in citation counts from any other publications. Citation counts are gathered from Google Scholar by searching for each publication and noting its number of citations (i.e. other publications that has used that publication as a reference). In the table below, a numbered list is used to show which publication in the References column it is related to. The technicality of each category is assessed by how the authors in that category describe their countermeasure, in terms of how technical it is. There are four levels of practicality which are shown in the bullet list below.

- Very Technical
- Mostly Technical
- Mostly Theoretical
- Very Theoretical

The level called *Very Technical* is generally where almost all countermeasures are ready for implementation into a system where they do not require further development in order to function as intended. Possible examples of such countermeasures could be software applications and software engines.

The level called *Mostly Technical* is generally where most countermeasures are ready for implementation into a system but are limited in some way and need further development in order to function as intended or are driven by something that could work in theory.

The level called *Mostly Theoretical* is generally where few technical countermeasures are proposed and where countermeasures are mostly driven by theoretical concepts or ideas, which have been tested in small experiments at most.

The level called *Very Theoretical* is generally where almost all countermeasures are driven by strongly theory-related ideas and concepts. Possible examples of such countermeasures could be

considering certain scientific theories to create new ways of thinking in how to tackle security challenges or theoretical ideas of technical solutions that has not been tested yet.

Table 9. Comparison between created categories in terms of research impact and practicality

Category	Citation count	Technicality	References
New Analysis Process for the Individual IDS	1. 0 2. 1 3. 110 4. 0 5. 5 6. 0 7. 0 8. 2 9. 3 10. 5 11. 2 12. 3 13. 0	Very Technical	1. Angelini et al., 2018 2. Babu et al., 2017 3. Friedberg, Skopik, Settanni, and Fiedler, 2015 4. Haas and Fischer, 2019 5. Kiesling, Ekelhart, Grill, Strauss, and Stummer, 2016 6. Kim, Choi, and Choi, 2018 7. Kumar, Rensink, and Stoelinga, 2018 8. Lanoe, Hurfin, and Totel, 2018 9. Luh, Schramm, Wagner, Janicke, and Schrittwieser, 2018 10. Nath and Mehtre, 2015 11. Rubio, Roman, Alcaraz, and Zhang, 2018 12. Sun, Hong, and Liu, 2016 13. Zhao and Qiu, 2018
System Vulnerability Analysis	1. 2 2. 13 3. 17 4. 0 5. 2 6. 29 7. 2 8. 0 9. 9 10. 6 11. 2	Mostly Technical	1. Bodström and Hämäläinen, 2018 2. Ekelhart, Kiesling, Grill, Strauss, and Stummer, 2015 3. Ghosh et al., 2015 4. Gonzalez-Granadillo, Rubio-Hernan, and Garcia-Alfaro, 2018 5. Han, Cheng, Zhang, and Feng, 2015 6. Kumar, Ruijters, and Stoelinga, 2015 7. Mediouni, Nouri, Bozga, Legay, and Bensalem, 2018 8. Nicol, 2018 9. Paul and Ni, 2017 10. Potteiger, Martins, and Koutsoukos, 2016 11. Rodríguez, Chang, Li, and Trivedi, 2016
Cooperative Intrusion Detection	1. 2 2. 2 3. 18 4. 8 5. 19 6. 0 7. 9	Very Technical	1. Kendrick, Criado, Hussain, and Randles, 2018 2. Nagar, Nanda, He, and Tan, 2017 3. Paridari et al., 2016 4. Rubio, Alcaraz, and Lopez, 2017 5. Settanni et al., 2017 6. Singh, Ozen, and Govindarasu, 2018 7. Zulkefli, Singh, and Malim, 2015
Network Obfuscation	1. 5 2. 4 3. 67 4. 3 5. 3 6. 13	Very Technical	1. Chowdhary, Alshamrani, Huang, and Liang, 2018 2. de Sá, da Costa Carmo, and Machado, 2018 3. Jafarian, Al-Shaer, and Duan, 2014 4. Jeon, Yun, and Kim, 2016 5. Smith, Zincir-Heywood, Heywood, and Jacobs, 2016 6. Zimba, Wang, and Chen, 2018

Investigate CCA Characteristics	1. 2 2. 8 3. 6 4. 9 5. 1 6. 1	Mostly Theoretical	1. Bodström and Hämäläinen, 2018 2. Luh, Schrittwieser, and Marschalek, 2016 3. Mehresh and Upadhyaya, 2015 4. Paudel, Smith, and Zseby, 2017 5. Pitropakis et al., 2018 6. Wang, Kwon, Ma, Zhang, and Xu, 2018
Game Theoretical Guidance of Defense	1. 4 2. 1 3. 3 4. 4	Mostly Technical	1. Fielder, Li, and Hankin, 2016 2. He and de Meer, 2017 3. Moothedath et al., 2018 4. Touhiduzzaman, Hahn, and Srivastava, 2018
Baiting the Attacker	1. 2 2. 3	Mostly Theoretical	1. Bodström and Hämäläinen, 2018 2. Gjermundrød and Dionysiou, 2015
Cybersecurity Information Sharing	1. 18	Very Technical	1. de Fuentes, González-Manzano, Tapiador, and Peris-Lopez, 2017

New Analysis Process for the Individual IDS is labeled as Very Technical since proposed countermeasures mostly involve solutions such as frameworks, IDSs and correlation engines.

System Vulnerability Analysis is labeled as Mostly Technical. Proposed countermeasures that are not purely technical involve identifying typical characteristics of CCAs and also identifying the most vulnerable parts of a system without following up with some type of security implementation. Otherwise, this category contains technical countermeasures.

Cooperative Intrusion Detection is labeled as Very Technical as it mainly focuses on deploying multiple devices as agents across a network, which often communicate to a central host that computes received data.

Network Obfuscation is labeled as Very Technical since they all focus on different types of technical network configurations.

Investigate CCA Characteristics is labeled as Mostly Theoretical because the aim is often to collect data about attack purposes, what characteristics CCAs have and other background information that is used for developing long-term countermeasures.

Game Theoretical Guidance of Defense is labeled as Mostly Technical because the proposed solutions in this category are very technical which often uses different algorithms to analyze different collected pieces of data, but are sometimes used to provide security advices to the user. When such advices are handed to the user, it is up to the user to turn the suggested solution into reality.

Baiting the Attacker is labeled as Mostly Theoretical because the authors mostly discus the possibilities of using honeypots for example. Although one technical solution is proposed, honeypots as a means for baiting the attacker is not a widely adopted security mechanisms that needs to be

improved in order to provide a good level of protection. This means that *Baiting the attacker* still is on a theoretical level.

Cybersecurity Information Sharing is labeled as Very Technical since the countermeasure simply is a framework that is ready to be implemented.

In terms of comparing the differences and similarities between the categories, *New Analysis Process for the Individual IDS*, *System Vulnerability Analysis*, and *Cybersecurity Information Sharing* share the same characteristic of requiring a considerable amount of time before most of the related countermeasures each their expected results. The same goes for their mitigation effects towards attacks in general because the proposed countermeasures themselves do not directly contribute to any mitigation effect. Instead, both categories mainly focus on long-term solutions that are designed to provide positive and consistent results.

New Analysis Process for the Individual IDS also have similar characteristics of proposed countermeasures in *Game Theoretical Guidance of Defense*. This applies to the design of integrating various sorts of information (e.g. databases, publicly available security information, or datasets of IDSs) into algorithms that are used to produce credible and useful information.

A clear difference between *Network Obfuscation* and *Investigate CCA Characteristics* is the technicality where *Network Obfuscation* solely focuses on network configuration and where *Investigate CCA Characteristics* has a more qualitative approach where theories are proposed by some publications.

Cooperative Intrusion Detection and *System Vulnerability Analysis* share the same idea of focusing on the network as a whole where all hosts and network flows are analyzed.

In terms of the focus towards different stages of a CCA, *New Analysis Process for the Individual IDS* is capable of detecting malicious actions used by CCAs during its final stages, whereas *Network Obfuscation* effectively mitigates initial phases of a CCA where reconnaissance is performed by the attackers.

Baiting the Attacker and *Cybersecurity Information Sharing* are both used to only complement existing security mechanisms.

5.5 Suggestions

This section provides an educated guess to the research question regarding most suitable countermeasures. Specific suggestions are given at the later half of this section. First, a general discussion is given about some of the categories. *System Vulnerability Analysis* seem to be very important to begin with because an in-depth analysis of identifying possible vulnerabilities in a system is necessary to prevent future exploitations of them. Without formal risk assessments and vulnerability analyses, vulnerabilities may exist for longer periods, or even be known by in-house workers who simply do not report about it, allowing for insider attacks of disgruntled former employees. Even though countermeasures in this category proposes specific software to use, a security assessment is still the main idea. *Cooperative Intrusion Detection* may also be important because a CCA can be performed across several networks where an IDS monitors it locally and might not detect it because of that. Also, a single IDS may be weaker than both multiple IDSs and multiple agents cooperating in different ways. Such cooperative intrusion detection would presumably benefit from adopting new intrusion detection techniques, such as one of the proposed countermeasures from *New Analysis Process for the Individual IDS* as previously mentioned since state-of-the-art IDSs

in fact have limitations.

Other approaches such as *Network Obfuscation* are not considered an ideal solution to mitigate CCAs because they serve as the last countermeasures one would choose when there are no other choices left. This is motivated by that there may still be a chance for the attacker to identify valuable targets, but only a smaller one due to obscuring the network. *Baiting the Attacker* would only detect the attacker if he or she targets the particular information that a decoy is presenting. The attacker could just bypass it if the attacker simply happens to target other components than the bait component in the network. *Game Theoretical Guidance of Defense* and *Cybersecurity Information Sharing* aim at developing some form of plans for how to implement security measures in the future, which probably is not a short-term effective solution to the urgent problem of CCAs. *Investigate CCA characteristics* seem to be an intuitive solution because if it is known which type of traffic that is related to a CCA, they can be effectively prepared for. However, new analysis processes for IDSs are designed to detect any type of malicious network traffic and white-listing network activity could therefore might be more effective than adapting to specific network traffic such as from the CCA.

Categories that contain optimal countermeasures in the defense against CCAs are described as follows. Based on collected data, a security assessment should be thoroughly performed against the local system to preemptively identify as many vulnerabilities as possible that could be exploited by a CCA. Next, some cooperative intrusion detection solution should be implemented where multiple hosts monitor the whole organizational entity at different locations in the system so that they can see the whole picture of the system and its ongoing activities, and not just individual bits and pieces. Finally, the hosts that cooperate regarding intrusion detection should adopt some of the newly proposed intrusion detection technologies since such state-of-the-art technology is found inadequate. All these three approaches that are suggested to use in combination have one thing in common, namely that they are all heavily researched as compared to all the other approaches, as can be seen in the previous section (see Table 8).

Specific suggestions for mitigating CCAs as described as follows. Multiple specific countermeasures are suggested since not a single one is able to completely prevent CCAs. Therefore, multiple countermeasures are suggested where as many as possible is suggested to be combined. The problem has been assessed to be in need of short-term solutions that are able to mitigate the threat of CCAs to at least some extent. The countermeasure as presented by Moothedath et al. (2018) can be used to successfully detect CCAs, which is much needed since CCAs tend to be stealthy. The countermeasure of Gonzalez-Granadillo, Rubio-Hernan, & Garcia-Alfaro (2018) can be used to detect attacks that make use collateral damage. This countermeasure is important to consider since CCAs are commonly known to perform their attacks in multiple stages where different attack-mechanisms are combined. The countermeasure of Kumar, Ruijters, and Stoelinga, (2015) can be used to consider temporal attacks, since exploiting temporal dependencies is a typical characteristic of CCAs (see section 2.3). The countermeasure of Friedberg, Skopik, Settanni, and Fiedler (2015) make use of a whitelist IDS that is able to detect some of the activities used during the late stages of CCA. If initial phases of a CCA is the only stage that needs protection for, Chowdhary, Alshamrani, Huang, and Liang (2018) has presented a Moving Target Defense mechanism that can be used to effectively mitigate reconnaissance attacks.

6 Conclusions

Forty-eight (48) publications identified by a systematic literature search have been analyzed to identify countermeasures against CCAs. The answer to the research question regarding available countermeasures is shown in Appendix B. The data analysis resulted in dividing all countermeasures into eight categories based on whether the focus was on the attacker or target system, whether the countermeasure was aimed to be applied towards some certain network component, and general similarities between the proposed countermeasures. What can be seen from analyzing the timeline of publications throughout the years is that the research field has shifted from focusing on obscuring the attacker's view of the local network (i.e. preventing identification of legitimate or confidential information) to developing new technologies for an individual IDS. A suggestion on the most suitable countermeasure to mitigate CCAs toward power grids is to focus on a combination of three approaches, namely (i) performing vulnerability analyses and risk assessments to preemptively mitigate exploitation of internal components and removal of attack paths that can be used by an attacker to effectively propagate through the local network towards the main goal, (ii) using multiple instances of monitoring devices such as IDSs at different locations in a local or across several networks in order to analyze and understand the bigger picture of the whole network regarding its ongoing activity, and (iii) adopting a new analysis process for the individual IDS since existing IDSs has been identified as inadequate towards CCAs.

Specific countermeasures that are suggested to use are the following ones. The effect that each countermeasure has, as described in this thesis, is only based on the information from collected literature from this study. Game theoretical guidance of defense mechanism is able to detect CCAs, a tool that identifies potential collateral damage from multiple network events, a threat analysis tool that tries to identify temporal attacks, and a whitelist-IDS that is able to detect some of the attacks used in the late stages of a CCA. All of these specific suggestions are explained in more detail with references in the previous section (see section 5.5).

The validity of the study is partly motivated through its reproducibility, where the processes for how data is collected, extracted, and analyzed is clearly documented. Other aspects of this study that strengthens the validity of this study are that it covers four well-known literature databases, that the study is systematic, and that search queries were tested through a pre-study.

Differences between the results of this study and a study by Singh, Sharma, Moon, Moon, and Park (2016) is that Singh et al. (2016) only categorize countermeasures against CCAs based on the IDS type that is aimed to be improved or redesigned. The categories that Singh el al. (2016) define are NIDS, HIDS, purely semantic IDS, and multi-source IDS. This study makes a quite different categorization where different IDS redesigns belong to a single category because all types of countermeasures were considered for in this study (i.e. not just those considering IDSs).

An ethical impact as caused by this study revolves mainly around that IDSs are presented to have limitations towards multi-stage, low and slow attacks. A technical guide on how to exploit these limitations is not provided, but an attacker could use this information to his or her advantage by knowing where to start to search for technical information. On societal impacts that this study may have, it is considered something positive that this study spreads awareness of this problem. There are many important real world problems that research is made on, but the relevance of this particular topic is justified by the effects that a CCA may have on a critical infrastructure, such as the power grid, where many people can lose the electricity of their household which they depend on in their everyday lives. A certain finding from studying the selected literature is that proposed

countermeasures do not typically focus on a particular stage of a CCA. Rather, CCAs are focused on as a whole. An additional finding is that one author disagree on attack-graph generation is better than knowledge-based defense mechanisms.

7 Discussion

Although this study followed the guidelines of Kitchenham and Charters (2007), they were not followed in detail. These guidelines did however provide a solid foundation for the report structure, validity, reproducibility, and the overall process for how the systematic literature study was carried out. The initial phases of the study where the topic was introduced and where background information was given did require a lot of research, including information about IDSs since they seem to be mostly common in larger enterprise networks and critical infrastructures. Defining what a CCA is and describing its characteristics did also require deeper analysis, because CCAs are a rather new topic in combination with the rapid development of the field. Outlining the methodology and executing it was a straight-forward but time-consuming process where the guidelines of Kitchenham and Charters (2007) was followed, but in a simplified way.

The concept of CCAs is something very broad because a CCA can essentially exist in an unlimited number of variations, considering specific cyber-attacks mechanisms, stages, combinations of attacks, and number of targets. Although the concept of CCAs is abstract, the main idea is to focus on attacks that may cause great damage where the probability of the attack succeeding is reasonably high due to how the different components of a CCA might coordinate.

Areas of the study that could have been done differently involve the process of selecting literature, where different search queries were used for different databases. At first, the queries were only designed to be adjusted based on database limitations. Some databases allowed longer queries than others, which caused the search terms to be prioritized. Later, different content of literature in each database was considered, and the goal became to try to retrieve them all by selectively choosing terms for each database that hopefully would result in matching all relevant publications, based on search results during pre-study searches. An improvement would be to use the same terms for all databases, where multiple searches for each database are performed in order for all defined search terms to be used. Another area for improvement would be to motivate why some countermeasures were put into a certain category. That way, the reader would have more insight to the analysis process and would understand more about how the results came to be.

8 Future Work

The one single future work that is suggested to do is to investigate if there are some specific countermeasures against CCAs that must be tailored towards critical infrastructure beyond power grids such as the critical manufacturing of metal, machinery, electrical equipment, or transportation. The domain of critical manufacturing is chosen because it was identified as the most targeted critical infrastructure in terms of cyber incidents during 2015 (NCICC, 2015). IT systems used there may have vulnerabilities that are different from power grids as discussed in this study.

References

Akinrolabu, O., Agrafiotis, I., & Erola, A. (2018). The Challenge of Detecting Sophisticated Attacks: Insights from SOC Analysts. Proceedings of the 13th International Conference on Availability, Reliability and Security, 55:1–55:9. https://doi.org/10.1145/3230833.3233280

Aniello, L., Di Luna, G. A., Lodi, G., & Baldoni, R. (2011). A Collaborative Event Processing System for Protection of Critical Infrastructures from Cyber Attacks. In F. Flammini, S. Bologna, & V. Vittorini (Eds.), *Computer Safety, Reliability, and Security* (Vol. 6894, pp. 310–323). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-24270-0_23

ANS and Electricity Information Sharing and Analysis Center (E-ISAC) (2016). Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*.

Ashok, A., Hahn, A., & Govindarasu, M. (2014). Cyber-physical security of Wide-Area Monitoring, Protection and Control in a smart grid environment. *Journal of Advanced Research*, *5*(4), 481–489. https://doi.org/10.1016/j.jare.2013.12.005

Berndtsson, M., Hansson, J., Olsson, B., & Lundell, B. (Eds.). (2008). Thesis Projects: A Guide for Students in Computer Science and Information Systems. In *Thesis Projects: A Guide for Students in Computer Science and Information Systems* (pp. 122–144). https://doi.org/10.1007/978-1-84800-009-4_14

Braynov, S., & Jadiwala, M. (2003). Representation and analysis of coordinated attacks. *Proceedings of the 2003 ACM Workshop on Formal Methods in Security Engineering - FMSE '03*, 43–51. https://doi.org/10.1145/1035429.1035434

Industrial Control Systems Cyber Emergency Readiness Team (ICS-CERT). (2016). *ICS-CERT Year in Review 2016*. 28. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf

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, Pub. L. No. 32016L1148, OJ L 194 (2016). Retrieved from http://data.europa.eu/eli/dir/2016/1148/oj/eng

Elshoush, H. T., & Osman, I. M. (2011). Alert correlation in collaborative intelligent intrusion detection systems—A survey. *Applied Soft Computing*, *11*(7), 4349–4365. https://doi.org/10.1016/j.asoc.2010.12.004

Ericsson, G. N. (2010). Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure. Power Delivery, IEEE Transactions On, 25, 1501–1507. https://doi.org/10.1109/TPWRD.2010.2046654

European Commission. (2016). The Directive on security of network and information systems (NIS Directive) [Text]. Retrieved April 3, 2019 from https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

Fang, X., Misra, S., Xue, G., & Yang, D. (2012). Smart Grid — The New and Improved Power Grid: A Survey. *IEEE Communications Surveys Tutorials*, *14*(4), 944–980. https://doi.org/10.1109/SURV.2011.101911.00087

Fortinet. (2013). *Threats on the Horizon: The Rise of the Advanced Persistent Threat*. Retrieved from https://s3-us-west-2.amazonaws.com/itworldcanada/archive/Documents/whitepaper/ITW274A_Persistent_Threats.pdf

Kidwai, A. (2012). *The SLL&CS Research Handbook* (1. ed.). New Delhi: Jawaharlal Nehru University.

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering*.

Mehresh, R., & Upadhyaya, S. (2015). Surviving advanced persistent threats in a distributed environment – Architecture and analysis. *Information Systems Frontiers*, *17*(5), 987–995. https://doi.org/10.1007/s10796-015-9569-y

Moya, C., & Wang, J. (2018). Developing correlation indices to identify coordinated cyber-attacks on power grids. *IET Cyber-Physical Systems: Theory Applications*, *3*(4), 178–186. https://doi.org/10.1049/iet-cps.2018.5002

Nath, H. V., & Mehtre, B. M. (2015). Analysis of a multistage attack embedded in a video file. Information Systems Frontiers, 17(5), 1029–1037. https://doi.org/10.1007/s10796-015-9570-5

National Cybersecurity and Communications Integration Center (NCICC). (2015). NCCIC/ICS-CERT Year in Review (2015). 24. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf

Nazir, S., Patel, S., & Patel, D. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. Computers & Security, 70, 436–454. https://doi.org/10.1016/j.cose.2017.06.010

Nicol, D. M. (2018). Cyber Risk of Coordinated Attacks in Critical Infrastructures. Proceedings of the 2018 Winter Simulation Conference, 2759–2768. Retrieved from http://dl.acm.org/citation.cfm?id=3320516.3320845

Rob, R., Tural, T., McLorn, G. W., Sheikh, A., & Hassan, A. (2014). Addressing cyber security for the oil, gas and energy sector. *2014 North American Power Symposium (NAPS)*, 1–8. https://doi.org/10.1109/NAPS.2014.6965377

Singh, S., Sharma, P. K., Moon, S. Y., Moon, D., & Park, J. H. (2016). A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions. The Journal of Supercomputing. https://doi.org/10.1007/s11227-016-1850-4

Sisneros, M. J., Rivera, J., Jeantete, B. A., & Le, T. D. (2012). *Vermont Presentation.* Retrieved from https://www.osti.gov/biblio/1118150-vermont-presentation

Sun, C.-C., Hahn, A., & Liu, C.-C. (2018). Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, *99*, 45–56. https://doi.org/10.1016/j.ijepes.2017.12.020

Sun, C., Hong, J., & Liu, C. (2016). A coordinated cyber attack detection system (CCADS) for multiple substations. *2016 Power Systems Computation Conference (PSCC)*, 1–7. https://doi.org/10.1109/PSCC.2016.7540902

Sridhar, S. (2015). *Cyber risk modeling and attack-resilient control for power grid* (Doctor of Philosophy, Iowa State University, Digital Repository). https://doi.org/10.31274/etd-180810-3993

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in Computing (5th Edition)* (5th ed.). Upper Saddle River, NJ, USA: Prentice Hall Press.

Pitropakis, N., Panaousis, E., Giannakoulias, A., Kalpakis, G., Rodriguez, R. D., & Sarigiannidis, P. (2018). An Enhanced Cyber Attack Attribution Framework. In S. Furnell, H. Mouratidis, & G. Pernul (Eds.), Trust, Privacy and Security in Digital Business (pp. 213–228). Springer International Publishing.

Vasilomanolakis, E., Karuppayah, S., Mühlhäuser, M., & Fischer, M. (2015). Taxonomy and Survey of Collaborative Intrusion Detection. *ACM Computing Surveys*, *47*(4), 1–33. https://doi.org/10.1145/2716260

Wu, D., Ma, F., Javadi, M., & Jiang, J. N. (2016). Fast screening severe cyber attacks via transient energy-based impact analysis. *CSEE Journal of Power and Energy Systems*, *2*(3), 28–34. https://doi.org/10.17775/CSEEJPES.2016.00032

Xiang, Y., Wang, L., & Liu, N. (2017). Coordinated attacks on electric power systems in a cyber-physical environment. *Electric Power Systems Research*, *149*, 156–168. https://doi.org/10.1016/j.epsr.2017.04.023

Zhou, C. V., Leckie, C., & Karunasekera, S. (2010). A survey of coordinated attacks and collaborative intrusion detection. *Computers & Security*, *29*(1), 124–140. https://doi.org/10.1016/j.cose.2009.06.008

Appendix A – Selected Literature for the Study

Angelini, M., Bonomi, S., Borzi, E., Pozzo, A. D., Lenti, S., & Santucci, G. (2018). An Attack Graph-based On-line Multi-step Attack Detector. *Proceedings of the 19th International Conference on Distributed Computing and Networking*, 40:1–40:10. https://doi.org/10.1145/3154273.3154311

Babu, V., Kumar, R., Nguyen, H. H., Nicol, D. M., Palani, K., & Reed, E. (2017). Melody: Synthesized Datasets for Evaluating Intrusion Detection Systems for the Smart Grid. *Proceedings of the 2017 Winter Simulation Conference*, 78:1–78:12. Retrieved from http://dl.acm.org/citation.cfm?id=3242181.3242264

Bodström, T., & Hämäläinen, T. (2018). A Novel Method for Detecting APT Attacks by Using OODA Loop and Black Swan Theory. In X. Chen, A. Sen, W. W. Li, & M. T. Thai (Eds.), *Computational Data and Social Networks* (pp. 498–509). Springer International Publishing.

Chowdhary, A., Alshamrani, A., Huang, D., & Liang, H. (2018). MTD Analysis and Evaluation Framework in Software Defined Network (MASON). *Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*, 43–48. https://doi.org/10.1145/3180465.3180473

de Fuentes, J. M., González-Manzano, L., Tapiador, J., & Peris-Lopez, P. (2017). PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing. *Computers & Security*, *69*, 127–141. https://doi.org/10.1016/j.cose.2016.12.011

de Sá, A. O., da Costa Carmo, L. F. R., & Machado, R. C. S. (2018). A controller design for mitigation of passive system identification attacks in networked control systems. *Journal of Internet Services and Applications*, *9*(1), 2. https://doi.org/10.1186/s13174-017-0074-z

Ekelhart, A., Kiesling, E., Grill, B., Strauss, C., & Stummer, C. (2015). Integrating attacker behavior in IT security analysis: a discrete-event simulation approach. *Information Technology and Management*, *16*(3), 221–233. https://doi.org/10.1007/s10799-015-0232-6

Fielder, A., Li, T., & Hankin, C. (2016). Modelling Cost-Effectiveness of Defenses in Industrial Control Systems. In A. Skavhaug, J. Guiochet, & F. Bitsch (Eds.), *Computer Safety, Reliability, and Security* (pp. 187–200). Springer International Publishing.

Friedberg, I., Skopik, F., Settanni, G., & Fiedler, R. (2015). Combating advanced persistent threats: From network event correlation to incident detection. *Computers & Security*, *48*, 35–57. https://doi.org/10.1016/j.cose.2014.09.006

Ghosh, N., Chokshi, I., Sarkar, M., Ghosh, S. K., Kaushik, A. K., & Das, S. K. (2015). NetSecuritas: An Integrated Attack Graph-based Security Assessment Tool for Enterprise Networks. *Proceedings of the 2015 International Conference on Distributed Computing and Networking*, 30:1–30:10. https://doi.org/10.1145/2684464.2684494

Gjermundrød, H., & Dionysiou, I. (2015). CloudhoneyCY: An Integrated Honeypot Framework for Cloud Infrastructures. *Proceedings of the 8th International Conference on Utility and Cloud Computing*, 630–635. https://doi.org/10.1109/UCC.2015.110

Gonzalez-Granadillo, G., Rubio-Hernan, J., & Garcia-Alfaro, J. (2018). A Pyramidal-based Model to Compute the Impact of Cyber Security Events. *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 19:1–19:10. https://doi.org/10.1145/3230833.3230847

Haas, S., & Fischer, M. (2019). On the Alert Correlation Process for the Detection of Multi-step Attacks and a Graph-based Realization. *SIGAPP Appl. Comput. Rev.*, *19*(1), 5–19. https://doi.org/10.1145/3325061.3325062

Han, Z., Cheng, L., Zhang, Y., & Feng, D. (2015). Operating System Security Policy Hardening via Capability Dependency Graphs. In J. Lopez & Y. Wu (Eds.), *Information Security Practice and Experience* (pp. 3–17). Springer International Publishing.

He, X., & de Meer, H. (2017). A Stochastic Game-Theoretic Model for Smart Grid Communication Networks. In S. Rass, B. An, C. Kiekintveld, F. Fang, & S. Schauer (Eds.), *Decision and Game Theory for Security* (pp. 295–314). Springer International Publishing.

Jafarian, J. H. H., Al-Shaer, E., & Duan, Q. (2014). Spatio-temporal Address Mutation for Proactive Cyber Agility Against Sophisticated Attackers. *Proceedings of the First ACM Workshop on Moving Target Defense*, 69–78. https://doi.org/10.1145/2663474.2663483

Jeon, S., Yun, J.-H., & Kim, W.-N. (2016). Obfuscation of Critical Infrastructure Network Traffic Using Fake Communication. In C. G. Panayiotou, G. Ellinas, E. Kyriakides, & M. M. Polycarpou (Eds.), *Critical Information Infrastructures Security* (pp. 268–274). Springer International Publishing.

Kendrick, P., Criado, N., Hussain, A., & Randles, M. (2018). A self-organising multi-agent system for decentralised forensic investigations. *Expert Systems with Applications*, *102*, 12–26. https://doi.org/10.1016/j.eswa.2018.02.023

Kiesling, E., Ekelhart, A., Grill, B., Strauss, C., & Stummer, C. (2016). Selecting security control portfolios: a multi-objective simulation-optimization approach. *EURO Journal on Decision Processes*, *4*(1), 85–117. https://doi.org/10.1007/s40070-016-0055-7

Kim, G., Choi, C., & Choi, J. (2018). Ontology Modeling for APT Attack Detection in an IoT-based Power System. *Proceedings of the 2018 Conference on Research in Adaptive and Convergent Systems*, 160–164. https://doi.org/10.1145/3264746.3264786

Kumar, R., Rensink, A., & Stoelinga, M. (2018). LOCKS: A Property Specification Language for Security Goals. *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, 1907–1915. https://doi.org/10.1145/3167132.3167336

Kumar, R., Ruijters, E., & Stoelinga, M. (2015). Quantitative Attack Tree Analysis via Priced Timed Automata. In S. Sankaranarayanan & E. Vicario (Eds.), *Formal Modeling and Analysis of Timed Systems* (pp. 156–171). Springer International Publishing.

Lanoe, D., Hurfin, M., & Totel, E. (2018). A Scalable and Efficient Correlation Engine to Detect Multi-Step Attacks in Distributed Systems. *2018 IEEE 37th Symposium on Reliable Distributed Systems (SRDS)*, 31–40. https://doi.org/10.1109/SRDS.2018.00014

Luh, R., Schramm, G., Wagner, M., Janicke, H., & Schrittwieser, S. (2018). SEQUIN: a grammar inference framework for analyzing malicious system behavior. *Journal of Computer Virology and Hacking Techniques*, *14*(4), 291–311. https://doi.org/10.1007/s11416-018-0318-x

Luh, R., Schrittwieser, S., & Marschalek, S. (2016). TAON: An Ontology-based Approach to Mitigating Targeted Attacks. *Proceedings of the 18th International Conference on Information Integration and Web-Based Applications and Services*, 303–312. https://doi.org/10.1145/3011141.3011157

Mediouni, B. L., Nouri, A., Bozga, M., Legay, A., & Bensalem, S. (2018). Mitigating Security Risks Through Attack Strategies Exploration. In T. Margaria & B. Steffen (Eds.), *Leveraging Applications of Formal Methods, Verification and Validation. Verification* (pp. 392–413). Springer International Publishing.

Mehresh, R., & Upadhyaya, S. (2015). Surviving advanced persistent threats in a distributed environment – Architecture and analysis. *Information Systems Frontiers*, *17*(5), 987–995. https://doi.org/10.1007/s10796-015-9569-y

Moothedath, S., Sahabandu, D., Clark, A., Lee, S., Lee, W., & Poovendran, R. (2018). Multi-stage Dynamic Information Flow Tracking Game. In L. Bushnell, R. Poovendran, & T. Başar (Eds.), *Decision and Game Theory for Security* (pp. 80–101). Springer International Publishing.

Nagar, U., Nanda, P., He, X., & Tan, Z. (2017). A Framework for Data Security in Cloud Using Collaborative Intrusion Detection Scheme. *Proceedings of the 10th International Conference on Security of Information and Networks*, 188–193. https://doi.org/10.1145/3136825.3136905

Nath, H. V., & Mehtre, B. M. (2015). Analysis of a multistage attack embedded in a video file. *Information Systems Frontiers*, *17*(5), 1029–1037. https://doi.org/10.1007/s10796-015-9570-5

Nicol, D. M. (2018). Cyber Risk of Coordinated Attacks in Critical Infrastructures. *Proceedings of the 2018 Winter Simulation Conference*, 2759–2768. Retrieved from http://dl.acm.org/citation.cfm?id=3320516.3320845

Paridari, K., El-Din Mady, A., La Porta, S., Chabukswar, R., Blanco, J., Teixeira, A., … Boubekeur, M. (2016). Cyber-physical-security Framework for Building Energy Management System. *Proceedings of the 7th International Conference on Cyber-Physical Systems*, 18:1–18:9. Retrieved from http://dl.acm.org/citation.cfm?id=2984464.2984482

Paudel, S., Smith, P., & Zseby, T. (2017). Attack Models for Advanced Persistent Threats in Smart Grid Wide Area Monitoring. *Proceedings of the 2Nd Workshop on Cyber-Physical Security and Resilience in Smart Grids*, 61–66. https://doi.org/10.1145/3055386.3055390

Paul, S., & Ni, Z. (2017). Vulnerability analysis for simultaneous attack in smart grid security. *2017 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 1–5. https://doi.org/10.1109/ISGT.2017.8086078

Pitropakis, N., Panaousis, E., Giannakoulias, A., Kalpakis, G., Rodriguez, R. D., & Sarigiannidis, P. (2018). An Enhanced Cyber Attack Attribution Framework. In S. Furnell, H. Mouratidis, & G. Pernul (Eds.), *Trust, Privacy and Security in Digital Business* (pp. 213–228). Springer International Publishing.

Potteiger, B., Martins, G., & Koutsoukos, X. (2016). Software and Attack Centric Integrated Threat Modeling for Quantitative Risk Assessment. *Proceedings of the Symposium and Bootcamp on the Science of Security*, 99–108. https://doi.org/10.1145/2898375.2898390

Rodríguez, R. J., Chang, X., Li, X., & Trivedi, K. S. (2016). Survivability Analysis of a Computer System Under an Advanced Persistent Threat Attack. In B. Kordy, M. Ekstedt, & D. S. Kim (Eds.), *Graphical Models for Security* (pp. 134–149). Springer International Publishing.

Rubio, J. E., Alcaraz, C., & Lopez, J. (2017). Preventing Advanced Persistent Threats in Complex Control Networks. In S. N. Foley, D. Gollmann, & E. Snekkenes (Eds.), *Computer Security – ESORICS 2017* (pp. 402–418). Springer International Publishing.

Rubio, J. E., Roman, R., Alcaraz, C., & Zhang, Y. (2018). Tracking Advanced Persistent Threats in Critical Infrastructures Through Opinion Dynamics. In J. Lopez, J. Zhou, & M. Soriano (Eds.), *Computer Security* (pp. 555–574). Springer International Publishing.

Settanni, G., Skopik, F., Shovgenya, Y., Fiedler, R., Carolan, M., Conroy, D., … Olli, P. (2017). A collaborative cyber incident management system for European interconnected critical infrastructures. *Journal of Information Security and Applications*, *34*, 166–182. https://doi.org/10.1016/j.jisa.2016.05.005

Singh, V. K., Ozen, A., & Govindarasu, M. (2018). A Hierarchical Multi-Agent Based Anomaly Detection for Wide-Area Protection in Smart Grid. *2018 Resilience Week (RWS)*, 63–69. https://doi.org/10.1109/RWEEK.2018.8473514

Smith, R. J., Zincir-Heywood, A. N., Heywood, M. I., & Jacobs, J. T. (2016). Initiating a Moving Target Network Defense with a Real-time Neuro-evolutionary Detector. *Proceedings of the 2016 on Genetic and Evolutionary Computation Conference Companion*, 1095–1102. https://doi.org/10.1145/2908961.2931681

Sun, C., Hong, J., & Liu, C. (2016). A coordinated cyber attack detection system (CCADS) for multiple substations. *2016 Power Systems Computation Conference (PSCC)*, 1–7. https://doi.org/10.1109/PSCC.2016.7540902

Touhiduzzaman, M., Hahn, A., & Srivastava, A. (2018). A Diversity-based Substation Cyber Defense Strategy utilizing Coloring Games. *IEEE Transactions on Smart Grid*, 1–1. https://doi.org/10.1109/TSG.2018.2881672

Wang, F., Kwon, Y., Ma, S., Zhang, X., & Xu, D. (2018). Lprov: Practical Library-aware Provenance Tracing. *Proceedings of the 34th Annual Computer Security Applications Conference*, 605–617. https://doi.org/10.1145/3274694.3274751

Zhao, T., & Qiu, X. (2018). Detection of IP Gangs: Strategically Organized Bots. In P. Perner (Ed.), *Advances in Data Mining. Applications and Theoretical Aspects* (pp. 254–265). Springer International Publishing.

Zimba, A., Wang, Z., & Chen, H. (2018). Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. *ICT Express*, *4*(1), 14–18. https://doi.org/10.1016/j.icte.2017.12.007

Zulkefli, Z., Singh, M. M., & Malim, N. H. A. H. (2015). Advanced Persistent Threat Mitigation Using Multi Level Security – Access Control Framework. In O. Gervasi, B. Murgante, S. Misra, M. L. Gavrilova, A. M. A. C. Rocha, C. Torre, … B. O. Apduhan (Eds.), *Computational Science and Its Applications -- ICCSA 2015* (pp. 90–105). Springer International Publishing.

Appendix B – Identified Countermeasures

The selected publications for the study are listed below. These identified countermeasures provide answers to the research question regarding available countermeasures. Identified countermeasures are presented in this section by the use of the data extraction forms and the created categories from the data analysis.

Identified countermeasures from category *New analysis for the Individual IDS* are presented below (see Table 10).

Table 10. Available countermeasures from category *New Analysis Process for the Individual IDS*

Authors, year of publication	***Title***	**Aspect of a CCA**	**Countermeasure**	**Application domain**
Angelini et al., 2018	*An Attack Graph-based On-line Multi-step Attack Detector*	Early stage in general	Improve the IDS with a software engine for event correlation and visualization that uses IDS data and an attack-graph	Modern distributed systems, e.g. power grids
Babu et al., 2017	*Melody: Synthesized Datasets for Evaluating Intrusion Detection Systems for the Smart Grid*	CCA in general	Simulation of a modern power grid environment and use various treatments to show how it behaves so that an IDS can learn and more easily differentiate between normal and abnormal behavior.	The power grid
Friedberg, Skopik, Settanni, & Fiedler, 2015	*Combating advanced persistent threats: From network event correlation to incident detection*	CCA in general	An anomaly detection model based on white-listing, logs, and relationships between local applications and devices.	IT systems
Haas & Fischer, 2019	*On the Alert Correlation Process for the Detection of Multi-step Attacks and a Graph-based Realization*	CCA in general	A correlation algorithm that isolates attacks, identifies attack scenarios, and assembles multi-stage attacks from larger alert sets.	IT systems
Kiesling, Ekelhart, Grill, Strauss, & Stummer, 2016	*Selecting security control portfolios: a multi-objective simulation-optimization approach*	CCA in general	A decision support component to prevent deployment of acute short-term security measures, which relies on formal modeling of security knowledge, IT system models and threats, discrete-event simulation of attacks, and an algorithm that identifies security control portfolios	Organizations' information infrastructures

Kim, Choi, & Choi, 2018	*Ontology Modeling for APT Attack Detection in an IoT-based Power System*	Early stage in general	An ontology-based attack detection system capable of early detection of and response to CCAs by analyzing their attacking patterns, using the proposed inference rules.	IoT-based power systems
Kumar, Rensink, & Stoelinga, 2018	*LOCKS: A Property Specification Language for Security Goals*	CCA in general	A formal specification language that allows a security practitioner to express as well as compose security goals in a declarative manner, and formulate both qualitative and quantitative security goals embracing wide number of attributes such as cost, damage, probability, etc.	Modern day enterprises
Lanoe, Hurfin, & Totel, 2018	*A Scalable and Efficient Correlation Engine to Detect Multi-Step Attacks in Distributed Systems*	Early phase in general	A correlation engine that aim to predict attacks based on when a given number of attack steps have been detected. It is based on correlation rules, where each rule describes a known and multi-step attack that may affect the system.	SCADA environments in particular, but also distributed systems
Luh, Schramm, Wagner, Janicke, & Schrittwieser, 2018	*SEQUIN: a grammar inference framework for analyzing malicious system behavior*	CCA in general	An IT system behavior inference and classification methodology based on the Sequitur algorithm, which is formalized through a context-free grammar extended by semantic attributes (i.e. attribute grammar).	IT systems in general
Nath & Mehtre, 2015	*Analysis of a multistage attack embedded in a video file*	Early phase in general	Attack detection using API calls.	Computer users of general IT networks
Rubio, Roman, Alcaraz, & Zhang, 2018	*Tracking Advanced Persistent Threats in Critical Infrastructures Through Opinion Dynamics*	CCA in general	Opinion dynamics that permits to trace the attack throughout all its stages along the network by correlating different anomalies measured over time, thereby taking the persistence of threats and the criticality of resources into consideration.	Critical infrastructures
Sun, Hong, & Liu, 2016	*A coordinated cyber attack detection system (CCADS) for multiple substations*	CCA in general	Identifying the relations among detected events	Power grids
Zhao & Qiu, 2018	*Detection of IP Gangs: Strategically*	CCA in general	Clustering-based detection algorithms inspired by single-linkage clustering,	IT systems in general

	Organized Bots		optimized for large quantities of data	

Identified countermeasures from category *System Vulnerability Analysis* are presented below (see Table 11).

Table 11. Available countermeasures from category *System Vulnerability Analysis*

Authors, year of publication	***Title***	**Aspect of a CCA**	**Countermeasure**	**Application domain**
Bodström & Hämäläinen, 2018	*A Novel Method for Detecting APT Attacks by Using OODA Loop and Black Swan Theory*	Early stage in general	Reflect on improbable events, contradiction between the idea of a CCA and reality, the unknown duration of a CCA, and that duplicate information hinder learning. Bait attackers with decoys. Analyze all network traffic.	Digital infrastructures
Ekelhart, Kiesling, Grill, Strauss, & Stummer, 2015	*Integrating attacker behavior in IT security analysis: a discrete-event simulation approach*	CCA in general	A security simulation tool to assess how secure a system is toward attacks and changes to the system.	IT systems
Ghosh et al., 2015	*NetSecuritas: An Integrated Attack Graph-based Security Assessment Tool for Enterprise Networks*	CCA in general	An algorithm that generate attack-graphs related to the local system by comparing exploit databases and results from network scanners, and then recommends certain security measures.	Enterprise networks
Gonzalez-Granadillo, Rubio-Hernan, & Garcia-Alfaro, 2018	*A Pyramidal-based Model to Compute the Impact of Cyber Security Events*	CCA in general	A geometrical model to compute multiple simultaneous events based on their coverage, residual risk and potential collateral damage as pyramidal instances. Internal data about the target system (e.g., users, resources) is used to compute the base of the pyramid, and external data about the attacker (e.g., knowledge, motivation, skills) is used to compute its height.	Cyber-physical system
Han, Cheng, Zhang, &	*Operating System Security Policy*	CCA in general	Generate a capability dependency graph to describe an attacker's potential	Operating systems

Feng, 2015	*Hardening via Capability Dependency Graphs*		capabilities and the dependency relationships among these capabilities. Based on the capability dependency graph, a solution is developed to automate the task of hardening operating system security in terms of misconfigurations.	
Kumar, Ruijters, & Stoelinga, 2015	*Quantitative Attack Tree Analysis via Priced Timed Automata*	CCA in general	Computes the resources needed for a successful attack, as well as the associated attack paths, and generates various attack values, attack paths, top-10 worst attacks, and pareto-optimal curves.	Critical infrastructures e.g. power grids
Mediouni, Nouri, Bozga, Legay, & Bensalem, 2018	*Mitigating Security Risks Through Attack Strategies Exploration*	CCA in general	A risk assessment approach that allows to synthesize defense configurations making sophisticated attacks harder to achieve. The resources (e.g. cost) that an attack requires is considered to be the hardness criterion.	Organization's information systems
Nicol, 2018	*Cyber Risk of Coordinated Attacks in Critical Infrastructures*	CCA in general	Path-based cyber assessments increase computational complexity when extended from attack paths with single endpoints to attacks that include multiple endpoints. Protection based assessments of attack costs on the infrastructure.	Critical infrastructures e.g. power grid
Paul & Ni, 2017	*Vulnerability analysis for simultaneous attack in smart grid security*	CCA in general	Vulnerability analysis for simultaneous attack using a modified cascading failure simulator to automatically find the strongest attack combinations for reaching maximum damage in terms of generation power loss and time to reach black-out	Power grid
Potteiger, Martins, & Koutsoukos, 2016	*Software and Attack Centric Integrated Threat Modeling for Quantitative Risk Assessment*	CCA in general	A quantitative, integrated threat modeling approach that merges software and attack centric threat modeling techniques. A standardized, quantitative approach to model the security of components as well as the system as a whole by taking inter-connectedness into account.	Cyber-physical systems
Rodríguez, Chang, Li, & Trivedi, 2016	*Survivability Analysis of a Computer System Under an Advanced Persistent Threat*	CCA in general	Evaluate the survivability of a computer system under an APT attack by quantitatively assessing the system survivability in terms of security attributes but also provide insights on the cost/revenue trade-offs of investment efforts in system recovery such as	IT systems

	Attack		vulnerability mitigation strategies. Realized by using a variant of stochastic Petri nets.	

Identified countermeasures from category *Cooperative Intrusion Detection* are presented below (see Table 12).

Table 12. Available countermeasures from category *Cooperative Intrusion Detection*

Authors, year of publication	***Title***	**Aspect of a CCA**	**Countermeasure**	**Application domain**
Kendrick, Criado, Hussain, & Randles, 2018	*A self-organising multi-agent system for decentralised forensic investigations*	CCA in general	An agent-based framework for the analysis of cyber events that performs automatic data collection and analysis by using forensic-inspired processes to search for information useful during the analysis of a security event	Organizations in general
Nagar, Nanda, He, & Tan, 2017	*A Framework for Data Security in Cloud Using Collaborative Intrusion Detection Scheme*	CCA in general	Collaborative agent-based IDS framework. An alert correlation analysis with attack information and enables the cloud user to take quick and timely preventive action.	Cloud environment
Paridari et al., 2016	*Cyber-physical-security Framework for Building Energy Management System*	CCA in general	A cyber-physical security framework that executes a resilient policy whenever an attack is detected. Attacks are detected using security analytics driven by EMS data, where the physical correlations between the data-points are identified to detect outliers and then the control loop is closed using an estimated value in place of the outlier.	Energy management systems for buildings e.g. SCADA
Rubio, Alcaraz, & Lopez, 2017	*Preventing Advanced Persistent Threats in Complex Control Networks*	CCA in general	Modeling CCA evolution during execution. Multi-agent system to detect the CCA based on the topological changes suffered in the network, observed by hierarchically chosen nodes. Use of redundancy edges and random routing protocols to overcome the network deformation provoked by the CCA.	Industrial Control and Automation Systems
Settanni et al., 2017	*A collaborative cyber incident management*	CCA in general	A model for national comprehensive cross-organizational cyber incident	European interconnected critical

	system for European interconnected critical infrastructures		management for critical infrastructures.	infrastructures
Singh, Ozen, & Govindarasu, 2018	*A Hierarchical Multi-Agent Based Anomaly Detection for Wide-Area Protection in Smart Grid*	CCA in general	Two-level hierarchical architecture which consists of local agent controllers, operating at different areas, which are constantly monitored by an central agent.	Power grid
Zulkefli, Singh, & Malim, 2015	*Advanced Persistent Threat Mitigation Using Multi Level Security – Access Control Framework*	CCA in general	Multi-level security and access control. Create awareness among users about actions that can present a threat to the company.	Organizations in general

Identified countermeasures from category *Network Obfuscation* are presented below (see Table 13).

Table 13. Available countermeasures from category *Network Obfuscation*

Authors, year of publication	***Title***	**Aspect of a CCA**	**Countermeasure**	**Application domain**
Chowdhary, Alshamrani, Huang, & Liang, 2018	*MTD Analysis and Evaluation Framework in Software Defined Network (MASON)*	CCA in general	Frequently reconfiguring the network by rerouting traffic, changing ports of local services, changing IP addresses.	Cloud networks
de Sá, da Costa Carmo, & Machado, 2018	*A controller design for mitigation of passive system identification attacks in networked control systems*	The stage of reconnaissance (explicit)	Prevent the attacker from modelling the target system by initiating fake control function messages internally.	Industrial Control Systems
Jafarian, Al-Shaer, & Duan, 2014	*Spatio-temporal Address Mutation for Proactive Cyber Agility Against Sophisticated Attackers*	The stage of reconnaissance (explicit)	Host-to-IP binding of each destination host to vary randomly across the network based on spatial and temporal randomization. This spatio-temporal randomization will distort attackers' view of the network by causing the collected reconnaissance information to expire as	Enterprise networks

			attackers transition from one host to another or if they stay long enough in one location.	
Jeon, Yun, & Kim, 2016	*Obfuscation of Critical Infrastructure Network Traffic Using Fake Communication*	The stage of traffic sniffing inside SCADA network (explicit)	An obfuscation method for CIS network traffic to interfere with information extraction. Achieved by creating fake communication at the transaction level, which includes an acknowledgement and response.	Critical Infrastructure Networks
Smith, Zincir-Heywood, Heywood, & Jacobs, 2016	*Initiating a Moving Target Network Defense with a Real-time Neuro-evolutionary Detector*	The stage of reconnaissance (explicit)	Moving network target defense approach	Modern IT systems and networks in general
Zimba, Wang, & Chen, 2018	*Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems*	CCA in general	A network segmentation approach based on nodes in different SCADA and production subnets, and network propagation, that are vulnerable to the WannaCry attack.	Critical infrastructures & Industrial Control Systems

Identified countermeasures from category *Investigate CCA Characteristics* are presented below (see Table 14).

Table 14. Available countermeasures from category *Investigate CCA Characteristics*

Authors, year of publication	***Title***	**Aspect of a CCA**	**Countermeasure**	**Application domain**
Bodström & Hämäläinen, 2018	*A Novel Method for Detecting APT Attacks by Using OODA Loop and Black Swan Theory*	Early stage in general	Reflect on improbable events, contradiction between the idea of a CCA and reality, the unknown duration of a CCA, and that duplicate information hinder learning. Bait attackers with decoys. Analyze all network traffic.	Digital infrastructures
Luh, Schrittwieser, & Marschalek, 2016	*TAON: An Ontology-based Approach to Mitigating Targeted Attacks*	CCA in general	Semantic assessment for planning an organization's defense against CCAs and helps to under-stand how, why, and by whom certain resources are targeted.	IT infrastructure
Mehresh & Upadhyaya, 2015	*Surviving advanced persistent threats in a distributed environment – Architecture and analysis*	CCA in general	A survivability architecture that involves tamper-resistant and surreptitious detection and node-to-node verification of suspicious events. The solution aims to identify Attacker Intent, Objectives and Strategies (AIOS) and to design targeted recoveries that promote survivability.	Distributed environment
Paudel, Smith, & Zseby, 2017	*Attack Models for Advanced Persistent Threats in Smart Grid Wide Area Monitoring*	CCA in general	Attack trees are used to model an APT's dependencies and building blocks	Power grids, Wide Area Monitoring Systems in particular
Pitropakis et al., 2018	*An Enhanced Cyber Attack Attribution Framework*	CCA in general	Framework that performs attribution of malicious parties behind APT campaigns, to increase societal resiliency. Gathers heterogeneous data coming from APT reports and publicly available information from social media and data collected from components monitoring behavioural activity. Uses honeypots and proposes optimal cybersecurity actions.	Critical infrastructures (most concerning) e.g. an electric power grid
Wang, Kwon, Ma, Zhang, & Xu, 2018	*Lprov: Practical Library-aware Provenance Tracing*	CCA in general	Analyze a system to identify the origin of an attack through a combination of library tracing and sys-call tracing	Contemporary enterprise networks

Identified countermeasures from category *Game Theoretical Guidance of Defense* are presented below (see Table 15).

Table 15. Available countermeasures from category *Game Theoretical Guidance of Defense*

Authors, year of publication	***Title***	**Aspect of a CCA**	**Countermeasure**	**Application domain**
Fielder, Li, & Hankin, 2016	*Modelling Cost-Effectiveness of Defenses in Industrial Control Systems*	CCA in general	A simulation-driven game of defenders and attackers, where the defender has a set of security measures to choose from, and learns over time which measures that are the most effective ones and can therefore develop a plan for real-life attack situations.	Industrial Control Systems
He & de Meer, 2017	*A Stochastic Game-Theoretic Model for Smart Grid Communication Networks*	Early stage in general	A stochastic game-theoretic model with a symmetric information and positive stop probabilities in order to assess the threat of multistage cyber-attacks, where the defender makes correct optimal proactive defense decisions.	Power grid communication networks
Moothedath et al., 2018	*Multi-stage Dynamic Information Flow Tracking Game*	CCA in general	A game theoretic framework modeling real-time detection of multi-stage APTs via Dynamic Information Flow Tracking, which taints and tracks malicious information flows through a system and inspects the flows at designated traps.	IT systems in general
Touhiduzzaman, Hahn, & Srivastava, 2018	*A Diversity-based Substation Cyber Defense Strategy utilizing Coloring Games*	CCA in general	A game-theoretic graph coloring technique to determine the optimal allocation of security mechanisms diversity that minimizes the impact of security vulnerabilities to the grid	Power grid

Identified countermeasures from category *Baiting the Attacker* are presented below (Table 16).

Table 16. Available countermeasures from category *Baiting the Attacker*

Authors, year of publication	***Title***	**Aspect of a CCA**	**Countermeasure**	**Application domain**
Bodström & Hämäläinen, 2018	*A Novel Method for Detecting APT Attacks by Using OODA Loop and Black Swan Theory*	Early stage in general	Reflect on improbable events, contradiction between the idea of a CCA and reality, the unknown duration of a CCA, and that duplicate information hinder learning. Bait attackers with decoys. Analyze all network traffic.	Digital infrastructures
Gjermundrød & Dionysiou, 2015	*CloudhoneyCY: An Integrated Honeypot Framework for Cloud Infrastructures*	CCA in general	A collection of low-interaction and high-interaction honeypots deployed in the cloud infrastructure with the purpose of collecting and analyzing attack data that aids in constructing attack profiles.	Cloud infrastructure

Identified countermeasures from category *Cybersecurity Information Sharing* are presented below (Table 17).

Table 17. Available countermeasures from category *Cybersecurity Information Sharing*

Authors, year of publication	***Title***	**Aspect of a CCA**	**Countermeasure**	**Application domain**
de Fuentes, González-Manzano, Tapiador, & Peris-Lopez, 2017	*PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing*	CCA in general	Cybersecurity information sharing by using a protocol across organizations where thousands of cyber incidents listed online can be aggregated in seconds.	Organizations