

15. Vietnam

Vietnam has put in place a suite of strategies for cyber security and the advancement of its national power in cyberspace, including in the military domain. The governance structures for cyber policy operate through the ruling Communist Party of Vietnam's authoritarian political system. The government has implemented several policies that have contributed to robust growth in the ICT sector and to significant progress in the construction of e-government platforms. However, many government agencies still grapple with cyber-security issues because of a lack of funds and a huge shortage of cyber-security talent. The Communist Party's concerns regarding the threat

of internal subversion probably draw resources away from technical cyber-skills training and towards ideological work and the management of public opinion, thereby reducing investment in both defensive and offensive cyber capabilities. While overall offensive cyber capabilities are likely to be nascent or weak, the covert government-linked group APT32 could probably launch relatively sophisticated cyber attacks. Vietnam is a third-tier cyber power but it has considerable digital ambition and potential. If it can strengthen its key cyber-security skills, support its ICT firms and invest in advanced technology to protect its digital infrastructure, it could realise that potential.

Strategy and doctrine

Vietnam's laws and regulations surrounding cyber security were rather disparate until 2010, when it released its first national road map, 'Approving the National Planning on Development of Digital Information Security'.¹ The plan was more comprehensive and ambitious than those that most other countries had produced by that point. Its four overarching goals, aimed at addressing technical and legal weaknesses in the country's information security, were: to ensure the security of network and information infrastructure; to ensure the safety of data and applications; to train cyber-security professionals and increase public awareness of

information security; and to enhance the legal framework for information security, especially relating to computer crime and encryption. Funding was provided to train personnel in state agencies and bolster information security in the Ministry of Information and Communications (MIC), the Ministry of Public Security (MPS), the Government Cipher Committee and the Ministry of Industry. The road map also identified the need to encourage research and development (R&D).

A Network Information Security Plan was launched in 2016, aiming to augment the 2010 road map by outlining further objectives for the period 2016–20.²

List of acronyms

AIS	Authority of Information Security
ASEAN	Association of Southeast Asian Nations
CPV	Communist Party of Vietnam
ICT	information and communications technology
MIC	Ministry of Information and Communications
MND	Ministry of National Defence

MPS	Ministry of Public Security
NCSC	National Cyber Security Monitoring Centre
NSCER	National Steering Committee for Emergency Response
VNCERT	Vietnam Computer Emergency Response Team
VNPT	Vietnam Posts and Telecommunications Group
VPA	Vietnamese People's Army

It emphasised R&D and governmental cooperation with Vietnamese information-security firms through outsourcing, and set targets for the establishment of home-grown brands of information-security products. Vietnamese ICT associations were identified as key players in promoting this initiative.³ The plan also advocated the nationwide coordination of responses to security incidents. It foreshadowed the development of minimum security requirements for key national systems (both critical infrastructure and more sensitive government communications). Individual companies would be obliged to take responsibility for security by adhering to the relevant regulations, and to submit to regular audits of this compliance. The plan also promoted cyber-security drills for government- and private-sector entities, along with their participation in international forums.

For the Vietnamese government, cyber security is not just a technical question of protecting networks but also involves controlling the political content carried by those networks – as demonstrated, for example, by the Law on Network Information Security passed in November 2015.⁴ While this law focused primarily on technical and management aspects of preventing unauthorised access to ICT systems, it made clear that censorship and monitoring of domestic political expression would be a high priority for the government. It also flagged the need to control international exchanges in cyberspace, defining as illegal any information-related activity that the government considered a threat to national security, whether carried out by Vietnamese or foreign entities.

The Cyber Security Law passed in June 2018 was even more overtly political in its purpose, aiming to protect national security and ensure ‘social order and safety in cyberspace’ (Article 1).⁵ It included extensive definitions around content acceptability that were not part of the 2015 law. For example, in Article 8, it described as ‘strictly prohibited’ any attempt to ‘oppose the State’ or to distort history by ‘denying revolutionary achievements’. One of the most controversial elements of the 2018 law was enforced data localisation⁶ for all domestic and foreign companies operating in Vietnam, a move seen by the foreign companies as infringing on their business confidentiality and intellectual-property rights.⁷

The first official public document to convey Vietnam’s perspective on applying cyber to the military domain was the National Defence Law, also introduced in 2018.⁸ It described ‘information warfare’ as ‘activities and measures to disable the enemy’s information systems and secure Vietnam’s information systems’, which it included in the concept of ‘all-people national defense’ (Article 2), and specifically mentioned both cyber warfare and information warfare. The same year saw a Politburo resolution announcing a new ‘Strategy for the Homeland Protection in Cyberspace’,⁹ designed to develop a whole-of-society response, though centred on the armed forces, and to combine cyber defence with counter-attack.¹⁰

A defence white paper published in 2019 presented cyberspace as the fifth operational domain – alongside land, air, sea and space – in which to defend Vietnam’s national sovereignty.¹¹

Governance, command and control

Security policy, including for cyberspace, is directed by the Politburo of the Communist Party of Vietnam (CPV). The armed forces, through their Cyber Command, have a more central role in censorship and political surveillance than is the case in most countries, and therefore the Central Military Commission of the CPV, Vietnam’s highest decision-making body for national security, is probably the main command and governance authority for cyberspace policy. Other departments close to the party leadership, such as the Propaganda Department, also play a role in dealing with the most sensitive security issues.

The cyber policies dictated by the CPV leadership are implemented primarily by the MIC, the MPS and the Ministry of National Defence (MND), with the MIC as the coordinator for more technical aspects of cyber security as well as broad policies on content management.¹² Within the MIC, the Vietnam Computer Emergency Response Team (VNCERT)¹³ coordinates nationwide incident-response activities, collects and shares information on incidents and malware, directs cyber operations, and undertakes the testing of the cyber defences of public- and private-sector entities.¹⁴ The Authority of Information Security (AIS) formulates laws and policies regarding information security, and implements technical

measures to protect critical information infrastructure,¹⁵ while the National Electronic Authentication Centre secures electronic transactions through digital signatures and other authentication services.¹⁶

The MPS has two cyber-security departments – Cyber Security and High-tech Crime Prevention (A05), and Information Security and Communications (A87). A05 is tasked with preventing cyber crime, including online gambling and the spreading of false information, and cooperates with foreign investigation agencies on cases involving foreign cyber criminals. It also provides advice on cyber-security laws and policies, and promotes high-tech solutions aimed at boosting the government's capacity to counter cyber crime.¹⁷ A87 plays an advisory role on matters of policy, on legal aspects of security in the fields of culture, information and communication, and on countering criticism of the CPV and the leaking of state secrets.¹⁸

The MND directs two cyber-security departments – Cyber Command and the Government Cryptographic Agency. Cyber Command, established in August 2017 as an upgrade of the former Information Technology Department, reports to the Chief of the General Staff, who in turn is subordinate to the defence minister (a Politburo member). Comprising the Command Headquarters, three brigades, testing centres and a data centre, its responsibilities include political work, technical and logistical issues, and professional cyber operations.¹⁹ The Government Cryptographic Agency is in charge of securing the state's encrypted networks and R&D of related technologies.²⁰

The Vietnamese People's Army (VPA) contains a special cyber unit, Force 47, tasked with protecting the CPV against 'false news' and disseminating state propaganda. It has a task force whose personnel, numbering more than 10,000,²¹ have received training in ideological discipline and information warfare.²² They often operate on social-media platforms, including Facebook and YouTube, aiming to pre-empt any spreading of hostile information prior to major political events.

There is not enough information in the public domain to allow a confident assessment of the effectiveness of the governance and command arrangements for Vietnam's cyber forces, beyond the observation that strict obedience to the chain of command is enforced.

Core cyber-intelligence capability

Vietnam's cyber-intelligence capabilities lie in the MPS, MND and MIC. Within the MPS, the General Department of Intelligence and the General Department of Security (GDS) collect domestic and foreign intelligence. Inside the GDS, the specialist unit A42 monitors telephone calls, emails and the internet using systems procured from foreign vendors.²³ Also within the MPS, the Department for Cyber Security and High-tech Crime Prevention (AO5 – see previous section) has invested in modern technical equipment²⁴ and has joined Microsoft's Government Security Program to enhance its awareness of cyber threats.²⁵

Within the MND, the General Department of Military Intelligence is responsible for domestic and foreign intelligence. Cyber Command, although not an intelligence agency, is likely to possess cyber-intelligence capabilities that would have evolved from the VPA's proven signals-intelligence capacity during the Vietnam War. Also operating within the MND, the Government Cryptographic Agency is a vital part of Vietnam's cyber-intelligence capability, being responsible for ensuring the cyber security of the country's civilian and military leaders.

In its role as coordinator for all government departments concerned with cyber security, the MIC also possesses cyber-intelligence capabilities. Its National Cyber Security Monitoring Centre works alongside the VNCERT and provincial Cyber Security Control Centres²⁶ in monitoring Vietnamese cyberspace for potential threats.

Vietnam's cyber-intelligence capability is amplified to some degree by a group known to cyber-security companies as APT32.²⁷ Though apparently a non-state entity, it is assessed to have informal links to the government. Its cyber-espionage operations have been widely documented by US cyber-security companies and appear to have been quite proficient, with targets including foreign companies, the Association of Southeast Asian Nations (ASEAN) and Chinese government institutions (including those managing China's response to COVID-19). Overall, however, Vietnam's cyber-intelligence capability is likely to be weak, in part because of the country's shortage of skilled workers in the ICT domain.²⁸

Cyber empowerment and dependence

In 2019 the Politburo announced the target that Vietnam's digital economy should contribute 20% of GDP by 2025 and at least 30% by 2030,²⁹ as compared with 15% in 2018.³⁰ This will only be achievable with significant policy reform and large-scale new investment. The government has been pushing forward initiatives such as the National Digital Transformation Programme, launched in 2020,³¹ and has prioritised e-government projects.³² It also claims that the ICT sector has been growing at an impressive average annual rate of 30% for a number of years (the precise period is not stated).³³ However, in almost all indicators of ICT readiness, Vietnam ranks behind Malaysia and far behind Singapore, though just ahead of Indonesia.³⁴ In 2020 the country's internet penetration rate reached 70%³⁵ and its e-commerce market

was the third biggest in Southeast Asia, just behind those in Indonesia and Thailand.³⁶ Though significant progress has been made, there is still some way to go in terms of digital transformation. For example, cashless payments account for only a small proportion of total payments, and cash-on-delivery payment methods are preferred even for e-commerce transactions.³⁷

In the field of artificial intelligence (AI), Vietnam fared quite well in a ranking of the top 50 countries based on their contributions to the two most prestigious AI conferences in 2020: it was placed 27th, ahead of Malaysia and Thailand but behind Singapore.³⁸ The same study compiled a ranking of the global top 100 companies in AI research in 2020: it was dominated by US and Chinese companies but Vietnam's VinAI was also included, in 32nd place.³⁹ Founded by a former employee of Google DeepMind, VinAI provides applied AI solutions and is also the first Vietnamese research laboratory to cover areas such as machine learning and deep learning.⁴⁰ AI has already been applied in sectors such as health-care, education, transport, agriculture and e-commerce, though overall it is still in the early stages of development.⁴¹ The government announced a ten-year strategy for AI R&D in January 2021, setting the goal of becoming one of the world's top 50 countries in the field by 2030.⁴²

Vietnam has a reasonable degree of national ownership of its telecommunications networks

Vietnam has a reasonable degree of national ownership of its telecommunications networks, owning about 75% of the equipment, and hopes to achieve 100% domestic production of that equipment by 2022.⁴³ Viettel, a military-owned telecoms carrier, is part of a consortium developing a high-performance undersea cable, capable of carrying more than 140 Tb/s of traffic, that will connect China (Hong Kong and Guangdong), Japan, the Philippines, Singapore, Thailand and Vietnam as part of the Asia Direct Cable project, due to be completed by the end of 2022.⁴⁴ It has also successfully tested 5G technology.⁴⁵ Vietnam Posts and Telecommunications Group (VNPT) exports to more than 30 countries.⁴⁶

In terms of space-based connectivity, VNPT operates two communications satellites, VINASAT-1 and VINASAT-2.⁴⁷ Vietnam also has two Earth-observation satellites, operated by the Vietnam National Space Centre (VNSC) and the Space Technology Institute of the Vietnam Academy of Science and Technology. The space industry relies heavily on foreign assistance and investment – for example, Japanese experts were involved in building one of the Earth-observation satellites, the VNSC's *MicroDragon*, launched from Japan in 2019,⁴⁸ and India has been collaborating with Vietnam's National Remote Sensing Department in building a tracking and telemetry station that potentially has military uses.⁴⁹

Cyber security and resilience

Vietnam has been constructing an elaborate set of mechanisms, policies and laws for national cyber security for over a decade. The efforts have paid off to some degree but there is much progress still to be made. According to Microsoft reporting in 2020, the country had the highest rate of ransomware attacks in the Asia-Pacific, it was one of the three countries in the region most affected by malware attacks⁵⁰ and it ranked sixth in the world for unintentional downloads of malicious code.⁵¹

In response to the growing cyber threats, the National Cyber Security Monitoring Centre⁵² (NCSC) was established under the AIS in 2018. Its primary focus is to support and supervise the cyber security of

all public- and private-sector entities, to provide early warnings against cyber attacks, and to share information with domestic and international agencies. In partnership with a coalition of information-security companies, the NCSC has launched an information-sharing and security-monitoring system that connects the ministries of the central government with the country's provincial administrations.⁵³ In 2020, for example, it cooperated with the MIC and MPS in containing the VN84App spyware that was targeting smartphone users.⁵⁴

In terms of overall national resilience, it is difficult to form a clear picture. The 'Strategy for the Homeland Protection in Cyberspace'⁵⁵ and its implementation plan would appear to be the main policy document setting out the response plans for serious cyber incidents, but the texts are not available. Vietnam responds to such incidents through the National Steering Committee for Emergency Response (NSCER),⁵⁶ which the MIC assists by directing and coordinating emergency-response efforts domestically or internationally.⁵⁷ The VNCERT is responsible for responding to lower-level cyber incidents but participates in the NSCER along with cyber-related agencies in the MIC, MPS and the MND. The VNCERT also works with other, smaller CERTs at the ministerial, provincial and local levels; with enterprises engaged in telecommunications, internet services, data storage, banking and financial activities; and with organisations that manage critical information infrastructure or industrial control systems.⁵⁸ In 2019 VNCERT conducted a nationwide cyber-security exercise with almost 300 participants.⁵⁹

The private sector has been playing an increasing role in promoting information security, including by creating its own cyber-security industry – for example, Viettel has created a subsidiary providing managed cyber-security services;⁶⁰ VNPT conducts cyber-security research and invests in relevant start-ups; and eight companies have come together to form the Vietnam Cyber Security Assessment and Audit Club, aiming to improve the assessment and auditing of cyber-security services nationwide.

Overall, however, Vietnam still faces significant cyber-security challenges. It remains to be seen whether

the NSCER is capable of coordinating effectively across the public and private sectors. The MIC has stated that there are not enough trained personnel to create the necessary CERTs and that the emergency-response network is 'unconnected' and 'unprofessional'.⁶¹ Investments in research and training that were approved in 2014 have yet to be implemented;⁶² a 2019 study suggested that almost half of government agencies lacked the funds necessary to implement cyber security;⁶³ and in 2020, reporting on its campaign to upgrade cyber security, the government noted that 30% of ministries had not yet reached the target level.⁶⁴ Vietnam ranked 50th out of 175 countries in the 2018 Global Cybersecurity Index compiled by the International Telecommunication Union.⁶⁵

Global leadership in cyberspace affairs

Vietnam focuses its cyber diplomacy on ASEAN, enthusiastically promoting cyber-security cooperation between members and with the group's external partners. Under the ASEAN Plus Three framework, for example, Hanoi hosted a December 2020 meeting with China, Japan and South Korea on international collaboration in cyber security and countering cyber crime.⁶⁶ Within ASEAN, Vietnam works actively towards cooperation on cyber norms⁶⁷ and the creation of a formal cyber-security cooperation mechanism.⁶⁸ The VNCERT hosted the June 2020 ASEAN-Japan Cyber Exercise, which focused on methods for countering fake websites.⁶⁹

Vietnam frequently collaborates with foreign governments and corporations to broaden its cyber-security capabilities. In 2019, for example, the NCSC signed a contract with Kaspersky to address information-security challenges,⁷⁰ and in 2020 the MPS collaborated with India,⁷¹ Brunei⁷² and Malaysia⁷³ on countering cyber crime. The country is part of the global Forum of Incident Response and Security Teams and the Asia-Pacific Computer Emergency Response Team (APCERT).⁷⁴ It has privately expressed an interest in close collaboration with the United States and Australia in matters of cyber security, but there are diplomatic obstacles because of human-rights concerns regarding Vietnamese cyber-security law. Nevertheless, both the

Vietnam still faces significant cyber-security challenges

US and Australia undertake activities with Vietnam in less sensitive areas of cyberspace policy such as international legal training and the development of smart cities.

Offensive cyber capability

It is unlikely that Vietnam's Cyber Command is well positioned to engage in offensive cyber operations against foreign adversaries, given its extensive domestic political roles and responsibilities and, according to its chief of staff, its lack of appropriate facilities, equipment

and cyber weapons.⁷⁵ Force 47 probably does not possess the technical abilities for significant offensive cyber because its mission is primarily political, mainly involving the management of public opinion by countering hostile viewpoints and creating propaganda.⁷⁶ The covert government-linked group APT32 is mainly engaged in industrial and other types of espionage rather than offensive cyber, but it probably possesses some capabilities that could be repurposed for an offensive effect. Overall, developing an offensive cyber capability does not appear, so far, to have been a high priority for the CPV.

Notes

- 1 Prime Minister's Decision No. 63/QĐ-TTg, 'Approving the National Planning on Development of Digital Information Security through 2020', 2010, <https://vanbanphapluat.co/decision-no-63-qd-ttg-approving-the-national-planning-on-development-of-digital-information-security-through-2020>.
- 2 Prime Minister, 'Phê Duyệt Phương Hướng, Mục Tiêu, Nhiệm Vụ Bảo Đảm An Toàn Thông Tin Mạng Giai Đoạn 2016–2020', 27 May 2016, <https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Quyết-dinh-898-QĐ-TTg-phuong-huong-muc-tieu-nhiem-vu-bao-dam-an-toan-thong-tin-mang-2016-2020-313149.aspx>.
- 3 Key players in promoting the Vietnamese information-security industry include the Vietnam Software and IT Services Association, the Vietnam Association for Information Processing, the Vietnam Internet Association, the Vietnam Information Security Association and the Vietnam E-commerce Association.
- 4 National Assembly, 'Luật an toàn thông tin mạng', 86/2015/QH13, 19 November 2015. For an official translation, see <https://vanbanphapluat.co/law-no-86-2015-qh13-on-cyberinformation-security-2015>.
- 5 National Assembly, 'Luật An Ninh Mạng', 24/2018/QH14, 12 June 2018, <https://luatvietnam.vn/an-ninh-quoc-gia/luat-an-ninh-mang-2018-164904-d1.html>. For an unofficial translation, see <https://data.allens.com.au/pubs/pdf/priv/cupriv22jun18.pdf>.
- 6 Thomas J. Treutler and Giang Thi Huong Tran, 'Update on the Implementation of Vietnam's New Cybersecurity Law and Status of Implementing Decrees', Tilleke & Gibbins, 18 December 2019, <https://www.lexology.com/library/detail.aspx?g=8833627c-e189-4d60-a472-6ee742cc38fd>.
- 7 The data-localisation obligation for foreign companies applies to those that provide telecoms services, data storage and sharing, e-commerce, social media and online electronic games.
- 8 National Assembly, 'Luật Quốc Phòng', 22/2018/QH14, 8 June 2018, <https://thuvienphapluat.vn/van-ban/bo-may-hanh-chinh/Luat-quoc-phong-340395.aspx>.
- 9 Politburo Resolution 29NQ/TW dated 25 July 2018. See Vu Van Hien, 'Enhancing the homeland protection under the Party's platform', *National Defence Journal*, 10 November 2020, <http://tapchiquptd.vn/en/theory-and-practice/enhancing-the-homeland-protection-under-the-partys-platform/16265.html>; and Ngo Xuan Lich, 'The whole military resolves to successfully fulfil the military-defence tasks in 2019', *National Defence Journal*, 4 January 2019, <http://tapchiquptd.vn/en/theory-and-practice/the-whole-military-resolves-to-successfully-fulfil-the-militarydefence-tasks-in-2019/13088.html>.
- 10 Ngọc Thụy Tran, 'Những Vấn Đề về Bảo vệ Tổ Quốc Trên Không Gian Mạng', *Quan khu 7*, 3 October 2019, <https://baoquankhu7.vn/nhung-van-de-ve-bao-ve-to-quoc-tren-khong-gian-mang--191939649-0015044s34010gs>.
- 11 Ministry of National Defence, '2019 Viet Nam National Defence', October 2019, p. 52, http://news.chinhphu.vn/Uploaded_VGP/phamvanthua/20191220/2019VietnamNationalDefence.pdf.
- 12 National Assembly, 'Luật An Ninh Mạng', 24/2018/QH14.
- 13 See 'VNCTERT/CC Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam', <http://vnctert.gov.vn>.
- 14 Ministry of Information and Communications, 'Cybersecurity Emergency Response Center established', 14 October 2019, <https://>

- english.mic.gov.vn/Pages/TinTuc/139865/Cybersecurity-Emergency-Response-Center-established.html.
- 15 Ministry of Information and Communications, 'Authority of Information Security', 19 July 2020, <https://english.mic.gov.vn/pages/thongtin/114301/Authority-of-Information-Security.html>.
 - 16 Ministry of Information and Communications, 'The National Electronic Authentication Centre', 19 July 2020, <https://english.mic.gov.vn/pages/thongtin/114304/NEAC.html>.
 - 17 'Chủ động, quyết liệt trong phòng, chống tội phạm trên không gian mạng', Thua Thien Hue Provincial Party Committee, 21 January 2020, <https://tinhuythue.vn/tin-tuc-trong-nuoc/kh-cn/chu-dongquyet-liet-trong-ph-ograde-ngchong-toi-pham-tr-ecirc-n-kh-ocirc-ng-gian-mang.htm>.
 - 18 'Cục An ninh Văn hóa, thông tin, truyền thông báo công dân Bắc', *Tiền Phong*, 5 May 2018, <https://www.tienphong.vn/xa-hoi/cuc-an-ninh-van-hoa-thong-tin-truyen-thong-bao-cong-dang-bac-1269610.tpo>.
 - 19 Ministry of National Defence, '2019 Viet Nam National Defence'.
 - 20 *Ibid.*, pp. 66–7.
 - 21 'Hon 10.000 người trong 'Lực lượng 47' đấu tranh trên mạng', *Tuổi Trẻ*, 25 December 2017, <https://tuoitre.vn/hon-10-000-nguoi-trong-luc-luong-47-dau-tranh-tren-mang-20171225150602912.htm>. It is unclear from this source if the personnel engage only in political surveillance or if some also conduct other cyber operations.
 - 22 Maj. Gen., Associate Prof. Nguyen Hung Oanh, 'The Political Officer College grasps and executes the Politburo's Resolution 35', *National Defence Journal*, 16 October 2019, <http://tapchiquptd.vn/en/research-and-discussion/the-political-officer-college-grasps-and-executes-the-politburos-resolution-35/14514.html>.
 - 23 Carlyle A. Thayer, 'The Apparatus of Authoritarian Rule in Vietnam', *Critical Studies of the Asia Pacific Series*, vol. 31, no. 2, 2014, pp. 279–83, https://link.springer.com/chapter/10.1057/9781137347534_7#aboutcontent.
 - 24 Hai Thanh Luong et al., 'Understanding Cybercrimes in Vietnam: From Leading-Point Provisions to Legislative System and Law Enforcement', *International Journal of Cyber Criminology*, vol. 13, no. 2, 2019, <https://www.cybercrimejournal.com/LuongetalVol13Issue2IJCC2019.pdf>.
 - 25 'VN to join Microsoft's network security protection programme', *Viet Nam News*, 20 December 2019, <https://vietnamnews.vn/society/570139/vn-to-join-microsofts-network-security-protection-programme.html>.
 - 26 Le Linh, 'Xây dựng trung tâm điều hành an ninh mạng đầu tiên cả nước', *Diễn Đàn*, 17 May 2019, <https://enternews.vn/xay-dung-trung-tam-dieu-hanh-an-ninh-mang-dau-tien-ca-nuoc-150441.html>.
 - 27 For some background, see Nick Carr, 'Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations', *FireEye*, 14 May 2017, <https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html>.
 - 28 Tran Luu, 'Vietnam determines to develop digital economy', *Saigon Online*, 4 February 2020, https://sggpnews.org.vn/science_technology/vietnam-determines-to-develop-digital-economy-85491.html.
 - 29 Bui Thanh Truan, 'Difficulties and challenges in the development of digital economy in Vietnam', *Political Theory*, 25 August 2020, <http://lyluanchinhtri.vn/home/en/index.php/practice/item/723-difficulties-and-challenges-in-the-development-of-digital-economy-in-vietnam.html>.
 - 30 Chinese Academy of Information and Communications Technology, 'Quánqiú shùzì jīngjì xīn tújǐng (2019 nián)', October 2019, p. 12, <http://www.caict.ac.cn/kxyj/qwfb/bps/201910/P020191011314794846790.pdf>.
 - 31 See Prime Minister, 'Introducing Program for National Digital Transformation by 2025 with Orientations Towards 2030', Decision 749/QĐ-TTg, 3 June 2020, <https://vanbanphapluat.co/decision-749-qd-ttg-2020-introducing-program-for-national-digital-transformation>. By 2030 this programme aims to achieve the following: a digital economy that contributes 30% of GDP; digital transformation in the government sector so that Vietnam becomes one of the top four ASEAN countries in the UN e-government ranking; nationwide 5G mobile-network coverage; and access to broadband internet for the entire population.
 - 32 Samaya Dharmaraj, 'Vietnam Committed to Supporting its Digital Economy with E-government', *OpenGov Asia*, 28 November 2019, <https://www.opengovasia.com/vietnam-committed-to-supporting-its-digital-economy-with-e-government>.
 - 33 Ministry of Information and Communications, 'VN's IT industry maintains growth momentum', 25 December 2019, <https://english.mic.gov.vn/Pages/TinTuc/140438/VN-s-IT-industry-maintains-growth-momentum.html>.
 - 34 George Ingram, 'Development in Southeast Asia: Opportunities for donor collaboration', *Brookings Center for Sustainable Development*, December 2020, pp. 31–2, <https://www.brookings.edu/wp-content/uploads/2020/12/Development-Southeast-Asia-Ch2-Digital.pdf>.

- 35 Simon Kemp, 'Digital 2020: Vietnam', DataReportal, 18 February 2020, <https://datareportal.com/reports/digital-2020-vietnam>.
- 36 'How can Vietnam's e-commerce players foster greater market growth?', Tech Wire Asia, 3 February 2020, <https://techwireasia.com/2020/02/how-can-vietnams-e-commerce-players-foster-greater-market-growth>.
- 37 'Cashless payment remains low in Vietnam: CIEM', VietnamPlus, 24 June 2019, <https://en.vietnamplus.vn/cashless-payment-remains-low-in-vietnam-ciem/154911.vnp>.
- 38 Gleb Chuvpilo, 'AI Research Rankings 2020: Can the United States Stay Ahead of China?', 21 December 2020, <https://chuvpilo.medium.com/ai-research-rankings-2020-can-the-united-states-stay-ahead-of-china-61cf14b1216>.
- 39 *Ibid.*
- 40 'Who We Are – The First AI Research Lab in Vietnam with a Focus on Fundamental Research', VinAI Research, <https://www.vinai.io/about-us>.
- 41 'Vietnam Prioritises Artificial Intelligence Development', *Star*, 9 September 2019, <https://www.thestar.com.my/business/smebiz/2019/09/09/vietnam-prioritises-artificial-intelligence-development>.
- 42 'Vietnam strives to enter world's Top 50 in terms of AI by 2030', VietnamPlus, 28 January 2021, <https://en.vietnamplus.vn/vietnam-strives-to-enter-worlds-top-50-in-terms-of-ai-by-2030/195485.vnp>.
- 43 'Việt Nam nhờ Mỹ kiểm định thiết bị 5G do Việt Nam sản xuất để có đủ khả năng vào thị trường Mỹ', ICT News, 21 January 2020, <https://ictnews.vietnamnet.vn/cuoc-song-so/viet-nam-nho-my-kiem-dinh-thiet-bi-5g-do-viet-nam-san-xuat-de-co-du-kha-nang-vao-thi-truong-my-40145.html>.
- 44 Ministry of Information and Communications, 'Viettel among investors of new high-speed under-sea cable ADC', 22 June 2020, <https://english.mic.gov.vn/Pages/TinTuc/142715/Viettel-among-investors-of-new-high-speed-under-sea-cable-ADC.html>.
- 45 Leo Kelion, 'Giới chuyên gia ngạc nhiên trước tuyên bố của Viettel về mạng 5G', BBC News Vietnamese, 21 January 2020, <https://www.bbc.com/vietnamese/vietnam-51190570>.
- 46 'Vietnamese telecom giants on race of exporting telecom equipments', Xinhua, 24 February 2017, http://www.xinhuanet.com/english/2017-02/24/c_136082932.htm.
- 47 Union of Concerned Scientists, 'UCS Satellite Database', updated 1 January 2021, <https://www.ucsusa.org/resources/satellite-database>.
- 48 'Vietnam's MicroDragon Earth Observation Satellite Successfully Launched From Japan', SpaceWatch Asia Pacific, January 2019, <https://spacewatch.global/2019/01/vietnams-microdragon-earth-observation-satellite-successfully-launched-from-japan>.
- 49 Nandini Sarma, 'Southeast Asian Space Programmes: Capabilities, challenges and collaborations', Observer Research Foundation, 7 March 2019, https://www.orfonline.org/research/southeast-asian-space-programmes-capabilities-challenges-collaborations-48799/#_ednref12.
- 50 M. Anh, 'Việt Nam là quốc gia có tỷ lệ nhiễm mã độc tống tiền cao nhất khu vực', *Doanh nhân*, 24 June 2020, <https://doanhnhansaigon.vn/it/viet-nam-la-quoc-gia-co-ty-le-nhiem-ma-doc-tong-tien-cau-nhat-khu-vuc-1099286.html>.
- 51 Microsoft, 'Microsoft Security Endpoint Threat Summary 2019', June 2020, <https://3er1viui9wo3opkxh1v2nh4w-wpengine.netdna-ssl.com/wp-content/uploads/prod/sites/570/2020/02/Microsoft-Security-Endpoint-Threat-Summary-2019-Updated.pdf>.
- 52 See 'Giới thiệu về NCSC', National Cyber Security Monitoring Centre, <https://khonggianmang.vn/intro>.
- 53 Phan Nghia, 'Vietnam introduces new information security system to facilitate e-governance', *VnExpress*, 29 November 2019, <https://e.vnexpress.net/news/news/vietnam-introduces-new-information-security-system-to-facilitate-e-governance-4019639.html>.
- 54 Bao Lam and Chau An, 'Data stealing spyware rears head in Vietnam', *VnExpress*, 23 June 2020, <https://e.vnexpress.net/news/news/data-stealing-spyware-rears-head-in-vietnam-4119828.html>.
- 55 Vu, 'Enhancing the homeland protection under the Party's platform'; Ngo, 'The whole military resolves to successfully fulfil the military-defence tasks in 2019'.
- 56 Prime Minister, 'Quyết Định: Ban Hành Quy Định Về Hệ Thống Phương Án Ứng Cứu Khẩn Cấp Bảo Đảm An Toàn Thông Tin Mạng Quốc Gia', 05/2017/QĐ-TTg, 16 March 2017, <https://vanbanphapluat.co/quyet-dinh-05-2017-qd-ttg-he-thong-phuong-an-ung-cuu-khan-cap-bao-dam-an-toan-thong-tin-mang-quoc-gia>.
- 57 'PM sets up national cybersecurity committee', *Vietnam Law & Legal Forum*, 2 April 2017, <https://vietnamlawmagazine.vn/pm-sets-up-national-cybersecurity-committee-5785.html>.
- 58 Prime Minister, 'Quyết Định: Ban Hành Quy Định Về Hệ Thống Phương Án Ứng Cứu Khẩn Cấp Bảo Đảm An Toàn Thông Tin Mạng Quốc Gia'.
- 59 'Vietnam records more than 6,200 cyber attacks in seven months', *AsiaOne*, 1 August 2019, <https://www.asiaone.com/digital/vietnam-records-more-6200-cyber-attacks-seven-months>.

- 60 'The first information security ecosystem built by Vietnamese', Acrofan, 20 February 2020, <https://us.acrofan.com/detail.php?number=239640>.
- 61 Samaya Dharmaraj, 'Vietnam strengthens human resources for information security tasks', OpenGov Asia, 9 July 2019, <https://www.opengovasia.com/vietnam-strengthens-human-resources-for-information-security-tasks>.
- 62 *Ibid.*
- 63 Chau An, 'Vietnam carries potential to be a cybersecurity powerhouse: minister', VnExpress, 17 April 2019, <https://e.vnexpress.net/news/business/economy/vietnam-carries-potential-to-be-a-cybersecurity-powerhouse-minister-3910754.html>.
- 64 'Cyber attacks targeting Vietnam's information systems down 7.8 pct', VietnamPlus, 4 November 2020, <https://en.vietnamplus.vn/cyber-attacks-targeting-vietnams-information-systems-down-78-pct/189811.vnp>.
- 65 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 63, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCL01-2018-PDF-E.pdf.
- 66 Ministry of Public Security, 'Asean +3 conference on cyber security opens in Hanoi', 29 December 2020, <http://en.bocongan.gov.vn/international-relations-cooperation/asean-3-conference-on-cyber-security-opens-in-hanoi-t7615.html>.
- 67 Li Ying Lee, 'New ASEAN committee to implement norms for countries' behaviour in cyberspace', Channel News Asia, 2 October 2019, <https://www.channelnewsasia.com/news/singapore/asean-cyberspace-working-level-committee-cybersecurity-11963602>.
- 68 'ASEAN Member States Agree to Move Forward on a Formal Cybersecurity Coordination Mechanism', CSA Singapore, 2 October 2019, <https://www.csa.gov.sg/news/press-releases/amcc-release-2019>.
- 69 'Vietnamese tech experts join transnational cyber-attack exercise', *Việt Nam News*, 26 June 2020, <https://vietnamnews.vn/society/748743/vietnamese-tech-experts-join-transnational-cyber-attack-exercise.html>.
- 70 'National Cyber Security Center signs deal with Kaspersky for online security', VietNamNet, 24 January 2019, <https://english.vietnamnet.vn/fms/science-it/216749/national-cyber-security-center-signs-deal-with-kaspersky-for-online-security.html>.
- 71 'Vietnam-India strategic partnership in the fields of defence and security', *National Defence Journal*, 29 August 2017, <http://tapchiquptd.vn/en/events-and-comments/vietnam-india-strategic-partnership-in-the-fields-of-defence-and-security/10541.html>.
- 72 'Việt Nam, Brunei, boost co-operation in combating crimes', *Việt Nam News*, 14 February 2020, <https://vietnamnews.vn/politics-laws/592275/viet-nam-brunei-boost-co-operation-in-combating-crimes.html>.
- 73 Ministry of Public Security, 'Vietnam, Malaysia promote cooperation in security', 14 February 2020, <http://en.bocongan.gov.vn/international-relations-cooperation/vietnam-malaysia-promote-cooperation-in-security-t6508.html>.
- 74 Adam Bannister, 'APCERT holds cyber drill to stress-test response capabilities of 32 CSIRTs', The Daily Swig, 6 April 2020, <https://portswigger.net/daily-swig/apcert-holds-cyber-drill-to-stress-test-response-capabilities-of-32-csirts>.
- 75 'Xây dựng lực lượng Tác chiến không gian mạng, đáp ứng yêu cầu nhiệm vụ bảo vệ Tổ quốc', *Tạp chí Quốc phòng*, 17 October 2019, <http://tapchiquptd.vn/vi/bao-ve-to-quoc/xay-dung-luc-luong-tac-chien-khong-gian-mang-dap-ung-yeu-cau-nhiem-vu-bao-ve-to-quoc/14505.html>.
- 76 'Hơn 10.000 người trong 'Lực lượng 47' Đấu tranh trên mạng', *Tuổi Trẻ*.