Comparative Study of a Cybersecurity Curriculum To Support Digital Transformation in The Public Sector

Dhoni Kurniawan

Policy Analyst, National Cyber and Crypto Agency, Jakarta (Email: dhoni.kurniawan@bssn.go.id**)**

Ratih Mumpuni Arti[2]

Policy Analyst, ,National Cyber and Crypto Agency, Jakarta (Email: ratih.mumpuni@bssn.go.id)

Abstract

The Covid 19 pandemic that has occurred in all parts of the world since early 2020 has forced all humans to follow digital transformation. This momentum is considered good for the acceleration of digital transformation, which since the issuance of Presidential Decree Number 95 of 2018 has begun to be initiated. Digital transformation marks a radical rethinking of how an organization uses technology, people and processes to fundamentally change business performance. Digital transformation occurs in the economic, social and public sphere with the aim of creating innovation, encouraging inclusiveness and increasing efficiency and productivity. Although it is absolutely related to digital technology, digital transformation is not just technology but also takes into account other elements such as infrastructure, policies, leadership, digital literacy, mindset, data, research and cybersecurity. Cybersecurity is a crucial prerequisite because interconnection in the digital world demands data privacy and information security. In fact, the demands of cybersecurity in digital transformation are not matched by human resources who are experts in the cyber field. APTIKOM states that each year in Indonesia it only manages to produce 40 thousand - 50 thousand bachelors of information technology competence, while the need is predicted to reach 600 thousand people per year. At the higher education level, the curriculum in cybersecurity study programs tends to focus on technical areas only. Even though. Cybersecurity is a complex matter that requires a multidisciplinary approach such as experts in regulation and policy, governance and information security risk management, and so on.

This research is a qualitative descriptive study. The author uses a comparative method to compare the cybersecurity curriculum in Indonesia with the Netherlands, which has a multi-disciplinary cybersecurity curriculum. So that we get multidisciplinary curriculum recommendations that can be applied in the cybersecurity curriculum in Indonesia.

Keywords:

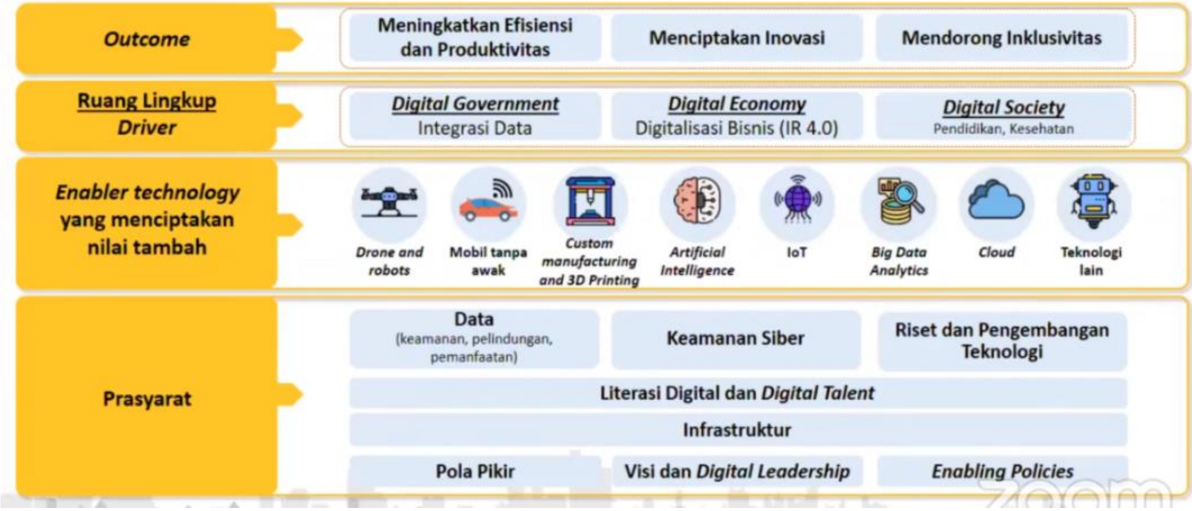
digital transformation; covid 19 pandemic; cyber security; curriculum

Introduction

Digital transformation is sweeping the modern world of business as organizations become increasingly cloud-based, automated and global. Digital transformation marks a radical rethinking of how an organization uses technology, people and processes to fundamentally change business performance, says George Westerman, MIT principal research scientist and author of Leading Digital: Turning Technology Into Business Transformation. Digital transformation requires cross-departmental collaboration in pairing business-focused philosophies with rapid application development models.

It is undeniable that now Indonesia is moving towards digital, almost as a whole several sectors have started to carry out digital transformation. Indonesia's achievements in 2019 have been very good, especially in the digital economy. This means that in business terms, Indonesia is already on the right step. However, not only in the business sector, digital transformation is also carried out by the government as an effort to improve the performance of the quality of service to the community. The Concept of Digital Transformation Framework in Indonesia can be senn in the following figure.

Figure 1.
Concept of Digital Transformation Framework



Outcome

Meningkatkan Efisiensi dan Produktivitas

Menciptakan Inovasi

Mendorong Inklusivitas

Ruang Lingkup Driver

Digital Government Integrasi Data

Digital Economy Digitalisasi Bisnis (IR 4.0)

Digital Society Pendidikan, Kesehatan

Enabler technology yang menciptakan nilai tambah

Prasyarat

Data (keamanan, pelindungan, pemanfaatan)

Keamanan Siber

Riset dan Pengembangan Teknologi

Literasi Digital dan *Digital Talent*

Infrastruktur

Pola Pikir

Visi dan *Digital Leadership*

Enabling Policies

Source: Ministry of National Development Planning

The Indonesian government has issued Presidential Regulation Number 95 of 2018 concerning Electronic-Based Government Systems (SPBE) as the basis for implementing government that utilizes information and communication technology to provide services to SPBE users. The aim is to achieve clean, effective, efficient, transparent and accountable governance and to improve efficiency and integration of SPBE administration. With this Presidential Regulation, it is hoped that there will be an impetus for digital transformation, especially in the public sector.

There are five strategies that are being carried out by the Indonesian government in accelerating digital transformation. **First,** underlying the strategy with regulations and policies. What must be done is to continue to improve and align regulations with digital developments, align local regulations, involve stakeholders and carry out data-based decision processes. **Second**, develop human resource capabilities and open opportunities for future intelligence and talents. Forge partnerships with the private sector to assess and develop digital skills. Designing curricula and adapting to digital data and technology as well as building edtech platforms and workforce information platforms. **Third,** building infrastructure and mastering technology by expanding access and infrastructure development is carried out to achieve the target of internet services in 12,500 villages / kelurahan that have not been reached by the internet. Completion of the necessary supporting technology, such as the construction of a national data center. **Fourth,** accelerating initiatives with funding and incentives by supporting technology adoption from all sectors, establishing digital funding mechanisms for all ministries / agencies and properly allocating government spending for digital initiatives. **Fifth,** fostering a digital ecosystem by encouraging partnerships and integrating stakeholders to encourage inclusion, building an ecosystem that supports industry needs, international collaboration.

The pressure from the Covid-19 pandemic was felt in various areas of life, not only in economic life but also in social life. Large-scale Social Restrictions also provide the basis for working from home, learning from home and also worshiping from home. These social restrictions have the impact of accelerating digital transformation, which in fact the jargon of transformation has been echoed for several years or has been around for a long time, but still the logic of the old way of working still dominates. With the existence of Covid 19, it forces us to adjust various kinds of jobs. So, the topic of digital transformation is not an option but a necessity.

Services that are fast, easy, affordable, and of quality are an obligation that must be done by the government to the community. To achieve this, it is necessary to transform public services to digital to accelerate and facilitate services. Digitalization of public services is a necessity in an effort to increase transparency and improve the quality of services to the community, especially in the conditions of the Covid-19 pandemic. There are many preparations that must be done in this digital transformation, especially governance, such as preparing virtual meetings, virtual meetings and new rules that keep one's personal data and work confidentiality guaranteed. By continuing to produce work procedures that are more effective and efficient than before, the digital transformation of the bureaucracy can drive productivity and the confidentiality of our work is guaranteed.

The demand for personal data security guarantees as well as information security at work makes cybersecurity the foundation and enabler of digital transformation in Indonesia. These opportunities are comparable to the increasingly diverse and increasing threat of cyber attacks. The National Cyber Security Operations Center (Pusopkamsinas) of the National Cyber and Crypto Agency (BSSN) managed to detect 149,783,617 cyber attacks that occurred in Indonesia in the first half of 2020. When compared to cyber attacks that occurred in the first semester of 2019, the number of attacks in this has increased fivefold. The higher level of connectivity, accompanied by the use of massive digitalization, is one of the driving factors that have led to the high number of cyber attacks.

Without cyber security, Indonesia's digital transformation process will certainly be disrupted. Indonesia is estimated to have been ranked third as the target of cyber attack threats after the US and India. According to the 2020 State of Application Services (SOAS) Report, one of the triggers is the gap in security experts which not only occurs in Indonesia, but is one of the main concerns in the Asia Pacific. More than 76 percent of companies across the Asia Pacific report a high gap in security expertise.

Indonesia is projected to have a shortage of experts and semi-experts in the field of information technology of 600,000 people per year. The projection is based on McKinsey's data which states that Indonesia will experience a gap of 9 million digital talents by 2030. According to the Association of Informatics and Computer Science Colleges (APTIKOM), each year there are only 40-50 thousand informatics scholars from 850 campuses throughout Indonesia. Furthermore, according to APTIKOM, there are very few universities that have study programs related to information security / cybersecurity, namely only 22 universities that have cybersecurity study programs and almost all of them are in Java. List of Study Program Names in Higher Education related to cybersecurity are described on table 1 below:

Table 1.
List of Study Program Names related to Cybersecurity

Academic Program	Vocational Program
Bachelor/Master/Doctoral :	**Associate Graduate :**
1. Information System	1. Information System
2. Information Technology	2. Information Technology
3. Information System and Technology	**Bachelor :**
	1. Information System Security
	2. Immigration Information System Security
	3. Cyber security engineering
	Master :
	Digital Forensic and Cybersecurity

Source: Decree of the Director General of Learning and Student Affairs Number 46/B/HK/ 2019

In order to achieve good governance based on the development of information and communication technology, competent human resources are needed in the application of SPBE as the most important and strategic asset in the organization. One of the fulfillment channels is through universities. In addition to the lack of quantity problems, it is felt that many of the digital talents of college graduates are not ready to enter the world of work.

The issue of human resource digital talents who are not ready to enter the world of work is material for introspection for universities. Is it true that the profile of college graduates who teach cybersecurity is in accordance with the needs of the job? Until now, all universities that teach cybersecurity still use a curriculum that focuses only on technical fields. Meanwhile, non-technical fields have not yet become the focus. Even though the need for cybersecurity work is not only doing things that are technical in nature. Things such as the formulation of regulations and policies, public management, leadership, even fields such as economics and psychology are also important.

Cybersecurity curriculum reform in higher education is absolutely necessary. Making comparisons and then adopting from cybersecurity curricula in other countries that already understand that cybersecurity requires a multidisciplinary approach can be one way to accelerate the implementation of cybersecurity curriculum reform.

Methods

The research method is the method used by researchers in collecting research data. By applying appropriate research methods, well-structured facts and theories will be produced, by formulating objectively, rationally and systematically the symptoms contained in an object. This study aims to describe the factual and accurate reality of the cybersecurity curriculum in higher education. Therefore, this study uses a qualitative approach. Qualitative research method is a research method used to examine the condition of natural objects, where the researcher is the key instrument, the data collection technique is done by triangulation, data analysis is inductive and the results of qualitative research emphasize meaning rather than generalization.

The data collection technique is done by using the literature / documentation study method. The documentation method is looking for data or things or variables in the form of notes, transcripts, books, newspapers, magazines, inscriptions, meeting minutes, agendas. In this study, the documents examined were reports or regulations regarding cybersecurity curricula in Indonesia and other countries.

The first step, review, compared and analyzed the curriculum that already exist in Indonesia and Netherland. The second step is to review the curriculum guide issued by NIST and Cybersecurity Occupational Map. The third step is to conduct a comparative analysis between the guidance and the curriculum of Cyber security in Indonesia. So we can find a comprehensive cybersecurity curriculum posture that is suitable for application in Indonesia.

Results and Discussion

In the Results and Discussion section, the author will present the results of a literature study which is divided into 3 sessions. The first session describes the guidelines for cyber security curriculum formulation published by NIST and published by NCCA Indonesia. In the second session, it will explain the curriculum of cybersecurity study programs in Indonesia and as a comparison for cybersecurity study programs in the Netherlands. In the third session, the author make comparisons to get curriculum recommendations that have a multidisciplinary approach and are in accordance with the guidelines as described in the first session.

A. The Guidelines for Cyber Security Curriculum

1. NIST Spesial Publication 80 – 181 : National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, is a partnership between government, academia, and the private sector that seeks to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our nation secure and economically competitive.

NICE is committed to cultivating an integrated cybersecurity workforce that is globally competitive from hire to retire, prepared to protect our nation from existing and emerging cybersecurity challenges.

Throughout this document, the combined terms "cybersecurity workforce" is shorthand for a workforce with work roles that have an impact on an organization's ability to protect its data, systems, and operations. Included are new work roles that have been known traditionally as information technology (IT) security roles. Those roles have been added to this workforce framework to highlight their importance to the overall cybersecurity posture of an organization. Additionally, some of the work roles described herein include the shorter term cyber to be inclusive of sectors where cyber has become the conversational norm for this field.

A cybersecurity workforce includes not only technically focused staff, but also those who apply knowledge of cybersecurity when preparing their organization to successfully implement its mission. A knowledgeable and skilled cybersecurity workforce is needed to address cybersecurity risks within an organization's overall risk management process.

The NICE Framework provides a reference for educators to develop curriculum, certificate or degree programs, training programs, courses, seminars, and exercises or challenges that cover the KSAs and Tasks described in the NICE Framework. Human resource staffing specialists and guidance counselors can use the NICE Framework as a resource for career exploration.

The NICE Framework' identification of tasks in work roles allows educators to prepare learners with the specific KSAs from which they can demonstrate the ability to perform cybersecurity tasks. Academic institutions are a critical part of preparing and educating the cybersecurity workforce. Collaboration among public and private entities, such as through the NICE program, enables such institutions to determine common knowledge and abilities that are needed. In turn, developing and delivering curricula that are harmonized with the NICE Framework lexicon allows institutions to prepare students with the skills needed by employers. As the pipeline of students finding desired jobs in cybersecurity increases, more students will be attracted to academic cybersecurity programs as a pathway to a career.

Table 2 provides a description of each category described by NICE Framework. Each includes a two character abbreviation for quick reference of the category and to support the creation of NICE Framework work role identities.

Table 2.
NICE Framework Description

Categories	Specialty Areas	Decriptions
Securely Provision (SP): Conceptualizes, design, procures, and/or builds secure information technology (IT) system with responsibility for aspect of system and/or network development	Risk Management (RSK)	Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.
	Software Development (DEV)	Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives
	System Architecture (ARC)	Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology

Categories	Specialty Areas	Decriptions
		and environmental conditions (e.g., law and regulation) into system and security designs and processes.
	Technology R&D (TRD)	Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology and environmental conditions (e.g.,law and regulation) into system and security designs and processes.
	Systems Requirements Planning (SRP)	Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.
	Test and Evaluation (TST)	Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for costeffective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT
	Systems Development (SYS)	Works on the development phases of the systems development life cycle.
Operate and Maintain **(OM):** Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.	Data Administration (DTA)	Develops and administers databases and/or data management systems that allow for the storage, query, protection, and utilization of data.
	Knowledge Management (KMG)	Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
	Customer Service and Technical Support (STS)	Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
	Network Services (NET)	Installs, configures, tests, operates, maintains, and manages networks and their

Categories	Specialty Areas	Decriptions
		firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.
	Systems Administration (ADM)	Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.
	Systems Analysis (ANA)	Studies an organization's current computer systems and procedures, and designs information systems solutions to help the organization operate more securely, efficiently, and effectively. Brings business and information technology (IT) together by understanding the needs and limitations of both.
Oversee and Govern (OV): Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.	Legal Advice and Advocacy (LGA)	Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes, and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.
	Training, Education, and Awareness (TEA)	Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate.
	Cybersecurity Management (MGT)	Oversees the cybersecurity program of an information system or network, including managing information security implications within the organization, specific

Categories	Specialty Areas	Decriptions
		program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.
	Strategic Planning and Policy (SPP)	Develops policies and plans and/or advocates for changes in policy that support organizational cyberspace initiatives or required changes/enhancements.
	Executive Cyber Leadership (EXL)	Supervises, manages, and/or leads work and workers performing cyber and cyber-related and/or cyber operations work.
	Program/Project Management (PMA) and Acquisition	Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that use information technology (IT) (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life cycle.
Protect and Defend (PR): Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.	Cyber Defense Analysis (CDA)	Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network to protect information, information systems, and networks from threats
	Cyber Defense Infrastructure Support (INF)	Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the

Categories	Specialty Areas	Decriptions
		computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.
	Incident Response (CIR)	Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.
	Vulnerability Assessment and Management (VAM)	Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.
Analyze (AN): Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence	Threat Analysis (TWA)	Identifies and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.
	Exploitation Analysis (EXP)	Analyzes collected information to identify vulnerabilities and potential for exploitation.
	All-Source Analysis (ASA)	Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.

Categories	Specialty Areas	Decriptions
	Targets (TGT)	Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.
	Language Analysis (LNG)	Applies language, cultural, and technical expertise to support information collection, analysis, and other cybersecurity activities.
Collect and Operate (CO): Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence	Collection Operations (CLO)	Executes collection using appropriate strategies and within the priorities established through the collection management process
	Cyber Operational Planning (OPL)	Performs in-depth joint targeting and cybersecurity planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.
	Cyber Operations (OPS)	Performs activities to gather evidence on criminal or foreign intelligence entities to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.
Investigate **(IN):** Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.	Cyber Investigation (INV)	Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering

Categories	Specialty Areas	Decriptions
	Digital Forensics (FOR)	Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

Source : NIST Special Publication 80 - 181

2. The Cybersecurity Occupational Map – Indonesia

In order to create a cyber environment and implement a safe, reliable and reliable electronic system to advance and grow the digital economy by increasing cyber competitiveness and innovation, as well as building awareness and sensitivity to national security and resilience in cyberspace, the Indonesian government seeks to build the strength of Indonesian human resources. . Among them through the preparation of Occupational Maps and Work Competency Standards. In accordance with the management of HR competencies that have been formulated through the Manpower Law, Government Regulations relating to the establishment of the National Professional Certification Agency, the Minister of Manpower Regulation and the Minister of Communication and Information Technology Regulations have formulated the Occupational Map in the field of National Information and Communication Technology.

The Cybersecurity Occupational Map is prepared with the aim of providing clarity to the workforce, academia and industry regarding the definition of tasks, competencies, powers and careers in the Cybersecurity field. Occupational map is a document containing mapping of occupations in a field or sector based on competency standards, qualifications and national competency levels. The Cybersecurity Occupation Map is an inseparable part of the ICT National Occupation Map compiled in the Indonesian National Qualifications Framework (KKNI). The Occupation Map maps the various types of positions, occupations, and professions contained in the Cybersecurity sector.

To sharpen the analytical framework in identifying and formulating the occupation and competency of human resources for cybersecurity and passwords, a framework called "The Unified Kill Chain" developed by the Cyber Security Academy is also used to understand the threat behavior of cyber attacks. Cyber Security Academy is a think tank in the field of cyber security founded by Leiden University, Delft University of Technology and The Hague University of Applied Sciences which are all based in the Netherlands.

The use of the Unified Kill Chain framework aims to understand the characteristics and behavior of cyber threats in carrying out attacks. Through a comprehensive understanding of the Technique, Tactic and Procedure (TTP) of cyber attacks, the identification process of occupational needs and HR competencies can meet the needs of various industrial sectors that manage electronic systems.

The National Occupational Cybersecurity Map contains 30 Occupations at levels 5-9, based on the KKNI qualification level, the occupation types of Cybersecurity are as follows:

Table 3.
The occupation types of Cybersecurity in Indonesia

Qualification	Occupation
5	a. Cryptographic Technician b. Cryptographic Administrator c. Junior Cyber Security d. Cyber Security Operator
6	a. ICT Security product evaluator b. Cryptographic Analyst c. Cryptographic Module Analyst d. Vulnerability Assessment Analyst e. Network Security Administrator f. Cyber Security Administrator g. Cyber Security Awareness Officer h. Cyber Security Analyst i. Cyber Security Incident Analyst j. Digital Evidence First Responder
7	a. Cryptographic specialist b. Cryptographic Engineer c. ICT Security Product Lead Evaluator d. Cybersecurity Manager e. Network Security Manager f. Cybersecurity Awareness Lead Officer g. Incident Response Team Manager h. Information Security Auditor i. Threat Hunter j. Penetration Tester, Cyber Security Governance Officer k. Digital Forensic Analyst
8	a. Cyber Risk Specialist b. Security Architect c. Cryptographic Specialist d. Cyber Incident Investigation Manager e. Cyber Forensic Specialist
9	Chief Of Information Security Officer (CISO)

Source : The Cybersecurity Occupational Map, BSSN 2019

B. An overview of cybersecurity curriculum in Indonesia and Netherland

1. Cyber Security Engineering – Bachelor Degree, Indonesia

The Cybersecurity Engineering curriculum was prepared in 2016 by National Cyber and Crypto Polytechnic (NCCP) based on the latest developments in cybersecurity, so it is believed to be able to answer the challenges of National Cyber and Crypto Agency (NCCA) tasks in the cybersecurity domain. Until now, this curriculum has been the reference for the cybersecurity curriculum in Indonesia.

The curriculum is a type of applied study program (vocational) so that for each semester credit unit (credits) the teaching allocation given meets the composition of 40% theory and 60% practice / response. The curriculum consists of 144 (SKS) which must be completed by official bond students over a period of 4 years. The curriculum of the RKS study program has approximately 2434 hours of practicum to achieve competency skills / special skills of study program graduates. The detail of the curriculum are described in table 4 below :

Table 4.
Cybersecurity curriculum structure in NCCP Indonesia

First Year	First Semester	a. Pendidikan Agama
		b. Bahasa
		c. English
		d. Basic Mathematic
		e. Pancasila/Ideology
		f. Introduction to Cryptology
		g. Introduction to ICT
	Second Semester	a. Aljabar Linier Element
		b. Basic Electronics
		c. Information Security Fundamentals
		d. Law and Ethics
		e. Intelligent
		f. Basic Statistic
		g. Data Structure, Algorithm and Programming
Second Year	First Semester	a. Computer Architecture
		b. Database with SQL
		c. Computer Network Fundamental
		d. Operating System Fundamental
		e. Crypto Device Operational
		f. Introduction Web Programming
		g. Telecommunication System
	Second Semester	a. Data Base Security
		b. Data Communication
		c. Hardware Programming
		d. Convergence Network Protocol
		e. Routing and Switching
		f. Advanced Operating System
		g. Distributed System

Third Year	First Semester	a. Network System Administration b. Network Security Fundamental c. Wireless Telecommunication and Network d. Web Security e. Cloud computing f. Network Programming with Python
	Second Semester	a. Firewall and Network Security Perimeter b. Malicious Software c. Research Methodology d. Penetration Testing e. Network Security Protocol f. Virtualization Technology
Fourth Year	First Semester	a. Intrution Detection System b. Wireless Network Security c. Network Forensic d. Network Planning and Management and Data Center e. Field Practise f. Digital Forensic g. Final Project Seminar
	Second Semester	a. Secure Operation and Incident Response b. Cyber Security Governance c. Final Project

Source : NCCP, 2020

We can conclude from the table that all course are technical subject. It could happen because the type of the curriculum is vocational so it focuses on practice/technique.

2. Cyber Security – Master Degree, Netherland

This academic executive master's programme is developed by Leiden University, Delft University of Technology and The Hague University of Applied Sciences. They have combined their knowledge and expertise in education for professionals in this field in the Cyber Security Academy (CSA) in The Hague. Also various private partners are involved. Leiden University is responsible for the programme.

The academic executive master's programme Cyber Security is multidisciplinary; the programme covers technological as well as legal, administrative, economic and psychological aspects of digital security. Participants can either choose a technical or a governance specialisation.

The master's programme is part time and lasts two years (including thesis). The programme consists of four phases: conceptualisation, specialisation, elaboration and research. The detail of the curriculum are described in table 5 below :

Table 5.
Cybersecurity Curriculum Structure in Leiden University,Netherland

First Year	First Semester	a. Introduction to cyberspace b. Introduction to cybersecurity c. Cyber risk
	Second Semester	a. Legal Perspectives on Cyber Security and cyber security economics b. Technical Measures and Intervention c. Network Security d. Cyber security Management in Organisations e. Regulating Security in Cyber space
Second Year	First Semester	a. Case study in Cyber Security b. Global Politics of Cyber Security c. Elaboration Phase
	Second Semester	h. Research/Thesis

Source: https://www.universiteitleiden.nl/en/education/study-programmes/master/cyber-security

The curriculum in the master degree at Leiden University is stated to have used a multidisciplinary approach. Apart from studying technical fields, this curriculum also provides space for courses in legal, economy, organizational management, regulating and even global politics.

C. Comparison between NIST SP 80-181, Cybersecurity National Occupational Map, Cybersecurity Curriculum in Indonesia

After explaining the guidelines for preparing cybersecurity curricula and cybersecurity curricula in Indonesia and the Netherlands, this section will compare them to determine compliance and to provide comprehensive / multidisciplinary curriculum recommendations. The comparison can be seen in the table below.

Table 6.
Comparison between NIST SP 80-181; Cybersecurity National Occupational Map; Cybersecurity Curriculum in Indonesia and The Netherland

NIST SP 80-181 (Specialty Area)	The Cybersecurity Occupation Map (Occupation)	Cybersecurity Curriculum in Indonesia (Y/N)	Information
Risk Management (RSK)	Cyber Risk Specialist Cybersecurity Manager Incident Response Team Manager Information Security Auditor	Y	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation
Software Development (DEV)	ICT security Product Evaluator ICT security Product Lead Evaluator	Y	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs. Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.
System Architecture (ARC)	Security Architect Cryptographic Specialist	Y	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and

NIST SP 80-181 (Specialty Area)	The Cybersecurity Occupation Map (Occupation)	Cybersecurity Curriculum in Indonesia (Y/N)	Information
			solution architectures, and the resulting systems supporting those missions and business processes.
Technology R&D (TRD)	Cryptographic Engineer Cryptographic Analyst Cryptographic Module Analyst Cryptographic Module Engineer	Y	Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.
System Requirement Planning(SRP)	Cybersecurity Manager Cryptographic Specialist	Y	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions
Test and Evaluation (TST)	ICT security Product Evaluator ICT security Product Lead Evaluator	Y	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions
System Development (SYS)	Cryptographic Specialist Cryptographic Module Engineer	Y	Designs, develops, tests, and evaluates information system security throughout the systems development life cycle.
Data Administration (DTA)	Network Security Administrator Cryptographic Analyst	Y	Examines data from multiple disparate sources with

NIST SP 80-181 (Specialty Area)	The Cybersecurity Occupation Map (Occupation)	Cybersecurity Curriculum in Indonesia (Y/N)	Information
	Cryptographic Module Analyst		the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.
Knowledge Management (KMG)	Cybersecurity Awareness Lead Officer	Y	Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
Customer Service and Technical Support (STS)	Cryptographic Module Technician Cryptographic Administrator Junior Cybersecurity Cyber security operator	Y	Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable)
Network Services (NET)	Network Security Administrator Cyber risk specialist Cryptographic Administrator Cryptographic Module Technician Junior Cybersecurity	Y	Plans, implements, and operates network services/systems, to include hardware and virtual environments.

NIST SP 80-181 (Specialty Area)	The Cybersecurity Occupation Map (Occupation)	Cybersecurity Curriculum in Indonesia (Y/N)	Information
System Administrator (ADM)	Cryptographic Administrator Cryptographic Technician Junior Cyber security Cybersecurity Operator Network Security Administrator	Y	Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls;and adhering to organizational security policies and procedures).
System Analyst (ANA)	Cyber Risk Specialist Information Security Auditor Cryptographic Analyst Cryptographic Specialist Cryptographic Engineer	Y	Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.
Legal Advice and Advocacy (LGA)	CISO Cybersecurity Governance Officer	N	Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.
Training Education and Awareness (TEA)	CISO Cybersecurity Manager Cybersecurity Awareness Lead Officer Cybersecurity Awareness Officer	N	Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.

NIST SP 80-181 (Specialty Area)	The Cybersecurity Occupation Map (Occupation)	Cybersecurity Curriculum in Indonesia (Y/N)	Information
Cybersecurity Management (MGT)	CISO Cyber Risk Specialist Cryptographic Specialist	N	Individual who manages the Communications Security (COMSEC) resources of an organization or key custodian for a Crypto Key Management System (CKMS).
Strategic Planning and Policy (SPP)	CISO Cyber Risk Specialist Information Security Auditor Cybersecurity Governance Officer	N	Develops cyberspace workforce plans, strategies, and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.
Executive Cyber Leadership	CISO	N	Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.
Program/Project Management (PMA and Acquisition	CISO Cyber Risk Specialist Information Security Auditor Cybersecurity Governance Officer	N	Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with agency or enterprise

NIST SP 80-181 (Specialty Area)	The Cybersecurity Occupation Map (Occupation)	Cybersecurity Curriculum in Indonesia (Y/N)	Information
			priorities.
Cyber Defence Analysis (CDA)	Network Security Administrator Information Security Auditor Cryptographic Module Engineer Security Architect Incident Response Team Manager	Y	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.
Cyber Defence Infrastructure Support (INF)	Cybersecurity Analyst Cryptographic Analyst Security Architect Incident Response Team Manager	Y	Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.
Incident Response (CIR)	Incident Response Team Manager	Y	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
Vulnerability Assessment and Management (VAM)	CISO Cyber Security Governance Officer Cryptographic Specialist Vulnerability Assessment Analyst Cyber security Manager Network Security Manager	Y	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities
Threat Analysis (TWA)	Threat Hunter Penetration Tester Vulnerability Assessment Analyst	Y	Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects,

NIST SP 80-181 (Specialty Area)	The Cybersecurity Occupation Map (Occupation)	Cybersecurity Curriculum in Indonesia (Y/N)	Information
			processes, analyzes, and disseminates cyber threat/warning assessments
Exploitation Analysis (EXP)	Information Security Auditor Cybersecurity Administrator Network Security Administrator	Y	Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.
All source Analysis (ASA)	CISO Cryptographic Specialist Cybersecurity Manager Network Security Administrator	Y	Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations
Targets (TGT)	Threat Hunter Penetration tester Vulnerability Assessment Analyst	Y	Conducts advanced analysis of collection and opensource data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on

NIST SP 80-181 (Specialty Area)	The Cybersecurity Occupation Map (Occupation)	Cybersecurity Curriculum in Indonesia (Y/N)	Information
			knowledge of target technologies, digital networks, and the applications on them.
Language Analysis (LNG)	CISO Cyrptographic Specialist Cybersecurity Governance Officer	N	Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates and maintains language-specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.
Collection Operation (CLO)	Cyber security Analyst Cyber security Manager Cyber security Governance Officer	N	Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection

NIST SP 80-181 (Specialty Area)	The Cybersecurity Occupation Map (Occupation)	Cybersecurity Curriculum in Indonesia (Y/N)	Information
			capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.
Cyber Operational Planning (OPL)	Cyber security Analyst Cyber security Manager Cyber security Governance Officer	Y	Evaluates collection operations and develops effects based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.
Cyber Operations (OPS)	Junior Cybersecurity Cyber security Operator Cyber security Administrator Cyber security Analyst Cyber security Manager	Y	Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence

NIST SP 80-181 (Specialty Area)	The Cybersecurity Occupation Map (Occupation)	Cybersecurity Curriculum in Indonesia (Y/N)	Information
			activities to support organization objectives in cyberspace
Cyber Investigation (INV)	Digital Evidence First Responder Incident Response Team Manager Cyber security Incident Analyst Cyber Incident Investigation Manager Cyber Forensic Specialist	Y	Conducts collection, processing, and/or geolocation of systems to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executes on-net operations.
Digital Forensics (FOR)	Digital Evidence First Responder Incident Response Team Manager Cyber Incident Investigation Manager Cyber Forensic Specialist	Y	Conducts detailed investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents. Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

From the table above it is known that there are several things that are not yet included in the cybersecurity curriculum in Indonesia, namely :

1. In all specialty areas in the Oversee and Govern category : Legal Advice and Advocacy (LGA); Training, Education, and Awareness (TEA); Cybersecurity Management (MGT); Strategic Planning and Policy (SPP); Executive Cyber Leadership (EXL); Program/Project Management (PMA) and Acquisition.
2. Language Analysis (LNG) in the Analyze category.

Conclusion

A. Summary

1. Cybersecurity occupation map released by the National Cyber and Cyrpto Agency is in line with the NIST Special Publication 80 - 181 concerning the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.
2. The curriculum for the Cybersecurity Study Program has not been adjusted to the cybersecurity occupation map. This is one of the reasons why university graduates are not ready to work.
3. Cybersecurity curriculum reform is needed by adding courses related to Legal advice and Advocacy, Training Education and Awareness, Cybersecurity Management, Strategic Planning and Policy, Executive Leadership, Project Management and Language Analysis.

B. Suggestion

Need to follow up activities such as :

1. Conduct comparative study with several countries which already have multidisciplinary curriculum in higher education level.
2. Opening new/higher degree cybersecurity study program that have multidisciplinary approach with the aim to fulfill the needs of a non technical cybersecurity workforce.

References

Journal article retrieved from database without DOI

Kristophorus Hadiono, Rina Candra Noor Santi. (2020). Menyongsong Transformasi Digital. *Proceeding SENDIU 2020,* 81-84. Retrieved from www.researchgate.net/publication/343135526

Ludi Awaludin. (2019). Strategi Penguatan Kompetensi SDM TIK dalam Mengotimalkan Penerapan SPBE. Jurnal Ilmu Sosial dan Politik Paradigma Polistaat 118 - 134

Newspaper article on website

Maulana Firmansyah. (2020, Juli 01). Indonesia jadi negara dengan serangan siber tertinggi. *Lokadata.* Retrieved from https://lokadata.id/artikel/indonesia-jadi-negara-dengan-serangan-siber-tertinggi

Adi Permana. (2020, September 18). Dampak Positif Pandemi COVID-19 Bagi Akselerasi Transformasi Digital. Retrieved from https://www.itb.ac.id/news/read/57613

Website

Cyber security curriculum in National Cyber and Crypto Polytechnic, retrieved from https://poltekssn.ac.id/?page_id=554.

Cyber security curriculum in University Leiden Netherland, retrieved from https://www.universiteitleiden.nl/en/education/study-programmes/master/cyber-security

C. Boulton, "What is digital transformation? A necessary disruption | CIO," CIO Asean. [Online]. Available: https://www.cio.com/article/3211428/what-is-digital-transformation-a-necessarydisruption.html. [Accessed: 12 October 2020].

Website document

The Cybersecurity Occupation Map, National Cyber and Crypto Agency Indonesia, retrieved from https://www.bssn.go.id

NIST Special Publication 80 – 181 : National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework