ISEAS YUSOF ISHAK INSTITUTE

ISSUE: 2024 No. 78

ISSN 2335-6677

PERSPECTIVE

RESEARCHERS AT ISEAS – YUSOF ISHAK INSTITUTE ANALYSE CURRENT EVENTS

Singapore | 3 October 2024

Vietnam Strengthens Cyber Capabilities for Political Stability, National Defence, and Socio-economic Development

*Bich Tran**

A vendor uses her mobile phone as she sits in front of a garage door in the colours and shapes of the Vietnamese flag in Hanoi on 28 August 2024. (Photo by Nhac NGUYEN/AFP).

** Bich Tran is a postdoctoral fellow at the Lee Kuan Yew School of Public Policy and a former visiting fellow at the ISEAS – Yusof Ishak Institute.*

ISSUE: 2024 No. 78
ISSN 2335-6677

EXECUTIVE SUMMARY

- Vietnam's efforts to enhance its cyber capabilities are driven by the need to protect the regime of the Communist Party of Vietnam, defend national sovereignty and achieve socio-economic development goals.

- Vietnam has made significant investments in developing digital infrastructure, training a skilled cybersecurity workforce, and strengthening the legal framework for cyberspace governance through domestic initiatives and international cooperation.

- The government must strike a delicate balance between ensuring stability and effective regulation of cyberspace on the one hand and protecting individual rights and promoting innovations on the other.

- Vietnam's ability to effectively leverage its growing cyber capabilities will be a key determinant of its success in the 21st century.

INTRODUCTION

In the rapidly evolving digital landscape of the 21st century, Vietnam has emerged as a significant player in the realm of cybersecurity and has been impressive in its digital transformation. This article examines Vietnam's multifaceted approach to developing its cyber capabilities, driven by the imperatives of regime survival, national defence, and socio-economic development. As the country navigates the complex challenges and opportunities presented by cyberspace, it has made substantial investments in digital infrastructure, cyber personnel, and legal frameworks. By analysing Vietnam's motivations, strategies, and specific initiatives in enhancing and leveraging its cyber capabilities, the article provides comprehensive insights into the country's approach in the digital age.

VIETNAM'S PERCEPTION OF CYBERSPACE AND CYBERSECURITY

The Vietnamese government considers cyberspace an integral and inseparable component of national sovereignty, akin to land, islands, maritime zones, and airspace. It asserts that each nation holds supreme and absolute rights over the cyberspace within its control.[1] This concept of cyber sovereignty is understood as "the right of a nation to exercise independent, complete and full legislative, executive and judicial control within the scope of its national network territory, in accordance with international law and the nature of cyberspace".[2]

Cyberspace has become an integral part of Vietnam's society. As of April 2024, the country's internet penetration rate stands at 79.3 per cent of the population, surpassing the global average and neighbouring countries such as China, the Philippines, and Indonesia.[3] This high level of internet usage has contributed to Vietnam's emergence as a major software hub in Southeast Asia.[4] This high level of internet usage presents new opportunities for national development, but it also serves as an environment for conducting cyber warfare and information operations. Consequently, Vietnam maintains that protecting national sovereignty in cyberspace safeguards its independence, sovereignty, and territorial integrity, and provides a peaceful and stable environment for national development.[5]

Ensuring cybersecurity in Vietnam is a whole-of-government endeavour that involves the coordinated efforts of multiple ministries and stakeholders. The Ministry of Defence, Ministry of Public Security, and Ministry of Information and Communications play pivotal roles in shaping and implementing the country's cybersecurity strategies. Additionally, the Ministry of Foreign Affairs contributes to international cooperation and diplomatic aspects of cybersecurity, while the Ministry of Science and Technology focuses on technological innovations and research in this domain. The Ministry of Finance is involved in allocating resources and managing the financial aspects of cybersecurity initiatives. Beyond these key ministries, other government departments also contribute to Vietnam's cybersecurity efforts, each bringing their specific expertise and responsibilities. This collaborative approach extends beyond government entities to include various organisations, individuals, telecommunications companies, and Internet service providers,[6] reflecting Vietnam's recognition of cybersecurity as a multifaceted challenge that requires a unified and diverse response from all sectors of society.

MOTIVATIONS

Regime Survival

One of the primary drivers behind Vietnam's endeavours to enhance its cyber capabilities is the preservation of the Communist Party of Vietnam's (CPV) ruling power and survival. The CPV is determined to guard against what it sees as a "peaceful evolution"[7]—efforts by external forces to seek regime change without using military means. The late General Secretary Nguyen Phu Trong, for example, urged all cadres, party members, civil servants and public employees to remain loyal to the Party's principles and vigilant against signs of "peaceful evolution", including "self-evolution" and "self-transformation".[8] These terms refer to the erosion of socialist ideals and the adoption of capitalist or Western values. Dissidents and opposition groups have leveraged platforms such as Facebook, TikTok, Twitter (now X), and Zalo to spread anti-government messages and challenge the CPV's authority.[9] By enhancing its cyber capabilities, the CPV aims to better monitor, control, and counter the spread of anti-government sentiments online, thus safeguarding its power and the stability of the regime.

National Defence

Vietnamese officials regard cyberspace as an important battlefield, alongside air, land, sea, and outer space domains.[10] In July 2016, two weeks after the arbitral tribunal ruling that invalidated China's nine-dash line, a hacking group known as 1937cn, believed to be Chinese, took control of flight information screens and sound systems at Vietnam's two major airports. They displayed messages supporting Beijing's claims in the South China Sea, while renouncing claims by Hanoi and Manila.[11] This incident heightened Vietnam's awareness of its vulnerabilities in cyberspace.

China also employs subtler tactics to promote its claims in the digital realm, such as inserting the nine-dash line in popular media. In 2019, for instance, Vietnam only realized that Abominable—a collaboration between DreamWorks Animation and China-based Pearl Studio—contained the infamous nine-dash line after it had been shown in theatres for a week.[12] The inclusion of the line in the movie was seen as an attempt by China to legitimize its territorial claims. These incidents, whether carried out by state or non-state actors, serve as clear examples of how cyberspace has become an arena in the territorial disputes between Vietnam and China.

In its 2022 "National Cybersecurity and Safety Strategy to Proactively Respond to Challenges from Cyberspace, with a Vision toward 2030", Vietnam explicitly identifies the protection of national sovereignty in cyberspace as one of its main priorities.[13] As tensions in the South China Sea persist, Vietnam will need to continue strengthening its cyber capabilities to deter, detect, and deal with threats in the digital domain and defend its national interests.

Vietnam has also recognized the crucial role of cyber capabilities in achieving its socio-economic objectives. Its government has set ambitious goals of becoming an upper-middle income economy by 2030 and a high-income developed country by 2045.[14] To support these objectives, the 2022 "National Strategy on Digital Economy and Digital Society Development to 2025, with a Vision to 2030" has been implemented. It aims to increase the share of the digital economy to 20 per cent of GDP by 2025 and 30 per cent by 2030. In terms of the digital society, the strategy sets targets for smartphone ownership among adults, with a goal of reaching 80 per cent by 2025 and 95 per cent by 2030.[15]

Recognizing the potential of e-government, Vietnam has also placed emphasis on streamlining administrative processes, reducing corruption, and enhancing the delivery of public services to its citizens and businesses. By 2025, the government aims to have 100 per cent of administrative procedures available through fully online public services, and be ranked among the top 30 leading e-Government nations by 2030.[16]

However, the country has faced challenges in the form of cyberattacks and online fraud, resulting in significant financial losses and public distress. According to the Vietnam National Cyber Security Company, there were 13,900 reported cyberattacks targeting government agencies, banking systems, financial institutions, industrial systems, and other critical infrastructure in 2023.[17] In the same year, there were also nearly 16,000 reports from Vietnamese internet users concerning online fraud, resulting in an estimated loss of 390 trillion dong (approximately 16.6 billion USD), equivalent to 3.6 per cent of GDP.[18] These figures only represent reported incidents, and the actual damages could be significantly higher. As a result, Vietnam has recognized the urgent need to enhance its cyber capabilities to address these threats effectively.

EFFORTS TO ENHANCE CYBER CAPABILITIES

Improving Digital Infrastructure

Vietnam recognizes that a robust and reliable digital infrastructure is essential for its digital transformation. In recent years, the government has committed to developing the country's broadband networks, data centres, and cloud computing, as well as to meeting international IT standards.

The country has heavily invested in broadband telecommunications networks to ensure large capacity and high speed. The "Planning of Information and Communication Infrastructure for the Period 2021-2030, with a Vision to 2050" was approved in 2024, setting ambitious targets. By 2025, the goal is to provide 100 per cent of households with access to fibre optic cables, and 90 per cent of fixed internet users with an average speed of 200 Mb/s. By 2030, the goal is to ensure that all users have access to speeds exceeding 1 Gb/s, with 99 per cent of the population covered by the 5G mobile broadband network.[19]

To achieve these targets, Vietnam plans to develop 4-6 more international submarine fibre optic cable routes. For remote, border, sea, island, and currently uncovered areas, the use of satellite coverage systems is being prioritized. To enhance its satellite transmission system, Vietnam has plans to replace the Vinasat 1 and 2 satellites.[20]

Vietnam has also invested in data centre and cloud computing infrastructure. By 2025, the aim is to establish at least three national-level multi-purpose data centre clusters, with 70 per cent of Vietnamese enterprises using domestic cloud computing services. By 2030, the goal is to develop large-scale data centre clusters according to green standards, interconnected and shared to form a network of data centre clusters.[21] These investments will enable Vietnam to store, process, and analyse large amounts of data for various purposes.

In addition to domestic efforts, Vietnam has recognized the importance of international cooperation in developing its digital infrastructure. In 2022, for example, Vietnam signed a Memorandum of Understanding (MOU) on cooperation in digital economy development with Singapore,[22] and in 2023, it signed an MOU with Indonesia related to digital infrastructure development.[23] The United States has also pledged support for Vietnam's efforts in developing high-quality digital infrastructure.[24] These partnerships will provide Vietnam with access to expertise, technology, and financial resources.

In developing its cyber infrastructure, Vietnam has made use of standards set by the Common Criteria Recognition Arrangement (CCRA), despite not being a member of this organisation. The CCRA is an international agreement enabling 31 participating countries to mutually recognise each other's information technology security certifications.[25] By utilising this widely recognised standard, Vietnam aims to ensure that its digital infrastructure meets high benchmarks for security and reliability, which is crucial for attracting investment and fostering innovation in the digital economy.

By investing in digital infrastructure, encompassing both physical assets and security standards, Vietnam aims to create a strong foundation for its digital transformation and socio-economic development. However, Vietnam will need to address challenges such as ensuring equitable access to digital services across the country, developing the necessary skills and expertise to operate and maintain these systems, and securing the financial resources required for these investments.

Training Cyber Personnel

Vietnam is dedicated to building a strong and skilled cyber workforce, with efforts focused on both quantity and quality. A significant step in this direction was the establishment of the Vietnam Cyber Emergency Response Centre (VCERC) in 2019.[26] The centre is tasked with organising simulation exercises, training, and workshops to enhance information security knowledge and skills for agencies, organisations, and businesses. Moreover, it develops an information security incident response force, thereby contributing substantially to the growth and proficiency of Vietnam's cybersecurity workforce.

In January 2022, Prime Minister Pham Minh Chinh approved the "Raising Awareness, Universalizing Skills, and Developing Human Resources for National Digital Transformation

By 2025, with Orientations to 2030" project. The goal of this project is to provide digital skills training to all government employees and train 5,000 high-quality digital technology graduates each year by 2025, increasing to 20,000 per year by 2030.[27]

Vietnam has also collaborated with international partners to enhance the quality of its cyber personnel. For instance, in 2016, the Vietnamese Ministry of Public Security signed an MOU on cyber security with the Indian Ministry of Electronics and Information Technology, which includes training and capacity building programmes.[28] The United States, Japan, and Australia also pledged to support Vietnam's human resource development in digital capability enhancement.[29] The United States, in particular, is supporting Vietnam's transition to a competent digital workforce to accelerate the growth of its digital economy. For example, the United States Agency for International Development allocated US$2.2 million for the period 2021-2023 for the "Workforce for an Innovation and Start-up Ecosystem" project, focusing on Hanoi, Ho Chi Minh City, and Mekong Delta provinces.[30] After two years, this project has collaborated with nine private and non-profit educational organizations, providing funding for digital skills training for 500 educators and over 3,000 students from more than 60 colleges and universities.[31]

Since 2019, Vietnam's cyber personnel has benefited from training, workshops and exercises offered by the ASEAN–Singapore Cybersecurity Centre of Excellence (ASCCE). These cover diverse areas such as international law, cyber strategy development, legislative frameworks, cyber norms, and other crucial cybersecurity policy matters. Additionally, the centre offers specialized technical training for Computer Emergency Response Teams (CERTs). The ASCCE also facilitates the exchange of open-source intelligence on cyber threats and attacks, as well as sharing best practices among member states.[32]

On 19 June 2023, Vietnam also participated in the "Project for Enhancing ASEAN-Japan Capacity Building Program for Cybersecurity and Trusted Digital Services". This initiative aims to enhance the ability of ASEAN countries to effectively respond to and handle cybersecurity threats and incidents by expanding training programmes for their cyber workforces.[33]

Vietnam is a member of the Global Forum on Cyber Expertise (GFCE), an international platform that brings together over 200 stakeholders from around the world. This forum serves as a hub for collaboration on various cybersecurity domains, including policy development, strategy formulation, cybercrime prevention, incident response, safeguarding critical infrastructure, and fostering a culture of cybersecurity awareness and skills. Through its member-driven working groups, the GFCE aims to enhance global cooperation, disseminate effective practices across regions, and stimulate research to address knowledge gaps in the field of cybersecurity.[34]

By investing in the quantity and quality of its cyber personnel, Vietnam aims to create a robust and resilient cybersecurity workforce that can protect the country's digital sovereignty, support its digital transformation, and contribute to its socio-economic development. However, Vietnam will need to address challenges such as ensuring the relevance and effectiveness of training programmes, attracting and retaining skilled personnel in the public sector, and keeping pace with the rapidly evolving technological landscape.

Vietnam has made significant efforts to regulate cyber activities through the establishment of a relatively comprehensive legal framework, including several documents that collectively govern various aspects of cyberspace.

The 2015 Law on Cyber Information Security contains a civil code, along with technical standards and regulations on cyber information security.[35] The 2015 Criminal Code includes articles 286, 287, 289, and 290 addressing various cybercrimes, such as spreading disruptive programmes, obstructing network operations, illegal access to networks, and using networks for property appropriation.[36] The 2018 Law on Cyber Security serves to govern and oversee various activities and measures aimed at safeguarding national security, as well as maintaining public order in cyberspace.[37] The 2018 Law on Protection of State Secrets prohibits drafting or storing documents with state secrets on Internet-connected devices, except when legally required for preservation.[38] The 2023 Telecommunications Law opens the door for wholly foreign-owned investments in basic telecommunications services, data centres, and cloud computing services.[39]

Notably, Vietnam's international cooperation has played a significant role in drafting these documents. For instance, the European Union's sharing of experience and legal expertise contributed to the development of Vietnam's 2018 Cybersecurity Law and subsequent decrees.[40] Furthermore, Vietnam's participation in the UN framework of responsible state behaviour in cyberspace has provided valuable guidance for developing its domestic laws.[41]

These legal documents demonstrate Vietnam's commitment to regulating cyber operations and addressing the challenges posed by the digital age. While the effectiveness of these laws and regulations in practice may vary, they provide a foundation for Vietnam to further develop its cyber capabilities and protect its national interests in cyberspace. However, as Vietnam continues to strengthen its legal framework for cyber governance, it is also crucial for the country to balance the need for effective regulation with the protection of individual rights and the promotion of innovation in the digital economy.

EXAMPLES OF LEVERAGING CYBER CAPABILITIES

Task Force 47

To protect the CPV, the General Political Department of the People's Army of Vietnam has established Task Force 47, named after its Directive No. 47 issued in 2016. Its mission is to counter "wrongful views" promoted by "hostile forces", often labelled as elements of a "peaceful revolution" by the regime.[42] Comprised of over 10,000 members, Task Force 47 reportedly includes military officials and personnel who perform their regular duties, but also serve as Internet commentators when needed.[43] The unit operates under the military's chain of command, with members receiving training and guidance on how to identify and counter unfavourable content online. Rather than focusing on the technical aspects of cyberspace, their strategy revolves around countering unfavourable views through propaganda approaches.

Cyberspace Operations Command

In August 2017, Vietnam created the Cyberspace Command, a combat unit that operates directly under the Ministry of National Defence. The Command is responsible for "defending national sovereignty in cyberspace, countering information warfare, cyberwarfare and safeguarding the Homeland in cyberspace".[44] It is also expected to have advanced capabilities in cyber defence, cyber intelligence, and possibly even offensive cyber operations. The establishment of this unit reflects Vietnam's awareness of the growing importance of cyberspace as a domain of military operations and its need for specialized resources and expertise to address cyber threats.

National Public Service Portal

In 2019, Vietnam launched the National Public Service Portal. The portal aims to simplify and digitize government processes, making it easier for citizens and businesses to interact with government agencies and access essential services. As of June 2024, 4,536 administrative procedures have been made available as online public services.[45] By investing in e-government and digital transformation, Vietnam aims to create a more efficient, transparent, and responsive government that can better serve the needs of its citizens and support the country's socio-economic development goals.

CONCLUSION

Vietnam's efforts to boost its cyber capabilities reflect the country's recognition of the critical importance of cyberspace for its national security, economic prosperity, and social development. The country has made significant investments in developing digital infrastructure, training cyber personnel, and strengthening legal framework. Its ability to effectively leverage its cyber capabilities will be a key determinant of its success in the 21st century.

ENDNOTES

[1] Ministry of Information and Communications, "Không gian mạng và chiến lược bảo vệ chủ quyền "vùng lãnh thổ đặc biệt" của quốc gia" [Cyberspace and the strategy for protecting the sovereignty of the nation's "special territory"], 20 May 2023, https://mic.gov.vn/khong-gian-mang-va-chien-luoc-bao-ve-chu-quyen-vung-lanh-tho-dac-biet-cua-quoc-gia-197158520.htm
[2] Ministry of Public Security, "Yêu cầu và nghĩa vụ bảo vệ chủ quyền quốc gia trên không gian mạng" [Requirements and obligations for protecting national sovereignty in cyberspace], 7 July 2023, https://bocongan.gov.vn/tin-tuc/yeu-cau-va-nghia-vu-bao-ve-chu-quyen-quoc-gia-tren-khong-gian-mang-t35646.html
[3] DataReportal, "Digital 2024 April Global Statshot Report," 24 April 2024, https://datareportal.com/reports/digital-2024-april-global-statshot.
[4] World Bank, "Digital Progress and Trends Report 2023," 2024,https://openknowledge.worldbank.org/server/api/core/bitstreams/95fe55e9-f110-4ba8-933f-e65572e05395/content, p. 30.
[5] Ministry of Information and Communications, "Không gian mạng"

[6] VGP, "Nghị Định Về Ngăn Chặn Xung Đột Thông Tin Trên Mạng" [Decree on Preventing Information Conflicts on the Internet], 14 October 2016, https://datafiles.chinhphu.vn/cpp/files/vbpq/2016/11/142.signed.
[7] 12th Party Central Committee, "Báo cáo chính trị của Ban Chấp hành Trung ương Đảng khoá XII tại Đại hội đại biểu toàn quốc lần thứ XIII của Đảng" [Political Report of the 12th Party Central Committee at the 13th National Congress of the Party], 23 March 2021, https://tulieuvankien.dangcongsan.vn/ban-chap-hanh-trung-uong-dang/dai-hoi-dang/lan-thu-xiii/bao-cao-chinh-tri-cua-ban-chap-hanh-trung-uong-dang-khoa-xii-tai-dai-hoi-dai-bieu-toan-quoc-lan-thu-xiii-cua-3734.
[8] Nguyen Phu Trong, "Xây dựng và phát triển đối ngoại, ngoại giao Việt Nam toàn diện, hiện đại, mang bản sắc 'cây tre Việt Nam'" [Building and Developing Vietnam's Foreign Affairs and Diplomacy to be Comprehensive, Modern, and Imbued with the 'Vietnamese Bamboo' Identity], 2023, p.119.
[9] Vietnam.vn, "Bảo vệ chủ quyền quốc gia trên không gian mạng" [Protecting national sovereignty in cyberspace], 5 May 2023, https://www.vietnam.vn/bao-ve-chu-quyen-quoc-gia-tren-khong-gian-mang/.
[10] Vietnam.vn, "Bảo vệ chủ quyền quốc gia trên không gian mạng".
[11] Vnexpress.net, "Cyber terrorists attack flight info screens at Vietnam's 2 major airports," 29 July 2016, https://e.vnexpress.net/news/news/cyber-terrorists-attack-flight-info-screens-at-vietnam-s-2-major-airports-3444504.html.
[12] Associated Press, "Vietnam bans animated 'Abominable' over South China Sea map," 16 October 2019, https://apnews.com/arts-and-entertainment-movies-general-news-aa84fa2df6d541bd992a46c0761f1742.
[13] Prime Minister, "Phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030" [Approving the National Cybersecurity Strategy, proactively responding to challenges from cyberspace to 2025, with a vision to 2030], 10 August 2022, https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Quyet-dinh-964-QD-TTg-2022-phe-duyet-Chien-luoc-An-toan-An-ninh-mang-quoc-gia-den-2025-525540.aspx.
[14] 12th Party Central Committee, "Báo cáo chính trị."
[15] Prime Minister, "Chiến lược quốc gia phát triển kinh tế số và xã hội số đến năm 2025, định hướng đến năm 2030" [National strategy for digital economy and digital society development to 2025, with a vision to 2030], 31 March 2022, https://thuvienphapluat.vn/van-ban/Thuong-mai/Quyet-dinh-411-QD-TTg-2022-phe-duyet-Chien-luoc-quoc-gia-phat-trien-kinh-te-so-va-xa-hoi-so-508672.aspx.
[16] Prime Minister, "Quyết định số 942/QĐ-TTg của Thủ tướng Chính phủ: Phê duyệt Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số giai đoạn 2021 - 2025, định hướng đến năm 2030" [Decision No. 942/QD-TTg of the Prime Minister: Approving the E-Government Development Strategy towards the Digital Government for the 2021-2025 period, with orientation to 2030], 15 June 2021, https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Quyet-dinh-942-QD-TTg-2021-Chien-luoc-phat-trien-Chinh-phu-dien-tu-huong-toi-Chinh-phu-so-477851.aspx.
[17] Vietnam.net, "Bảo vệ chủ quyền quốc gia trên không gian mạng".
[18] Dan Tri, "Lừa đảo trực tuyến gây thiệt hại tương đương 3,6% GDP" [Online fraud causes damage equivalent to 3.6% of GDP], 13 May 2024, https://dantri.com.vn/suc-manh-so/lua-dao-truc-tuyen-gay-thiet-hai-tuong-duong-36-gdp-20240513162835898.htm
[19] Prime Minister, "Quyết định 36/QĐ-TTg 2024 phê duyệt Quy hoạch hạ tầng thông tin và truyền thông 2021-2030" [Decision 36/QD-TTg 2024 approving the Information and Communication Infrastructure Planning 2021-2030], 11 January 2024, https://thuvienphapluat.vn/van-ban/Xay-dung-Do-thi/Quyet-dinh-36-QD-TTg-2024-phe-duyet-Quy-hoach-ha-tang-thong-tin-va-truyen-thong-2021-2030-595184.aspx.
[20] Prime Minister, "Quyết định 36/QĐ-TTg 2024."
[21] Prime Minister, "Quyết định 36/QĐ-TTg 2024."

[22] Ministry of Information and Communications, "Vietnam and Singapore strengthen ties in digital economy development," 28 February 2022, https://english.mic.gov.vn/vietnam-and-singapore-strengthen-ties-in-digital-economy-development-197152791.htm
[23] Antara, "Indonesia, Vietnam to ink MoU on digital cooperation," 10 May 2023, https://en.antaranews.com/news/281229/indonesia-vietnam-to-ink-mou-on-digital-cooperation.
[24] White House, "Joint Leaders' Statement: Elevating United States-Vietnam Relations to a Comprehensive Strategic Partnership," 11 September 2023, https://web.archive.org/web/20240312143005/https://www.whitehouse.gov/briefing-room/statements-releases/2023/09/11/joint-leaders-statement-elevating-united-states-vietnam-relations-to-a-comprehensive-strategic-partnership/
[25] Common Criteria, "About the Common Criteria," n.d., https://www.commoncriteriaportal.org/ccra/index.cfm
[26] VNCERT/CC, "Giới thiệu về Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam" [Introduction to the Vietnam Cyber Emergency Response Centre], 18 November 2021, https://vncert.vn/post/193/ve-vncert-cc
[27] Prime Minister, "Phê duyệt Đề án 'Nâng cao nhận thức, phổ cập kỹ năng và phát triển nguồn nhân lực chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030" [Approving the Project "Raising awareness, universalizing skills and developing national digital transformation human resources to 2025, with orientation to 2030"], 28 January 2022, https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Quyet-dinh-146-QD-TTg-2022-pho-cap-ky-nang-va-phat-trien-nguon-nhan-luc-chuyen-doi-so-502108.aspx.
[28] Ministry of External Affairs of India, "Joint Statement between India and Vietnam during the visit of Prime Minister to Vietnam," 3 September 2016, https://www.mea.gov.in/bilateral-documents.htm?dtl/27362/Joint_Statement_between_India_and_Vietnam_during_the_visit_of_Prime_Minister_to_Vietnam.
[29] White House, "Joint Leaders' Statement"; VietnamPlus, "Vietnam, Japan issue joint statement on elevation of relations to comprehensive strategic partnership," 27 November 2023, https://en.vietnamplus.vn/vietnam-japan-issue-joint-statement-on-elevation-of-relations-to-comprehensive-strategic-partnership/271923.vnp; Prime Minister of Australia, "Joint statement on the elevation to a comprehensive strategic partnership between Vietnam and Australia," 07 March 2023, https://www.pm.gov.au/media/joint-statement-elevation-comprehensive-strategic-partnership-between-vietnam-and-australia.
[30] USAID, "USAID Workforce for an Innovation and Start-up Ecosystem (WISE)," n.d., https://www.usaid.gov/vietnam/fact-sheets/usaid-workforce-innovation-and-start-ecosystem-wise.
[31] U.S. Embassy & Consulate in Vietnam, "United States – Vietnam Digital Workforce Development Program Addresses Digital Divide," 24 January 2024, https://vn.usembassy.gov/united-states-vietnam-digital-workforce-development-program-addresses-digital-divide-trains-3000-students-and-establishes-new-partnerships/.
[32] CSA, "ASEAN-Singapore Cybersecurity Centre of Excellence," n.d., https://www.csa.gov.sg/News-Events/Press-Releases/2021/asean-singapore-cybersecurity-centre-of-excellence
[33] Mission of Japan to ASEAN, "Opening Ceremony of the Training Program for the ASEAN-Japan Cybersecurity Capacity Building Centre in Thailand," 19 June 2023, https://www.asean.emb-japan.go.jp/itpr_en/pr23_0619en.html.
[34] GFCE, "About," n.d. https://thegfce.org/
[35] National Assembly, "Law No. 86/2015/QH13 on Cyberinformation Security," 19 November 2015, https://thuvienphapluat.vn/van-ban/EN/Cong-nghe-thong-tin/Law-No-86-2015-QH13-on-Cyberinformation-Security-2015/303120/tieng-anh.aspx.
[36] National Assembly, "Bộ luật Hình sự 2015" [Penal Code 2015], 27 November 2015, https://thuvienphapluat.vn/van-ban/Trach-nhiem-hinh-su/Bo-luat-hinh-su-2015-296661.aspx.

[37] National Assembly, "Luật An ninh mạng 2018" [Law on Cybersecurity 2018], 12 June 2018, https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Luat-an-ninh-mang-2018-351416.aspx.
[38] National Assembly, "Luật Bảo vệ bí mật nhà nước 2018" [Law on Protection of State Secrets 2018], 15 November 2018, https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Luat-Bao-ve-bi-mat-nha-nuoc-2018-337064.aspx.
[39] National Assembly, "Luật Viễn thông" [Telecommunications Law], 24 November 2023, https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Luat-Vien-thong-24-2023-QH15-535782.aspx.
[40] Khanh Phi, Vietnam and EU strengthen cooperation in ensuring cybersecurity, 28 April 2022, https://hanoitimes.vn/vietnam-and-eu-strengthen-cooperation-in-ensuring-cybersecurity-320646.html
[41] United Nations, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," 22 July 2015,https://documents.un.org/doc/undoc/gen/n15/228/35/pdf/n1522835.pdf
[42] Tuoi Tre News, "Vietnam has 10,000-strong 'cyber troop': general," 26 December 2017, https://web.archive.org/web/20171226084329/https://tuoitrenews.vn/news/politics/20171226/vietnam-has-10000strong-cyber-troop-general/43326.html.
[43] Nguyen The Phuong, "The Truth About Vietnam's New Military Cyber Unit," The Diplomat, 10 January 2018, https://thediplomat.com/2018/01/the-truth-about-vietnams-new-military-cyber-unit/.
[44] Ministry of National Defence, "Vietnam National Defence," 2019, https://mod.gov.vn/wcm/connect/08963129-c9cf-4c86-9b5c-81a9e2b14455/2019VietnamNationalDefence.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-08963129-c9cf-4c86-9b5c-81a9e2b14455-mXO.UaH, p.86.
[45] Ministry of Industry and Trade of Vietnam, "National Public Service Portal," n.d., https://dichvucong.gov.vn/p/home/dvc-trang-chu.html.

ISEAS Perspective is published electronically by:
ISEAS - Yusof Ishak Institute

30 Heng Mui Keng Terrace
Singapore 119614
Main Tel: (65) 6778 0955
Main Fax: (65) 6778 1735

Get Involved with ISEAS.

Please click here:
https://www.iseas.edu.sg/support/get-involved-with-iseas/