# Quantitative Information Security Vulnerability Assessment for Norwegian Critical Infrastructure

Yi-Ching Liao(✉)

Secure-NOK AS, Oslo, Norway
yi-ching.liao@securenok.com
https://www.securenok.com

**Abstract.** A single information security vulnerability exploitation within Norwegian critical infrastructure can have a significant impact on Norwegian society, even causing cascading effects on other countries. Therefore, it is essential to conduct a quantitative vulnerability assessment to secure the weakest link. However, quantifying vulnerabilities to the entire Norwegian critical infrastructure has not been properly conducted in the literature. Defining the sectors responsible for or involved in providing vital functions in Norwegian society as the scope, we propose a methodology of six processes to conduct a quantitative vulnerability assessment by integrating the information from three sources: (1) the regional Internet registry, (2) the banner crawlers, and (3) the vulnerability database. We present and visualize the results of the vulnerability assessment from four different aspects: (1) vulnerability, (2) window of exposure, (3) impact, and (4) exploitability. Based on the results, we can easily identify power supply and transport as the weakest link. Compared to the entire country, the vital societal functions are better secured. Such assessment should be conducted continuously and automatically by specified public authorities to identify, classify, quantify, and prioritize the time-varying vulnerabilities.

**Keywords:** Critical infrastructure · Quantitative information security vulnerability assessment · Norway

## 1 Introduction

Information security vulnerabilities are continuously growing, from 6,447 vulnerabilities in 2016 to 17,308 vulnerabilities in 2019, according to the statistics from the National Vulnerability Database (NVD) [11]. A single vulnerability exploitation within Norwegian critical infrastructure, which is essential for the maintenance of vital societal functions [1], can lead to cascading impacts across sectors in Norway or even across national borders [15]. However, the sectors responsible for or involved in providing vital functions (e.g., power supply, transport, etc.)


A. Rashid and P. Popov (Eds.): CRITIS 2020, LNCS 12332, pp. 31–43, 2020.
https://doi.org/10.1007/978-3-030-58295-1_3

in Norwegian society have different capacities for identifying time-varying vulnerabilities. To secure the weakest link, it is essential to conduct a quantitative vulnerability assessment for Norwegian critical infrastructure.

After identifying the research gap in Sect. 2, we demonstrate the different definitions of critical infrastructure and define the scope for quantitative vulnerability assessment in Sect. 3. Afterwards, we describe the methodology of six processes for conducting a quantitative vulnerability assessment in Sect. 4, and present and visualize the results from four different aspects in Sect. 5. Finally, we address the research limitations in Sect. 6, and conclude and identify the future work in Sect. 7.

## 2 Related Work

Quantifying vulnerabilities to the entire Norwegian critical infrastructure has not been properly conducted in the literature. Defining vulnerability as "a measure of system susceptibility to threat scenarios", Ezell [3] quantified vulnerability by measuring deterrence, detection, delay, and response. However, the proposed model was only applied to a medium-sized clean water system. Describing vulnerability as "a susceptibility to threats and hazards that substantially will reduce the ability of the system to maintain its intended function", Holmgren [5] proposed a framework for quantitative vulnerability assessment based on the studies from Swedish Defence Research Agency. Nevertheless, the suggested framework was only applied to electric power delivery.

Genge and Enăchescu [4] proposed a Shodan-based vulnerability assessment tool, which verifies the feasibility of integrating Shodan, Common Vulnerabilities and Exposures (CVE), and Common Vulnerability Scoring System (CVSS) for vulnerability assessment. However, the proposed tool was only applied to 12 Class C networks assigned to universities, telecommunications operators, railway systems, a bank, and a power company. To fill up the identified research gap, we follow the definition from National Institute of Standards and Technology (NIST), which specifies vulnerability as "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source" [10], and conduct a quantitative vulnerability assessment for Norwegian critical infrastructure.

## 3 Definitions and Sectors of Critical Infrastructure

The definition of critical infrastructure varies [15]. European Union defines critical infrastructure as "an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions" [1]. The selection of critical infrastructure sectors varies between countries as well. The most commonly selected critical

infrastructure sectors include: energy, information and communications technology, transportation, health, water, finance and banking, government, food supply and distribution, chemical industry, public safety, law enforcement, nuclear sector, dams and flood defense, critical manufacturing, defense industry, and space sector [15].

Norway defines critical infrastructure as "the facilities and systems which are necessary to maintain or recover vital societal functions". Additionally, Norway describes vital societal functions as "the functions which are necessary to meet the societal basic needs and the population's sense of security" [2] or "the functions that society could not cope without for seven days or less without this threatening the safety and/or security of the population" [14]. Compared with other countries, Norway does not regard the space sector and the defense industry as critical infrastructure sectors [15]. Following these definitions, we determine these sectors as the scope to conduct a quantitative vulnerability assessment for Norwegian critical infrastructure.

## 4 Methodology

We follow six processes for conducting a quantitative vulnerability assessment for Norwegian critical infrastructure, which are explained as follows:

### 4.1 Summarize the Sectors Responsible for Vital Societal Functions

Norwegian Directorate for Civil Protection (DSB) has defined 14 vital societal functions and listed 126 sectors responsible for or involved in providing vital functions in Norwegian society [14]. We utilize these vital societal functions for further analysis and comparison in Subsect. 4.6 and employ the listed sectors as search keywords to retrieve sector-relevant IP addresses from the regional Internet registry in Subsect. 4.2.

### 4.2 Retrieve Sector-Relevant IP Addresses from Réseaux IP Européens (RIPE)

Réseaux IP Européens Network Coordination Centre (RIPE NCC) is the regional Internet registry which serves Europe, the Middle East, and parts of Central Asia. The RIPE NCC website [16] provides full-text search which enables us to use the sector names in Subsect. 4.1 as search terms to search over the RIPE database object data. For IP address retrieval, we search over only the full text of the "inetnum" database object, which specifies one or more IPv4 addresses.

Among the 126 sectors listed by DSB, there are 18 general terms, such as infrastructure owners, system owners, providers, and private businesses, which cannot be utilized as search terms. For sectors like regional health authorities, we extend the search terms to "Helse Sør-Øst RHF", "Helse Vest RHF", "Helse Midt-Norge RHF", and "Helse Nord RHF" based on publicly available information [8]. Another example is about the power and grid companies. We broaden

the search scope with 143 search terms according to the lists of the largest Norwegian power and grid companies [12].

In case of no results found, we look up the domain name holder's information in the Norwegian domain registration directory service [13] and use the holder's information as the search term to search over the full text of the RIPE "inetnum" database object. If no results found again, we utilize the website's IP address if available. As a result, we retrieve 1,202,124 IP addresses from RIPE, which are utilized in Subsect. 4.4 for mapping with the vulnerable IP addresses.

For a comprehensive mapping, we generate tabular data with six fields: IP address, "netname", "descr", "org-name", sector name, and vital societal function. The "netname" attribute, which is the combination of letters, digits, and the underscore or hyphen character, represents the name of a range of IP addresses. The attribute "descr" and "org-name" specify the description and the name of the organization respectively. The name of the organization can be found in the "org-name" attribute if in American Standard Code for Information Interchange (ASCII) character encoding. If non-ASCII, the name of the organization can be stored in the "descr" attribute. Therefore, in addition to IP address, we can utilize the combination of "netname", "descr", and "org-name" attributes for extensive mapping with the vulnerable IP addresses in Subsect. 4.4.

### 4.3 Search Vulnerable IP Addresses Through Shodan

In this paper, we employ Shodan to search vulnerable IP addresses in Norway. Shodan, unlike the traditional web search engines, gathers the content of the banners instead of merely web pages. The banner, which describes the services on a device [6], can be utilized for vulnerability assessment. CVE Identifiers (CVE IDs) represent the publicly known vulnerabilities, and the Shodan crawlers store CVE IDs as property if the service is regarded as vulnerable. In addition to searching vulnerable IP addresses, we employ CVE IDs to correlate the severity of vulnerabilities in Subsect. 4.5.

For vulnerability assessment, we first downloaded all CVE IDs from the MITRE Corporation [9] on March 26th, 2020. We used these CVE IDs to get the total number of vulnerable IP addresses in Norway through Shodan from March 26th to 30th, 2020. The result shows Norwegian IP addresses are regarded as vulnerable to 1,598 CVE IDs. Knowing the publicly known vulnerabilities in Norway, we utilized these CVE IDs to download the results of vulnerable IP addresses into JavaScript Object Notation (JSON) files through Shodan from March 30th to April 2nd, 2020. Each JSON file contains the banners and other meta-data [6], from which we filtered out two fields: IP address and the organization which owns the IP address. As a result, we have 739,933 records with three fields: CVE ID, IP address, and organization, which show 431 organizations and 32,519 IP addresses in Norway are regarded as vulnerable by Shodan.

Even though Shodan provides the information about the organization which owns the IP address, we retrieve the "netname", "descr" and "org-name" attributes from RIPE for comprehensive mapping with the sector-relevant IP addresses in Subsect. 4.4. As a result, we generate tabular data with four fields:

vulnerable IP address, "netname", "descr", and "org-name". The combination of "netname", "descr", and "org-name" attributes enables us to retrieve the corresponding vital societal function.

### 4.4 Mapping the IP Addresses and the Attribute Combination Between RIPE and Shodan

To understand the scope of vulnerable IP addresses owned by the sectors responsible for vital societal functions in Norway, we map the 1,202,124 IP addresses retrieved from RIPE in Subsect. 4.2 with the 32,519 IP addresses regarded as vulnerable by Shodan in Subsect. 4.3. There are 496 IP addresses owned by the sectors responsible for or involved in providing vital functions in Norwegian society with 632 distinct CVE IDs.

For an extensive mapping, we utilize the combination of "netname", "descr", and "org-name" attributes to retrieve the vital societal functions from the tabular data in Subsect. 4.2 and the vulnerable IP addresses with corresponding CVE IDs from the tabular data in Subsect. 4.3. As a result, we generate tabular data with three fields: vulnerable IP address, vital societal function, and CVE ID. There are 540 vulnerable IP addresses with 12 different vital societal functions and 671 distinct CVE IDs.

### 4.5 Correlate the Vulnerability Published Dates and Scores from NVD

CVE ID, which represents each publicly known vulnerability, can be utilized to correlate information provided by NVD. For further analysis and comparison in Subsect. 4.6, we utilize the 1,598 CVE IDs in Subsect. 4.3 to retrieve the published date, the CVSS impact subscore, and exploitability subscore from NVD. Even though the current version of CVSS is 3.1, not all CVE IDs have CVSS version 3.1 scores. Therefore, for a comprehensive analysis, we correlate CVSS version 2 scores instead.

To illustrate the window of exposure, we calculate the number of years between the CVE published date and March 26th, 2020, when we started to search vulnerable IP addresses through Shodan. To facilitate quantitative vulnerability assessment, we utilize the CVSS scores to demonstrate the severity of vulnerabilities. The CVSS base metric group, which defines the fundamental characteristics of a vulnerability, contains three impact metrics on the CIA triad: confidentiality, integrity, and availability. The three impact metrics measure the degree of loss of confidentiality, integrity, and availability into three levels: none, partial, and complete, if a vulnerability is exploited successfully. The CVSS base metric group includes another three metrics about exploitability: access vector, access complexity, and authentication metrics [7]. For an in-depth analysis in Subsect. 4.6, we retrieve impact and exploitability subscores instead of the overall score.

### 4.6 Analyze and Compare Between the Vital Societal Functions and the Whole Country

No records of vulnerable IP address found with two vital societal functions: financial services and electronic communication networks and services. The infeasibility of utilizing the general terms among the sectors listed by DSB (e.g., infrastructure owners and providers) as search terms for RIPE can lead to no records of vulnerable IP address found with electronic communication networks and services. For comparing between 12 vital societal functions, we analyze from the following four aspects: vulnerability (the count of CVE IDs), window of exposure (the number of years since the vulnerability has been published), impact (the CVSS impact subscore), and exploitability (the CVSS exploitability subscore). Moreover, we calculate the average count, years, and scores per vulnerable IP address to compare between 12 vital societal functions and the whole country. The major reason we choose to sum the CVSS subscores for comparison lies in the CVSS base equation "BaseScore = round_to_1_decimal(((0.6 * Impact) + (0.4 * Exploitability) − 1.5) * f(Impact)); f(impact) = 0 if Impact = 0, 1.176 otherwise", which is the foundation of CVSS scoring that calculates a base score ranging from 0 to 10 [7]. The analysis and comparison can be further enhanced if the asset criticality is available in the future.

## 5 Results

The results of the quantitative vulnerability assessment for Norwegian critical infrastructure are presented as follows:

### 5.1 Vulnerability

The tabular data in Subsect. 4.4 summarizes 671 distinct CVE IDs in connection with vital societal functions, 41.99% of distinct CVE IDs in Norway. Table 1 enumerates the distinct count of CVE IDs between the vital societal functions in descending order. As is presented, power supply, transport, and governance and crisis management hold higher distinct count of CVE IDs than other vital societal functions. Figure 1 illustrates the average count of CVE IDs per vulnerable IP address between the vital societal functions with the whole Norway's average count: 22.62 as the outermost line. Note that we sort the vital societal functions according to DSB's categorization: (1) governability and sovereignty: governance and crisis management, defense; (2) security of the population: law and order, health and care, emergency services, ICT security in the civil sector, nature and the environment, and (3) societal functionality: security of supply, water and sanitation, power supply, transport, satellite-based services.

### 5.2 Window of Exposure

Table 2 provides the total number of years since the vulnerability has been published between the vital societal functions in descending order, which implies

**Table 1.** The distinct count of CVE IDs between the vital societal functions

| Vital societal function | Distinct count of CVE IDs |
|---|---|
| Power supply | 587 |
| Transport | 454 |
| Governance and crisis management | 237 |
| Emergency services | 218 |
| Nature and the environment | 176 |
| Health and care | 156 |
| Water and sanitation | 154 |
| Security of supply | 134 |
| ICT security in the civil sector | 88 |
| Satellite-based services | 72 |
| Defense | 71 |
| Law and order | 53 |

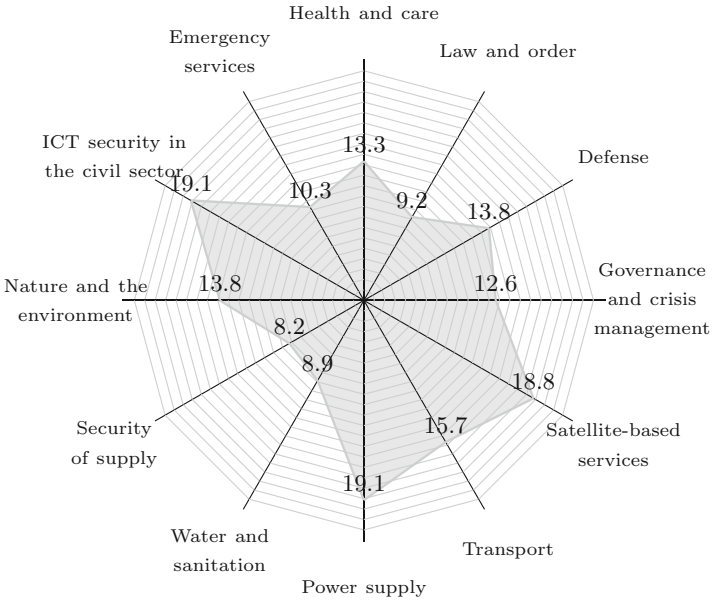


**Fig. 1.** The average count of CVE IDs per vulnerable IP address between the vital societal functions with the whole country's average count: 22.62 as the outermost line

the risk of vulnerabilities can be accepted or transferred among the vital societal functions. As the table suggests, power supply, transport, and nature and the environment have longer window of exposure than other vital societal functions. Figure 2 expresses the average number of years since the vulnerability has been published per vulnerable IP address between the vital societal functions with the whole Norway's average number of years: 246.33 as the outermost line, which suggests the publicly known vulnerabilities are mitigated quicker than general.

Note that in case of the system starting up after the vulnerability published date, the window of exposure will be overestimated.

**Table 2.** The total number of years since the vulnerability has been published between the vital societal functions

| Vital societal function | Total number of years |
|---|---|
| Power supply | 26124.8 |
| Transport | 16050.3 |
| Nature and the environment | 10605.9 |
| Health and care | 9795.3 |
| Governance and crisis management | 8338.8 |
| Emergency services | 7150.6 |
| Water and sanitation | 5458.5 |
| Security of supply | 4745.3 |
| Satellite-based services | 4020.6 |
| ICT security in the civil sector | 2254.4 |
| Law and order | 753.8 |
| Defense | 620.3 |

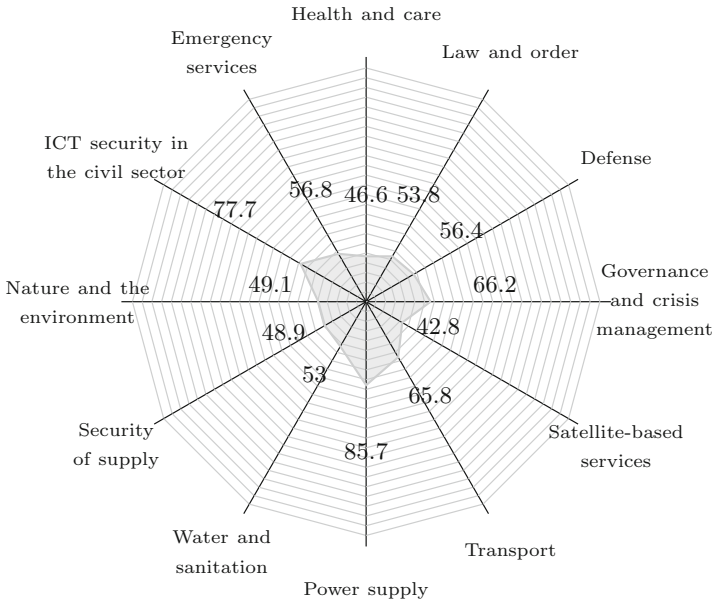


**Fig. 2.** The average number of years since the vulnerability has been published per vulnerable IP address between the vital societal functions with the whole country's average number of years: 246.33 as the outermost line

### 5.3 Impact

The total CVSS impact subscore of the vital societal functions is 102,769.6, 3.22% of the total CVSS impact subscore of vulnerable IP addresses in Norway, which is 3,193,033.8. Table 3 enumerates the sum of CVSS impact subscore between the vital societal functions in descending order, which indicates the degree of loss of confidentiality, integrity, and availability if a vulnerability is exploited successfully. As is observed, power supply, transport, and nature and the environment have higher impact caused by vulnerability exploitation than other vital societal functions. Figure 3 illustrates the average of CVSS impact subscore per vulnerable IP address between the vital societal functions with the whole Norway's average score: 196.37 as the outermost line. As the diagram suggests, the vital societal functions have less impact of vulnerability exploitation on the CIA triad than the entire country.

### 5.4 Exploitability

The total CVSS exploitability subscore of the vital societal functions is 198,373.2, 3.07% of the total CVSS exploitability subscore of vulnerable IP addresses in Norway, which is 6,464,958.2. Table 4 presents the sum of CVSS exploitability subscore between the vital societal functions in descending order. The CVSS exploitability subscore measures how the vulnerability is exploited, the complexity of the attack, and the number of times an attacker must authenticate for vulnerability exploitation [7]. Similar to the CVSS impact subscore, power supply, transport, and nature and the environment have higher exploitability than other vital societal functions. Figure 4 depicts the average of CVSS exploitability subscore per vulnerable IP address between the vital societal functions with the whole Norway's average score: 397.6 as the outermost line. As shown in the figure, the vital societal functions have less vulnerability exploitability than the entire country.

## 6 Discussions

We can easily identify power supply and transport as the weakest link of Norwegian critical infrastructure based on the results of the quantitative vulnerability assessment. Table 1 can also be utilized as a priority ranking of the vital societal functions for vulnerability remediation. Even though we cannot eliminate the possibility that broadening the search scope for the power and grid companies in Subsect. 4.2 may lead to more vulnerabilities found, the results demonstrate different capacities for vulnerability management between the vital societal functions. Therefore, it is essential to secure the weakest link by supporting critical infrastructure sectors to identify, classify, quantify, and prioritize the vulnerabilities.

We can simply understand the vulnerability level of critical infrastructure compared to the entire country through visualization. The results also imply

**Table 3.** The sum of CVSS impact subscore between the vital societal functions

| Vital societal function | Sum of CVSS impact subscore |
|---|---|
| Power supply | 25734.1 |
| Transport | 17537.3 |
| Nature and the environment | 13371.4 |
| Health and care | 12608.1 |
| Satellite-based services | 7396.0 |
| Governance and crisis management | 7378.0 |
| Emergency services | 6399.7 |
| Water and sanitation | 4700.2 |
| Security of supply | 4195.7 |
| ICT security in the civil sector | 2138.2 |
| Defense | 686.0 |
| Law and order | 624.9 |

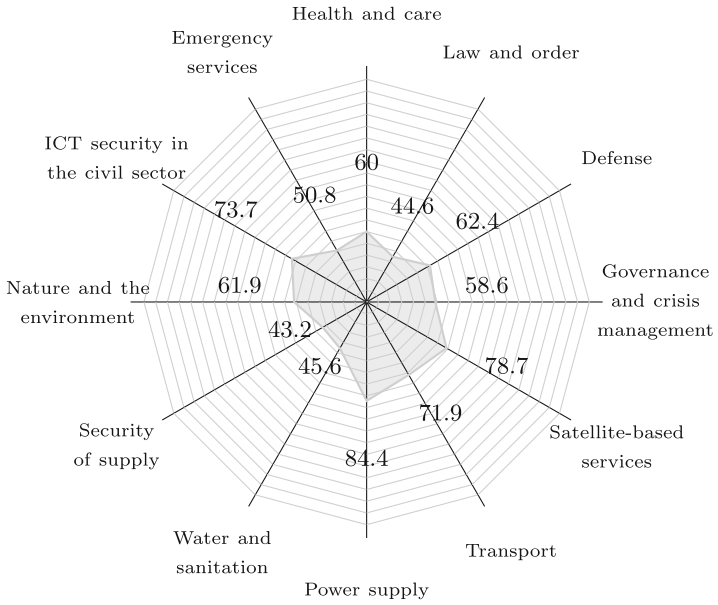


**Fig. 3.** The average of CVSS impact subscore per vulnerable IP address between the vital societal functions with the whole country's average score: 196.37 as the outermost line

the possibility of honeypot deployment within ICT security in the civil sector. Due to the time-varying vulnerabilities and the strong inter-dependencies between vital societal functions, it is important to conduct such quantitative vulnerability assessment continuously and automatically. Nevertheless, the process to retrieve sector-relevant IP addresses in Subsect. 4.2 can be one of the

**Table 4.** The sum of CVSS exploitability subscore between the vital societal functions

| Vital societal function | Sum of CVSS exploitability subscore |
|---|---|
| Power supply | 51612.5 |
| Transport | 33637.5 |
| Nature and the environment | 26111.7 |
| Health and care | 24495.6 |
| Satellite-based services | 15659.4 |
| Governance and crisis management | 13874.7 |
| Emergency services | 11110.6 |
| Water and sanitation | 7711.8 |
| Security of supply | 6729.2 |
| ICT security in the civil sector | 5009.3 |
| Defense | 1331.5 |
| Law and order | 1089.4 |

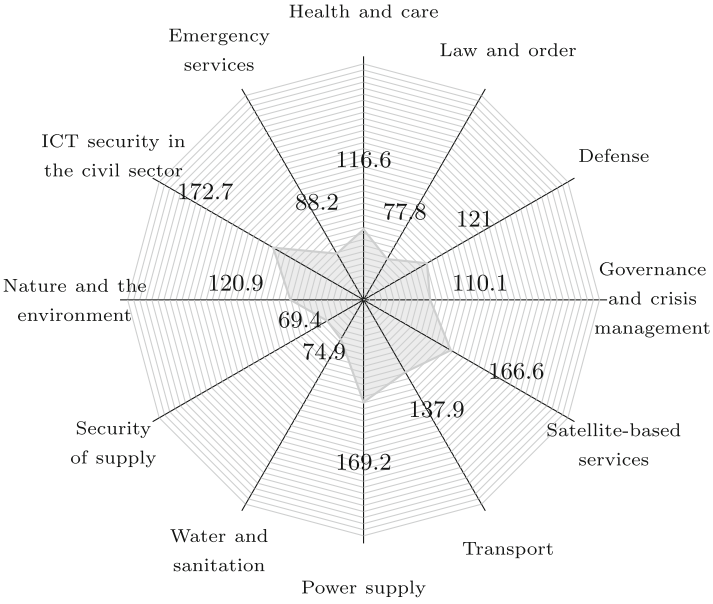


**Fig. 4.** The average of CVSS exploitability subscore per vulnerable IP address between the vital societal functions with the whole country's average score: 397.6 as the outermost line

automation challenges. Currently the full-text search is only provided through the RIPE NCC website [16], which hinders the process for automation.

As for the scope for quantitative vulnerability assessment, it is difficult to ensure the completeness and accuracy due to the general terms among the sectors listed by DSB. The infeasibility of utilizing these general terms as search terms for RIPE can lead to no records of vulnerable IP address found. Additionally,

only Internet-facing devices registered in Norway are included for vulnerability assessment. Air-gapped devices or sector-relevant IP addresses registered outside of Norway are beyond the scope of this paper.

In addition to the scope for quantitative vulnerability assessment, it is also challenging to verify the completeness and accuracy of the vulnerable IP addresses found by Shodan. For instance, the deployment of honeypots can affect the accuracy of vulnerability assessment. Even though the processes for verifying the vulnerabilities [17] and identifying the honeypots [18] are still ongoing, it is better for specified public authorities to gather the content of the banners for vulnerability assessment to ensure the completeness and accuracy of assessment scope and results. Moreover, with the comprehensive list of assets and asset criticality, the analysis and comparison results based on the sum of CVSS subscores can be further enhanced.

## 7 Conclusions and Future Work

We propose a methodology of six processes for conducting a quantitative information security vulnerability assessment for Norwegian critical infrastructure, which denotes the potential for an automated system for quantitative vulnerability assessment. In the future, with the authorities' complete list of assets and asset criticality for Norwegian critical infrastructure, such automated system can facilitate the vulnerability management by identifying, classifying, quantifying, and prioritizing the vulnerabilities discovered. With visualized notification and remediation suggestion correlated with open-source intelligence to each sector, this automated system can continuously secure the weakest link of vital societal functions by providing dynamic security awareness for administrators and enabling proactive responses.

**Acknowledgments.** This research is conducted as a part of the CybWin project funded by the Research Council of Norway.

## References

1. Council of the European Union: Council Directive 2008/114/EC, December 2008. http://data.europa.eu/eli/dir/2008/114/oj/eng
2. Departementenes Servicesenter, Informasjonsforvaltning: NOU 2006: 6, April 2006. https://www.regjeringen.no/no/dokumenter/nou-2006-6/id157408/
3. Ezell, B.C.: Infrastructure vulnerability assessment model (I-VAM). Risk Anal. Int. J. **27**(3), 571–583 (2007)
4. Genge, B., Enăchescu, C.: ShoVAT: Shodan-based vulnerability assessment tool for internet-facing services. Secur. Commun. Netw. **9**(15), 2696–2714 (2016). https://doi.org/10.1002/sec.1262
5. Holmgren, J.: A framework for vulnerability assessment of electric power systems. In: Murray, A.T., Grubesic, T.H. (eds.) Critical Infrastructure, pp. 31–55. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-68056-7_3
6. Matherly, J.: Complete guide to Shodan (2015)

7. Mell, P., Scarfone, K., Romanosky, S.: A Complete Guide to the Common Vulnerability Scoring System Version 2.0 (2007). https://www.first.org/cvss/v2/cvss-v2-guide.pdf
8. Ministry of Health and Care Services, Search Results: De regionale helseforetakene, November 2014. https://www.regjeringen.no/no/tema/helse-og-omsorg/sykehus/innsikt/nokkeltall-og-fakta---ny/de-regionale-helseforetakene/id528110/
9. MITRE Corporation: CVE List, March 2020. https://cve.mitre.org/data/downloads/index.html
10. National Institute of Standards and Technology (NIST): Glossary - vulnerability (2020). https://csrc.nist.gov/glossary/term/vulnerability
11. National Institute of Standards and Technology (NIST): National Vulnerability Database (NVD) - Statistics Results (2020). https://nvd.nist.gov/vuln/search/statistics?adv_search=false&form_type=basic&results_type=statistics&search_type=all
12. Nettbureau AS: Alle norske strømleverandører (2020). https://xn--strm-ira.no
13. Norid AS: The registry for Norwegian domain names (2020). https://www.norid.no/en/domeneoppslag/hvem-har-domenenavnet/
14. Norwegian directorate for civil protection (DSB): vital functions in society. Technical report (2017). https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf
15. OECD: Good Governance for Critical Infrastructure Resilience (2019). https://doi.org/10.1787/02f0e5a0-en
16. RIPE NCC: RIPE Database Text Search (2020). https://apps.db.ripe.net/db-web-ui/fulltextsearch
17. Shodan: Facet Analysis (2020). https://beta.shodan.io/search/facet?query=net%3A0%2F0&facet=vuln.verified
18. Shodan: Honeypot Or Not? (2020). https://honeyscore.shodan.io/