Cybersecurity Governance in Indonesia and the Netherlands

Gstrein, Oskar Josef; Blauth, Tais; Rahman, Faiz; Mantovani, Anisa Pratita Kirana; Wiharani, Annisa Paramita

Published in:
European Cybersecurity Journal

VOLUME 9 (2023) ISSUE 1

European Cybersecurity Journal

Strategic perspectives on cybersecurity management and public policies

European Cyber Security Cooperation: Overview and Challenges

Heli Tiirmaa-Klaar

Cybersecurity is a Global Public Good

Interview with Francesca Bosco

ANALYSES • POLICY REVIEWS • OPINIONS

The Kosciuszko Institute

European Cybersecurity Journal

Strategic perspectives on cybersecurity management and public policies

The European Cybersecurity Journal (ECJ) is a specialised publication devoted to cybersecurity. The main goal of the Journal is to provide concrete policy recommendations for European decision-makers and raise awareness on both issues and problem--solving instruments.

ISSN: 2450-21113

Citations: This journal should be cited as follows:
"European Cybersecurity Journal"
Volume 9 (2023) Issue 1, page reference

The Kosciuszko Institute

Published by:
The Kosciuszko Institute
ul. Feldmana 4/9-10
31-130 Kraków

Phone: 00 48 12 632 97 24
E-mail: editor@cybersecforum.eu

Contents

ARTICLE

Cybersecurity Governance in Indonesia and the Netherlands: Towards More Cooperation

OSKAR J. GSTREIN
ASSISTANT PROFESSOR, DEPARTMENT OF GOVERNANCE AND INNOVATION AT CAMPUS FRYSLÂN OF THE UNIVERSITYOF GRONINGEN

TAIS FERNANDA BLAUTH
PHD RESEARCHER, DEPARTMENT OF GOVERNANCE AND INNOVATION AT CAMPUS FRYSLÂN OF THE UNIVERSITY OF GRONINGEN

FAIZ RAHMAN
ADJUNCT RESEARCHER, CENTER FOR DIGITAL SOCIETY (CFDS); LECTURER, FACULTY OF LAW, UNIVERSITAS GADJAH MADA, INDONESIA, PHD RESEARCHER, LEIDEN LAW SCHOOL, UNIVERSITEIT LEIDEN

ANISA PRATITA KIRANA MANTOVANI
ADJUNCT RESEARCHER, CENTER FOR DIGITAL SOCIETY (CFDS), UNIVERSITAS GADJAH MADA, INDONESIA; HEAD OF PUBLIC POLICY AND GOVERNMENT RELATIONS, INDONESIAN E-COMMERCE ASSOCIATION (IDEA)

ANNISA PARAMITA WIHARANI
ADJUNCT RESEARCHER, CENTER FOR DIGITAL SOCIETY (CFDS), UNIVERSITAS GADJAH MADA; PHD RESEARCHER, DEPARTMENT OF INTERNATIONAL RELATIONS AND INTERNATIONAL ORGANIZATION, UNIVERSITY OF GRONINGEN

ABSTRACT:
This article analyses cybersecurity frameworks which address cybercrime, safeguarding critical infrastructure, approaches to cyberwar and cyberespionage in Indonesia and the Netherlands. We compare approaches addressing cybersecurity-related challenges in an international context. While Indonesia and the Netherlands share some common history, significant differences in geographical location, population size, socio-economic status, and other factors remain. Despite substantial differences, both nations face comparable challenges, which present opportunities for closer cooperation. This paper underscores the need for making a concerted effort to foster dialogue and collaboration.

Keywords: cybersecurity, Indonesia, Netherlands, governance, cooperation, regulation

Funding notice: Research on this paper was funded through a Nuffic/Orange Knowledge Programme grant (OKP-TMT+.20/0011) aiming at 'Enhancing Higher Education Capacity for An Interdisciplinary Cybersecurity Study Program'. This project was implemented in collaboration between researchers of the Center for Digital Society (CfDS), located at the Faculty of Political Sciences, Gadjah Mada University, Yogyakarta/Indonesia and the Data Research Centre (DRC) at Campus Fryslân, University of Groningen/The Netherlands.

1. Introduction

The number of cyberattacks has grown in recent years (Europol, 2021, pp. 10–16), especially during the COVID-19 pandemic (Chigada & Madzinga, 2021). Increasing geopolitical tensions and the use of emerging technologies such as machine learning to enhance cyberattacks reinforce this development (Brooks, 2023). This illustrates the need for national governments to deal with cybersecurity-related issues. Studies considering such efforts frequently focus on the comparison of policies of a few very large and powerful actors – such as the United States or the People's Republic of China (see e.g. Jisi & Ran, 2019; Goel, 2020). In this article, we compare Indonesia and the Netherlands.

While the two countries have some shared (colonial) history, they face similar cybersecurity-related challenges emerging in the 21st century. Nevertheless, the different socio-economic and geopolitical context remains relevant and provides fertile ground for analysis and discussion from an unconventional angle.

Indonesia has the fourth-largest population among countries globally and the 10th largest purchasing power parity economy, making it the largest economy in Southeast Asia (World Bank, 2022). Moreover, Indonesia is ranked 9th for average daily internet use, with 204.7 million internet users – 73.7% of the total Indonesian population (social & KEPIOS, 2022a). As a developing

country and emerging economy in the world, these statistics illustrate considerable economic potential, especially when considering its innovative use of data and e-commerce. The Netherlands, in contrast, has one of the highest Internet penetration rates in the world. A report shows that Internet users in the Netherlands have reached 16.5 million, which is 96% of the of the country's total population (social & KEPIOS, 2022b). Thus, the threat of cyberattacks increasingly affects the lives of the Dutch population and the Dutch economy. With this article, we aim to raise awareness of the differences and commonalities between the two countries to identify themes for enhanced cooperation. This study might also be relevant for European states with comparable historical relationships with countries outside the continent.

1.1 Context of the study

Indonesia and the Netherlands are key partners in many different areas. As proposed by Robert Keohane and Joseph Nye (1998, pp. 77, 81), the interconnectedness of states through numerous channels emphasizes the importance of cooperation when addressing shared challenges. Indonesia and the Netherlands share a complex web of interdependencies through channels such as trade, diplomacy, and technological networks. Specifically, Indonesia and the Netherlands collaborate, for instance, in the economic (Kingdom of the Netherlands, 2020), educational (Nuffic, 2023), and cultural sectors (Vermeulen, 2020). In addition, the countries have been strengthening their cooperation in cybersecurity. As Indonesia and the Netherlands have established bilateral trade and investment relations in various sectors, enhancing cybersecurity collaboration is crucial to safeguard the thriving trade and investment partnership in various industries. Cyber threats have the potential to severely affect business operations, confidential information, intellectual property, and innovative creations. Collaborative cybersecurity governance efforts can ensure the continuity and secure the bilateral economic activities and trade flow. Among the initiatives, we highlight those presented in Table 1.

Year	Agreement/Initiative	Remarks
2018	Letter of Intent expressing the commitment of the governments to enhancing bilateral cooperation in cyberspace, signed on 3 July of 2018.	This letter was signed by the Foreign Minister of the Netherlands, Stef Blok, and the Head of the Indonesian National Cyber and Crypto Agency in Jakarta.
2019	ASEAN-EU Statement on Cybersecurity Cooperation	This document emphasized the commitment of ASEAN and the EU, in which Indonesia and the Netherlands are part of the respective organizations, to promote an open, secure, stable, accessible, and peaceful ICT environment through strengthening cooperation on cyber issues.
2019	EU-Indonesia's 4th Security Policy Dialogue, 12 November 2019	The dialogue aimed at strengthening EU-Indonesia cooperation on security issues, including cybersecurity. The commitment for cooperation further emphasized in the 5th and 6th Security Policy Dialogue in 2020 and 2021.
2017-2022	Orange Knowledge Programme (OKP) - Nuffic	The Dutch OKP aims at contributing to "societies' social and economic development by strengthening knowledge and skills of professionals and organisations". Indonesia has been one of the participating countries and cybersecurity one of the priorities of the programme.
2021	Indonesia-Netherlands Cyber Policy Dialogue, held on the 21stof January of 2021.	The dialogue reinforced "the two countries' ongoing commitment to enhance bilateral engagement on, and mutual understanding of, cyber issues".
2021-2022	OKP Tailor-Made Training Plus – 'Enhancing Higher Education Capacity for an Inter-Disciplinary Cybersecurity Study Program'	The Ministry of Foreign Affairs of the Netherlands provided funding for grants within the OKP, managed by the agency Nuffic (OKP-TMT+.20/00119). One of the projects was focused on capacity building in the field of cybersecurity, promoting collaboration between higher education institutions in Indonesia and the Netherlands. This article was written as part of this initiative, by an independent and international team of researchers, both from Indonesia and the Netherlands.

Table 1. Selected Indonesia-Netherlands Cooperation Initiatives Related to Cybersecurity. Source: Compiled by Authors, 2023.

As Indonesia's digital population continues to grow rapidly, the need for effective cybersecurity measures becomes increasingly crucial. The country has faced numerous challenges securing its diverse and expansive digital ecosystem as the accelerated growth of internet users and mobile internet connections increase the number of cyber threats and cyber-attacks to a level which has not been seen before. From 2019 to 2021, Indonesia experienced a 5-fold increase in cyberattacks (Kiswondari, 2021). The National Cyber and Crypto Agency (Badan Siber dan Sandi Negara, BSSN) noted that throughout 2021, there were 1,637,973,022 traffic anomalies detected, which is a significant increase from the 2020 figure of 495,337,202 (Rahman et al., 2021). The number of cyberattacks has surged with various types of attacks emerging, such as malware deployment, capturing websites, data breaches, data manipulation, as well as illegal content distribution (National Information and Communication Technology Council, 2018). The vulnerabilities are further exacerbated by infrastructure with poor cyber-resilience and generally low digital literacy rates. Moreover, Indonesia does not have a comprehensive Cybersecurity Act to provide a legal basis for cybersecurity. Hence, cybersecurity is currently regulated through various sectoral acts and implementing legislation.

Ultimately, collaboration with the Netherlands could provide valuable insights and guidance as Indonesia continues to develop and enhance its cybersecurity governance mechanisms. Such a partnership could benefit both countries, especially as cybersecurity threats multiply.

As for the Netherlands, the country is in a unique position to capitalise on the opportunities brought about by digitalisation. Nevertheless, cyber-attacks and threats are on the rise as cybercriminals continuously develop new ways to commit various

types of attacks and exploit system vulnerabilities (National Cyber Security Centre, 2019). In particular, the deployment of ransomware and Distributed Denial of Service (DDoS) attacks pose a considerable threat to national security and may have disruptive consequences for society. Therefore, the country needs to strengthen its defences against cybercrime, in particular through enhanced cooperation between the public and private sectors (National Coordinator for Counterterrorism and Security, 2022, pp. 15–18). This includes improving the country's digital resilience and ensuring that laws and regulations stay up to date, which is also mandated by emerging strict regulation of the European Union.

Collaboration can help both countries to benefit from each other's advancements and contribute to developing cutting-edge cybersecurity solutions. In addition to that, the historical ties between Indonesia and the Netherlands may serve as a foundation for closer collaboration in various areas, including cybersecurity governance. Building upon these historical connections can foster trust, mutual understanding, and shared objectives, which in turn can facilitate more effective joint efforts in addressing cybersecurity challenges. It is essential to recognize the potential benefits of such collaboration and work towards leveraging these historical ties for the greater good.

1.2 Methodology

The examples in Table 1 demonstrate a wide range of collaborative initiatives between the Netherlands and Indonesia, including, but not limited to, raising awareness, increasing cyber resilience, and capacity building. This article aims to investigate how Indonesia and the Netherlands compare in terms of cybersecurity regulation and governance. To this end, we evaluate the international and regional contexts of the countries, analyse national frameworks, and discuss recent challenges. Moreover, we seek to answer the following sub-questions:

- Which issues are being identified by both countries relating to cybersecurity?
- Which common characteristics can be identified by comparing the different national governance models in an international context?
- How do Indonesia and the Netherlands contrast in their cybersecurity national governance models?
- What are the main possibilities for further cooperation between the countries in cybersecurity on a bilateral and multilateral level?

This methodology is based on an analysis of government documents and websites, reports, and academic literature. We have only reviewed papers/documents/reports/web pages available in English, Dutch, German and Indonesian, due to the composition of the research team, with researchers from Europe and Indonesia.

2. Indonesian Cybersecurity Governance Framework in a Nutshell

The Indonesian government has paid increasing attention to cybersecurity issues in response to the rise in cyberattacks and cybercrime over the past decade. Cybercrime was explicitly mentioned as a top priority in the previous Indonesian National Medium-Term Development Plan.[1] The RPJMN 2020-2024[2] states that the development of the current national cybersecurity governance framework is based on indicators of the Global Cybersecurity Index (GCI), which

1 RPJMN – see e.g. Appendix of Presidential Regulation No. 5 of 2010 on National Mid-Term Development Plan Year 2010-2014 2, Book II Strengthening Inter-Sectoral Development Synergy, II.5-13, 5-42-43, 6-49; Appendix of Presidential Regulation No. 2 of 2015 on National Mid-Term Development Plan Year 2015-2019, Book II Sectoral Development Agenda, 5-35, 9-24-25).

2 See Appendix IV of Presidential Regulation No. 18 of 2020 on National Mid-Term Development Plan Year 2020-2024, A.7.44-A.7.46

consists of five pillars. The pillars cover legal, technical, and organisational aspects, as well as capacity development and cooperation (International Telecommunication Union, 2020, p. vii.). See Table 2 for more detailed information compiled by the authors.

Stakeholders & Governmental Actors	
National Cyber and Crypto Agency (BSSN)	An executive agency with primary responsibilities in the field of cybersecurity. It focuses on the formulation, establishment, and implementation of technical policies in the field of cybersecurity. The BSSN also coordinates the formulation of the National Cyber Security Strategy. The ID-SIRTII/CC is currently coordinated by the National Cyber Security Operations Centre at the BSSN.
Ministry of Communication and Informatics	The primary institution dealing with content violations in cyberspace. It has the power to remove illegal content. In recent years, the MCI has also been concerned with raising cyber security awareness, improving the quality of human resources, and improving cyber security technology.
Ministry of Defence	One of the leading institutions in developing cyber security and resilience in Indonesia's defence sector, including through the development of a cyber defence strategy.
Indonesian National Armed Force (TNI)	The National Armed Forces are implementing cyber defence measures. They are at the forefront of cyber warfare. In recent years, cyber defence has become a regular discussion among three branches – Army, Navy and Air Force. The National Armed Forces also carry out a routine cyber defence exercise and promote several initiatives to improve the cyber-related skills of soldiers.
Indonesian National Police (POLRI)	The National Police has a Cybercrime Directorate, which is part of the Criminal Investigation Unit.
National Intelligence Agency (BIN)	The National Intelligence Agency's focus is on strengthening cyber intelligence as a means of early detection of threats, challenges, and disturbances from domestic and abroad.
Personal data protection authority (*Lembaga Pelindungan Data Pribadi*, to be established)*	The Personal Data Protection (PDP) Authority is a new institution introduced to implement the recently enacted PDP Act. This authority is designed as an executive agency. The PDP Authority is yet to be formally established. The establishment will be regulated through a Presidential Regulation.
Legislation	
Electronic Information and Transactions Act (EIT Act)	This is currently the main act regulating cyberspace in general. The act regulates 'prohibited acts', including illegal access, interception, data and systems interferences, misuse of devices, computer-related forgery, computer-related fraud, and speech-related violations.

Electronic Information and Transactions Act (EIT Act)	This is currently the main act regulating cyberspace in general. The act regulates 'prohibited acts', including illegal access, interception, data and systems interferences, misuse of devices, computer-related forgery, computer-related fraud, and speech-related violations.
Personal Data Protection Act (PDP Act)	On 20 September 2022, the House of Representatives passed the PDP Bill. The new PDP Act effectively came into force on 17 October 2022. The PDP Act defines personal data, establishes rights of data subjects, regulates the processing of personal data, the obligations of the data controller and data processor, as well as inward and outward transfer of personal data. It establishes sanctions (administrative and criminal), a data protection authority, international cooperation, community participation, dispute resolution, as well as individual remedies.
Telecommunication Act	The Act imposes obligations on public and private telecommunications operators to protect telecommunications equipment and networks from any interference and to maintain the confidentiality of information in telecommunications networks. This Act also serves as the legal basis for the establishment of the ID-SIRTII/CC, which is currently being coordinated by the BSSN.
Government Regulation on Implementation of Electronic Systems and Transactions (GR EST)	This is the implementing regulation of the EIT Act. The GR EST further regulates the obligations of electronic system providers in the public and private sectors to secure their electronic systems by fulfilling various requirements provided. Moreover, the GR EST also provides several articles related to personal data protection, including principles and obligations for Electronic System Provider to protect their users' data.
Presidential Regulation on Electronic-Based Government System	This Presidential Regulation emphasises the importance of security as a central aspect of developing an Electronic-Based Government System (SPBE). The National SPBE Master Plan also highlights that strengthening security is one of the priority agendas in the first phase of the SPBE strategic plan.
Presidential Regulation on National Cyber and Crypto Agency	The Regulation serves as the legal basis for the establishment of National Cyber and Crypto Agency (BSSN).
Presidential Regulation on Vital Information Infrastructure Protection	The purpose of this Regulation is to protect the public interest against any disruption of vital information infrastructure caused by the misuse of electronic information and transactions that disrupt public order.
Minister of Defence Regulation on Cyber Defence Guidelines	This regulation serves as guidance for the Ministry of Defence and National Armed Forces to implement cyber defence. The guideline covers four essential aspects to be developed—policy, organisation, technology, and human resource.
Indonesian Criminal Code	This act is frequently being used by the National Police for tackling issues concerning cybercrime, especially fake news in the digital space. On 2 January 2023, the new Indonesian Criminal Code was enacted, which repealed the previous Criminal Code. The new Criminal Code also revoked several articles related to cybercrime offences previously regulated in the EIT Act.
Initiatives and Tools	
Technical	• ID-SIRTII/CC – currently under BSSN coordination. • Gov-CSIRT – sectoral CSIRT. • Organisational Standards such as Indonesia's National Standard (Standar Nasional Indonesia - SNI) IEC/ISO 27001:2013, SNI ISO/IEC 27018:2016, Trust+Positive, and KAMI (*Information Security Index*). • Standard for Professional from National Standard of Work Competency.
Capacity Building	• BSSN's National Polytechnic of Crypto and Cyber (*Politeknik Sandi dan Siber Nasional*, *Poltekssn*). • Cyberhub.id, a digital hub that brings various government and non-government stakeholders to form a cybersecurity ecosystem in Indonesia. • Cybersecurity Hub by Ministry of Education and Culture. • Born to Control – Cybersecurity Talent Pool. • National Digital Literacy Movement (GNLD). • Digital Intelligence Course (*Kelas Kecerdasan Digital*) – MCI, UGM, and various industries and associations.
Cooperation	• Indonesia - KOICA- ITB in cyber investigation. • Plans to develop cooperation with Singapore to Defence Industry and Cyber Defence. • MIKTA interregional cooperation. • Cooperation with Industries, such as Huawei, Cisco, EC-Council.

Cooperation	• Bilateral cooperation in cybersecurity with e.g., Australia, South Korea, Romania, the Netherlands, and the UK. • Triple helix collaboration between the MCI with association, academic community, and also industries.

Table 2. Indonesia Cybersecurity Governance. Source: Compiled by Authors, 2023.

Indonesia is still developing a comprehensive Cybersecurity Act. Currently, legislation related to cybersecurity is scattered over various sectoral laws. Accompanying regulations are being used to implement them (Indonesia, 2019). The main acts and implementing regulations include the Electronic Information and Transactions Act (EIT Act), the Telecommunications Act, the Government Regulation on the Implementation of Electronic Systems and Transactions (GR EST), the Presidential Regulation on the Protection of Vital Information Infrastructure (PR VIIP), and the Minister of Communications and Informatics Regulation on the Protection of Personal Data on Electronic System. Although other sectoral laws and implementing regulations with provisions related to cybersecurity exist, most of them only regulate cybersecurity-related aspects in general (Hidayat & Juaningsih, 2022).

Regarding stakeholders and government actors, the main actor specifically assigned to implementing cybersecurity promoting measures is the National Cyber and Crypto Agency (BSSN). The main tasks of this executive agency concerning cybersecurity are to formulate, establish, and implement technical policies in the field of cybersecurity (Indonesia, 2021). Given the broad scope of cybersecurity, other government institutions also have a role in implementing cybersecurity, including the Ministry of Communications and Informatics (MCI), the Ministry of Defence, the State Intelligence Service, the National Police, and the National Armed Forces.

Apart from legislation and stakeholders, the Indonesian government has also implemented several initiatives and tools through various institutions. The intent is to leverage the potential of cyber-resilient infrastructure, foster technical readiness, and promote digital literacy. These initiatives result from cooperation between the government and stakeholders on the national and international levels.

3. The Dutch Cybersecurity Governance System

This section provides a high-level overview of cybersecurity governance in the Netherlands. It first turns to institutions and frameworks existing at the national level, before briefly elaborating on the European and International context – which is rapidly changing in the aftermath of the invasion of the Russian Federation in Ukraine.

3.1 National level

The main stakeholders that can be identified are governmental actors such as the National Cyber Security Centre (NCSC), the Cyber Security Council (CSR), the Radiocommunications Agency, as well as the General Intelligence and Security Service of the Ministry of the Interior and Kingdom Relations (AIVD). While cooperating, these institutions have different roles in enhancing the Dutch cybersecurity level. An overview of relevant legislation is provided in Table 3.

Stakeholders & Governmental Actors	
National Cyber Security Centre (NCSC)	Key organization within the cybersecurity framework. As part of the Ministry of Justice and Security, the NCSC is responsible for "making the Netherlands more resilient to cybercrime".
Cyber Security Council (CSR)	This independent advisory body of the Dutch government is focused on working at the strategic level to strengthen cybersecurity in the country. In this capacity, the CSR provides advice, expert reports, organizes meetings and symposiums, among other activities.
Radiocommunications Agency	The Radiocommunications Agency (in Dutch, *Agentschap Telecom*) is designated as the National Cybersecurity Certification Authority (NCCA) in the Netherlands. The responsibilities and powers of the NCCA are detailed in the Cybersecurity Act.
General Intelligence and Security Service of the Ministry of the Interior and Kingdom Relations (AIVD)	The AIVD safeguards national security by identifying risks and threats before they become apparent through the gathering of intelligence and risk analysis. Its tasks and areas of interest are detailed in the 2017 Intelligence and Security Services Act (Wiv 2017).
Legislation	
Security of Network and Information Systems Act (Wbni Act)	In effect since 9 November 2018. According to the Wbni Act, suppliers of critical services, digital services providers, and the central government must take measures to prevent cybercrime, protecting their network and information systems. In addition, these organisations must report cybersecurity incidents to the NCSC. The main aim of the Wbni is to mitigate the consequences of cyber-attacks while increasing the country's digital resilience.
Ministerial Decision on Network and Information Systems Security (Bbni)	Created to clarify some aspects of the Wbni. For example, it details what the essential service providers are and how an incident should be reported.
Dutch Telecommunications Act	According to the Dutch Telecommunications Act (in Dutch, *Telecommunicatiewet*), providers should "minimize the risk of threats to their safety and security, ensure continuity and notify the competent authority of any cyberthreats or incidents".
Selected Dutch criminal laws	Police Data Act, Criminal Data Act, Dutch Criminal Code (Wvsr), and Computercrime I, II, III Acts.

Initiatives and Tools	
Netherlands Fraud Help Desk	Offers information and shares cybersecurity-related trends in the country. It also provides warnings against frauds and scams, sharing relevant and updated information and alerts on the website and social media. Without any investigative capacity, the Help Desk focuses on raising awareness and protecting people against cybercrime.
Digital Trust Center (EZK)	The Digital Trust Center helps enterprises to have their digital security in order and ensures that they are digitally resilient.
Information Sharing and Analysis Centers (ISACs)	ISACs are non-profit organizations gathering information on cyber threats and allowing two-way sharing of information between the private and public sector.

Table 3. The Netherlands Cybersecurity Governance. Source: Compiled by Authors, 2023.

The Netherlands has imposed various types of regulations, standards, and protocols for organisations to follow in data handling and in information security. Furthermore, the Netherlands has also passed various criminal provisions detailing many digital crimes – the most important ones are mentioned in Table 3 as well. Lastly, the Netherlands has rolled out various initiatives and tools that help the country not to fall victim to cybercrime. An important initiative of this kind is, for instance, the Fraud Help Desk, administrating all recent reports of country-wide frauds (Fraudehelpdesk.nl, 2023). Finally, enterprises and organisations are being engaged through various initiatives whose aim is to help ensure compliance with all cybersecurity requirements.

3.2 European and international level

Considering the political and geographical position of the Netherlands, it is also important to take into account initiatives at the international level – particularly the Council of Europe and the European Union. While it goes beyond the scope of this article to mention all relevant frameworks in detail, it is appropriate to name the most important ones. It should also be stressed that in this section, we focus on frameworks directly addressing cybersecurity, whereas related frameworks, such as the 2016 EU General Data Protection Regulation, might also have a considerable impact on the cybersecurity landscape (Wicki-Birchler, 2020). Some of them might also create pathways towards more cooperation – or at least indirect harmonisation of laws – with Indonesia.

As the only internationally binding treaty on the subject, the Budapest Convention on Cybercrime – also known as the 2001 Convention on Cybercrime – is of central importance (Wicki-Birchler, 2020, p. 65). The Convention aims to regulate cybercrime and create a standardised policy to protect society against cyber threats. As of July 2023, 68 states have ratified the convention, with additional 2 states having provided signatures in the absence of ratification (Council of Europe, 2023). The Netherlands ratified the convention in 2006. According to the Budapest Convention, ratifying states should align their national laws and procedures with its provisions, either by creating new laws or amending existing ones. It remains the most significant international instrument addressing cybercrime and is open to ratification by states that are not members of the Council of Europe. The Convention has gained recognition worldwide, with countries like the United States, Argentina, Australia, Canada, and Japan, as well as many others across Africa, Asia, Latin America, and the Pacific Ocean, signing and ratifying it (Council of Europe, 2023).

The convention has been extended through two additional protocols. The first protocol, focusing on xenophobia and racism, aimed to penalise acts of a racist and xenophobic nature committed through computer systems (Council of Europe, 2006). In 2021, a second protocol was added, addressing enhanced cooperation and disclosure of electronic evidence across borders (Council of Europe, 2022; Spiezia, 2022). This protocol aims to facilitate cross-border investigations and overcome challenges posed by shifting or unknown jurisdictions in the digital age.

At the level of the European Union, the Network and Information Security (NIS) Directive from 2016 was the first EU-wide legislation on cybersecurity. It is aimed at achieving a high common level of cybersecurity across Member States (Markopoulou et al., 2019). However, its implementation faced challenges, leading to fragmentation in the European Union and differences between the Member States. In response, the European Union worked on the NIS2 Directive, which aims to strengthen security requirements, address supply chain security, streamline reporting obligations, and introduce stricter supervisory measures and enforcement requirements, including harmonised sanctions across the EU. NIS2 was adopted by the European Parliament and the Council in November 2022, entering into force on 16 January 2023. Member States have until 17 October 2024 to transpose their measures into national law (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS 2 Directive), 2022; Schmitz-Berndt, 2021; Schmitz-Berndt & Chiara, 2022).

However, in Member States such as the Netherlands, questions remain on how to concretely transpose the enhanced lists of cybersecurity requirements in public and private sector organisations (e.g. which institutions count as essential services providers, which as digital service providers, how to implement heightened technical and organisation cybersecurity requirements, etc.).

These developments must be considered together with establishing the 2019 EU Cybersecurity Act, a framework that strengthens the mandate of the European Union Agency for Cybersecurity (ENISA). The Cybersecurity Act contains provisions to establish certification schemes enhancing the security of information and communications technology products, services, and processes (European Union, 2023b). Considering the most recent events in Ukraine, the European Commission has further proposed to work on a Cyber Resilience Act (European Union, 2022) and a Cyber Solidarity Act (European Union, 2023a). The former should result in a comprehensive and enhanced cybersecurity framework to guarantee cybersecurity over the entire product lifecycle on the European single market, whereas the latter establishes emergency funding to tackle big cyber-incidents with the support of ENISA and the European Cybersecurity Competence Centre established in 2021.

4. Comparison and Pathways Towards Enhanced Cooperation

In this section, we compare the analysis presented above and summarise it along guiding themes such as legislation and international cooperation, technology and infrastructure, human capacity, and digital literacy.

4.1 Legislation & international cooperation

As outlined in Table 1, several bilateral and multilateral efforts have been made to pave the way towards more cooperation between Indonesia

and the Netherlands. However, such initiatives remain limited to political statements of intent or cooperation among research institutions. This raises the question of whether overarching international frameworks have indirectly affected harmonisation. Although Indonesia has not formally ratified or accessed the Council of Europe's Budapest Convention, it has been highly influential in shaping the country's approach to national cybersecurity governance. The Indonesian EIT Act of 2008, particularly Chapter VII, lists similar offenses to those outlined in the Convention on Cybercrime, although several articles were revoked by the newly enacted Indonesian Criminal Code.

Additionally, content-related offences in Indonesia are regulated per the Convention's provisions. Thus, the Convention has played a significant role in framing Indonesia's cybersecurity governance framework. Whether the recent EU efforts mentioned above will have a similar effect seems too early to conclude at this point.

4.2 Technology & infrastructure

Both countries recognise the need for improved infrastructure to mitigate cyberattacks risks. In Indonesia, cyberattacks through malware, website defacement, data breaches, and data manipulation have increased significantly in recent years. Moreover, Internet users are becoming increasingly suspicious of the practices in the IT/technology industry (UGM, 2022b), while there are questions from the government regarding reliance on foreign data platforms. Such issues are also well known in the Netherlands, as the country experiences an increasing amount of cyberattacks but also faces questions relating to international data transfers (e.g. to the United States; see e.g. Gstrein & Zwitter, 2021). In the past years, DDoS and ransomware attacks have targeted educational institutions, the financial sector, public organisations, and Internet Service Providers. Furthermore, the reported number and duration of DDoS attacks have been significant, putting the Dutch National Internet Providers Management Organisation in a difficult position to defend against those incidents in 2021 (National Coordinator for Counterterrorism and Security, 2022, p. 35, 36, 39). This highlights the need to enhance the cybersecurity of technology and (critical) infrastructure in both countries.

4.3 Human capacity & digital literacy

Indonesia must enhance human capacity to effectively mitigate the effects of cyberattacks and increase digital literacy to prevent them. It requires more than a sophisticated infrastructure and legislation to create a secure cyberspace, as some types of cyberattacks happen using social engineering methods. Social engineering takes advantage of the negligence of tech users in securing their personal information. A recent survey by the MCI showed that the Digital Literacy Index of Indonesians scored at 3.49 (average) in 2021 (Center, 2022). In collaboration with an independent consultant, Katadata, the Ministry assessed citizens with four pillars of Indonesia's digital literacy curriculum: Digital Ethics, Digital Culture, Digital Skills, and Digital Safety. The finding of the survey shows that Digital Safety scores the lowest. Therefore, low awareness of cybersecurity issues among the public and government officials is also a concern that must be addressed to improve cybersecurity in Indonesia (Ashari, 2020).

In comparison, the Netherlands is in top position in Europe regarding digital literacy and digital skills. In 2021, it was reported that 80% of its population had at least 'basic' or 'above basic' digital skills (Dutch Statistics Institute – CBS, 2022). Furthermore, the Netherlands recognises the need to develop high-quality cybersecurity knowledge. For this reason, in the past years, the government has encouraged and invested in developing higher education courses and research on cybersecurity, e.g. the National Cybersecurity Research Agenda (National Cyber Security Centre, 2019). However, the Dutch government also recognises that there is a shortage of highly trained cybersecurity professionals. This shortage leads to insufficient cybersecurity knowledge in organisations, often causing them to be not sufficiently resilient.

5. Conclusion

In this article, we presented an unusual comparison of cybersecurity governance in two different countries and analysed their respective policies. Despite those differences, Indonesia and the Netherlands face similar cybersecurity-related challenges and have initiated cooperative efforts to address them. With its large population and developing economy, Indonesia is vulnerable to cyber threats due to rapid spread of the Internet, especially through mobile connections. The country has experienced a significant increase in cyberattacks, facilitated by an infrastructure that lacks resilience, and a low digital literacy rate of the population. In contrast, the Netherlands has a high Internet penetration rate and higher digital literacy rates. Nevertheless, challenges remain as the enhanced connectivity results in more potential for attacks and require more maintenance through qualified personnel.

Both countries need to develop their governance frameworks and infrastructure to address these challenges.

Indonesia needs to develop comprehensive cybersecurity legislation. This will provide a legal basis for cybersecurity, lend more legitimacy to the topic, and enable better coordination among various government institutions. The Netherlands should continue to enhance digital resilience and ensure that laws and regulations keep pace with evolving cyber threats, in collaboration with European and international partners. Furthermore, both countries should prioritise awareness programs to educate the public, organisations, and government agencies about cybersecurity risks and best practices. Capacity-building initiatives, such as training programs and partnerships among higher education institutions, can facilitate developing a skilled workforce (see e.g. the online course on 'digital intelligence', UGM, 2022a). Finally, despite increasing geopolitical tensions, international cooperation remains instrumental in improving cybersecurity.

It is evident that Indonesia and the Netherlands face distinct cybersecurity challenges due to their geographic locations. By collaborating, these two countries can bridge the gap between regional cybersecurity initiatives, paving the way for cross-regional knowledge sharing and collaboration. The selection of Indonesia and the Netherlands as a case study for enhanced cybersecurity cooperation is justified by the unique challenges, complementary capabilities, bilateral relations, and cultural diversity they represent. The collaborative efforts between these two countries can lead to significant advancements in cybersecurity governance and offer valuable insights for other nations facing similar cybersecurity challenges. In this spirit, both Indonesia and the Netherlands should continue their collaborative efforts in cybersecurity through bilateral and multilateral partnerships. In addition, the collaboration will help understand and appreciate both countries' different cultural, societal, and geopolitical perspectives, leading to more inclusive and comprehensive cybersecurity policies that reflect the diverse needs and priorities of both nations. Sharing best practices, exchanging threat intelligence, and participating in international forums will facilitate knowledge sharing and strengthen the collective response. ■

About the authors:

Oskar J. Gstrein is an Assistant Professor at the Department of Governance and Innovation at Campus Fryslân of the University of Groningen in the Netherlands, where he is also a member of the Data Research Centre (DRC).

Tais Fernanda Blauth is a PhD researcher at the Department of Governance and Innovation at Campus Fryslân of the University of Groningen (The Netherlands), where she is also a member of the Data Research Centre.

Faiz Rahman is an Adjunct Researcher at the Center for Digital Society (CfDS) and a Lecturer at the Faculty of Law, Universitas Gadjah Mada, Indonesia. He is currently a PhD researcher at The Van Vollenhoven Institute for Law, Governance and Society, Leiden Law School, Universiteit Leiden, the Netherlands.

Anisa Pratita Kirana Mantovani is an Adjunct Researcher at the Center for Digital Society (CfDS), Universitas Gadjah Mada, Indonesia. She currently holds the position of the Head of Public Policy and Government Relations at the Indonesian E-Commerce Association (idEA).

Annisa Paramita Wiharani is an Adjunct Researcher at the Center for Digital Society (CfDS), Universitas Gadjah Mada, a PhD researcher at The Department of International Relations and International Organization, University of Groningen (The Netherlands), and a Lecturer at the Department of International Relations, Catholic University of Parahyangan, Indonesia.

References

Ashari, M. (2020). Keamanan Informasi: Sudah Saatnya Kita Peduli. In Kementerian Keuangan Republik Indonesia. https://www.djkn.kemenkeu.go.id/kpknl-kisaran/baca-artikel/13113/Keamanan-Informasi-Sudah-Saatnya-Kita-Peduli.html

Brooks, C. (2023, March 5). Cybersecurity Trends & Statistics For 2023; What You Need To Know. Forbes. https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/

Center, K. insight. (2022). Indeks Literasi Digital Indonesia Masuk Kategori Sedang Pada 2021. In Katadata. https://databoks.katadata.co.id/datapublish/2022/01/20/indeks-literasi-digital-indonesia-masuk-kategori-sedang-pada-2021

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. South African Journal of Information Management, 23(1), 1–11. https://doi.org/10.4102/sajim.v23i1.1277

Council of Europe. (2006, March 1). Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189). Treaty Office. https://www.coe.int/en/web/conventions/full-list

Council of Europe. (2022, May 12). Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). Treaty Office. https://www.coe.int/en/web/conventions/full-list

Council of Europe. (2023, July 7). Chart of signatures and ratifications of Treaty 185. Treaty Office. https://www.coe.int/en/web/conventions/full-list

Dutch Statistics Institute - CBS. (2022, May 12). Dutch digital skills at the top in Europe [Webpagina]. Statistics Netherlands. https://www.cbs.nl/en-gb/news/2022/19/dutch-digital-skills-at-the-top-in-europe

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS 2 Directive), 2022/2555 (2022).

European Union. (2022, September 15). Cyber Resilience Act | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

European Union. (2023a, June 20). The EU Cyber Solidarity Act | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

European Union. (2023b, June 30). The EU Cybersecurity Act | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

Europol. (2021). Internet Organised Crime Threat Assessment (IOCTA) 2021 (p. 45). Publication Office of the European Union, Luxembourg.

Fraudehelpdesk.nl. (2023). About Fraud Help Desk. Fraude Help Desk. https://www.fraudehelpdesk.nl

Goel, S. (2020). National Cyber Security Strategy and the Emergence of Strong Digital Borders. Connections, 19(1), 73–86.

Gstrein, O. J., & Zwitter, A. J. (2021). Extraterritorial application of the GDPR: Promoting European values or power? Internet Policy Review, 10(3). https://doi.org/10.14763/2021.3.1576

Hidayat, R. N., & Juaningsih, I. N. (2022). Legal Protection For The Community In Cyber Space Through Regulation Forming With The Omnibus Method. IPMHI Law Journal, 2(2), 143–156.

Indonesia, R. of. (2019). Naskah Akademik Rancangan Undang-Undang tentang Keamanan dan

Ketahanan Siber (Academic Draft of Cyber Security and Resillience Bill).

Indonesia, R. of. (2021). Presidential Regulation No. 28 of 2021 on National Cyber and Crypto Agency.

International Telecommunication Union. (2020). Global Cybersecurity Index 2020. In ITU Publications. ITU Publications.

Jisi, W., & Ran, H. (2019). From cooperative partnership to strategic competition: A review of China–U.S. relations 2009–2019. China International Strategy Review, 1(1), 1–10. https://doi.org/10.1007/s42533-019-00007-w

Kamara, I., Leenes, R., & Stuurman, K. (2020). The Cybersecurity Certification Landscape in the Netherlands after the Union Cybersecurity Act. Tilburg Institute for Law, Technology, and Society - Commissioned by the National Cyber Security Centre of the Netherlands. https://www.ncsc.nl/documenten/rapporten/2020/oktober/2/the-cybersecurity-certification-landscape-in-the-netherlands-after-the-union-cybersecurity-act

Keohane, R. O., & Nye, J. S. (1998). Power and Interdependence in the Information Age. Foreign Affairs, 77(5).

Kingdom of the Netherlands. (2020, March). Dutch Economic Mission to Indonesia. The Netherlands andYou;MinistryofForeignAffairs.https://www.netherlandsandyou.nl/latest-news/news/2020/04/16/dutch-economic-mission-to-indonesia-march-2020

Kiswondari. (2021). Serangan Siber di Indonesia Meningkat 5 Kali Lipat, Kebocoran Data Salah Satunya. In SINDOnews. https://nasional.sindonews.com/read/527718/12/serangan-siber-di-indonesia-meningkat-5-kali-lipat-kebocoran-data-salah-satunya-1630408129

Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review, 35(6), 105336. https://doi.org/10.1016/j.clsr.2019.06.007

National Information and Communication Technology Council. "Pengembangan Keamanan Siber Nasional," 2018.National Coordinator for Counterterrorism and Security. (2022). Cyber Security Assessment Netherlands (CSAN) 2022 (p. 52). Ministry of Justice and Security. https://english.nctv.nl/binaries/nctv-en/documenten/publications/2022/07/04/cyber-security-assessment-netherlands-2022/Cyber+Security+Assessment+Netherlands+2022.pdf

National Cyber Security Centre. (2019, July 1). National Cybersecurity Agenda—National Cyber Security Centre [Onderwerp]. Nationaal Cyber Security Centrum. https://english.ncsc.nl/topics/national-cybersecurity-agenda

Nuffic. (2023). StuNed Scholarships. Study in Holland. https://www.studyinholland.nl/finances/stuned-scholarships

Rahman, J., Azhari, M. L., Tamba, S. R., Ramadhan, A. N., Fakhriyah, I., Hilmi, M. A., Hartadi, E. E., & Kristallia, R. (2021). Laporan Tahunan Hasil Monitoring Keamanan Siber 2021. In A. Nugroho & F. E. Prasaja (Eds.), Laporan Tahunan. Badan Siber dan Sandi Nasional Republik Indonesia.

Schmitz-Berndt, S. (2021). European Union · Cybersecurity is Gaining Momentum – NIS 2.0 is on its Way. European Data Protection Law Review, 7(4), 580–585. WorldCat.org. https://doi.org/10.21552/edpl/2021/4/14

Schmitz-Berndt, S., & Chiara, P. G. (2022). One step ahead: Mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive. International Cybersecurity Law Review, 3(2), 289–311. https://doi.org/10.1365/s43439-022-00058-7

social, W. are & KEPIOS. (2022a). Digital 2022 Indonesia.

social, W. are & KEPIOS. (2022b). Digital 2022: The Netherlands.

Spiezia, F. (2022). International cooperation and protection of victims in cyberspace: Welcoming Protocol II to the Budapest Convention on Cybercrime. ERA Forum, 23(1), 101–108. https://doi.org/10.1007/s12027-022-00707-8

UGM. (2022a). Kecerdasan Digital. Kecerdasan Digital 2022. https://kecerdasandigital.id/

UGM, C. for D. S. (2022b). Diskusi Keamanan Siber Bagi Para Pemangku Kebijakan Pandemi.

Vermeulen, R. (2020). Cultural cooperation Indonesia-Netherlands 2021-2024. DutchCulture. https://dutchculture.nl/en/cultural-cooperation-indonesia-netherlands-2021-2024

Wicki-Birchler, D. (2020). The Budapest Convention and the General Data Protection Regulation: Acting in concert to curb cybercrime? International Cybersecurity Law Review, 1(1), 63–72. https://doi.org/10.1365/s43439-020-00012-5

World Bank. (2022, April 5). The World Bank in Indonesia [Text/HTML]. World Bank. https://www.worldbank.org/en/country/indonesia/overvi