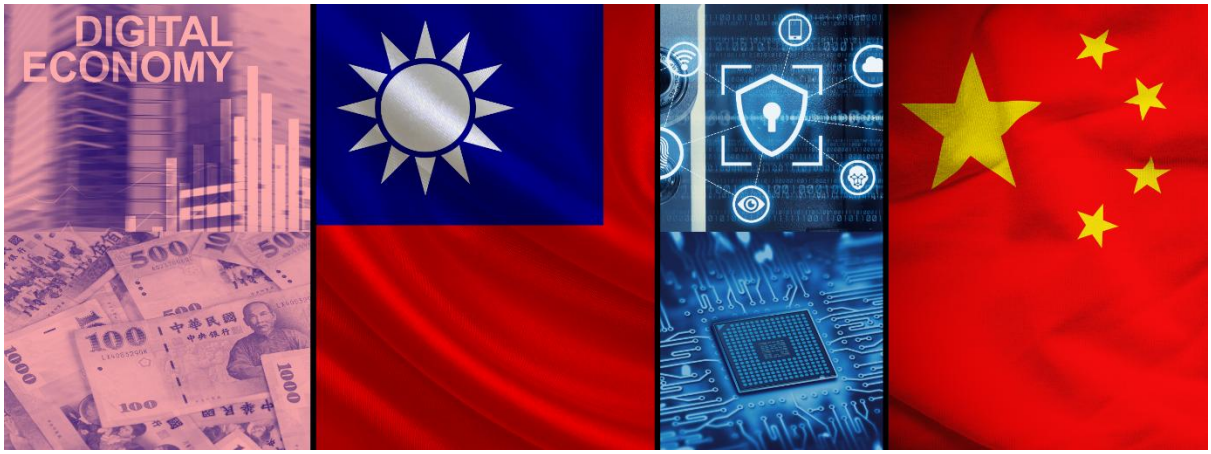


Judul Tugas Akhir Skripsi:

Implementasi *National Cyber Security Program* (NCSP) Taiwan dalam Merespons Ancaman Siber Tiongkok untuk Membangun Stabilitas Ekonomi Digital (2019 – 2023)

Tugas Akhir Skripsi ini diajukan untuk memenuhi persyaratan dalamF memperoleh gelar Sarjana Hubungan Internasional

Nama : Annisa Salsabilla

NIM : 2110412176

PROGRAM STUDI HUBUNGAN INTERNASIONAL

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK

UNIVERSITAS PEMBANGUNAN NASIONAL

VETERAN JAKARTA

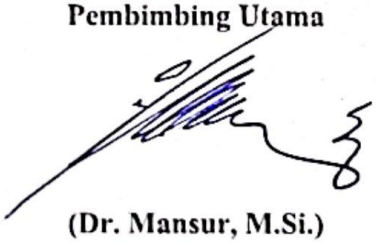
Implementasi *National Cyber Security Program* (NCSP) Taiwan dalam Merespons Ancaman Siber Tiongkok untuk Membangun Stabilitas Ekonomi Digital (2019 – 2023)

The Implementation of Taiwan's National Cyber Security Program (NCSP) in Responding to China's Cyber Threats to Build Digital Economic Stability (2019–2023)

Oleh :
Annisa Salsabilla
2110412176

SKRIPSI
Untuk memenuhi salah satu syarat ujian
Memperoleh gelar sarjana pada Program Studi Hubungan Internasional

Telah disetujui oleh Tim Pembimbing pada tanggal seperti di bawah ini
Jakarta, 24 Juli 2025
Pembimbing Utama



(Dr. Mansur, M.Si.)

PROGRAM STUDI ILMU HUBUNGAN INTERNASIONAL
FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA
2025

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar:

Nama : Annisa Salsabilla

NIM : 2110412176

Program Studi : S1 Hubungan Internasional

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan ini maka, saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 24 Juli 2025

Yang menyatakan,

(Annisa Salsabilla)

PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan di bawah ini:

Nama	: Annisa Salsabilla
NIM	: 2110412176
Fakultas	: Ilmu Sosial dan Ilmu Politik
Program Studi	: S1 Hubungan Internasional

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right)* atas karya ilmiah saya yang berjudul:

(IMPLEMENTASI *NATIONAL CYBER SECURITY PROGRAM* (NCSP) TAIWAN DALAM MERESPONS ANCAMAN SIBER TIONGKOK UNTUK MEMBANGUN STABILITAS EKONOMI DIGITAL (2019-2023))

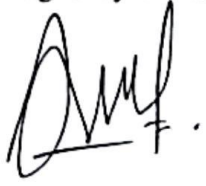
Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini. Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database),* merawat dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya:

Dibuat di : Jakarta,

Pada tanggal : 24 Juli 2025

Yang menyatakan,



(Annisa Salsabilla)

PENGESAHAN TUGAS AKHIR

NAMA	: Annisa Salsabilla
NIM	: 2110412176
PROGRAM STUDI	: S1 Hubungan Internasional
JUDUL	: Implementasi *National Cyber Security Program* (NCSP) Taiwan dalam Merespons Ancaman Siber Tiongkok untuk Membangun Stabilitas Ekonomi Digital (2019-2023)

Telah berhasil dipertahankan dihadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar sarjana pada Program Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Pembangunan Nasional Veteran Jakarta.

Pembimbing

(Dr. Mansur, M.Si.)

Penguji 1

(Dr. Shanti Darmastuti, S.IP, M.Si.)

Penguji 2

(I Nyoman Aji S. R., S.Sos., M.IR.)

Ketua Program Studi
Hubungan Internasional

(Wiwick Rukmi D. A., S.IP., M.Si.)

Ditetapkan di : Jakarta
Tanggal Ujian : 19 Juni 2025

IMPLEMENTASI *NATIONAL CYBER SECURITY PROGRAM* (NCSP) TAIWAN DALAM MERESPONS ANCAMAN SIBER TIONGKOK UNTUK MEMBANGUN STABILITAS EKONOMI DIGITAL (2019-2023)

ABSTRAK

Pesatnya transformasi digital di Taiwan menjadikannya salah satu pemain utama dalam ekonomi digital global sekaligus target ancaman siber yang semakin rumit, khususnya dari Tiongkok. Selama periode 2019-2023, intensitas serangan meningkat, berbarengan dengan pandemi COVID-19 dan ketegangan geopolitik, yang menimbulkan tekanan besar terhadap infrastruktur kritis, sektor semikonduktor, dan sistem informasi publik. Untuk merespons situasi tersebut, Taiwan mengimplementasikan *National Cyber Security Program* (NCSP) sebagai strategi utama dalam memperkuat pertahanan siber nasional dan menjaga keberlanjutan ekonomi digitalnya. Penelitian ini menganalisis bagaimana NCSP dijalankan sebagai respons strategis terhadap ancaman siber yang bersifat sistematis, mulai dari spionase hingga kampanye disinformasi. Dengan pendekatan kualitatif deskriptif dan studi literatur, serta kerangka teori keamanan non-tradisional, keamanan siber, kebijakan siber, dan ekonomi digital, penelitian ini menemukan bahwa NCSP fokus pada penguatan perlindungan infrastruktur informasi kritis, pengembangan industri keamanan siber dalam negeri, peningkatan kapasitas SDM, dan perluasan kerja sama internasional. Meski menunjukkan kemajuan kelembagaan dan respons yang adaptif, program ini masih menghadapi tantangan krusial seperti kekurangan talenta siber dan kesiapan menghadapi ancaman berbasis AI. Temuan ini memperlihatkan pentingnya integrasi antara keamanan dan pembangunan digital dalam merespons dinamika ancaman era digital, serta memberikan kontribusi bagi pengembangan studi dan kebijakan keamanan digital di tingkat nasional dan global.

Kata Kunci: Keamanan Siber, *National Cyber Security Program* (NCSP), Ekonomi Digital, Taiwan, Ancaman Siber Tiongkok

THE IMPLEMENTATION OF TAIWAN'S NATIONAL CYBER SECURITY PROGRAM (NCSP) IN RESPONDING TO CHINA'S CYBER THREATS TO BUILD DIGITAL ECONOMIC STABILITY (2019-2023)

ABSTRACT

Taiwan's rapid digital transformation has positioned it as a key player in the global digital economy, while also making it a prime target of increasingly complex cyber threats, particularly from China. Between 2019 and 2023, the intensity of these threats grew, coinciding with the COVID-19 pandemic and rising geopolitical tensions. These challenges placed significant pressure on Taiwan's critical infrastructure, semiconductor industry, and public information systems. In response, the Taiwanese government implemented the National Cyber Security Program (NCSP) as a central strategy to strengthen its national cyber defense and maintain the sustainability of its digital economy. This study examines how the NCSP was implemented as a strategic response to systematic cyber threats, ranging from espionage to large-scale disinformation campaigns. Using a qualitative descriptive approach and literature study, and grounded in the frameworks of non-traditional security, cybersecurity, cyber policy, and digital economy, the research finds that the NCSP focuses on strengthening the protection of critical information infrastructure, developing the domestic cybersecurity industry, improving human resource capacity, and expanding international cooperation. While the program has made institutional progress and shown adaptive responses, it still faces key challenges, particularly the cyber talent gap and preparedness for AI-based threats. These findings highlight the importance of integrating security and digital development to effectively address evolving threats in the digital era, and contribute to the broader discourse on cybersecurity policy and digital economy strategies at both national and global levels.

Keywords: Cybersecurity, National Cyber Security Program (NCSP), Digital Economy, Taiwan, Chinese Cyber Threats

KATA PENGANTAR

Dengan penuh rasa syukur, penulis menyampaikan apresiasi yang mendalam atas selesainya skripsi yang berjudul "**Implementasi *National Cyber Security Program* (NCSP) Taiwan dalam Merespons Ancaman Siber Tiongkok untuk Membangun Stabilitas Ekonomi Digital (2019 – 2023)"** sebagai salah satu syarat untuk memperoleh gelar Sarjana Ilmu Hubungan Internasional di Universitas Pembangunan Nasional "Veteran" Jakarta.

Skripsi ini tidak akan pernah terwujud tanpa dukungan dari berbagai pihak yang telah memberikan semangat, bimbingan, serta kepercayaan sepanjang proses penulisannya. Oleh karena itu, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Allah SWT, atas limpahan rahmat, kekuatan, dan ketenangan hati yang diberikan-Nya dalam setiap langkah perjuangan akademik ini.
2. Untuk diri sendiri yang terus belajar menerima kegagalan, merayakan kemajuan sekecil apa pun, dan tetap mencoba meski berkali-kali ragu. Terima kasih sudah berani untuk terus melangkah, yang tetap percaya bahwa semua ini layak diperjuangkan.
3. Kedua orang tua, Bapak Haliman dan Ibu Harsi, serta Adik Arsyad Narendra atas doa yang tidak pernah putus, cinta yang tulus, dan semua bentuk pengorbanan yang menjadi fondasi dari setiap langkah ini.
4. Bapak Dr. Mansur, M.Si., sebagai dosen pembimbing yang telah sabar membimbing di tengah segala kekurangan dan keterbatasan penulis. Arahan dan koreksi yang diberikan menjadi bekal berharga dalam menyempurnakan penelitian ini, sekaligus pelajaran hidup tentang ketelitian dan keteguhan.
5. Ucapan terima kasih juga penulis sampaikan kepada para dosen dan tenaga pendidik yang telah menjadi bagian penting dalam perjalanan akademik penulis. Setiap materi kuliah, diskusi, dan pengalaman belajar yang diberikan telah membentuk cara pandang dan wawasan penulis dalam memahami dinamika hubungan internasional.

6. Diplomat Senior di Kementerian Luar Negeri Republik Indonesia, Bapak Arsi dan jajarannya yang telah menjadi sumber inspirasi dan teladan selama masa magang. Terima kasih atas wejangan dan dukungan yang memperkuat mimpi penulis untuk suatu hari kembali dan turut serta mengabdi di jalur diplomasi.
7. Sahabat terdekat yang selalu hadir dalam suka maupun duka, Fariezka Safa Salsabila dan Anisa Fitri Maharani. Terima kasih telah menjadi ruang aman untuk berbagi cerita, menangis, tertawa, dan merayakan pencapaian sekecil apa pun. Kehadiran kalian adalah pengingat bahwa penulis tidak pernah benar-benar sendiri dalam proses ini.
8. Teman seperjuangan di bangku perkuliahan; April, Acha, Cipa, Dapa, Ida, Untsa, Halim, Sipa, Andrian, Sekar, dan teman-teman HI UPNVJ angkatan 2021. Terima kasih atas kerja sama, diskusi produktif, dan kebersamaan yang begitu berarti selama empat tahun menempuh perjalanan ini.
9. Teman-teman magang AMEROP Kemlu; Fabian, Saki, Nanda, Anya, Salmaa, Naura, Gladys, Alvin, Sofwan, Aldrick, dan Fadhil. Kebersamaan kita tak hanya memperkaya pengalaman magang, tapi juga meninggalkan kenangan hangat yang akan selalu penulis syukuri. Terima kasih telah menjadi bagian berharga dalam perjalanan ini.
10. Organisasi dan komunitas yang pernah menjadi rumah belajar dan tumbuh bagi penulis, yaitu BEM UPNVJ dan FPCI UPNVJ. Terima kasih atas ruang untuk berkembang, berkontribusi, dan mengenal diri lebih dalam.

Akhir kata, penulis menyadari bahwa karya ini masih jauh dari sempurna. Namun, dengan segala keterbatasan, skripsi ini disusun dengan penuh dedikasi dan ketulusan. Semoga karya ini dapat memberikan manfaat dan menjadi sumbangan kecil bagi pengembangan kajian hubungan internasional, khususnya dalam isu keamanan siber dan ekonomi politik internasional.

Jakarta, 24 Juli 2025

Annisa Salsabilla

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

GLOSARIUM

A

ACS *(Administration for Cyber Security)* Lembaga pelaksana kebijakan keamanan siber di tingkat eksekutif Taiwan yang berada di bawah naungan MODA, dibentuk sebagai hasil restrukturisasi dari DCS.

AI *(Artificial Intelligence)* Kecerdasan Buatan; teknologi canggih yang menjadi fokus dalam pengembangan ekonomi digital dan juga menjadi tantangan baru dalam ancaman siber (misalnya *AI-based threats*).

AIS3 *(Advanced Information Security Summer School)* Program pelatihan keamanan siber praktis berskala nasional di Taiwan yang dirancang untuk menumbuhkan minat dan keahlian talenta muda.

APT *(Advanced Persistent Threat)* Jenis serangan siber canggih, tersembunyi, dan berkelanjutan, seringkali dilatarbelakangi oleh negara, yang menargetkan entitas spesifik untuk tujuan spionase atau sabotase.

C

CERT *(Computer Emergency Response Team)* Tim tanggap darurat insiden siber yang menangani aspek teknis saat terjadi serangan sebagai bagian dari lingkup pertahanan terpadu.

CIIP *(Critical Information Infrastructure Protection)* Perlindungan Infrastruktur Informasi Kritis; salah satu pilar utama strategi NCSP yang fokus melindungi 8 sektor vital negara (energi, keuangan, telekomunikasi, dll.) dari serangan siber.

CSMA *(Cyber Security Management Act)* Undang-Undang Manajemen Keamanan Siber Taiwan yang mulai berlaku pada 1 Januari 2019, memberikan landasan hukum yang kuat bagi seluruh tugas keamanan siber nasional.

D

DDoS *(Distributed Denial of Service)* Jenis serangan siber yang bertujuan melumpuhkan sebuah layanan *online* (misalnya situs web pemerintah) dengan cara membanjirinya dengan lalu lintas data dari berbagai sumber.

DIGI+ *(Digital Nation & Innovative Economy Development Program)* Rencana pembangunan masyarakat digital Taiwan (2017-2025) yang menjadi *blueprint* atau kerangka utama bagi agenda ekonomi digital dan inovasi negara tersebut.

I

ISAC *(Information Sharing and Analysis Center)* Pusat Berbagi dan Analisis Informasi; sebuah entitas yang memfasilitasi pertukaran informasi ancaman siber secara *real-time* di antara para pemangku kepentingan dalam sektor industri tertentu (misalnya F-ISAC untuk keuangan).

IoT ***(Internet of Things)*** Konsep di mana berbagai perangkat saling terhubung melalui internet untuk berbagi data, menjadi pendorong Revolusi Industri 4.0 yang sekaligus memperluas lingkup ancaman siber.

M

MODA ***(Ministry of Digital Affairs)*** Kementerian Urusan Digital Taiwan; didirikan pada Desember 2022 sebagai pusat kendali digital nasional yang mengonsolidasikan fungsi transformasi digital, tata kelola data, dan keamanan siber.

N

NCSP ***(National Cyber Security Program)*** Program Keamanan Siber Nasional Taiwan; kebijakan jangka panjang yang menjadi objek utama penelitian, yang berevolusi dalam beberapa fase untuk memperkuat pertahanan siber nasional.

NICS ***(National Institute of Cyber Security)*** Institut Keamanan Siber Nasional; lembaga teknis di bawah MODA yang bertugas mengembangkan teknologi keamanan siber inovatif dan mendukung pembinaan talenta.

NICST ***(National Information and Communication Security Taskforce)*** Satuan Tugas Keamanan Informasi dan Komunikasi Nasional; lembaga di bawah Eksekutif Yuan yang didirikan pada 2001 untuk merumuskan dan mengoordinasikan kebijakan keamanan siber nasional Taiwan.

R

Ransomware Jenis perangkat lunak berbahaya *(malware)* yang mengenkripsi data korban dan meminta tebusan untuk mengembalikannya. Contohnya adalah serangan *ColdLock* yang menargetkan Taiwan.

S

SOC ***(Security Operation Center)*** Pusat Operasi Keamanan; unit yang bertugas memantau, menganalisis, dan merespons ancaman keamanan siber secara berkelanjutan dalam sebuah organisasi atau negara.

T

TSMC ***(Taiwan Semiconductor Manufacturing Co.)*** Perusahaan manufaktur semikonduktor terbesar di dunia yang berbasis di Taiwan dan menjadi aset ekonomi serta geopolitik yang sangat vital bagi negara tersebut.

Z

ZTA ***(Zero Trust Architecture)*** Arsitektur Kepercayaan Nol; model keamanan siber modern yang diadopsi Taiwan, yang mengasumsikan tidak ada pengguna atau perangkat yang sepenuhnya dapat dipercaya, sehingga verifikasi ketat diperlukan untuk setiap upaya akses.