Causality network formation with ChatGPT

Dmitry Lande
National Technical University of Ukraine – Igor Sikorsky Kyiv Polytechnic Institute
Leonard Strashnoy
University of California, Los Angeles (UCLA)

Annotation

This work is dedicated to describing and comparing the results of two methods for constructing networks of causal relationships in cyber security vulnerability. Both methods are based on using the ChatGPT system, trained on a linguistic network, but the scenarios for constructing networks are fundamentally different. The first approach involves repeatedly executing the same prompt to the ChatGPT system, i.e., simulating the activity of multiple experts solving the same problem. The second approach involves initially decomposing the problem of cyber security vulnerability into partial problems and then identifying concepts and causes of these partial problems using similar prompts. As can be seen from experimentally obtained data, the network constructed by the first method contains significantly fewer nodes than in the second case, with many nodes' reliability confirmed by their repeated appearance in AI responses (the reliability of selected concepts was also verified through expert analysis). The network obtained through primary decomposition contains significantly more nodes, with much less repetition. This network turned out to be much closer in structure to a hierarchical network. The paper describes a comprehensive methodology that integrates tools for intelligent analytics and network visualization. To visualize constructed networks, authors used AT&T's GaphViz graph visualization library which allowed them to create graphs in SVG format with hyperlinks to search engines corresponding to each node and edge. The article describes a complex methodology applied specifically within the cyber security vulnerability domain but it can be used for building cause-and-effect networks in other domains as well.

Keywords: ChatGPT, Reason Networks, Domain model, Artificial experts, Decomposition, Graph visualization, GraphViz, Cyber Security Vulnerability

Introduction

Among the tasks being solved today by large linguistic models, such as ChatGPT [1], are machine translation, summarization and retelling of texts, generation of new texts, and extraction of topics and questions to texts. The capabilities in extracting named entities allow using ChatGPT in factographic systems, particularly in medicine and economics. Naturally, intellectual

Electronic copy available at: https://ssrn.com/abstract=4464477

chats integrate with external systems such as geographic information [2], graph analysis and visualization systems. In works [3, 4], authors have shown how networks of relationships between literary characters can be formed; subject area networks with "general-specific" connections; as well as causal networks.

This paper is devoted to describing a methodology for forming causal networks using two different methods. If the first method is a variant of the one presented in [4], then the second method based on a decomposition of the main concept is introduced here for the first time.
The results obtained from network content formation can be visualized autonomously using software tools like Gephi (gephi.org) [5] – a popular program for visualizing graph structures.
Within this work, we present a network visualization program built on top of AT&T's GraphViz library. To load data into its environment CSV format suits perfectly so all requests to ChatGPT will be accompanied by format requirements.
The formed causal networks should later provide an opportunity to implement system analysis procedures including scenario analysis. Traditionally forming causal networks requires significant time investment and involvement from experienced experts.

Description of approaches

The task consists in constructing a causality network corresponding to a given problem (concept). It is assumed that ChatGPT has covered enough subject matter during its training process. Specifically, this article focuses on creating a cyber security vulnerability causality network.
In work [3] there was introduced virtual expert swarm agents concept which allows for identifying causes through special prompts addressed to ChatGPT followed by multiple repetitions according to mentioned article approach. Fig 1 (upper part) schematically represents this methodology for forming Network 1.
At the same time, one of the main procedures used in system analysis is decomposition. Within the second method, it is proposed to decompose the main concept into several partial concepts (in this work a decomposition into 10 partial concepts was implemented). Then for each partial concept, a similar prompt is formed allowing us to determine its main causes. This constitutes Methodology 2 which is schematically depicted on Fig 1 (lower part).
In Appendix 2 there are provided prompts ensuring the decomposition of the main concept and ten similar prompts allow the determination of their causes.

Electronic copy available at: https://ssrn.com/abstract=4464477

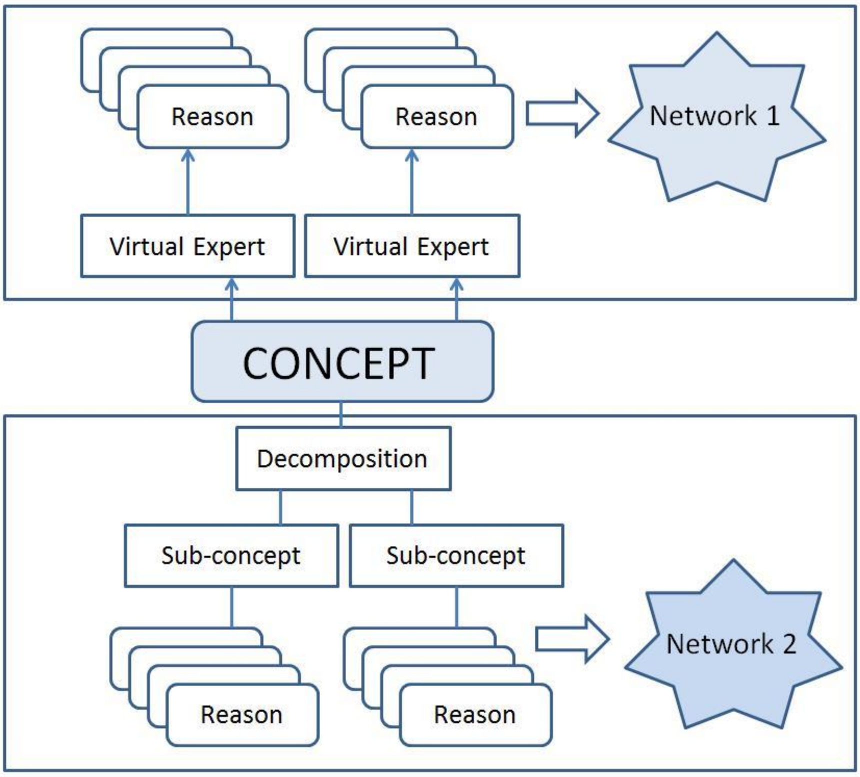


Figure 1. Two methods of constructing causal networks.

Method 1: Repeated execution of the same prompt.

As part of the first methodology, multiple executions of the same prompt to the ChatGPT system are proposed, that is, emulating the activity of multiple experts solving the same task. Thus, ChatGPT is proposed to work out a certain prompt in order to obtain a set of reasons for the primary concept (cyber security vulnerability). The ChatGPT system can help in obtaining content for a formatted file (fields corresponding to character names separated by semicolons). For example, such a simple prompt is used:

```
Name 10 reasons for the term "cyber security vulnerability".  Each reason must contain no more than three
words. Present the answer in the form: "reason; cyber security vulnerability". Each entry is on a separate
line.
```

The system outputs a response in the following format:

```
Software bugs; cyber security vulnerability
Misconfigured systems; cyber security vulnerability
Weak encryption; cyber security vulnerability
Unpatched software; cyber security vulnerability
Social engineering attacks; cyber security vulnerability
Phishing scams; cyber security vulnerability
Insider threats; cyber security vulnerability
Malware infections; cyber security vulnerability
Network vulnerabilities; cyber security vulnerability
```

Electronic copy available at: https://ssrn.com/abstract=4464477

Data leakage; cyber security vulnerability

The results of the 10-fold application of this prompt are presented in Appendix 1.

The ChatGPT system can provide different answers at different times when processing text. Each such answer can be perceived as the answer of a virtual expert, and by generalizing the answers of such a "swarm" of experts, a more complete answer can be obtained. By implementing a swarm of virtual experts several times with the same prompt considered earlier, the combined CSV file containing ChatGPT's responses is loaded for analysis and visualization using software developed by the authors based on GraphViz [5] library.

Graphviz (from Graph Visualization Software) is a package of utilities for automatic graph visualization specified in DOT language description format, as well as additional textual and graphical programs, widgets and libraries used in software development to visualize structured data. Developed by AT&T laboratory specialists, it is distributed with open-source files under an EPL license.

The program interface located online at http://bigsearch.space/uli.html (Fig. 2) allows entering ChatGPT responses into an input field and launching directed network visualization (the "Draw" button).

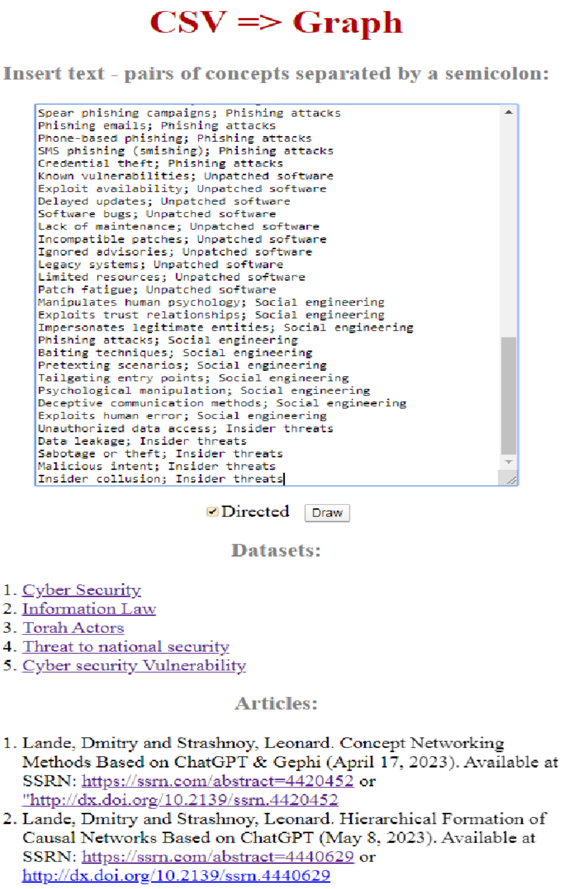
The program allowed us to output a graph corresponding to the network (Fig. 3), as well as a list of all network nodes with their frequency of occurrence. As a result of performing the above prompt ten times using Methodology 1 on this topic, we constructed a hierarchical network consisting of 77 nodes.

The most frequent nodes in the network according to Methodology 1 are:

Node	Frequency
CYBER SECURITY VULNERABILITY	100
MALWARE INFECTIONS	4
INSIDER THREATS	4
WEAK PASSWORDS	3
SOCIAL ENGINEERING ATTACKS	3
PHISHING SCAMS	2
MISCONFIGURED SYSTEMS	2
NETWORK VULNERABILITIES	2
NETWORK MISCONFIGURATIONS	2
DATA LEAKAGE	2
SOFTWARE VULNERABILITIES	2
SOFTWARE BUGS	2
UNPATCHED SYSTEMS	2
WEAK ENCRYPTION	2
EXPLOITABLE SOFTWARE VULNERABILITIES	2
ZERO-DAY EXPLOITS	2
WEAK ACCESS CONTROLS	2

Electronic copy available at: https://ssrn.com/abstract=4464477

LACK OF ENCRYPTION	2
UNPATCHED SOFTWARE	2



CSV => Graph

Insert text - pairs of concepts separated by a semicolon:

```
Spear phishing campaigns; Phishing attacks
Phishing emails; Phishing attacks
Phone-based phishing; Phishing attacks
SMS phishing (smishing); Phishing attacks
Credential theft; Phishing attacks
Known vulnerabilities; Unpatched software
Exploit availability; Unpatched software
Delayed updates; Unpatched software
Software bugs; Unpatched software
Lack of maintenance; Unpatched software
Incompatible patches; Unpatched software
Ignored advisories; Unpatched software
Legacy systems; Unpatched software
Limited resources; Unpatched software
Patch fatigue; Unpatched software
Manipulates human psychology; Social engineering
Exploits trust relationships; Social engineering
Impersonates legitimate entities; Social engineering
Phishing attacks; Social engineering
Baiting techniques; Social engineering
Pretexting scenarios; Social engineering
Tailgating entry points; Social engineering
Psychological manipulation; Social engineering
Deceptive communication methods; Social engineering
Exploits human error; Social engineering
Unauthorized data access; Insider threats
Data leakage; Insider threats
Sabotage or theft; Insider threats
Malicious intent; Insider threats
Insider collusion; Insider threats
```

☑ Directed

Datasets:

1. Cyber Security
2. Information Law
3. Torah Actors
4. Threat to national security
5. Cyber security Vulnerability

Articles:

1. Lande, Dmitry and Strashnoy, Leonard. Concept Networking Methods Based on ChatGPT & Gephi (April 17, 2023). Available at SSRN: https://ssrn.com/abstract=4420452 or "http://dx.doi.org/10.2139/ssrn.4420452
2. Lande, Dmitry and Strashnoy, Leonard. Hierarchical Formation of Causal Networks Based on ChatGPT (May 8, 2023). Available at SSRN: https://ssrn.com/abstract=4440629 or http://dx.doi.org/10.2139/ssrn.4440629

Figure 2. User interface

Electronic copy available at: https://ssrn.com/abstract=4464477

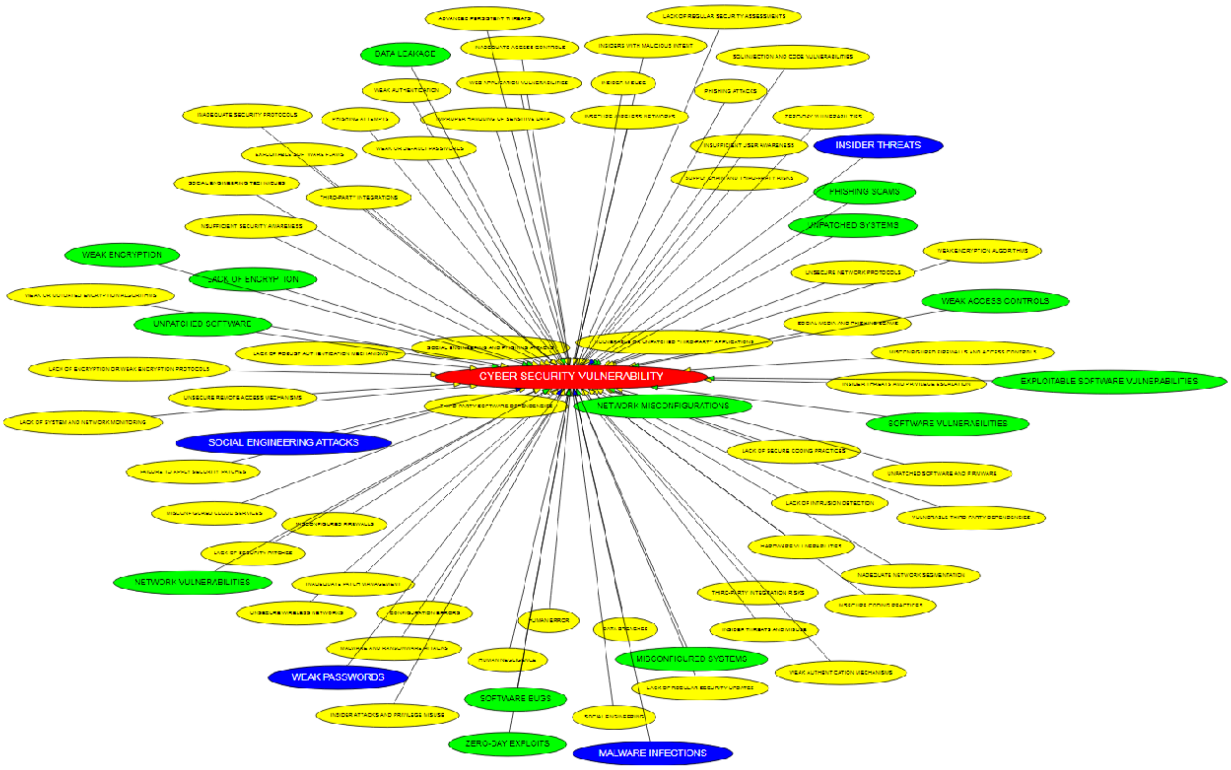

ADVANCED PERSISTENT THREATS
LACK OF REGULAR SECURITY ASSESSMENTS
DATA LEAKAGE
INADEQUATE ACCESS CONTROLS
INSIDERS WITH MALICIOUS INTENT
SQL INJECTION AND CODE VULNERABILITIES
WEAK AUTHENTICATION
WEB APPLICATION VULNERABILITIES
INSIDER MISUSE
PHISHING ATTACKS
INADEQUATE SECURITY PROTOCOLS
PHISHING ATTEMPTS
IMPROPER HANDLING OF SENSITIVE DATA
EXPLOITABLE SOFTWARE FLAWS
WEAK OR DEFAULT PASSWORDS
INSUFFICIENT USER AWARENESS
INSIDER THREATS
SOCIAL ENGINEERING TECHNIQUES
THIRD-PARTY INTEGRATIONS
SUPPLY CHAIN AND THIRD-PARTY RISKS
PHISHING SCAMS
INSUFFICIENT SECURITY AWARENESS
UNPATCHED SYSTEMS
WEAK ENCRYPTION
WEAK ENCRYPTION ALGORITHMS
LACK OF ENCRYPTION
UNSECURE NETWORK PROTOCOLS
WEAK OR OUTDATED ENCRYPTION ALGORITHMS
WEAK ACCESS CONTROLS
UNPATCHED SOFTWARE
SOCIAL MEDIA AND PHISHING SCAMS
LACK OF ROBUST AUTHENTICATION MECHANISMS
SOCIAL ENGINEERING AND PHISHING ATTACKS
VULNERABLE OR UNPATCHED THIRD-PARTY APPLICATIONS
MISCONFIGURED FIREWALLS AND ACCESS CONTROLS
LACK OF ENCRYPTION OR WEAK ENCRYPTION PROTOCOLS
CYBER SECURITY VULNERABILITY
INSIDER THREATS AND PRIVILEGE ESCALATION
EXPLOITABLE SOFTWARE VULNERABILITIES
UNSECURE REMOTE ACCESS MECHANISMS
THIRD-PARTY SOFTWARE DEPENDENCIES
NETWORK MISCONFIGURATIONS
LACK OF SYSTEM AND NETWORK MONITORING
SOFTWARE VULNERABILITIES
SOCIAL ENGINEERING ATTACKS
LACK OF SECURE CODING PRACTICES
FAILURE TO APPLY SECURITY PATCHES
UNPATCHED SOFTWARE AND FIRMWARE
LACK OF INTRUSION DETECTION
MISCONFIGURED CLOUD SERVICES
VULNERABLE THIRD-PARTY DEPENDENCIES
MISCONFIGURED FIREWALLS
LACK OF SECURITY PATCHES
HARDWARE VULNERABILITIES
INADEQUATE NETWORK SEGMENTATION
NETWORK VULNERABILITIES
INADEQUATE PATCH MANAGEMENT
THIRD-PARTY INTEGRATION RISKS
INSECURE CODING PRACTICES
UNSECURE WIRELESS NETWORKS
CONFIGURATION ERRORS
HUMAN ERROR
DATA BREACHES
INSIDER THREATS AND MISUSE
MALWARE AND RANSOMWARE ATTACKS
HUMAN NEGLIGENCE
MISCONFIGURED SYSTEMS
WEAK AUTHENTICATION MECHANISMS
WEAK PASSWORDS
LACK OF REGULAR SECURITY UPDATES
SOFTWARE BUGS
INSIDER ATTACKS AND PRIVILEGE MISUSE
SOCIAL ENGINEERING
ZERO-DAY EXPLOITS
MALWARE INFECTIONS

Figure 3. Network obtained using Methodology 1

Method 2: Primary problem decomposition

The second approach involves primary problem decomposition, namely breaking down the cyber security vulnerability into partial problems and then using similar prompts to obtain concepts and causes of these partial problems. The authors propose the following prompt for decomposing into 10 partial problems:

> Decompose the concept of "cyber security vulnerability" into 10 partial concepts. Each partial concept must contain no more than three words. Present the answer in the form: "partial concept; cyber security vulnerability". Each entry on a separate line.

As a result, a typical prompt for identifying the cause within the framework of the overall problem of cyber security vulnerability is formed for each of the partial problems, for example:

> 1 Reason Prompt: Name 10 reasons for the concept of " **Weak encryption** " as part of the concept of "cyber security vulnerability". Each reason must contain no more than three words. In the format "reason; **Weak encryption** ". Each entry on a separate line.

The answers received from ChatGPT are combined, resulting in a network (Figure 4). This network contains 102 nodes, which significantly exceeds the network constructed using Methodology 1. Below are the most frequently encountered concepts involved in forming this network.

Node	**Frequency**
PHISHING ATTACKS	13

Electronic copy available at: https://ssrn.com/abstract=4464477

SOCIAL ENGINEERING	13
UNPATCHED SOFTWARE	12
INSIDER THREATS	12
WEAK PASSWORDS	12
ZERO-DAY EXPLOITS	11
WEAK ENCRYPTION	11
DATA BREACHES	11
CONFIGURATION ERRORS	11
MALWARE INFECTION	10
CYBER SECURITY VULNERABILITY	10
PHISHING EMAILS	2
MALWARE INFECTIONS	2
LACK OF ENCRYPTION	2

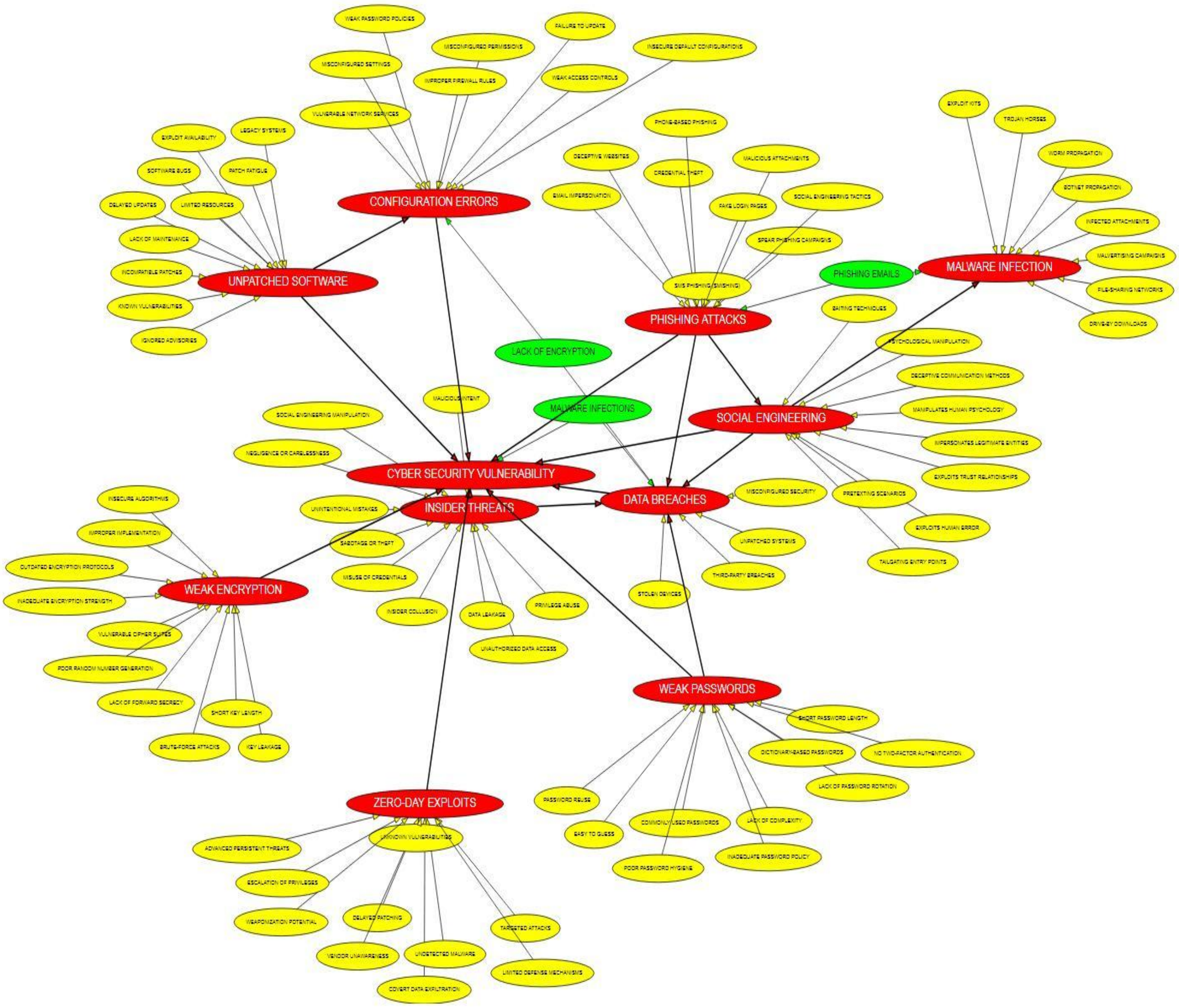


Figure 4. Network obtained using Methodology 2.

Electronic copy available at: https://ssrn.com/abstract=4464477

Combining the results

In practice, it is evident that the network obtained by logically combining networks formed according to methods 1 and 2 will have the advantages of both approaches. Indeed, this network (Fig. 5) in the considered domain turned out to be the most complete, containing 162 nodes, among which 25 participated in forming the network more than once. Such nodes listed below can be regarded as sources for further development of causal networks in the considered domain.

Node	**Frequency**
CYBER SECURITY VULNERABILITY	110
INSIDER THREATS	16
WEAK PASSWORDS	15
SOCIAL ENGINEERING	14
UNPATCHED SOFTWARE	14
PHISHING ATTACKS	14
ZERO-DAY EXPLOITS	13
WEAK ENCRYPTION	13
DATA BREACHES	12
CONFIGURATION ERRORS	12
MALWARE INFECTIONS	12
LACK OF ENCRYPTION	4
SOFTWARE BUGS	3
DATA LEAKAGE	3
UNPATCHED SYSTEMS	3
WEAK ACCESS CONTROLS	3
SOCIAL ENGINEERING ATTACKS	3
ADVANCED PERSISTENT THREATS	2
MISCONFIGURED SYSTEMS	2
PHISHING SCAMS	2
NETWORK MISCONFIGURATIONS	2
SOFTWARE VULNERABILITIES	2
PHISHING EMAILS	2
EXPLOITABLE SOFTWARE VULNERABILITIES	2
NETWORK VULNERABILITIES	2

Electronic copy available at: https://ssrn.com/abstract=4464477

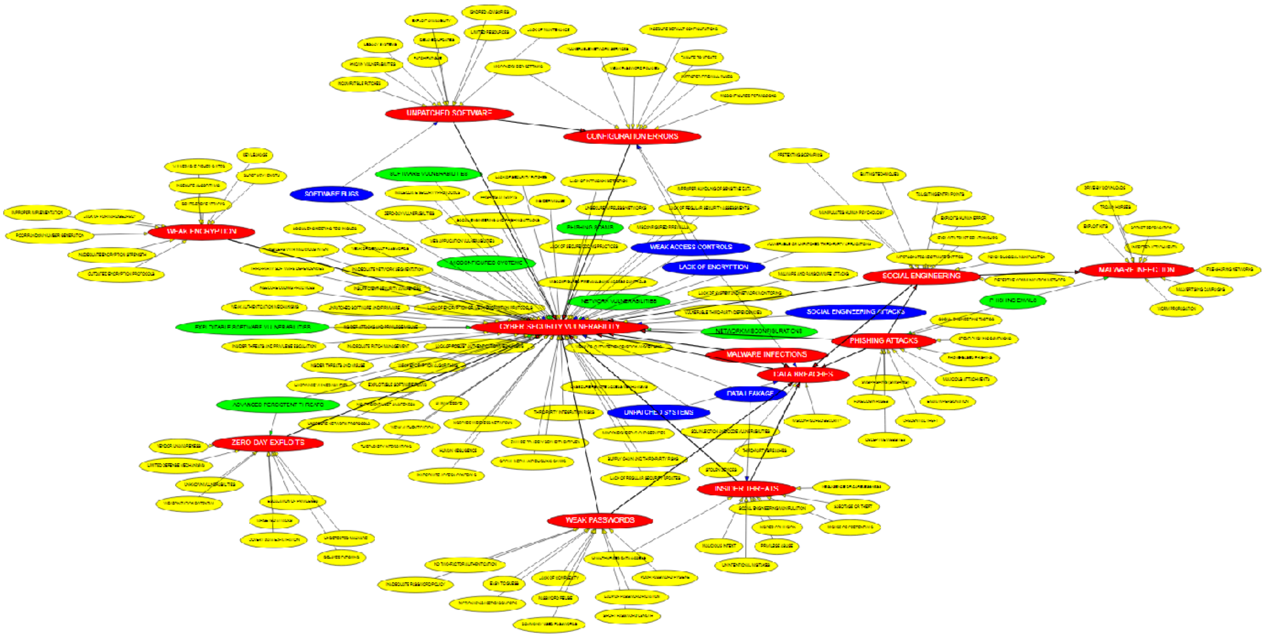


Figure 5. The network was obtained as a result of combining methods 1 and 2.

Conclusions

Methods for forming cause networks based on the use of ChatGPT have been proposed, demonstrated, and compared. Such networks can be used in the context of system and scenario analysis tasks.
The first method implemented the concept of virtual experts and showed the characteristics of networks formed using this approach. Based on an analysis of such a network, it can be concluded that it covers not the largest number of causes of the primary concept, which are relatively weakly connected (the network is hierarchical), but repeating the same causes among different "virtual experts" confirms their accuracy, so they can be good "raw material" for further analytical processing.
The second network obtained by initially decomposing the problem and subsequently identifying the causes of each partial problem is more extensive with the same number of references to ChatGPT as in the first case. This provides a wide field for research; however, at this point, repetition of concepts in such a network is minimal, and therefore its adequacy needs to be verified by expert review.
Finally, The third network that represents a logical combination of both previous networks is most complete within our considered domain. At this point, there are significant numbers of nodes participating in forming more than once i.e., those most important to our subject area. These nodes can be considered sources for further development.

A special interface was developed to visualize these generated networks directly transferring formatted responses from ChatGPT itself. The graphical interface developed using AT&T's GraphViz allowed us to create graphs where nodes and edges corresponded hyperlinks to queries made through web search engines.

The proposed approach was applied to the cyber security vulnerability domain but could also

Electronic copy available at: https://ssrn.com/abstract=4464477

apply across many other areas such as financial crises or military conflicts.

Limitations: Despite significant gains in resources (both time-wise and human-wise), it should be noted that both processes building cause-effect relationships between various phenomena as well as interpreting results require involvement from experienced data scientists familiar with studied domains ensuring the accuracy and reliability of results.

Literature

1. St. Wolfram. "What Is ChatGPT Doing ... and Why Does it Work?". – Wolfram Media, Inc. March 9, 2023. 112 p.
2. Tamilla Triantoro. Graph Viz: Exploring, Analyzing, and Visualizing Graphs and Networks with Gephi and ChatGPT (March 30, 2023). ODSC Community.
3. Lande, Dmitry and Strashnoy, Leonard. Concept Networking Methods Based on ChatGPT & Gephi (April 17, 2023). SSRN. Available at http://dx.doi.org/10.2139/ssrn.4420452
4. Lande, Dmitry and Strashnoy, Leonard. Hierarchical Formation of Causal Networks Based on ChatGPT (May 8, 2023). SSRN. Available at http://dx.doi.org/10.2139/ssrn. 4440629
5. Ken Cherven. “Mastering Gephi Network Visualization”. – Packt Publishing, 2015. 378 p.
6. Lambert M. Surhone, Mariam T. Tennoe, Susan F. Henssonow. Graphviz. VDM Publishing, 2010. 108 p.

Electronic copy available at: https://ssrn.com/abstract=4464477

Appendix 1. Prompts and answers for direct cause network formation.

Prompt: Name 10 reasons for the term "cyber security vulnerability". Each reason must contain no more than three words. Present the answer in the form: "reason; cyber security vulnerability". Each entry is on a separate line.

1 Software bugs; cyber security vulnerability Misconfigured systems; cyber security vulnerability Weak encryption; cyber security vulnerability Unpatched software; cyber security vulnerability Social engineering attacks; cyber security vulnerability Phishing scams; cyber security vulnerability Insider threats; cyber security vulnerability Malware infections; cyber security vulnerability Network vulnerabilities; cyber security vulnerability Data leakage; cyber security vulnerability	2 Human error; cyber security vulnerability Weak access controls; cyber security vulnerability Software vulnerabilities; cyber security vulnerability Network misconfigurations; cyber security vulnerability Inadequate security protocols; cyber security vulnerability Insufficient user awareness; cyber security vulnerability Third-party integrations; cyber security vulnerability Zero-day exploits; cyber security vulnerability Insecure coding practices; cyber security vulnerability Lack of regular security updates; cyber security vulnerability
3 Software vulnerabilities; cyber security vulnerability Weak passwords; cyber security vulnerability Network misconfigurations; cyber security vulnerability Social engineering attacks; cyber security vulnerability Phishing attempts; cyber security vulnerability Insider threats; cyber security vulnerability Lack of encryption; cyber security vulnerability Unpatched systems; cyber security vulnerability Malware infections; cyber security vulnerability Weak authentication; cyber security vulnerability	4 Inadequate access controls; cyber security vulnerability Misconfigured firewalls; cyber security vulnerability Exploitable software flaws; cyber security vulnerability Lack of security patches; cyber security vulnerability Insider misuse; cyber security vulnerability Weak encryption algorithms; cyber security vulnerability Vulnerable third-party dependencies; cyber security vulnerability Unsecure wireless networks; cyber security vulnerability Lack of intrusion detection; cyber security vulnerability Human negligence; cyber security vulnerability
5 Misconfigured cloud services; cyber security vulnerability Zero-day vulnerabilities; cyber security vulnerability Insecure wireless networks; cyber security vulnerability Web application vulnerabilities; cyber security vulnerability Improper handling of sensitive data; cyber security vulnerability Lack of system and network monitoring; cyber security vulnerability Exploitable software vulnerabilities; cyber security vulnerability Insider attacks and privilege misuse; cyber security vulnerability Lack of regular security assessments; cyber security vulnerability Third-party software dependencies; cyber security vulnerability	6 Weak or outdated encryption algorithms; cyber security vulnerability Unsecure remote access mechanisms; cyber security vulnerability Inadequate network segmentation; cyber security vulnerability Failure to apply security patches; cyber security vulnerability Lack of secure coding practices; cyber security vulnerability Social media and phishing scams; cyber security vulnerability Insider threats and privilege escalation; cyber security vulnerability Weak or default passwords; cyber security vulnerability Lack of robust authentication mechanisms; cyber security vulnerability Vulnerable or unpatched third-party applications; cyber security vulnerability
7 Software bugs; cyber security vulnerability Weak passwords; cyber security vulnerability Unpatched systems; cyber security vulnerability Social engineering attacks; cyber security vulnerability Phishing scams; cyber security vulnerability Insider threats; cyber security vulnerability Malware infections; cyber security vulnerability Network vulnerabilities; cyber security vulnerability Data leakage; cyber security vulnerability Misconfigured systems; cyber security vulnerability	8 Lack of encryption; cyber security vulnerability Unsecure network protocols; cyber security vulnerability Weak access controls; cyber security vulnerability Exploitable software vulnerabilities; cyber security vulnerability Insufficient security awareness; cyber security vulnerability Third-party integration risks; cyber security vulnerability Inadequate patch management; cyber security vulnerability Social engineering techniques; cyber security vulnerability Hardware vulnerabilities; cyber security vulnerability Insiders with malicious intent; cyber security vulnerability

Electronic copy available at: https://ssrn.com/abstract=4464477

9 Weak authentication mechanisms; cyber security vulnerability Unpatched software and firmware; cyber security vulnerability Insider threats and misuse; cyber security vulnerability Malware and ransomware attacks; cyber security vulnerability SQL injection and code vulnerabilities; cyber security vulnerability Misconfigured firewalls and access controls; cyber security vulnerability Social engineering and phishing attacks; cyber security vulnerability Lack of encryption or weak encryption protocols; cyber security vulnerability Supply chain and third-party risks; cyber security vulnerability Advanced persistent threats; cyber security vulnerability	10 Weak passwords; cyber security vulnerability Phishing attacks; cyber security vulnerability Unpatched software; cyber security vulnerability Social engineering; cyber security vulnerability Malware infections; cyber security vulnerability Insider threats; cyber security vulnerability Configuration errors; cyber security vulnerability Zero-day exploits; cyber security vulnerability Data breaches; cyber security vulnerability Weak encryption; cyber security vulnerability

Electronic copy available at: https://ssrn.com/abstract=4464477

Appendix 2. Prompts and answers for forming a network of causes based on initial decomposition.

Decomposition prompt: Decompose the concept of "cyber security vulnerability" into 10 partial concepts. Each partial concept must contain no more than three words.

Present the answer in the form: "partial concept; cyber security vulnerability". Each entry is on a separate line.

Weak encryption; cyber security vulnerability
Malware infections; cyber security vulnerability
Zero-day exploits; cyber security vulnerability
Weak passwords; cyber security vulnerability
Phishing attacks; cyber security vulnerability
Unpatched software; cyber security vulnerability
Social engineering; cyber security vulnerability
Insider threats; cyber security vulnerability
Configuration errors; cyber security vulnerability
Data breaches; cyber security vulnerability

1 Reason Prompt: Name 10 reasons for the concept of " **Weak encryption** " as part of the concept of "cyber security vulnerability". Each reason must contain no more than three words. In the format "reason; **Weak encryption** ". Each entry is on a separate line.

Short key length; Weak encryption
Insecure algorithms; Weak encryption
Improper implementation; Weak encryption
Lack of forward secrecy; Weak encryption
Vulnerable cipher suites; Weak encryption
Brute-force attacks; Weak encryption
Poor random number generation; Weak encryption
Outdated encryption protocols; Weak encryption
Key leakage; Weak encryption
Inadequate encryption strength; Weak encryption

2 Reason Prompt: Name 10 reasons for the concept of "**Malware infection** " as part of the concept of "cyber security vulnerability". Each reason must contain no more than three words. In the format "reason; **Malware infection** ". Each entry is on a separate line.

Phishing emails; Malware infection
Drive-by downloads; Malware infection
Infected attachments; Malware infection
Exploit kits; Malware infection
Malvertising campaigns; Malware infection
Trojan horses; Malware infection
Worm propagation; Malware infection
Botnet propagation; Malware infection
File-sharing networks; Malware infection
Social engineering; Malware infection

Electronic copy available at: https://ssrn.com/abstract=4464477

3 Reason Prompt: Name 10 reasons for the concept of “**Zero-day exploit** " as part of the concept of "cyber security vulnerability". Each reason must contain no more than three words. In the format "reason; **Zero-day exploit** ". Each entry is on a separate line.

Unknown vulnerabilities; Zero-day exploit
Targeted attacks; Zero-day exploit
Advanced persistent threats; Zero-day exploit
Undetected malware; Zero-day exploit
Vendor unawareness; Zero-day exploit
Limited defense mechanisms; Zero-day exploit
Delayed patching; Zero-day exploit
Covert data exfiltration; Zero-day exploit
Escalation of privileges; Zero-day exploit
Weaponization potential; Zero-day exploit

4 Reason Prompt: Name 10 reasons for the concept of “**Weak passwords**" as part of the concept of "cyber security vulnerability". Each reason must contain no more than three words. In the format "reason; **Weak passwords** ". Each entry is on a separate line.

Easy to guess; Weak passwords
Commonly used passwords; Weak passwords
Lack of complexity; Weak passwords
Password reuse; Weak passwords
No two-factor authentication; Weak passwords
Dictionary-based passwords; Weak passwords
Short password length; Weak passwords
Lack of password rotation; Weak passwords
Inadequate password policy; Weak passwords
Poor password hygiene; Weak passwords

5 Reason Prompt: Name 10 reasons for the concept of **“Phishing attacks "** as part of the concept of "cyber security vulnerability". Each reason must contain no more than three words. In the format "reason**; Phishing attacks** ". Each entry is on a separate line.

Email impersonation; Phishing attacks
Deceptive websites; Phishing attacks
Social engineering tactics; Phishing attacks
Fake login pages; Phishing attacks
Malicious attachments; Phishing attacks
Spear phishing campaigns; Phishing attacks
Phishing emails; Phishing attacks
Phone-based phishing; Phishing attacks
SMS phishing (smishing); Phishing attacks
Credential theft; Phishing attacks

Electronic copy available at: https://ssrn.com/abstract=4464477

6 Reason Prompt: Name 10 reasons for the concept of “**Unpatched software**" as part of the concept of "cyber security vulnerability". Each reason must contain no more than three words. In the format "reason; **Unpatched software** ". Each entry is on a separate line.

Known vulnerabilities; Unpatched software
Exploit availability; Unpatched software
Delayed updates; Unpatched software
Software bugs; Unpatched software
Lack of maintenance; Unpatched software
Incompatible patches; Unpatched software
Ignored advisories; Unpatched software
Legacy systems; Unpatched software
Limited resources; Unpatched software
Patch fatigue; Unpatched software

7 Reason Prompt: Name 10 reasons for the concept of “**Social engineering** " as part of the concept of "cyber security vulnerability". Each reason must contain no more than three words. In the format "reason; **Social engineering** ". Each entry on a separate line.

Manipulates human psychology; Social engineering
Exploits trust relationships; Social engineering
Impersonates legitimate entities; Social engineering
Phishing attacks; Social engineering
Baiting techniques; Social engineering
Pretexting scenarios; Social engineering
Tailgating entry points; Social engineering
Psychological manipulation; Social engineering
Deceptive communication methods; Social engineering
Exploits human error; Social engineering

8 Reason Prompt: Name 10 reasons for the concept of **“Insider threats"** as part of the concept of "cyber security vulnerability". Each reason must contain no more than three words. In the format "reason; **Insider threats** ". Each entry is on a separate line.

Unauthorized data access; Insider threats
Data leakage; Insider threats
Sabotage or theft; Insider threats
Malicious intent; Insider threats
Insider collusion; Insider threats
Privilege abuse; Insider threats
Misuse of credentials; Insider threats
Social engineering manipulation; Insider threats
Unintentional mistakes; Insider threats
Negligence or carelessness; Insider threats

Electronic copy available at: https://ssrn.com/abstract=4464477

9 Reason Prompt: Name 10 reasons for the concept of **“Configuration errors "** as part of the concept of "cyber security vulnerability". Each reason must contain no more than three words. In the format "reason; **Configuration errors** ". Each entry is on a separate line.

Misconfigured settings; Configuration errors
Weak access controls; Configuration errors
Insecure default configurations; Configuration errors
Lack of encryption; Configuration errors
Improper firewall rules; Configuration errors
Unpatched software; Configuration errors
Vulnerable network services; Configuration errors
Misconfigured permissions; Configuration errors
Weak password policies; Configuration errors
Failure to update; Configuration errors

10 Reason Prompt: Name 10 reasons for the concept of "**Data breaches** " as part of the concept of "cyber security vulnerability". Each reason must contain no more than three words. In the format "reason; **Data breaches** ". Each entry is on a separate line.

Insider threats; Data breaches
Phishing attacks; Data breaches
Weak passwords; Data breaches
Unpatched systems; Data breaches
Social engineering; Data breaches
Malware infections; Data breaches
Misconfigured security; Data breaches
Third-party breaches; Data breaches
Stolen devices; Data breaches
Lack of encryption; Data breaches

Electronic copy available at: https://ssrn.com/abstract=4464477