Hacktivism: will it pose a threat to Southeast Asia and, if so, what are the implications for Australia?

Colonel Penny Cumming

Australian Army

Abstract

This paper examines the threat posed to Southeast Asia by 'hacktivism', as well as its implications for Australia. It explores the concept of 'hacktivism'—actions by individuals or groups whose hacking activities are issue-motivated—with a particular focus on recent events in Southeast Asia, often arising in response to a physical event, such as actions relating to territorial claims in the South China Sea.

The paper contends that the recent increase in hacktivism in the region is likely to continue over the next decade. It asserts that the trend presents an even greater challenge when contrasted against the rapid growth in information technology, unsupported by sound cyber security. The paper concludes that while these developments provide a unique opportunity for Australia to engage in cyber-capacity building within the region, the opportunity has not gone unnoticed by others and that, unless Australia acts promptly, it risks regional isolation on cyber-security issues.

Introduction

Hacking is not a new threat. States appear to have accepted that global interconnectedness through cyberspace comes at the cost of potential cyber attacks, resulting in increasing importance for cyber security. But for cyber defences to be effective, the nature of the threat must be understood. While there is a multitude of hacker entities in cyberspace, a concerning trend is emerging in the Southeast Asian region of hacking activities against states in the aftermath of physical events that have challenged another state's sovereignty.

Popular media almost inevitably attributes such actions to Chinese or Russian state-sponsored hackers. However, research reveals that many of these actions are conducted by a different cyber entity, namely 'hacktivists'. This paper will explore the concept of 'hacktivism', with a particular focus on recent events in the Southeast Asian region, to determine whether hacktivists pose a threat to states in the region and, if so, the implications for Australia.

What is 'hacktivism'?

Cyberspace has a unique language, with many terms having multiple meanings. The term 'hackers' can be used to refer to state-sponsored entities acting at the direction and control of their government; criminal groups seeking access to online information for profit; or protestors taking cyber action in response to an issue of concern. This paper will focus on the last category and, for clarity, the term 'hacktivist' will be used to refer to those individuals or groups whose hacking activities are issue-motivated—in other words, hackers who are activists.

The category 'hacktivist' can be divided into further sub-categories, based both on their motivation—for example, political, social or nationalistic motives—and their target.[1] Hacktivists who are motivated by nationalism or patriotism tend to target government websites within the state offending their patriotic sentiments and will be referred to as 'hacktriots'—patriotic hackers. However, any categorisation of hacktivist groups based on target and motivation must be very elastic in concept as, in some cases, groups will flow across the spectrum of categorisation.[2]

The structure of hacktivist groups is equally dynamic. Many are self-described as 'do-ocracies', where individuals are bonded by the desire to take action in support of a common cause, and membership of the 'group' exists only for the duration of an individual's willingness to support the current objective of the group. This means that at any given time, group membership could comprise a few or a few hundred thousand.

The power of hacktivists

Typically, hacktivist cyber action will comprise defacing websites or distributed denial of service (DDoS) attacks, although it appears increasingly to be extending to the seizure and public disclosure of information from target systems.[3] These actions generally cause inconvenience and embarrassment but not physical damage. With the rapid expansion in technology and the technique-sharing that occurs between individuals and groups across the internet, the ability of hacktivists to take more substantive cyber actions in support of their cause will increase over the coming years. The latent power of these groups and the impact they can have both on individuals and states is demonstrated by the following two examples.

In early February 2011, Aaron Barr, CEO of the cyber-security company HBGary Federal publicly announced he had uncovered the identity of 30 members of 'Anonymous' a (a loosely associated inter-national network of activist and hacktivist entities) and that he would disclose them at an upcoming cyber-security conference. Within 48 hours, all data from the email servers of HBGary was posted online and the company's websites defaced. Barr's Twitter account was seized and his presentation on Anonymous was posted on the internet and ridiculed for its supposed inaccuracies.[4] Within a month, Barr had resigned, with the company later estimating the 'hack' had cost millions in lost revenue. Whether rhetorical or substantive, Barr's threat was perceived by Anonymous as a threat to a fundamental value of the group and the anonymity of the internet, and it responded with speed and career-ending action to protect itself.

The power possessed by such groups can also be used against states, as demonstrated by the involvement of Anonymous in Tunisia. During the Arab Spring, the Tunisian dictator Zine el-Abidine Ben Ali began blocking Tunisian web access to Wikileaks posts related to his and other Arab nations. This action prompted members of Anonymous, motivated by their principle of freedom of access to information, to launch #OpTunisia.

Over the ensuing weeks, Anonymous members crashed the Tunisian stock exchange website, distributed media reports about Tunisian uprisings both in and outside the country, and distributed internet 'care packages' to individuals inside Tunisia containing instructions on how to negate the internet restrictions in place and avoid government electronic surveillance.[5] While the precise impact of #OpTunisia on the subsequent downfall of the Tunisian government will never be known, it is clear that it was influential in disrupting government actions and enabling citizens to maintain communications outside the country.

These examples provide a glimpse of the potential power that hacktivist groups can harness when acting against states or individuals.[6] But they have also demonstrated a willingness to engage in cyber actions against other significant non-state actors, such as ISIS in the aftermath of the Paris attacks and a Mexican drug gang.[7] Hacktivists' power to disrupt by cyber means is only likely to expand in the future given the increasing societal reliance on the 'Internet of Things'.[8]

By way of recent example, in October 2016, a DDoS attack was conducted against major internet entities in the US and Europe, such as CNN, Twitter and Spotify, by utilising the source code for malware that had been released a few weeks earlier by other hackers. The DDoS attack was alleged to have harnessed almost 500,000 devices, primarily webcams and digital recorders connected to the internet, as 'botnets' to conduct the attack.[9]

Cyber clashes between powerful non-state actors, both virtual and physical, using a weaponised Internet of Things, provides only a hint of the potential chaos for states that could ensue in the future, given the mutual lack of adherence of such groups to the rule of law and the likelihood of cyber actions being conducted across the globe. But is hacktivism likely to be an issue in Southeast Asia?

Hacktivism in Southeast Asia

Recent reports are demonstrating that hacktivism is occurring in this region, with a noticeable trend in actions by hacktriots. The most significant example in the region is related to competing maritime claims in the South China Sea, with a distinct trend for cyber activities to occur between hacktriots immediately after physical events. The first instance of this occurring is alleged to have commenced in 2012, after an incident between Chinese and Filipino naval vessels in the vicinity of Scarborough Shoal, triggering cyber attacks against government websites in the Philippines.[10] Other examples include events in July 2016, where immediately after the decision of the Permanent Court of Arbitration regarding a claim by the Philippines against China, there was a rise in the number of cyber actions against the Filipino government, with over 68 government sites disrupted by DDoS attacks.[11]

Also in July 2016, reportedly in response to Vietnam's relocation of missile launchers to disputed islands in the South China Sea, cyber attacks occurred against Vietnamese airports and its national airline.[12] Flight screens at Vietnam's major airports displayed messages critical of Vietnam's claims in the South China Sea, accompanied by equally critical public-speaker broadcasts.

Simultaneously, the national airline's website was attacked and the data of more than 400,000 passengers was 'dumped' online.

While many media reports at the time criticised the Chinese government for these actions, such allegations underestimate or overlook the active hacktriot culture within China and the effects suffered by China in the ongoing cybergame in the South China Sea. For example, in 2015, Anonymous launched #OpStopReclamation against the Chinese government in protest at its reclamation work on reefs and shoals in disputed areas in the South China Sea, attacking 84 Chinese government and industry websites.[13] This resulted in a hacktivist group, 'China Hacker Army', threatening to destroy Anonymous and launching attacks against Vietnamese and Philippine government websites. Chinese hacktriot groups such as the Red Hacker Alliance and the Honker Union, at times numbering in the tens of thousands, have both been linked to cyber actions in response to perceived slights against Chinese interests.[14]

Away from the South China Sea, other regional examples of hacktivist actions include the cyber attacks by Indonesian groups against Australian government websites in 2013 in response to allegations of spying by Australian authorities on Indonesian officials. In November 2013, media outlets reported that Australian intelligence agencies had been spying on Indonesia authorities, primarily through telephone interception of the mobile telephone belonging to the wife of the then Indonesian President.

This allegation triggered a series of cyber actions against Australian government websites and, specifically, the Australian Secret Intelligence Service. Allegedly, as other Australian government website were proving too difficult to hack, hacktivists turned to other websites in Australia, prompting a warning by Anonymous Australia to Indonesian hackers to focus only on government websites rather than the Australian people or they would respond with a counter-attack.[15] In the same year, Malaysian hacktivists attacked Filipino government websites in response to a border incursion by a Filipino group on the island of Sabah.[16]

These and other examples demonstrate a growing trend both of hacktivism in the region but also, and perhaps of more concern to states, of ongoing cyber skirmishes between hacktriot groups. It is highly likely that both hacktivism and cyber conflicts between groups will increase in the future, fueled by the anonymity offered by the internet. In order to assess the impact this may have on states in the coming years, it is important to understand the region's cyber environment.

The Southeast Asian cyber environment

Consistent with its rapidly growing economic power, the cyber environment of Southeast Asia is also undergoing rapid expansion. But rapid expansion without solid foundations can leave open critical vulnerabilities, as noted by Lee Mihyun:

> Southeast Asia has the world's fourth-largest internet population, and smartphone usage is also surging. However, it has an underdeveloped system of data protection laws and weak adoption of cyber security best practices. Besides, illegal software is rampant, making it easier to infect systems with malware.[17]

This rapid growth in information technology, coupled with a lack of robust cyber security, is enabling a marked increase in adverse cyber actions in the region.[18] For example, Indonesia reportedly has the sixth highest number of internet users in the world (over 80 million) yet was subject to an estimated 3.9 million cyber attacks over the period 2010-13, including a ten-month period in 2012 where the prevalence of attacks were against government websites.[19]

The cyber environment in Southeast Asia can therefore be described as one of rapid expansion, inadequate cyber security and increasing levels of cyber attack. This, coupled with increasing societal reliance on networked technology and the presence of active and potentially powerful hacktivists groups, has all the makings of a perfect storm in the next 5-10 years.

At best, it requires states in the region to be cognisant of the presence of chaotic actors with latent power and a propensity to react to physical events in the region; at worst, an event in the real world will trigger a significant cyber response from hacktivists with damaging consequences to a state. With a number of fragile states in the region, this could have ramifications on regional stability. As noted by Alan Chong:

> What is of more concern in the Southeast Asian cyber conflict arena is the pattern of nationalistic and inward-oriented possibilities for causing bilateral and domestic mischief against a developing nation's social harmony.[20]

Implications for Australia

The implications for Australia over the next 5-10 years should not be underestimated, as it presents both challenges and opportunities. Given the substantial economic interests that Australia has in the region, it is in Australia's interests to work towards a secure and networked regional environment. As one of the most mature cyber nations in the region, Australia is well placed to take advantage of the opportunity to assist in the development of regional and individual national cyber-security capacity.

Detailed solutions for states to address the threat posed by hacktivism are beyond the scope of this paper. However, obvious measures include enhanced cyber security, improved domestic and transnational law enforcement frameworks for cybercrime, and greater engagement between states to address the transnational nature of the threat. While most states in the region are working towards improving their cyber security, the effectiveness of their actions, particularly in less developed states, is questionable. These factors, coupled with the ongoing threat, generate a pressing need for inter-state engagement on the issue.

Australia appears to have recognised the need for closer regional engagement, cooperation and capacity building in its current Cyber Security Strategy, albeit not specifically in response to the threat of hacktivistm.[21] The strategy foreshadowed a forthcoming international cyber engagement policy and the appointment of a Cyber Security Ambassador. It is understood that both will focus on greater regional engagement on cyber-security related issues. This is a positive development when viewed alongside other states' approaches, which echo the need for increased engagement between states.[22]

A failure to act promptly will risk Australia not only losing a key opportunity to shape and influence the regional cyber environment but also to take pro-active steps to seek to reinforce the region's stability. Australia should not assume its proximity to Southeast Asia offers it an advantage over any other state when engaging in the region on cyber issues. In 2016, Indonesia and Russia reached an agreement to cooperate in cyber security, as did India and Vietnam.[23] Singapore also recently announced a program aimed at aiding ASEAN states improve their cyber defences.[24] A failure to engage regional counterparts risks leaving open opportunities for other states, whose interests may not align with Australia.

It is also assessed that over the next 5-10 years, less-developed states in the region will become increasing cyber dependent as they seek to improve their economies. A failure by Australia to assist with cyber-capacity building leaves developing states in the region vulnerable to destabilising actions, not only by hacktivists but also by other nefarious entities such as cyber criminals or subversive state-sponsored hackers. Such regional instability potentially holds consequential effects for Australia both in terms of its own security and economic interests.

There is no easy solution to the challenge of hacktivism. Recent years have demonstrated an increase in hacktivist activities which is likely to increase in volume and effect over the next decade. Hacktivism in the

Southeast Asian region presents an even greater challenge when contrasted against the rapid growth in information technology, unsupported by sound cyber security. It does, however, provide a unique opportunity for Australia to engage in cyber-capacity building within the region while concurrently exploring measures that states can collectively take to address the threat of hacktivism. However, this opportunity has not gone unnoticed by other cyber-developed states and, unless Australia acts promptly, it risks regional isolation on cyber-security issues.

Notes

1 For example, the actions of the hacktivist group Anonymous against the Church of Scientology and the Motion Picture Association of America were clear demonstrations of social motives, namely opposition to the perceived repression of freedom of access to information, whereas the actions of the Red Hacker Alliance, a Chinese hacker group, consistently demonstrate motivation by nationalistic ideals as demonstrated by their cyber actions against the Japanese government in 2004 arising from disputes over the Diaoyu Islands. For further information on the actions of Anonymous against the above entities, see Quinn Norton, 'How Anonymous picks targets, launches attacks, and takes powerful organisations down', *Wired* [website], 7 March 2013, available at <https://www/wired.com/2012/07/ff_anonymous/> accessed 20 February 2017. For further information on the actions of the Red Hacker Alliance, see William Howlett, 'The rise of China's hacking culture: defining Chinese hackers', *ScholarWorks* [website], June 2016, p. 94, available at <http://scholarworks.lib.csusb.edu/etd/383/> accessed 13 February 2017.

2 For example, the hacktivist group Anonymous has taken a number of cyber actions in response to actions by states, such as OpRussia and OpUkraine in 2014 in response to Russian action in the Crimea.

3 A DDoS attack is where multiple computers are used to attack a target computer system with a flood of incoming messages or incoming connection requests, overwhelming the target system and forcing it to slow down or crash, thus denying service to legitimate users.

4 The notice left on HBGary Federal's website read: 'This domain has been seized by Anonymous under section #14 of the rules of the Internet'. The rules referenced originate from a website linked with the origins of Anonymous, with Rule 14 reading as follows: 'Do not argue with trolls – it means that they win'. See Norton, 'How Anonymous picks targets'.

5 Norton, 'How Anonymous picks targets'.

6 In its report 'Security predictions for 2016 and beyond', Trend Micro, a corporation specialising in cyber security, identified that hacktivists would seek to use increasingly destructive actions beyond DDoS and webpage defacement. The report is available at <http://www.trendmicro.com.au/vinfo/au/security/research-and-analysis/predictions/2016> accessed 14 February 2017.

7 Andrew Colarik and Rhys Ball, 'Anonymous versus ISIS: the role of non-state actors in self-defense', *Global Security and Intelligence Studies*, Vol. 2, No. 1, Fall 2016, available at <http://digitalcommons.apus.edu/gsis/vol2/iss1/4> accessed 21 February 2017; and Paul Rexton Kan, 'Cyberwar in the underworld: Anonymous versus Los Zetas in Mexico', *Yale Journal of International Relations,* 26 February 2013, available at <http://yalejournal.org/article_post/cyberwar-in-the-underworld-anonymous-versus-los-zetas-in-mexico/> accessed 21 February 2017.

8 The 'Internet of Things' is a phrase increasingly used to described computer systems and machines used in everyday life that are networked and connected to the internet; for example, 'smart' televisions.

9 Sam Thielman and Elle Hunt, 'Major cyber attack disrupts internet service across Europe and US', *The Guardian* [website], 21 October 2016, available at <https://www.theguardian.com/technology/2016/oct021/ddos-attack-dyn-internet-denial-service> accessed 20 February 2017.

10 See, for example, Anni Piiparinen, 'China's secret weapon in the South China Sea: cyber attacks', *The Diplomat* [website], 22 July 2016, available at <http://thediplomat.com/2016/07/chinas-secret-weapon-in-the-south-china-sea-cyber-attacks/> accessed 23 May 2017.

11 Piiparinen, 'China's secret weapon in the South China Sea'.

12 Anuj Goel, 'The great cyber game in the South China Sea', *Cyware* [website], 12 August 2016 available at <https://cyware.com/news/the-great-cyber-game-in-south-china-sea-883f7f39?PageSpeed=noscript> accessed 20 February 2017.

13 Joshua Philipp, 'Hacker war erupts over South China Sea conflict', *Epoch Times* [website], 1 June 2015, available at <http://www.theepochtimes.com/n3/1376246-hacker-war-erupts-over-south-china-sea-conflict/> accessed 20 February 2017.

14 The nature and actions of Chinese hacktivist groups are beyond the scope of this paper but, for further information, see Howlett, 'The rise of China's hacking culture'.

15 The rather chilling warning message from Anonymous Australia is available at <https://www.techinasia.com/indonesian-hackers-attacking-nongovernment-australian-sites-final-warning-anonymous-australia> accessed 11 March 2017. See also Tom Minear, 'Indonesian hackers believed to be responsible for bringing down Australian Secret Intelligence Service website', *Herald Sun* [website], 11 November 2013, available at <http://www.heraldsun.com.au/news/law-order/indonesian-hackers-believed-to-be-responsible-for-bringing-down-australian-secret-intelligence-service-website/news-story/bd57aa5b075fe6485700244aabef7e7f> accessed 11 March 2017; and Enricko Lukman, 'Indonesian hackers still attacking civilian Australian sites, gets final warning from Anonymous Australia', *Techinasia* [website], 11 November 2013, available at <https://www.techinasia.com/indonesian-hackers-attacking-nongovernment-australian-sites-final-warning-anonymous-australia> accessed 11 March 2013.

16 Charlie Campbell, 'Malaysia: at least 26 dead as police raid Sabah siege', *World Time* [website], 4 March 2013, available at <http://world.time.com/2013/03/04/malaysia-at-least-26-dead-in-ongoing-sabah-siege/> accessed 11 March 2017.

17 Lee Mihyun, 'Southeast Asia begins to prepare for cyber war: India turns to AI', *Huffington Post* [website], 23 January 2017, available at <http://www.huffingtonpost.com/asiatoday/southeast-asia-begins-to_b_14334812.html > accessed 12 February 2017.

18 The Philippines was rated as the 33rd country most prone to cyber threats out of 233 nations in 2105. In the same year, Indonesia reported a 33 per cent increase in cyber-

attacks while, in 2016, politically motivated cyber-attacks in the region increased by 58 per cent. See, for example, Paul Baka, 'Southeast Asia still has weak information security against cyber threats' *The Diplomat* [website], 12 October 2016, available at <http://thediplomat.com/2016/10/southeast-asia-still-has-weak-information-security-against-cyber-threats/> accessed 19 February 2017; Control Risks, 'Cyber threat in South East Asia – who is being targeted and why', *Control Risks* [website], December 2016, available at <https://www.controlrisks/co/en/our-thinging/analysis-cyber-threats-actors-and-targets_sea-2016> accessed 19 February 2017; and *Fire Eye,* 'Southeast Asia: an evolving cyber threat landscape', *Fire Eye* [website], March 2105 available at <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-southeast-asia-threat-landscape.pdf> accessed 13 February 2017.

19 Jacqueline Kelleher, 'Indonesia launches Cyber Security Agency', *OpenGovAsia* [website], 15 September 2015, available at <http://www.opengovasia.com/articles/6563-indonesia-launches-cyber-security-agency-in-wake-of-growing-threat-landscape> accessed 1 February 2017.

20 Alan Chong, 'China and Southeast Asia: offline information penetration and suspicions of online hacking. A view from Singapore', presentation at China's 'Cybersecurity and Cyberdefense Policies and Strategies Conference', Paris, 1 July 2013, available at <www.st-cyr.terre.defense.gouv.fr/.../5%20-%20Chaire_AlanChong_1juillet2013.pdf> accessed 31 January 2017.

21 Department of the Prime Minister and Cabinet, *Australia's Cyber Security Strategy*, Commonwealth of Australia: Canberra, April 2016, Chapter 4.

22 See, for example, Cyber Security Agency of Singapore, *Singapore's Cybersecurity Strategy,* October 2016, available at <https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy> accessed 13 February 2017; and Government of China, *International Strategy of Cooperation on Cyberspace,* 1 March 2017, available at <http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm> accessed 9 March 2017.

23 Baka, 'Southeast Asia still has weak information security against cyber threats'; and Mihyun, 'Southeast Asia begins to prepare for cyber war'.

24 Prashanth Parameswaran, 'Singapore unveils new ASEAN cyber initiative', *The Diplomat* [website], 14 October 2016, available at <http://thediplomat.com/2016/10/singapore-unveils-new-asean-cyber-initiative/?allpages=yes@print=yes> accessed 11 February 2017.