Cybercrime in Southeast Asia
Combating a global threat locally

Jonathan Lusthaus
About the author

Dr Jonathan Lusthaus is Director of the Human Cybercriminal Project in the Department of Sociology, University of Oxford. He is an Adjunct Associate Professor at UNSW Canberra Cyber and the author of *Industry of anonymity: inside the business of cybercrime* (Harvard University Press, 2018).

Acknowledgements

This report is built on the insights and information provided by numerous interview participants, and could not have been written without them. I’m also very grateful to a number of colleagues for commenting on earlier drafts of this work, including Nigel Phair, Tala Stevens and a number of readers who prefer not to be named. I also thank the three peer reviewers for their thoughtful suggestions. Finally, great thanks must go to ASPI staff for their guidance, and particularly to Elise Thomas for coordinating this endeavour.

What is ASPI?

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia’s defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

ASPI International Cyber Policy Centre

ASPI’s International Cyber Policy Centre (ICPC) is a leading voice in global debates on cyber and emerging technologies and their impact on broader strategic policy. The ICPC informs public debate and supports sound public policy by producing original empirical research, bringing together researchers with diverse expertise, often working together in teams. To develop capability in Australia and our region, the ICPC has a capacity building team that conducts workshops, training programs and large-scale exercises both in Australia and overseas for both the public and private sectors. The ICPC enriches the national debate on cyber and strategic policy by running an international visits program that brings leading experts to Australia.

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional.

ASPI

Tel +61 2 6270 5100
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_ICPC

© The Australian Strategic Policy Institute Limited 2020

This publication is subject to copyright. Except as permitted under the Copyright Act 1968, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Enquiries should be addressed to the publishers. Notwithstanding the above, educational institutions (including schools, independent colleges, universities and TAFEs) are granted permission to make copies of copyrighted works strictly for educational purposes without explicit permission from ASPI and free of charge.

First published May 2020.

ISSN 2209-9689 (online)
ISSN 2209-9670 (print)

Cover image: Illustration by Wes Mountain. ASPI ICPC and Wes Mountain allow this image to be republished under the Creative Commons License Attribution-Share Alike. Users of the image should use the following sentence for image attribution: ‘Illustration by Wes Mountain, commissioned by the Australian Strategic Policy Institute’s International Cyber Policy Centre.’
Cybercrime in Southeast Asia

Combating a global threat locally

Jonathan Lusthaus
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What’s the problem?</td>
<td>03</td>
</tr>
<tr>
<td>What’s the solution?</td>
<td>03</td>
</tr>
<tr>
<td>Introduction</td>
<td>04</td>
</tr>
<tr>
<td>Cybercrime as a local phenomenon</td>
<td>04</td>
</tr>
<tr>
<td>Cybercrime in Southeast Asia</td>
<td>06</td>
</tr>
<tr>
<td>Vietnam</td>
<td>06</td>
</tr>
<tr>
<td>Malaysia</td>
<td>07</td>
</tr>
<tr>
<td>Policy recommendations for regional work against cybercrime</td>
<td>08</td>
</tr>
<tr>
<td>Recommendation 1</td>
<td>09</td>
</tr>
<tr>
<td>Recommendation 2</td>
<td>09</td>
</tr>
<tr>
<td>Recommendation 3</td>
<td>10</td>
</tr>
<tr>
<td>Notes</td>
<td>11</td>
</tr>
<tr>
<td>Acronyms and abbreviations</td>
<td>12</td>
</tr>
</tbody>
</table>
What’s the problem?

Cybercrime is a serious threat facing Australia and the world, but this criminal activity is often wrongly viewed as a near invisible online phenomenon, rather than a ‘real world’ concern. Behind every attack sits one or more people in a physical location. Those people are products of particular socio-economic conditions, which influence the types of regional and local cybercrime activity they specialise in. Cybercrime isn’t evenly distributed around the globe, but is centred around hotspots, which offer potential breeding grounds or safe harbours from where offenders can strike. This is true in Australia’s own region, where some Southeast Asian countries are emerging as bases for serious regional, and even global, cybercrime threats. We’re not proactively tackling the locations where the cybercrime threat develops and matures.

What’s the solution?

Australia’s current approach to fighting cybercrime needs to be augmented to account more seriously for this local dimension, particularly in Southeast Asia, and our fight against cybercrime should be more targeted, enduring and forward-looking. While it makes sense to support international cooperation in the fight against cybercrime, those efforts need to be targeted to specific hotspots where the problem is the most acute and Australia’s contributions can provide the greatest value for money. This involves the identification of current or future cybercriminal hotspots within Australia’s near region.

Australia’s existing law enforcement capacity-building programs should be matched specifically to those countries producing the biggest cybercrime threat. Deeper relationships should also be developed between investigators in Australia and those countries through more cyber liaison posts and exchange programs. Finally, Australia should adopt prevention programs that seek to block offenders’ pathways into cybercrime and promote those programs to suitable cybercrime hotspots in the region.
Introduction

There’s a popular perception that cybercrime is an anonymous activity. With seemingly faceless attackers and so-called ‘darknet’ sites, a picture emerges of a threat unlike anything we’ve seen before. But cybercrime shouldn’t generate this kind of paradigm shift. As Peter Grabosky astutely argued almost 20 years ago, it’s ‘old wine in new bottles’.¹ The crime types—fraud, extortion, theft—remain the same; only the tools have changed. For the following analysis, I employ a broad definition: cybercrime is the ‘use of computers or other electronic devices via information systems such as organizational networks or the Internet to facilitate illegal behaviors’.²

The purpose of this report is to highlight how rooted in the conventional world cybercrime actually is. In many cases, there’s a strong offline dimension, along with a local one. All cyberattacks have one or more people behind them. Some of those offenders know each other in person. All are physically based somewhere and are the product of local socio-economic conditions. As a result, we see different ‘flavours’ of cybercrime coming out of different parts of the world. The specific focus of this analysis is on the nature of cybercrime within Southeast Asia and the local dynamics therein.

This report is structured in three parts. First, it outlines the nature of cybercrime as a local phenomenon, highlighting some of the most famous hubs around the world. Second, it zeroes in on the case of Southeast Asia. Finally, the report addresses potential policy solutions derived from this analysis, and particularly those that could be adopted by the Australian policy community.

The analysis contained in this report is informed not only by publications on cybercrime, but also by seven years of fieldwork carried out by the author in 20 countries. This involved interviews with 238 participants, including law enforcement agents, security professionals and former cybercriminals.³

Cybercrime as a local phenomenon

While cybercrime is often viewed essentially as an online and global phenomenon, it’s also an offline and local one.⁴ It’s true that many offenders participate in cybercrime so they can avoid real-world engagement with both their victims and their partners.⁵ For a number of others, though, the attacks on victims remain virtual, but they’re collaborating with cybercriminal partners in physical settings. Sometimes they meet online first and later move their relationship into the corporeal world. In other cases, offenders know each other well already, perhaps coming from the same community, neighbourhood, university or school.⁶

While still a niche area of research, this offline dimension is slowly attracting the attention of the research community.⁷ But what really needs to be emphasised is the importance of local conditions in shaping local cybercrime.⁸ Cybercrime might be a universal problem, but certain countries appear to harbour a greater threat than others. These cybercriminal hubs often have particular specialities, as well.
It’s worth quickly sketching some of the most famous cybercrime hubs around the world. Perhaps the best known of all is the former Soviet Union. That region produces the most technically capable offenders within cybercrime, who are often responsible for developing top-level malware and other tools that are used throughout the industry. An excellent education system produces an oversupply of able technologists in the labour market, who then struggle to find opportunities in a weak technology industry.

Another reputed cybercrime hub is Nigeria, which is known for far less technical forms of cybercrime. Nigerian cybercriminals have traditionally carried out ‘advance fee fraud’—the email scams familiar to users around the world. In more recent years, West African offenders have evolved. One growing threat is business email compromise, in which a scammer impersonates a CEO or other person to instruct an employee in the victim company to transfer funds into an account controlled by the criminals.

There are a number of other cybercrime hubs around the world. While it’s beyond the scope of the present report to discuss them all, Table 1 summarises some of them in a simplified fashion. The next section addresses the particular dynamics of cybercrime in some Southeast Asian examples.

Table 1: Geographical specialisations

<table>
<thead>
<tr>
<th>Country</th>
<th>Specialisations</th>
</tr>
</thead>
</table>
| Former Soviet Union | Malware production and distribution  
Other technical criminal endeavours (for example, spam and bullet-proof hosting) |
| Nigeria       | Advance fee fraud  
Other confidence scams (for example, email compromise and impersonation) |
| Romania       | Online auction fraud  
ATM fraud |
| China         | Online gaming theft  
Intellectual property theft (state affiliated) |
| Brazil        | Credit card fraud  
Banking Fraud |
| The West      | Cashing out and money mules  
Some hacking and malware exploitation |

Cybercrime in Southeast Asia

Southeast Asia provides an interesting cybercrime case study, as it includes populations of both local and foreign offenders. While offenders are spread across the region, certain countries contain a larger cybercriminal threat than others. As a result, the analysis below is focused on two interesting examples that pose some of the greatest threat in the region: Vietnam and Malaysia. The discussion of Vietnam is centred on the local community of ‘black hat’ (criminal) hackers and the threat they pose. With regard to Malaysia, the physical presence of Nigerian fraudsters is the most relevant topic to examine.

Vietnam

While China, South Korea and North Korea rank higher, some rate Vietnam towards the top of general hacking capability in Asia. Even if only a proportion of the local hacker population turned towards crime, that would make Vietnam one of the most serious cybercriminal threats in Southeast Asia. While some cybercriminals strike at home, Vietnam itself is not a target-rich environment, and major attacks there are not widely reported. One rare example was the Vietcombank case of 2016, in which 500 million dong (at writing about A$34,000) was extracted from a customer account.

For those Vietnamese attacking overseas, credit card fraud has traditionally been a popular endeavour. The conventional business model has been to target ecommerce sites and steal the databases of credit card details. The cybercriminals can either sell the card data in virtual marketplaces or buy products online themselves and ship them back to Vietnam. The latter approach became increasingly difficult as ecommerce sites blocked some deliveries to Vietnam in response to this malicious activity, so the cybercriminals adapted and found overseas ‘mules’ who could receive items and then mail them on to Vietnam. Vietnamese cybercriminals have also engaged in personal data theft, compromising email and other account credentials, and a number of other schemes.

While it's often important to make the point that cybercrime and hacking aren't synonymous, in Vietnam the dominant form of cybercrime is tied to hacking. While some parts of the world are known for malware or fraud, Vietnamese cybercrime appears to have a strong focus on intrusions. This is likely to be tied to the local context, in which there's a broader hacking culture and an ecosystem of Vietnamese forums alongside the international cybercriminal marketplaces. Education in computing and STEM disciplines more broadly is of a decent standard compared to that available in some other countries in the region, and there are recent efforts underway to improve it. There's also fairly widespread corruption, which can shelter criminal activity. One former cybercriminal rated Vietnamese corruption 'a good 8 of 10 points'.

Vietnam is a significant location of cybercriminality, particularly by regional standards. While a number of factors suggest that it could become a major international cybercrime hub, there are other factors that may be preventing the greater spread of cybercrime there. One is that the level of technical proficiency is much lower than that found in other cybercrime hubs, such as a number of countries of the former Soviet Union. This means that the threat faced from Vietnamese cybercriminals is
reduced. But there is also less of a push towards cybercrime in the first place, as job opportunities appear relatively robust. The Vietnamese economy has been growing in recent years. In particular, the technology sector is attracting investment and providing attractive salaries. There’s also a relatively established pipeline of top Vietnamese talent to foreign companies such as Google and Microsoft. While there remains a serious threat, these factors are probably keeping the problem of Vietnamese cybercrime from growing even further.

Malaysia

If the example of Vietnam is about local offenders striking internationally, the case of Malaysia is about foreign cybercriminals using that country as a base of operations. There is a community of local Malaysian cybercriminals, but the more pressing issue is the large presence of Nigerian fraudsters who have established themselves there. While Nigerian email scams are well known, many assume that the offenders are based in West Africa. There are indeed a number of offenders operating out of Nigeria, originally from inside internet cafes, and now making use of new mobile technology. But there are also Nigerian cybercriminals spread out across Africa and the world, including in the US, the UK, the Netherlands, India, the Philippines and Australia. Their presence in such countries can be for computing training, coordinating money-mule and other support operations, or running their own autonomous scam operations from those countries.

Curiously, for some time Malaysia has hosted one of the largest concentrations of Nigerian fraudsters. It isn’t yet clear why this is such a fertile location, but it’s of growing concern, as perhaps many thousands of such offenders are running hugely profitable enterprises. These are relatively low-tech scams, such as business email compromise, but can be hugely damaging in their scale and impact. The modus operandi of Nigerian scammers in Malaysia is similar to that in other jurisdictions. A fraudster may arrive in Malaysia and find members of his existing social networks already there—almost always men—who may serve as suitable collaborators. This is similar to cybercriminals based in Nigeria, who appear to favour working with those whom they know already and have some form of personal connection with. Such an expat fraudster may also seek to involve some Malaysians into his scam. One surprisingly common tactic across the globe is to find a local girlfriend and use her knowledge, language and accent to enhance the scheme. For instance, a particular operation might contact victims suggesting that a parcel is waiting at an airport, but that the duty needs to be paid to release it. Having local knowledge means that the airport information and details can be checked for accuracy to avoid suspicion, and if a number is listed in the scam materials a Malaysian will answer the phone, rather than a West African.
Policy recommendations for regional work against cybercrime

Australia’s existing approach to fighting cybercrime is built around enhancing international cooperation through increasing awareness, strengthening cybercrime legislation, law enforcement capacity building, and information sharing. Given the transnational nature of the threat, this is a sensible strategy, but it lacks specificity in its implementation, which could be more tactical and nuanced.

While cybercrime is an online and global threat, the Australian Government shouldn’t ignore the offline and local dimensions of the phenomenon. Cybercrime may be a universal problem, but some countries are more important hubs of cybercriminality than others. The status quo appears to be that any international action in this area is positive, regardless of where. But Australia will have greater success and make more cost-effective use of resources by targeting specific jurisdictions where cybercrime is a problem, with less focus on those places where the concern is limited. This potentially could be decided on the basis of the caseload of the Australian Federal Police (AFP) or intelligence, though other measures would also be possible. It’s likely that such assessments are already happening informally and internally, but they have yet to become part of a defined, sustained and published policy exercise.

Cybercrime might be different in each country, but the policy responses should usually be similar. The key task for governments such as Australia’s is less to determine what to do, but where to do it. The heart of this is to draw up a list of countries that pose the greatest cybercriminal threat to Australia, balanced against an assessment of where an Australian contribution might have the greatest effect.

Given limits to resources and influence, it’s unlikely that Australia will take the lead in combating Eastern European cybercrime, though it should continue to support broader international efforts in that area (and might be wise to have a dedicated cybercrime liaison officer based somewhere within the former Soviet Bloc for that purpose).

Within Australia’s strategic backyard, Southeast Asia presents a clearer and more manageable challenge. Policymakers and practitioners have already had some cybercrime engagement with the region, with a broad focus on the ‘Indo-Pacific’. But, again, the true value is to be found not by addressing a large region as a whole, but by identifying particular cybercriminal hubs, or future hubs. Vietnam and Malaysia are good places to start, but aren’t the only locations that should be evaluated.

For any chosen country, there needs to be a clear-eyed understanding of mutual benefit. Cybercrime is a universal problem. As internet usage and ecommerce in Southeast Asia grow, the number of local victims is also likely to grow. Australian law enforcement agencies have the skills, capacity and international connections to aid their regional partners in their own fight to protect their companies and citizens from cybercrime.
The following three recommendations continue Australia’s support for international cooperation on cybercrime, but ensure that it’s even more targeted, enduring and forward-looking.

**Recommendation 1**

Law enforcement capacity in the region has been improving but still has some way to go. For those countries that are facing large concentrations of cybercriminals, such as Malaysia, the challenge may overwhelm local capacity. When resources are limited, Southeast Asian countries may (reasonably) prioritise cases with local victims, rather than foreign ones.

Australia has a strong history of running cyber training programs in the region. Building on past efforts in this space, greater resources and further training opportunities for cyber-investigators in locations where the threat is the greatest should increase local capacity to take on cybercriminals. In places where corruption is a problem within law enforcement, greater support for anti-corruption programs may also be an asset.

**Recommendation 2**

Australian law enforcement can also play a greater role in supporting investigations in Southeast Asia. This has already happened in individual cases, but building more enduring relationships is important. One of the most effective ways of achieving that is through liaison officers. Cross-border cases are often aided by having investigators who know each other’s systems, and may even know each other personally. High-level bureaucratic procedures can often get bogged down without agents at the coalface who can expedite the process. In those situations, trusted relationships can be important.

The best ways of building such relationships in Southeast Asia is to increase the number of opportunities for Australian agents to spend significant spells in the region and to provide similar opportunities for Southeast Asians in Australia. This can be achieved through the AFP, the Australian Criminal Intelligence Commission (ACIC), or both, having dedicated cyber liaisons in Southeast Asia, particularly in cybercrime hubs that acknowledge the mutual benefits involved. With some exceptions, such as the Jakarta Cybercrime Centre, the focus thus far has been on placing cybercrime investigators and analysts with major allies such as the US and the UK, along with international policing bodies such as Europol. Those partnerships are important to continue for broader intelligence sharing, but great value could also be gained by expanding the use of liaisons to build relationships with countries where substantial cybercriminal operations are based, and where such a presence would be welcomed.

Improving investigation partnerships can also be achieved by ensuring that generalist AFP and ACIC liaisons who are already posted to cybercrime hubs do have cybercrime as a clear and core part of their portfolio, and the training and resources to match. This might be particularly useful in cases like Malaysia, where online fraud is the primary cybercrime threat but doesn’t always fall inside (somewhat arbitrary) bureaucratic definitions of cybercrime. Increasing opportunities for police exchange programs, perhaps tied to the capacity-building efforts noted above, would also allow for greater networking opportunities between Australian cyber police officers and their Southeast Asian counterparts.
Recommendation 3

Australia must be forward-looking in its approach to cybercrime. This involves not only identifying future cybercrime hubs in the region, but also acting to block cybercriminal pathways in at-risk countries. Policing approaches based on ‘prevention’ are gaining traction globally. The UK is playing a leading role, and the Dutch police have also invested in this space. Such approaches are less reactive. They rely on identifying young people who may become involved in serious offending and then intervening before prosecutions are required. Industry engagement is encouraged, with a clear goal of diverting young technologists to legitimate career paths.36

Cybercrime prevention strategies target the root causes of cybercrime, rather than dealing with the symptoms. These efforts should be supported, expanded and internationalised. Australia is well placed to establish a prevention program within the AFP and beyond, but the government shouldn’t stop there. Part of this program should involve evangelising these approaches to other countries as well, and Southeast Asia is a logical focus. But, again, countries where cybercrime is a particular concern should be targeted. Prevention programs also make much greater sense in states such as Vietnam, where the offenders are indigenous, rather than places such as Malaysia, which face foreign cybercriminals establishing a new base.

Cybercrime prevention in Southeast Asia must also involve private industry. In some nations, a major concern is that there are simply not enough good job opportunities in the technology sector. There’s a natural push for countries in the region to improve education in computing and cybersecurity, but if the supply of tech talent becomes too much, some of those individuals may turn to cybercrime. Australian Government prevention efforts should engage with companies in both Australia and Southeast Asia, encouraging partnerships, investment opportunities and job growth in local technology sectors. There may also be greater opportunities for skilled migration and labour mobility within the region. Those efforts might require the AFP to cooperate with other government agencies, such as the Department of Foreign Affairs and Trade. Given that countries such as Vietnam have already shown that they have capable workforces and human capital that can be tapped, these programs should also be of direct benefit to Australian companies, beyond the broader aim of blocking local pathways into cybercrime.
Notes


2. Samuel C McQuade, Understanding and managing cybercrime, Allyn and Bacon, Boston, 2006, 16.


4. For think tank reports focused on the online dimension of cybercrime, see Lillian Ablon, Martin C Libicki, Andrea A Golay, Markets for cybercrime tools and stolen data: hackers’ bazaar, RAND Corporation, Santa Monica, California, 2014; James Lewis, Economic impact of cybercrime, CSIS/McAfee, Washington DC, 2018.


11. Lusthaus, Industry of anonymity: inside the business of cybercrime, 74.


13. Interview with Malaysian law enforcement agent 3; interview with US law enforcement agent 10.

14. Interview with South Korean law enforcement agent 2; interview with Vietnamese hacker 1.


16. ‘Vietcombank account holder losses $23,000 in one night’, VietNamNet, 16 August 2016, online.


18. Interview with Vietnamese cybersecurity professional 7.

19. Interview with Vietnamese hacker 1.


21. Interview with Vietnamese cybersecurity professional 1; interview with Vietnamese law enforcement agent 1; interview with Vietnamese hacker 1.

22. Interview with former Vietnamese cybercriminal 1.

23. For further detail, see Lusthaus, ‘Modelling cybercrime development: the case of Vietnam’.


25. Interview with Vietnamese cybersecurity professional 1; interview with Vietnamese cybersecurity professional 7.

26. Interview with US law enforcement agent 10; interview with Malaysian law enforcement agent 3.


28. Interview with Nigerian cybersecurity professional 1; interview with former Nigerian law enforcement agent 1.

29. Interview with US law enforcement agent 10.


31. Interview with Malaysian law enforcement agent 1.

32. Interview with Malaysian law enforcement agent 3.


34. DFAT, Australia’s International Cyber Engagement Strategy, 32–43.

35. See, for example, David Bisson, ‘Criminal stole “a significant amount of data” in airport hacking attack’, Tripwire, 11 December 2017, online.

Acronyms and abbreviations

ACIC  Australian Criminal Intelligence Commission
AFP  Australian Federal Police
STEM  science, technology, engineering and mathematics
Some previous ICPC publications

- Taking Australian diplomacy digital
  - Dave Sharma

- Mapping China’s technology giants
  - Danielle Cave, Samatha Hoffman, Alan Jukes, Fengya Yang and Ewan Thomas

- Hacking democracies
  - Frogas Ferson, Sarah D’Souza, Matt Walker and Luke Coutts

- Picking flowers, making honey
  - The Chinese military’s collaboration with foreign universities
  - Alex Zalke

- The China Defence Universities Tracker
  - Exploring the military and security links of China’s universities
  - Alex Zalke

- Weaponised deep fakes
  - National security and democracy
  - Hannah Smith and Katherine Maxted

- Uyghurs for sale
  - ‘Re-education’, forced labour and surveillance beyond Xinjiang
  - Helen Rorke

- Engineering global consent
  - The Chinese Communist Party’s data-driven power expansion
  - Dr Samantha Himmels

- A new Sino-Russian high-tech partnership
  - Authoritarian innovation in a era of great power rivalry
  - Samuel Benfield and Dasha Novo