March - April 2020
ISSN: 0193-4120 Page No. 10900 - 10916

Cybersecurity Domains Classification Using MindMapping Technique forPublic Knowledge

Melwin Syafrizal[1], Siti Rahayu Selamat[2], Nurul Azma Zakaria[3]
[1]Department of Computer Engineering, UniversitasAmikom Yogyakarta, Indonesia.
[2 3]Center for Advanced Computing Technology,University Teknikal Malaysia, Melaka, Malaysia.

Article Info
Volume 83
Page Number: 10900 - 10916
Publication Issue:
March - April 2020

Abstract: Some reference books, ebooks, to scientific research publications in the field of cybersecurity introduce cybersecurity domains that differ according to the character of the organisation/business. Quite confusing for beginners to understand cybersecurity more deeply and understand the scope of security covered by cybersecurity. This review aims to provide the public with an understanding of the cybersecurity domain. The author uses literature review from various sources, printed documents and online and uses specific search keywords on search engines, then analyses per topic to be able to deduce appropriate cybersecurity domain criteria. Then the domains are further developed using sub-categories of cybersecurity that are more specific to their respective environments and are represented by mind mapping. Domain suitability testing through a series of observations on the implementation of cybersecurity in organisations/businesses. The contribution of this review paper is the cybersecurity domain for public needs, as knowledge for the community and business/organisational owners.

Keywords: *cybersecurity domain, mind mapping technique, organisation, business, public sector service, public knowledge.*

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 13 April 2020*

I. Introduction

Practitioners in the fields of IT, education, government, or business define the term cybersecurity by the scope of the organization/ business, or their respective areas of science, very varied, and vast[1]. There is a description, that cybersecurity is a rule, technique or tool to prevent attacks, or fields involving technology, people, information, and processes to ensure the security of enemy attacks[2], sometimes the term cybersecurity replaces the term of security information [3] or synonymous with security od IT [4]. There are also those that link cybersecurity with organizational assets and personal [5], privacy [6], and risk management [7],[8]. Although there is the public who are confused by these definitions, in fact, these definitions reinforce one another.

The difference in the definition of cybersecurity is related to the scope or form of organisation/ business, such as industry, government, education, etc. or depends on the field of science of each expert/cybersecurity implementer. It will also cause differences in the classification of cybersecurity

March - April 2020
ISSN: 0193-4120 Page No. 10900 - 10916

domains which are the priority of each organization/business. For example, if a cyber security definition is collection of rules, tools and techniques to prevent attacks involving people, data or information, technology, and processes to assure security from enemy attacks [2], then the cybersecurity domain can be: rules, standards, frameworks, security technique, types of cyber-attacks, tools, technology, education people, assets, event handling, etc.

What about cybersecurity goals? The purpose of cybersecurity is generally the same, namely to maintain the viability and development of business/organisations in the future, or to create a safe work environment where business/ organizations can remain resilient despite a violation or attack in cyberspace [4].

Lack of awareness or knowledge of users, staff or organizations on information security or cybersecurity will cause the level of involvement in securing information or assets owned very low [9],[10],[11]. Including responses in the event of an attack and risk mitigation [12].

This study aims to collect various references related to cybersecurity to be able to become a collection of knowledge and guidance for the public to understand cybersecurity as a whole from multiple basic things related to cybersecurity, such as domains, taxonomies, threat taxonomies, and their analysis.
Furthermore, the results of this study can be developed by other researchers to build cybersecurity domains and taxonomy of the latest cyber threats. For network administrators and systems, immediately prepare a guide or best practice for overcoming threats or cyberattacks. For the public or internet network users, it can be a reference to increase awareness, and understand things related to cyber and cybersecurity threats while surfing the internet.

The researcher will begin by giving a description/ definition of cyberspace, cybersecurity, and cybersecurity domains used in this study.

1.1 The Relationship of Cyberspace with Cybersecurity

Cybersecurity based on terms contained in [5]means cyberspace security. Cyberspace is a virtual place on the internet, where everyone around the world can do various activities, such as: studying, working, looking for entertainment, looking for information, chatting, business or buying and selling, etc.

Some other definitions/terms from cyberspace as follows:

> "*A complex environment, consisting of many software, many people's interactions, & services, using IT devices and connecting to internet networks. An environment and interaction do not exist in any physical form* [5]."
> *"Information technology infrastructure networks, including internet networks, telecommunications networks, and computer systems, which interdependence with processors and embedded controllers in critical industries* [13]*."*

Cyberspace has to do with organizational and personal assets. Besides, cyberspace also has stakeholder relations and threat agents. If further elaborated, the organization or person has physical and virtual assets. There are threats and vulnerabilities, as well as controls for management, organization and technical [14].

Consumers and Service Providers are the two stakeholders contained in ISO/IEC 27032: 2012 Standard.; Also, there are governments and regulations, investors and hackers. Organisations in cyberspace have a dual role, as providers, as well as consumers. As a provider, organisations provide services for use in cyberspace, and as consumers,

March - April 2020
ISSN: 0193-4120 Page No. 10900 - 10916

organisations can also use services provided by other providers. The application of organisational rules or policies in cyberspace is rather complicated. This complexity in cyberspace occurs because between rules for consumers or providers, requires the best planning and analysis, with comprehensive risk assessments, such as ISO/IEC 27032: 2012 risk management policies [14].

1.2 Does Cybersecurity = Information Security?

Some people often use "the term of cybersecurity" to replace "the term of information security"[15]. Protection of people and assets is in cybersecurity, while information security does not address this [3]. Cybersecurity protects systems that have connections to the internet, such as software, hardware, and data from enemy attacks in cyberspace. Information technology currently used and computer systems in organisations or businesses require protection from cyber attacks[16].

The cybersecurity security domain is different from other security domains, such as network security, application security, internet security, information security, computer security, and even different from security protection for critical information infrastructure (CIIP). However, according to ISO/IEC27032:2012, cybersecurity still has relevance to other security domains. Others say that cybersecurity covers all existing security domains [5].

Everything related to information security, infrastructure, systems, devices used by users for user security is cybersecurity [17]. Cybersecurity includes technology; all controls and processes are a result of design and development to protect and maintain systems, computer networks, data and information from the threat of cyber attacks. A statement from ITU-T X.1205, 2008, citing cybersecurity, as described below:

> *"Cybersecurity is a collection, policies, concepts of security, security protection, guidelines, risk management approaches, actions, training, best practices, guarantees and technologies that can be used to protect cyber environments and organizations and user assets* ...[18]."

Cybersecurity can also mean a joint effort to protect information assets, human beings, network infrastructure, computer systems, hardware and software, processes, services, including preventing, detecting and responding to abuse, attacks or threats from within or from outside or danger arising from natural disasters, as well as human error, intentional or unintentional, legal or illegal, the impact is large or small [19], [13], [20], [21].

1.3 Issue Related to Cybersecurity

Cybersecurity involves technology, data or information, private or government organisations, users or service providers, science and skills, and behaviour of technology users. Users must be aware of protecting themselves and the assets owned by all people and organisations. Placing security as a priority (private or government) organization, by engaging cybersecurity professionals to manage or assess risk/loss when an attack has an impact on a delay in the process or service [22],[23],[24],[2],[25].

Cybersecurity has sensitive issues, such as closing or reducing system weaknesses and closing access to personal information. Other problem such as increasing the skills and knowledge of staff/IT infrastructure managers, expanding the knowledge and alertness of service users, especially when browsing the internet [26]. Sensitive issues in the security sector will continue to grow. Significant risks such as system failure, theft or misuse of data, and theft of funds will be faced by individuals, businesses, or governments now and in the future [27],[28],[29].

March - April 2020
ISSN: 0193-4120 Page No. 10900 - 10916

One technology that is developing at this time is cloud computing. Cloud computing is essentially a shared computing system between users [30]. The cloud provides virtual resources through the internet with enormous challenges for privacy-protecting and data security [31].

Some definitions and statements about cybersecurity from several references, as explained in the Table 1.

Table 1. Cybersecurity Definition

No	Reference	Source Description	Definition of Cybersecurity
1	[2]	ACM - A Report in the Computing Curricula Series	Cyber Security is a field that involvestechnology, people, information, and processesto ensure security from enemy attacks.
2	[21]	Conference CISTI - Journal	Cybersecurity is a process of prevention, detection and response to an attack and includes an element of learning for continuousimprovement.
3	[20]	HM Government - Publication	Cybersecurity is the protection of the internet, including hardware/software, infrastructure, data and services provided on an online basis, from unauthorised access, danger or abuse of access. Includes intentional or unintentional threat by the system operator because it does not follow security rules or intentionallymanipulated.
4	[25]	AkamaiTechnologies, Inc. - Reseach Brief Report	During 2014-2015, the federal departmentcollectivelyreported an increase in cybersecurity incidents. Cyber risk and attacks are increasing and developingrapidly, so cybersecurity needs to be everyone'spriority.
5	[26]	Computer & Security - Journal	Cybersecurity is a global problem that needs to be addressed together by coveringweaknesses, improvingskills and preparing cybersecurity experts.
6	[23]	ISACA Study Guide - ebook	Cybersecurity is a fast-growing and ever-changing field, involvingprofessionalswho are concerned with implementing IT security. Cybersecurity is the responsibility of all organisations at every level, to be able to manage their cyber risks. Cybersecurity is part of information security.
7	[24]	Royal Society - Report	Cybersecurity is at the core of work with unique challenges, which have linkstomultidisciplinaryscience, technical, mathematics, social science and human behaviour.
8	[32]	Big Data Analytic - Journal	Cybersecurity is very important for the success of today's digital economy because security threats can come from within, or from outside. The ability todetect and predict risks from within an organisation with mitigation techniques is an essentialelement in cybersecurity.
9	[28]	Finra - Report	Cybersecurity is a significant risk facing the industry/company today and will be an essentialthingworthconsidering in the comingyears.
10	[22]	Springer - ebook	Securing cyberspace is everyone's responsibility. U.S. national security as a front-line defence/counterterrorism has an agenda toplace cybersecurity as a priority. The prosperity of the American economy in the 21st century will depend on cybersecurity. This world (cyberspace) has become a world that werely on every day. ... PresidentBarack Obama from the White House (May 29, 2009).
11	[27]	ITU - Publication	Cybersecurity is a sensitiveissue, both from a government or public business (private sector) perspective.
12	[29]	IIROC & OCRCVM - Best Practice Guide	Cybersecurity existsto protect companies from anything that endangers business, steal information or funds, or use company systems to attack company peers in the market.
13	[13]	CNSS - Glossary	The presence of cybersecurity is toprevent computer damage. Cybersecurity will provide protection, restore access to computers, electronic systems, and communication services, to those who have authority. Protect integrity, availability of information, authentication, confidentiality& non-repudiation.
14	[1]	Technology Innovation Management Review - Journal	Cybersecurity has many challenges; need to be considered by experts in various fields of science. Every definition in cybersecurity is meaningful, attracts the attention of stakeholders, is impartial, and is very useful.
15	[33]	Digital Government Research - Proceedings International Conference	Cybersecurity is an area correctly used to secure cyberspace.

16	[19]	Practical guide - ebook	Cybersecurity is a synergy between technology, processes (user activity) & efforts to protect information and networks from illegal access. Including protecting systems and computer equipment, as well as programs used toput, process, keep and transmit data, covered from the attacker, harm, &illegalingress.

Cybersecurity can also mean a joint effort to protect information assets, human beings, network infrastructure, computer systems, hardware and software, processes, services, including preventing, detecting and responding to abuse, attacks or threats from within or from outside or danger arising from natural disasters, as well as human error, intentional or unintentional, legal or illegal, the impact is large and small, [19],[13],[20],[21].

II. Related Work and Background

2.1 Cybersecurity Domains

Cybersecurity has links with several fields or domains, according to the model or form of organisation/business. For example, cybersecurity domains contained in NIST CSF are suitable for private sector organisations in the USA [34]or Federal Information Systems and Organizations [35]. NIST CSF has also been adopted or used as a reference for countries' cybersecurity frameworks, for the public sector to risk mitigation, etc.

The security domain in the NERC-CSS Standard for Bulk Power System (BPS) [36], the information security standard domain in ISO/IEC 27001: 2013 is suitable for both private and public organisations. This standard uses a process-based approach by establishing, maintaining, and increasing organisational ISMS [37]. PCI DSS is a security standard designed for banks or companies that issue credit cards [38].

To make it easier for the public to understand, manage, and mitigate risks and threats that might arise in the future, the author tries to summarise and conclude from several references as described inTabel 2.

Table 2. Cybersecurity or security domain from various references

Author	Description	Cybersecurity Domain (Category)
[36]	NERC-CSS Standard for Bulk Power System (BPS)	1) Critical Cyber Asset Identification; … 10) Information Protection
[39]	Cybersecurity in Cloud Computing Categories	• IT Asset Management, • Incident handling, • Knowledge accumulation.
[5]	ISO/IEC 27032:2012-Guidelines for Cybersecurity.	• Policies; • Methods and Processes; • People & Organization; • Applicable Technical Controls.
[37]	ISO/IEC 27001:2013 - ISMS.	1) Information Security Policies; … 13) Business Continuity… 14) Compliance.
[40]	General issue cybersecurity - journal	1) Physical Domain; 2) Information Domain; 3) Cognitive Domain; 4) Social Domain
[23]	ISACA Study Guide for student & instructor.	1) Cybersecurity Concepts; 2) Security Architecture Principles;

		… 5) Security Implications …
[41]	The World of Cybersecurity Map from the perspective of a CISSP certified	• Security Architecture • Security Operation • Governance • Risk Assessment • User Education • Threat Intelligence • Career Development • Framework and Standard • Physical Security
[34]	CSF NIST (policy framework for computer security for private sector organisations in US	• Identify • Protect • Detect • Respond • Recover
[42]	Control security domain for data center company from CSA-CCM	1) Application and Interface Security; … 15) Threat & Vulnerability Management.

The cybersecurity domains generally have subdomains again, for example from the ISO/IEC 27032:2012 standard, some of these cybersecurity domains can be developed or broken down into more detailed sub-domains, for example, "Domain ISO27032 Cybersecurity Capabilities" from Deloitte Touche Tohmatsu Limited (DTTL) company, as shown in Figure 1, consists of:

- Policies
  - Risk Assessment and Treatment
  - Information Asset Management
- Methods and Processes,
  - Cyber incident information sharing
  - Cyber incident handling
- People and Organization,
  - Information security policies & governance
  - Cybersecurity governance
- Applicable Technical Controls
  - End user workstation level controls
  - Implementation secure coding
  - Network monitoring response
  - Application level controls
  - Server level controls.

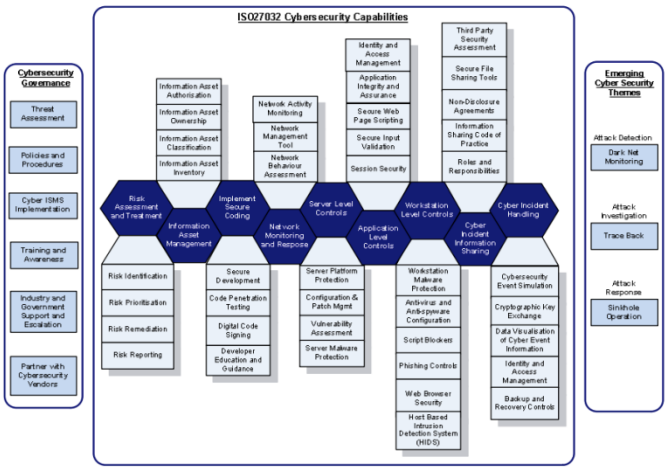

Fig 1. Domain of ISO27032 Cybersecurity Capabilities[43]

For example, the Risk Assessment and Treatment domain were developed in the following sub-domain categories, including risk identification, risk prioritization, risk remediation, and risk reporting. The domain of information asset management was developed into several sub-domains, including information asset inventory, information asset classification, information asset ownership, information asset authentication, etc.

A researcher/security expert using the mind-mapping technique (as shown in Figure 2) once published the map of cybersecurity domains version

March - April 2020
ISSN: 0193-4120 Page No. 10900 - 10916

2.0 [41], which describes the practice of cybersecurity domains and their sub-domains so that they can be a reference source for the public to understand cybersecurity. There are domain framework and standards, threat intelligence, user education, career development, security operations, governance, security architecture, physical security, and risk assessment. Each domain has a sub-domain that explains the relevance of domains to other things. For example, security operations, related to activities of protection, detection, recovery, prevention, “Security Information Event & Management” (SIEM), “Security Operations Center” (SOC), vulnerability management, incident response, data leakage, and active defence. Incident response is related to breach notification, containment, eradication, and investigation. The investigation related to forensics activities, and Recovery related to Disaster Recovery (DR), Business Continuity Plan (BCP).

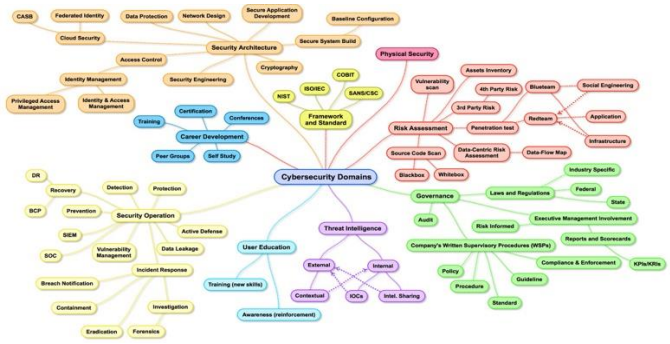

Fig 2. Cybersecurity Domains Mind-Map (version 2.0) from Jiang

The mind-mapping technique is a practical way to illustrate ideas and concepts. This technique helps someone to be able to think visually. Mind-maps help organize information, classify it, help analyze, understand characteristics, remember, summarize and produce new ideas better. Mind-Map techniques can be used as a guide for learning/teaching, developing and mapping ideas, to produce stronger research.

It is quite challenging to define a cybersecurity domain that is specific to various organisations/businesses because the models/types of organisa-tions are different. For example, non-profit and non-government organisations (NPOs and NGOs), which include arts/culture/heritage, charity/philan-thropy, economic development, education, health, religion, social, sports, & sector sustainability [44].

NAICS (North American Industrial Classification System), divides 20 types of industries (business) called "business sectors" [45][46], with 99 sub-sectors [47]using: Goods Producing Industry and Service Provider Industries.

The Kingdom of Malaysia developed the NIST CSF for the "Public Sector Cyber Safety Framework" (RAKKSSA) as shown in figure 3. This cybersecurity framework is a guideline for ministries and public sector agencies to obtain information in their cyberspace [48]. The eight main components of the RAKKSSA are: 1~Identify, 2~Protect, 3~Detect, 4~Respond, 5~Recover, 6~Procurement, 7~Security Audit, and 8~Enforce.

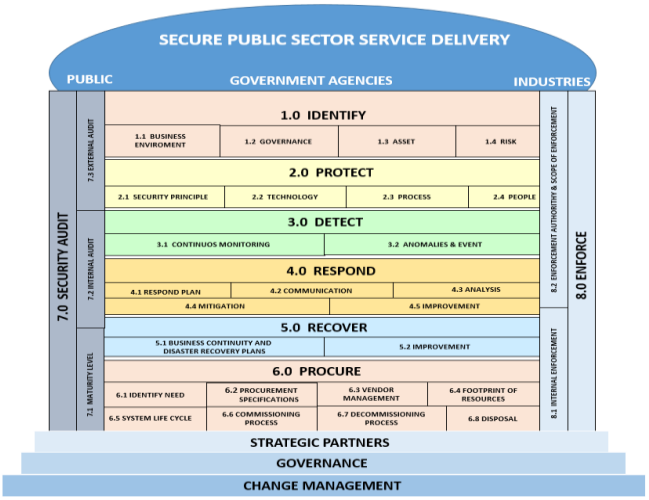

Fig 3. Cyber Security Framework for Public Sector (RAKKSSA) Malaysia[48]

This CSF specifically explains how to store confidential information and references made to the Head of the Government Security Office (CGSO) related to the classification, handling,

March - April 2020
ISSN: 0193-4120 Page No. 10900 - 10916

manufacturing, storage, handling or destruction of information. Not important from this CSF is the basic principle of proper and correct security, based on facts and risks.

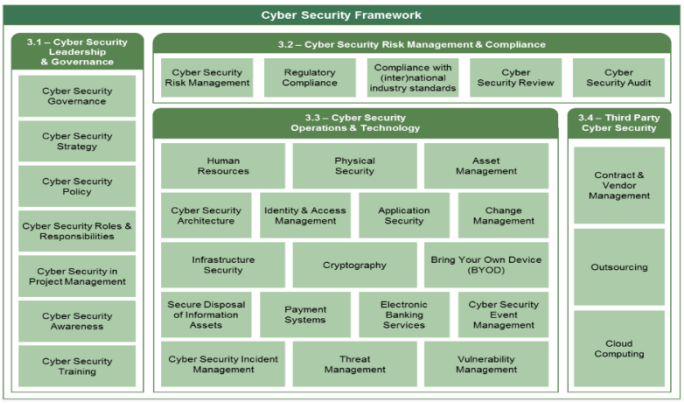

Fig 4. SAMA Cyber Security Framework [49]

The Kingdom of Saudi Arabia for the banking and financial sector also developed the SAME Cyber Security Framework (figure 4) based on industry-standard frameworks such as CSF NIST, PCI DSS, ISO 27001/27002, ISF SoGP for Information Security, and Basel II "International Convergence of Capital Measurement and Capital Standards." The SAME Cyber Security Framework is structured around 4 (four) main domains: 1) Cyber Security Leadership and Governance; 2) Cyber Security Risk Management and Compliance; 3) Cyber Security Operations and Technology; and 4)Third-Party Cyber Security [49].

The Cisco Cybersecurity Management Framework in Figure 5 is part of the Cisco Cybersecurity Management Program. The Cisco CMF design assumes that cybersecurity management is part of the business function. There are some similarities and differences between this standard Cisco CMF framework & several other CS frameworks.

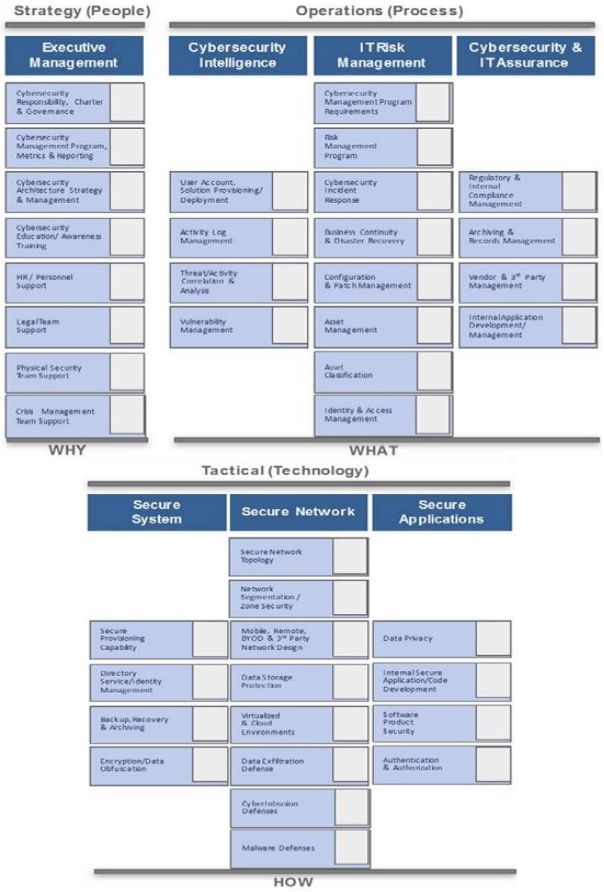

Fig 5. Cisco Cybersecurity Management Framework

The Cisco cybersecurity management framework is universal, can be used for states, industries, or countries. The Cisco CMF consists of three separate pillars: strategy, operation, and tactical (technology). Each layer is devoted to the control of a problem, the underlying problem is at the lower layer, and there is a more strategic problem at the upper layer (Cisco, 2017).

III. Research Method

To getenough literature about cybersecurity domains, literature searches are conducted from January 2018 toJune 2019, using search engines on the web. Search requests with the word cyber security (withoutdoublequotationmarks) or "cyber security" (with doublequotationmarks), or cybersecurity, or "cybersecurity," or cyber security domains, or cybersecurity domains.

The methodology for developing cybersecurity domains is as follows: The initial stages of the main domain of cybersecurity are identified and analyzed. Next, determine the cybersecurity category. The author tries to find the correlation between one domain with another in the context of cybersecurity. Next, develop this domain into several sub-domains according to the current reference, needs, and development of cybersecurity. Finally, map sub-domains into cybersecurity domain classes.

Author also tries to find references from images of the more specific and detailed cybersecurity domain mind-maps from search engines on the web. The categories or domains are organized both hierarchically and associatively to describe the relationship between the main subject "cybersecurity" and the categories that are in it and then make cybersecurity domain mind-maps based on the results of analysis and design sketches made by the previous author.

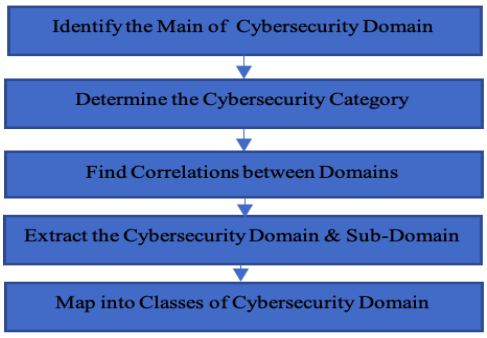

Fig 6. Research Flow & Domain Classification Method

The author also tests and interprets the results. Testing the cybersecurity domain prototype through a series of cyber event observations in the past two years, and is used to explore the relationships and connections between events & the domains in them. The contributions of this review paper are tables of the cybersecurity domain for private/public sector and public knowledge, as a reference for organisations and the public to understand cybersecurity broadly. Can be used directly or developed by private organisations/businesses, or individual government institutions tailored to business processes or rules or institutional needs.

IV. Result and Discussion

The author observes that the seven domains from "The Map of Cybersecurity Domains (version 2.0)" such as security architecture, security operations, governance, risk assessment, threat intelligence, physical security, and user education can be categorised as the primary domain because included in all cybersecurity framework domain references. Two other domains (Career Development, and Framework & Standards) are cybersecurity knowledge domains that need to be known to the public, including private/public organisations or businesses in implementing cybersecurity in organisations.

Private/pubic sector (organisations/businesses) need to consider the use of a cybersecurity framework to be implemented in their organisations/businesses to protect their current systems and operations. Given the use of information technology (IT) has been very massive. The use of computers, mobile phones or bring your own devices connected to the internet has become a necessity in the current 4.0 industrial revolution era.

Recent developments in information technology have triggered an increase in the number of cyber threats, and an increase in the need for the implementation of cybersecurity in various sectors of human activity, organisation/business, government to industry. The cybersecurity domain develops following current developments in IT.

After studying and comparing various definitions of cybersecurity, and several types of cybersecurity domains, the author tries to rearrange cybersecurity domains from multiple sources, to design a new Cybersecurity Domain in Tables 3.

The author tries to develop cybersecurity domains from 9 domains that existed previously in "The Map

of Cybersecurity Domains (version 2.0)", combined with the RAKKSSA framework, the Saudi Arabian Monetary Authority Cybersecurity Framework, and the Cisco Cybersecurity Management Framework.

Table 3. Cybersecurity Domains for Organization/Business or Public Sector Service

Operations & Technology • Human Resources/Security Career Development • Change Management • Threat Management • Asset Management • Vulnerability Management • Identity & Access Management • SIEM • SOC • Secure Disposal of Information Assets • Bring Your Own Device Protection • Cybersecurity & IT Architecture • Physical Security • Application Security • Infrastructure Security • Secure Payment Systems • Identification • Protection • Detection • Response • Recovery • Active Defense • Data Leakage
Risk Management & Compliance • Security Model • The triad of information security (CIA) implement • Business continuity planning • Procedures, and guidelines • Framework & Standards • Law, regulations and compliance • Threat modeling • Stakeholder Engagement • Perform Specialized Risk Activities • Risk Monitoring and Reporting • Risk Strategy and Planning • Risk Process Facilitation
Leadership & Governance • Governance • Strategy • Policy • Role & Responsibilities • Project Management • Awareness • Training
Risk Assessment • Vulnerability Scan • Assets Inventory • Data-Centric • Source Code Scan • Penetration Test • Risk Identification • Risk Analysis • Treatment Planning • Monitoring • Communication
Secure System Implementation • Cryptography • Network Security Design • Data Protection • Cloud Security • Access Control / Firewall • Security Architecture • Secure Application Development • Secure Databases • Secure Connection
Threat • Physical/Psychic Attack • Disaster • Nefarious Activity/Abuse • Outage • Failures/Malfunctions • Unintentional Damage/Loss (IT assets) • Legal • Unintentional Damages (Accidental) • Eavesdropping/Hijacking/Interception
Threat Intelligence • Tactical • Operational • Strategic • People • Process • DRM (Digital Rights Management)
Incident Handling 1. Identification 2. Recording 3. Incident Response 4. Communicating the Incident 5. Containment 6. Formulating a Response Strategy 7. Incident Classification 8. Incident Investigation 9. Forensic Analysis 10. Data Collection 11. Evidence Protection 12. Notify External Agencies 13. Eradication 14. Systems Recovery 15. Incident Documentation 16. Incident Damage and Cost Assessment 17. Review and Update the security policies, plan and procedures
Cyber Resilience • Risk Management • Asset Management • Controls Management

March - April 2020
ISSN: 0193-4120 Page No. 10900 - 10916

- Incident Management
- Situational Awareness
- Training and Awareness
- Vulnerability Management
- Service Continuity Management
- External Dependency Management
- Configuration and Change Management

Cyber Resilience Approach

- Govern & assure
- Identify & detect
- Manage & protect
- Respond & recover

Asset Management

- Asset Protection (Asset Security)
- Asset and Information classification
- Appropriate Retention
- Data Security Control
- Privacy Protection
- Ownership
  - Personal/People
  - Organizational
- Intangible Assets Management
- Tangible Assets Management

Procurement Service

- Identify need
- Specification
- Vendor Management
- Footprint of Resources
- System Life Cycle
- Commissioning Process
- Decommissioning Process
- Disposal

Security Audit

- Maturity Level
- Internal Audit
- External Audit

NIST-CSF for Secure Private & Public Sector Service

- Identity
- Protect
- Detect
- Respond
- Recover

Third Party

- Strategic Partner
- Outsourcing
- Cloud Computing Service
- Expertise
- Risk Transfer (collaboration)
- Pen tester/Security Analyzer
- Security Designer (consultancy)

Enforcement

- Internal Enforcement
- Enforcement Authority
- Enforcement Scope
- Enforcement Goals and Objectives

At present, the general public also needs to understand the domains contained in cybersecurity to increase knowledge and awareness. An instructor or educator can use mind mapping techniques to map learning material to be more easily understood and structured. The author tries to map matters related to cybersecurity and group them into 12 categories or domains for reference to public knowledge, as shown in Figure 7.

Furthermore, the authors develop each domain into sub-domains which will explain in more detail the matters relating to these domains.

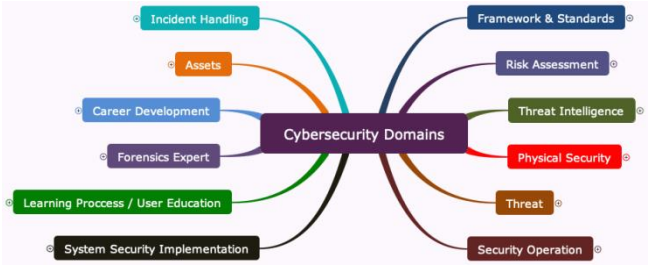

Fig 7. Cybersecurity Domains for Public Knowledge

Framework & Standards cybersecurity in Figure 7, has sub-domain: NIST CSF, NIST SPs 800-53 & 800-17, COBIT 5, COSO, CSA CCM, NERC CSS-CIP, TY CYBER, TY CYBER HITRUST CSF, PAS 555 (BSI), BS 7799-3 (BSI), Standards of Good Practice (SoGP), ISO/IEC 27001/27002 Standards, ISO/IEC 27032 Standard, CIS Critical Security Controls (SANS), Local Regulations Standards, and Industry-Specific Standards.

Each sub-domain in Framework & Standards has sub-sub-domains which are the scope of control of each standard.

Risk Assessment has sub-domains: Vulnerability Scan, Assets Inventory, 3rd Party Risk, Data-Centric, Source Code Scan, Penetration Test, Security Scanning, Risk Identification, Risk Analysis, Treatment Planning, Monitoring, and Communication.More detailed sub-domains are as shown in the next Figure 8.

March - April 2020
ISSN: 0193-4120 Page No. 10900 - 10916

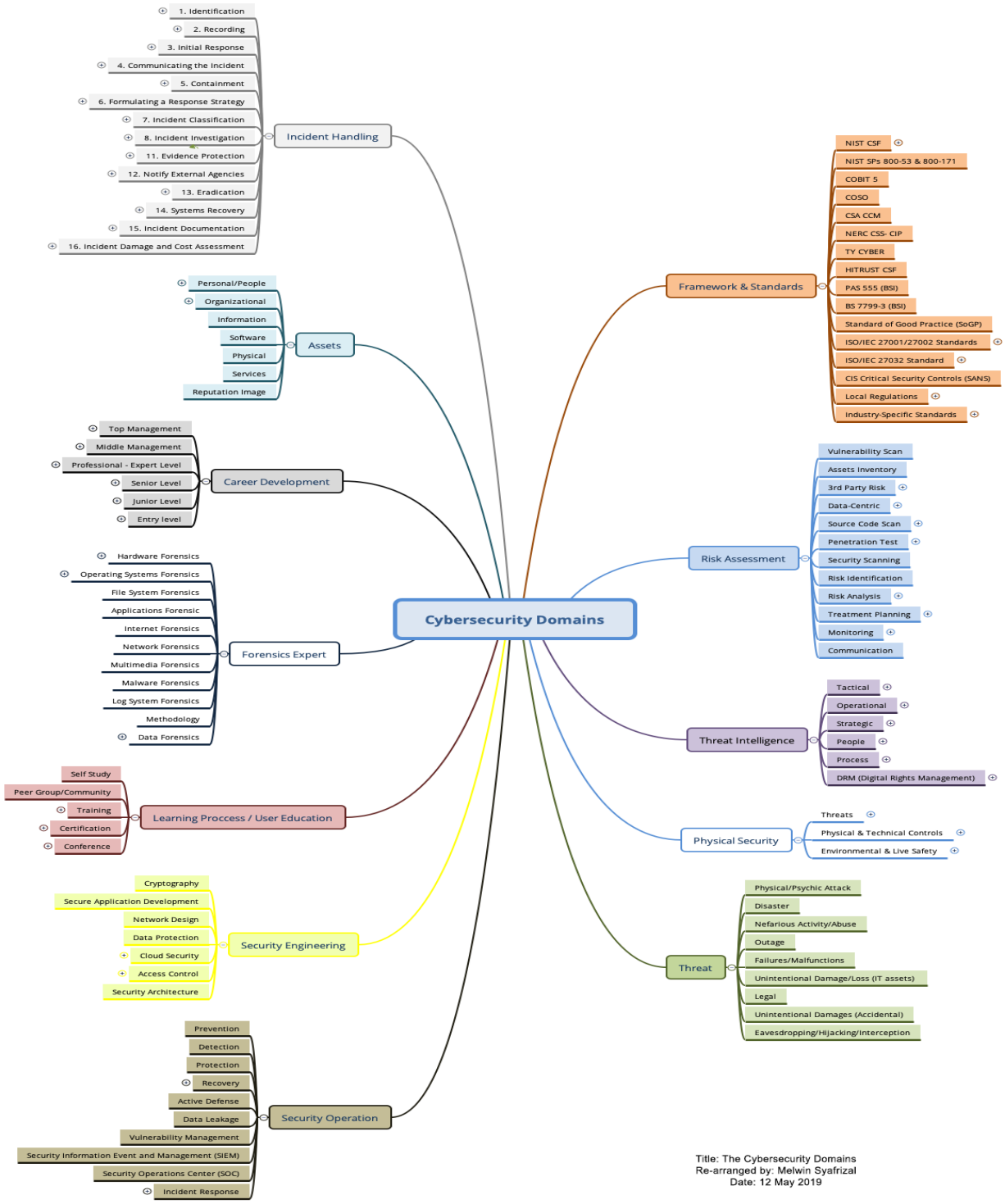

Fig 8. The Cybersecurity Domain by Melwin

Each sub-domain in Figure 8 has sub-domains and sub-sub-sub-domains up to 5 levels. But in this paper images can only be presented up to sub-domain level 2, because the image file size is too large.

Threat Intelligence domain has sub-domain: Tactical, Operational, Strategic, People, Process, DRM (Digital Rights Management).Physical Security domain has sub-domains: Threats, Physical & Technical Controls, Environmental & Live Safety.

Each sub-domain has sub-sub-domains as follows:

- Threats
  - Confidentiality

- Integrity
- Availability

- Physical & Technical Controls
  - Physical Controls
    - Guard
    - Dogs
    - Fencing
    - Lighting
    - Locks
    - CCTV
  - Facility Access Control Devices
    - Motion detectors
      - Alarms
      - Data Destruction
      - Technical Controls
      - Administrative Controls
      - Requirements planning (Choosing a secure site, Walls, Ceilings, Floors, Windows, Doors, Sprinkler System, Liquid and Gas lines, Air Con, Electrical requirements, Audit trails)
      - Security Management (Emergency Procedures)
      - Personal Controls
    - Site Access Controls
- Environmental & Live Safety
  - Electrical Power
    - Line Conditioner
    - UPS
    - Power Generator
    - Blackouts
    - Brownout
    - Dropout
    - Sag
    - Surge
    - Transient
    - Device/Equipment protection
    - Damage Protection
      - Disaster/Hazards (Natural, Man-made hazard, Environmental, Technological)
      - Fire detection, protection & suppression (Fire Protection)
      - Heating Ventilation and Air Conditioning (HVAC)
      - Humidity
      - Redundant Controls (Dual electric power feeds, Redundant generators, Redundant UPS Systems)
      - Theft Protection

The threat domain has sub-domains: PhysicalAttack, Disaster, Nefarious Activity/Abuse, Outage,Failures/Malfunctions, Unintentional Damage/Loss (IT assets), Legal, Unintentional Damages (Accidental), Eavesdropping/Hijacking/Interception.Moredetail-ed information (sub-domains) of threat domains will be discussed in the next paper.

Security operation domainhas sub-domain: Prevention, Detection, Protection, Recovery (Disaster Recovery & Business Continuity Plan), Active Defense, Data Leakage, Vulnerability Management, Security Information Event and Management (SIEM), Security Operations Center (SOC), Incident Response (breach notification ability, containment, eradication, investigation, & forensics).

Incident Handling Domain has seventeen sub-domain: 1. identification, 2. recording, 3. initial response, 4. communicating the incident, 5. containment, 6. Formulating a response strategy, 7. incident classification, 8. incident investigation, 9. data collection, 10. forensic analysis, 11. Evidence protection, 12. notify external agencies, 13. Eradication, 14. systems recovery, 15. incident documentation, 16. incident damage and cost assessment, 17. review and update the security policies, plan and procedures.

Assets domain in has few sub-domain: Asset Protection (Asset Security), Asset Management, Asset and Information classification, Appropriate retention, Data Security Control, Privacy Protection, Ownership (personal/people or organizational), Intangible Assets, Tangible Assets.

Career Development Domain has few sub-domain and sub-sub-domains, among others:

March - April 2020
ISSN: 0193-4120 Page No. 10900 - 10916

- *Top Management level*: Chief Information Security Officer (CISO), Chief Cyber Security Officer (CCSO), Chief Compliance Officer (CCO), Chief Security Officer (CSO), Chief Privacy Officer (CPO), Chief Risk Officer (CRO), System Director, Director of Security, Information Security Director, Cyber Security Executive Director, Safety & Security Program Director, Global Information Security Director, Sarbanes-Oxley (SOX) Compliance Director, VP Cyber Security & Compliance, Vice President-Global GRC (Governance, Risk and Compliance) Cyber Security Risk Management.
- *Middle Management level*: Executive Cyber Leadership, Cybersecurity Manager, Network Security Manager, Security Manager, Information Security Managers, Advisory Risk Cyber Security, Cybersecurity Senior Manager, Cyber Security Defense Operations Manager, Cyber Security Sales Executive, Cyber Security Account Executive, Data Security Sales Executive, Cyber Security Territory Account Executive.
- *Professional-Expert Level*: Information Systems Security Professional, IT Cybersecurity Specialist (INFOSEC), Lead Software Security Engineers, Senior Cybersecurity Specialist, Information Security Specialists, Cybersecurity Consultants, Network Security Analysts, Vulnerability Assessor, IT Security Auditors, Penetration Tester, Security Architect, Cybersecurity Analyst, Security Code Auditor, Information Security Analysts, Counterespionage analyst, Cryptographic Vulnerability Analyst, Cryptographer/Key Management Expert, Expert Vulnerability Assessment Analyst.
- *Senior Level*: Security Control Assessor, Senior Data Engineer, IT Quality Assurance, IT Quality Measurement Analyst, Cyber Hunt Threat Analyst, Cyber Instructor, Threat Analyst, Cryptanalyst, IT Auditor, Malware analyst, Exploitation Analyst, Cyber Crime Investigator, Cyber Defense Forensics Analyst, IT Security Management Supervisor, IT Security Management Coordinator, Safety and Security Program Supervision, Cyber Instructional Curriculum Developer, Cyber Defense Infrastructure Support Specialist.
- *Junior Level*: Jr. Cyber Security Analyst - Clearable Secret Level, Jr. Cybersecurity Support Specialist, Cyber security Integrator/Engineers, Information Assurance Engineers, IT Specialist (Network/Sysadmin), IT Security Management Clerk, Security Software Developers, Network Security Admins, Network Analyst Junior, IT Specialist (INFOSEC), Incident Responder, Cryptographer, Junior Data Engineer, Applied Cryptography Engineer, Junior Cyber Security Engineer, Junior Network Security Engineer, Technical Support Specialist, Cyber Defense Analyst, Cyber Intel Planner, Cyber Ops Planner, Bug Bounty Hunter, Cyber Defense Incident Responder, Jr Expert Vulnerability Assessment Analyst.
- *Entry level:* Network Administrator, Security Administrator, Network & Cloud Engineer, IT Security Management Staff, Network Operations Specialist.

Forensics Expert Domain in Figure 17 has few sub-domains: Hardware Forensics, Operating Systems Forensics, File System Forensics, Applications Forensic, Internet Forensics, Network Forensics, Multimedia Forensics, Malware Forensics, Log System Forensics, Methodology, Data Forensics.

Learning Process/User Education in Figure 18 describes sub-domains related to sources of information/learning cybersecurity material to understand knowledge and gain expertise, through:

- Self-study
- Peer-group/Community
- Training
  - Classical
  - Online
- Certification
  - Local Academy/Training Institution
  - National (Regional)
  - International
  - Professional Certification Institution
- Conference
  - Regional
  - International
  - Organization/Institution

System Security Implementation domain has sub-domain: System Security Roadmap, Cryptography, Secure Network Design, Firewall & Access Control, Security Architecture, Software Security, Application Security, Database Security, Web Security, Mobile Apps Security, Data Protection, & Cloud Security.

V. Conclusion and Future Works

The domain of cybersecurity wasinitiallyverylimitedtospecificareas according toorganisational references or adjustedto the operational requirements or company assets security need. However, the growth of information technology has increased the number of cybersecurity and the demand for cybersecurity or security in varioussectors of human activities, nonprofit organisationstoindustry.

Cybersecurity domain developed by the author, release Cybersecurity Domains for Organizations/Business or Public Sector Services and Cybersecurity Domains for Public Knowledge. In Cybersecurity Domains for Organizations/Businesses or Public Sector Services are the domains: Operation and Technology; Risk Management &Compliance; Leadership& Government; Security Audit; Risk management; Risky tasks; Handling of Incidents; Safe System Implementation; Threat; and Threat Intelligence; NIST-CSF for Secure Private/Public Sector Services; Asset Management; Implementation; Third-party; Virtual Resilience; Procurement Services; and the Cyber Resilience Approach.

The Cyber Security Domain for Public Knowledge has the following domains: Framework& Standards; Risk Assessment; Threat Intelligence; Physical Security; Threat; Security Operations; Incident Handling; Asset; Career Development; ForensicExpert; LearningProcess/User Education; System Security Implementation.

Sub-domains of these domains are a more detailed description of the main domain. Business/organisations and the public can more easily understand the relationship between the main domain with sub-domains, and sub-domains by looking for definitions and further references.

The more in-depth the user'sknowledge of a domain, the more it will be easier for users to understand related problems, and find solutions to these problems.For the public, students, and users of public networks or the internet, this information can be a reference toraise awareness, and understand mattersrelatingto cybersecurity and cyber threatswhilesurfing the web.

The results of this study still need to be developed by researchers by classifying cybersecurity domains (cybersecuritytaxonomy) for specific organisations/businesses/government institutions.

Need to make a more detailed description to explain the definition of domains and relationships between domains and sub-domains, so that it becomes the body of knowledge cybersecurity.

REFERENCES

[1] D. Craigen, N. Diakun-Thibault, and R. Purse, “Defining cyber-security,” *Technol. Innov. Manag. Rev.*, no. October, pp. 13–21, 2014.

[2] ACM, “Cybersecurity Curricula 2017,” 2017.

[3] R. Von Solms and J. Van Niekerk, “From Information Security to Cyber Security,” *Comput. Secur.*, vol. 38, pp. 97–102, 2013.

[4] PwC, “Cybersecurity and Business Continuity Management,” 2016.

[5] ISO/IEC27032, “ISO/IEC 27032:2012(en) Information technology — Security techniques — Guidelines for cybersecurity,” *ISO*, 2012. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en.

[6] A. Supriyanto, J. E. Istiyanto, and K. Mustofa, “Multi-layer Framework for Security and Privacy Based Risk Evaluation on E-Government,” *J. Theor. Appl. Inf. Technol.*, vol. 97, no. 5, pp. 1423–1433, 2019.

[7] ISO/IEC27005, “ISO/IEC 27005:2018(en)

Information technology-Security techniques-Information security risk management," *ISO*, 2018.[Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en.[Accessed: 21-Apr-2019].

[8] P. Eric Lachapelle and P. Mustafe Bislimi, "ISO 27001 Information Technology – Security Techniques Information Security – Management Systems - Requirements," 2015.

[9] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behav. Inf. Technol.*, vol. 33, no. 3, pp. 236–247, 2014.

[10] W. Rocha Flores, E. Antonsen, and M. Ekstedt, "Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture," *Comput. Secur.*, vol. 43, pp. 90–110, 2014.

[11] N. Sohrabi Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," *Comput. Secur.*, vol. 56, pp. 1–13, 2016.

[12] S. Furnell and I. Vasileiou, "Security education and awareness: just let them burn?," *Netw. Secur.*, vol. 2017, no. 12, pp. 5–9, 2017.

[13] CNSS, "Committee on National Security Systems (CNSS) Glossary," 2015.

[14] S. Hurttila, "From Information Security to Cyber Security Managent – ISO 27001 & 27032 Approach," Tallinn University of Technology, 2018.

[15] K. Thakur, M. Qiu, K. Gai, and L. Ali, "An Investigation on Cyber Security Threats and Security Models," *2015 IEEE 2nd Int. Conf. Cyber Secur. Cloud Comput.*, pp. 307–311, 2015.

[16] J. Srinivas, A. Kumar, and N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations," *Futur. Gener. Comput. Syst.*, vol. 92, pp. 178–188, 2018.

[17] S.Van Till, "All security is now cybersecurity," in *The five technological forces disrupting security*, Elsevier Inc., 2018, pp. 97–106.

[18] ITU, "Series X: Data Networks, Open System Communications and Security Telecommunication Security : Overview of cybersecurity," 2008.

[19] G. J. Touhill and C. J. Tauhil, *Cybersecurity for Executives: a Practical Guide*. Canada: John Wiley & Sons, Inc., 2014.

[20] HM Government, "National Cyber Security Strategy 2016-2021," 2016.

[21] A. M. Rea-Guaman, I. D. Sanchez-Garcia, T. S. Feliu, and J. A. Calvo-Manzano, "Maturity Models in Cybersecurity: a systematic review," *Iber. Conf. Inf. Syst. Technol. Cist.*, p. 6, 2017.

[22] N. Lee, Counterterrorism and Cybersecurity - Total Information Awareness. New York: Springer Science_Business Media, 2015.

[23] ISACA, *Cybersecurity Fundamentals Study Guide 2015*. ISACA, 2015.

[24] R. Society, "Progress & Research in Cybersecurity - Supporting a Resilient and Trustworthy System for the UK," 2016.

[25] Akamai, "The Future of Government Cybersecurity - Research Brief," 2018.

[26] M. Alali, A. Almogren, M. M. Hassan, I. A. L. Rassan, and M. Z. A. Bhuiyan, "Improving Risk Assessment Model of Cyber Security Using Fuzzy Logic Inference System," *Comput. Secur.*, vol. 74, pp. 323–339, 2018.

[27] ITU-ABIresearch, "Global Cybersecurity Index & CyberWellness Profiles," 2015.

[28] R. Kuhlman and J. Kempf, "Report on Cybersecurity Practices," 2015.

[29] IIROC and OCRCVM, "Cybersecurity Best Practices Guide For IIROC Dealer Members," 2015.

[30] B. Saeed Alghamdi, M. Elnamaky, M. Amer Arafah, M. Alsabaan, and S. Haj Bakry, "A Context Establishment Framework for Cloud Computing Information Security Risk Management Based on the STOPE View," *Int. J. Netw.Secur.*, vol.21, no.1, pp.166–176, 2019.

March - April 2020
ISSN: 0193-4120 Page No. 10900 - 10916

[31] M. H. R. Al-Shaikhly, H. M. El-Bakry, and A. A. Saleh, "Cloud Security Using Markov Chain and Genetic Algorithm," *J. Electron. Inf. Eng.*, vol. 8, no. 2, pp. 96–106, 2018.

[32] I. A. Gheyas and A. E. Abdallah, "Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis," *Big Data Anal. Access*, vol. 1, no. 1, p. 6, 2016.

[33] D. Klaper and E. Hovy, "A Taxonomy and a Knowledge Portal for Cybersecurity," *Proc. 15th Annu. Int. Conf. Digit. Gov. Res. - dg.o '14*, pp. 79–85, 2014.

[34] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," 2018.

[35] S.-53Ar4 NIST, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations Assessing Security and Privacy Controls in Federal Information Systems and Organizations," Gaithersburg, MD, 2014.

[36] C. NERC, "NERC Cyber Security Standards , CIP-002-1 through," 2006.

[37] ISO/IEC27001, "ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements," *ISO/IEC 27001:2013(en) Information technology — Security techniques — Information security management systems — Requirements*, 2013. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en. [Accessed: 21-Apr-2019].

[38] G. Ataya, "PCI DSS Audit and Compliance," *Inf. Secur. Tech. Rep.*, vol. 15, no. 4, pp. 138–144, 2011.

[39] T. Takahashi, Y. Kadobyashi, and H. Fujiwara, "Ontological Approach toward Cybersecurity in Cloud Computing Categories and Subject Descriptors," *Sci. Technol.*, pp. 100–109, 2010.

[40] Z. A. Collier, I. Linkov, and J. H. Lambert, "Four domains of cybersecurity: A risk-based systems approach to cyber decisions," *Environ. Syst. Decis.*, vol. 33, no. 4, pp. 469–470, 2013.

[41] H. Jiang, "The Map of Cybersecurity Domains (version 2.0)," *Linked In*, 2017. [Online]. Available: https://www.linkedin.com/pulse/map-cybersecurity-domains-version-20-henry-jiang-ciso-cissp/. [Accessed: 21-Apr-2019].

[42] C.S. Alliance *et al.*, "Cloud Security Alliance Cloud Controls Matrix (CSA-CCM) 3.0.1," 2018.

[43] Deloitte,"A Deloitte Practical Guide For ISO27032-Guidelines for Cybersecurity," 2012.

[44] T. A. Kirchner, J. B. Ford, J. Lindenmeier, B. Lowe, B. Mcdonald, and G. S. Mort, "Finding New Ways to Engage and Satisfy Global Customers," *Proc. Acad. Mark. Sci. Springer, Cham*, no. 02 April, pp. 23–24, 2019.

[45] J. M. Pierre, "On the Automated Classification of Web Sites," *Link¨oping Electron. Artic. Comput. Inf. Sci.*, vol. 6, no. 0, 2001.

[46] J. H. Carr and K. B. Anacker, "Microbusinesses in the United States : Characteristics and Sector Participation," 2013.

[47] Dennis Fixler, E. T. Morgan, J. William G. Bostic, J. B. Murphy, D. Talan, and P. Bugg, "North American Classification System," 2017.

[48] C. MAMPU, MIMOS, CGSO, "Rangka Kerja Keselamatan Siber Sektor Awam," 2016.

[49] SAMA, "Cyber Security Framework Saudi Arabian Monetary Authority," 2017.