Managing a digital revolution: cyber security capacity building in Myanmar

MANAGING A DIGITAL REVOLUTION

Cyber security capacity building in Myanmar1

Niels Nagelhus Schia and Lars Gjesvik

Introduction

Digitalization is exposing developing countries to a growing number of risks as well as opportunities associated with connecting to the Internet. Myanmar stands out as a critical case of both the pitfalls and the benefits Internet connection can bring. Amidst a political transition from military rule to a functioning democracy Myanmar is adding ICT to key areas like banking and e-government. Having been one of the least connected countries in the world only five years ago the country is now connecting to the Internet at an unprecedented pace, with few institutions in place to ensure the transition goes smoothly. The rapid expansion of Internet connectivity is connecting ever more people to an international world of business, discourse, and entertainment, but also crime, subterfuge, and discord. A crucial aspect for development in the years to come will be the harnessing of the benefits, as well as mitigating the downsides that inherently follow in the wake of Internet access (Schia, 2018). In this chapter, we examine the risks and potential benefits of Myanmar's embracement of digital technologies.

History and digital revolution

In 2010 Myanmar held its first general election in over 20 years. This was the fifth step in a seven-step transition roadmap to democracy. In 2011 the military junta was dissolved and replaced by a civilian government. In 2015 Aung San Suu Kyi won both houses and the freely elected Myanmar Parliament convened for the first time, after being under the thumb of military rule for over half a century. As the country has recently emerged from oppressive rule at the hands of the military junta, the military continues to hold a strong position in Myanmar politics, but the country has taken important steps towards a democratization of the society (Chan, 2016). In coexistence with this move towards a more open society the country has also tried to develop its economy and its capabilities on several issues, among these connecting to the Internet. Myanmar has moved rapidly from one of the countries with the least ICT coverage in the world to one where connectivity is growing at an unprecedented pace (Vota, 2015).

In 2011 the country was rated as the second-least connected country in the world, beating only North Korea, with an Internet penetration of under 1 per cent. The rapid connectivity is part of a government-initiated effort at modernizing the country that started in parallel with the democratization in 2011 (Calderaro, 2014). By the end of 2015 the number of subscribers in the country had ballooned to almost 50 per cent, indicating an increase in Internet subscribers of around 300 per cent yearly. The growth has been mostly related to smartphones, which make up around 80 per cent percent of all mobile phones in the country, a share that is higher than in most developed countries (Vota, 2015). While the fixed broadband Internet penetration is low, the mobile market has grown significantly since 2013, when the two foreign telephone operators Telenor (Norway) and Ooredo (Qatar) began investing in the Internet infrastructure in the country. In 2018, Myanmar is among the countries with the most substantial progress in the world concerning internet users."

Cyber security challenges in Myanmar

Being new to digital technologies the country still has significant unresolved issues relating to the securing and managing of this transition. A further

complicating element is that Myanmar is undergoing this rapid transformation into the digital age at the same time as the country is undergoing a profound political transition. The precariousness of political institutions combined with the known security threats emanating from digital technologies are both undermining the cyber security of Myanmar society. Adding internet connectivity as the same time as the country transitions away from a suppressive regime is heightening the risk that the technology can be used to exert government control and a return to old sins in acting as a tool for repression of minorities in the country (Calderaro, 2014).

As Myanmar struggles with an unstable political situation, the country is seeing new kinds of societal vulnerabilities emerging from digitalization, among them hate speech, cybercrime, and cyberattacks. The transition from military rule to a more democratic form of government, along with the recurring theme of ethnic conflict, creates an environment that is favorable to criminals and *bulletproof hosting.'* Already cybercrime is an existing, and growing, concern in Myanmar. As the growth in cybercrime rapidly outpaces the growth in digital transactions globally and the issue of criminal activities is set to grow in importance over the coming years. Due to the fluid nature of these criminal activities, states lacking legal frameworks and enforcements like Myanmar are likely to see a disproportional part of this growth (Threat Metrix, 2016).

As the country has connected to the Internet citizens have been allowed access to a wealth of information, resulting in a renaissance of sorts for independent media outlets and civil society groups. People have embraced social media and messaging applications such as Facebook and Viber, using these as their main, and often only, access point to the Internet. Facebook is in fact widely perceived as “the Internet” and is being used as a replacement for missing company websites, channels for file sharing, and communication between employees in public and private sector. This tendency has also been propelled by the collaboration between some social media companies and telephone operators. Telenor has for instance offered free Facebook through Telenor subscriptions. Despite this apparent positive development there are huge concerns relating to the security of these websites, as many of these applications are also pre-installed

when purchased.

In 2010 Myanmar was on the receiving end of what was at the time one of the largest Distributed Denial of Service-attacks (DDoS) to date. The attacks, which consists of flooding connection points with massive amounts of online traffic until they collapse, came in the run?up to the 2010 general election (Labovitz, 2010). As the infrastructure at the time was dependent on a single submarine fiber-optic cable, the attack succeeded in disconnecting the entire country from the Internet. Airline companies, public sector institutions, and citizens were cut off from online services for one month. The connection at the time was so limited that the attack was several hundred times larger than needed to shut down the connection. The government did not have the expertise or any established strategies to deal with the situation. China remedied the situations by providing Internet services for the important ministries through their border. While the source of the attacks has not been made public to this date, suspicion has been directed towards the military junta that governed the country, as dissident websites hosted outside of Myanmar had been targeted earlier in the year (Reporters Without Borders, 2010). There were also similar accusations raised at the Burmese military and government following restrictions of access and information in 2007 (Nizza, 2007).

This underlines the risks that digital technologies will erode the turn towards democratic governance, and whether controlling the political discourse has merely taken on another form. The most concerning development has been the rise of vigilante groups pushing a nationalistic agenda by attacking websites and news outlets that are critical of the government, or in some way positive to the country's Muslim minority (Hindstrom, 2016a). The most active of these group has been identified as the "Blink Hacker Group" which has targeted numerous media websites over the last few years. This group has been linked to the Myanmar military by the Swedish-based cyber security firm *Unleashed Research Lab* (Hindstrom, 2016b). Their report on the attacks tied the hacker-collective to military servers and training facilities, while the group itself has admitted on Facebook that it consists in part of "Pro-government" members (Unleashed, 2015). This is coupled with a general rise in Islamophobia, and the use of social

media as an instigator of violence between differing ethnic groups, and mainly aimed towards the ethnic Rohingya-minority.

The combination of ethnicity, suppression, and digital technologies has come under increased focus lately. Myanmar is one of the most ethnically and culturally diverse countries in the region, with a persistent tension between the Burman central government and the various minorities. The most well-known tension runs

between the Buddhist majority, and the ethnic Rohingya Muslim minority. A tension that has been transferred into the cyber realm with a growing number of incidents of hate-speech, as identified by a survey on digital security by the Myanmar Center for Responsible Business (Myanmar Centre for Responsible Business, 2015). A glaring problem in Myanmar's online world is in this sense the addition of social media to an already combustible ethnic situation. This mixture has already led to violent riots with two casualties as the result of rumors spread online (Calderaro, 2015). Since then hate speech has continued to spread and is becoming an increasingly pressing problem. Most of the hate speech is directed towards the Muslim majority, with a significant part of the hate speech including calls for violence and even killing of Muslims (Ibid.). In 2018 investigations by Reuters journalist Steve Stecklow exposed how the dependence on Facebook for digital communication acted as a driver for the genocide aimed at the Rohingya minority, highlighting the damaging potential digitalization and social media has in tense ethnic conflicts (Stecklow, 2018).

Cyber security in Myanmar *Contextual factors*

While leapfrogging into the digital age creates new opportunities and greater connectedness, it also creates challenges and pitfalls. Technological development and progress move fast, while norms and policy production move slowly and create a lag between policy and practice; this has become symptomatic for the digital age. The lag creates a huge gap between political regulation on the one hand and practice on the other, both internationally and nationally. This gap is also pertinent in Myanmar. Interviewees from fieldwork in 2016 and 2017 pointed at the need for cyber security capacity' building within the state institutions; for improving legal regulations and mechanisms; and for awareness campaigns, better

knowledge, and education. The new and distinct societal challenges and vulnerabilities stemming from digitalization vary from nation to nation and are shaped by the interface between digitalization, local and national policies, and large-scale global forces, elsewhere also described as the “cyber frontier” (Schia, 2018). Cyber security' and digital pitfalls must be understood and contextualized to local circumstances. Even though the digital age is relatively new, there are already several examples showing how this technology can be utilized either for democratization trends or by' authoritarian regimes to suppress public interests, democratic processes, and freedom of speech. Any outcome will depend on an interplay' between the new technology' and pre-existing political and economic circumstances. Digital technology may help authoritarian regimes regain control during democratic transition. Some scholars have found that authoritarian regimes or states wanting to repress an independent public sphere were more likely' to adopt and expand the Internet than were other autocracies (Rod & Weidmann, 2015).

Myanmar’s current political transition in tandem with the digital revolution is perhaps the country’s most distinct feature in this context. Certainly, one of the main factors determining the limited ability' to provide digital security in Myanmar is the glaring lack of resources, both human and financial. The lack of qualified personnel with sufficient training and skills in IT security' is obvious, and not just restricted to the public sector but private companies as well. This limitation puts severe strain on all aspects of cyber security' provision, from the development of regulations and policies to the day-to-day' management of digital events. Raising the competencies and resources available will be critical to enhance cy'ber security' and cyber resiliency in the years going forward. One initiative that has already' been taken is *The Digital Myanmar Study* (2018). This is a self-assessment of the country’s cyber security' capacities that was hosted by the Ministry' of Transport and Communication and facilitated by the World Bank, the Global Cyber Security Capacity' Centre at the University of Oxford (the GCSCC), and the Norwegian Institute of International Affairs (NUPI).[4] This evaluation identified challenges and produced useful recommendations to the Myanmar

government in five societal dimensions; cyber security strategy and policy, cy'ber security culture and society, cyber security education, training and skills, as well as on standards, organizations, and technologies. However, it is not clear to what extent the Myanmar government has had the capacity to follow up on the recommendations identified in this study.

The outreach to Oxford also highlights an important issue for Myanmar going forward, namely which approach and understanding of cyber security will be implemented. States approach cy'ber security from two main vantage points: one being championed by' western states and forming the basis for initiatives like the Oxford review takes a multistakeholder approach to cy'ber security where this security' is conceptualized as a public good. The other camp, most prominently championed by Russia and China, has a more state-centric approach to cy'ber security. This “cyber sovereign” approach does not separate state authority' in cy'berspace from state authority over the physical domain, and as such implies larger acceptance for surveillance and control. The majority' of states, however, do not fall into one of these categories but are understood as either uncommitted or “digital deciders”; states who are undecided but who have significant regional influence. For the ASEAN region Singapore is one such critical case that could have large regional influence, and a relationship that is worth paying attention to.

However, the most crucial relationship for Myanmar has historically been China. As long as Myanmar was a pariah state globally its relationship with its giant northern neighbor resembled that of a client state. China has also been tentatively identified as the culprit in several espionage campaigns where Myanmar was one of the victims. A 2015 FireEye investigation into the APT 30 group found that the group had been active in targeting ASEAN member-states (like Myanmar) for several years. While the group’s targets pointed towards the Chinese government, the group has not as of yet been definitely linked to any actor (FireEye, 2015). A similar pattern vas evident in the 2015 Arbor Networks investigation into the “Trochilus” campaign (Metzger, 2016). While both reports are hesitant at attributing China directly, other experts have hinted toward China being the likely

culprit. The recent democratization has changed the relationship between the two countries as Myanmar looks for other international engagements, and until very recently enjoyed improved relationships with western states (Maini & Sachdeva, 2017). This makes the choices and trajectory of the Myanmar cyber security approach in the years to come an interesting case in how developing states will place themselves within the increasingly contested battle on how to define cyber security. Stating which direction Myanmar will take is so far rather premature, as the approach and strategies are too underdeveloped to be accurately defined, a point we will turn to next.

Official policies and legal framework

In general, the approach to cyber security' in Myanmar is at a start-up stage, with an ad-hoc approach to capacity and blind spots in both official policies, regulation and competencies to deal with the challenges posed by digitalization. Some initial discussions and needs- assessment exercises have been run, but there is currently no official national cyber security strategy, few cyber security units in the public departments, and weak coherence in sets of policies across the ministries. This can partly be traced back to the newness of digital technologies in Myanmar, the revolutionary uptake of mobile connectivity in later years has necessarily led to a lag in political activity. Partly the general political upheaval of post-junta Myanmar has meant a flurry of political activity' wherein digital regulations has not been given prominence. Finally, the issues of Myanmar in managing digital technologies politically could be seen as a symptom of a larger trend wherein developing nations are struggling to provide digital security in a rapidly shifting technological environment.

The most clear-cut example of the inability' to provide sufficient security is the lack of a cyber security strategy or any overarching coherent framework for guiding the work on cyber security'. While a draft strategy has been under development for a long time, being the work of the Ministry of Transport and Communications in cooperation with the Asian Development Bank, no finalized version exists as of yet. Beyond the non-existence of an actual framework, the process with which the strategy was developed involved a small number of

ministries of agencies and taking in very little input from private companies or critical infrastructure owners. As a consequence, questions can be raised regarding the applicability' of the strategy when it comes into force. The non-inclusion of the very companies that will be tasked with providing cyber security in developing the strategy can be seen as troubling.

The lack of an overarching strategy in turn fragments the approach by various ministries and agencies, as a cross-sectorial issue is met by isolated initiatives. As ministries and agencies operate within their respective silos when it comes to detecting and responding to various risks and threats. As Myanmar has rapidly digitalized, the frequency of cyber incidents is growing rapidly and the fragmented approach is hampering the ability to manage it sufficiently. This is further complicated by the byzantine bureaucratic processes and structures that define much of the governmental work. For the issue of cyber security providing meaningful legislation and regulations is for instance dependent on the cooperation between the Ministry of Transport and Communication and the Ministry of Planning and Finance, a cooperation which so far has been limited and strained. Providing a clear overarching direction for these various approaches and conflicts of interests necessitates a cyber strategy tailored to the situation in Myanmar, providing clear incentives, benchmarks, and divisions of responsibility.

The lack of top-down political leadership is further reflected in the absence of awareness about critical infrastructures and their importance for modern societies. The very concept of critical infrastructures is not widely established, and subsequently neither is the cyber security of said infrastructures. The lacking mapping, categorization, and understanding of different infrastructures and the role they play in society limits the ability to secure them in a sufficient manner. As there does not exist any legal definition of what a critical infrastructure is, the framework for mapping and categorizing them is non-existent. As a first step creating a legal framework for what is considered critical infrastructure, as well as giving the responsibility of protecting said infrastructures to an institution, would be a starting point to improve critical infrastructure protection in Myanmar. The

increasing number of cyber incidents targeting institutions and infrastructures that are widely categorized as "critical" in other states, such as the central bank, highlights the importance of improving on this issue.

Moving towards the regulatory regime, the state of Myanmar cyber security legislation is also at an early stage, with large gaps and insufficient existing frameworks. Some laws are in place that cover some aspects of cyber security,

notable examples being the *Electronic Transactions Law (State Peace and Development Council Law No 5/2004)* covering some aspects of electronic data and cybercrime. This law defines the distribution of information that causes harms to minors (see, section 34(d)) via digital technology and networks as illegal, and it also allows electronic evidence to be brought before the court. The *Telecommunications Law* regulates access to and the use of telecommunication services (Electronic Transactions Law, 2004). Legislation covering issues like human rights, data protection, and child pornography is however not in place, making the overall legislative framework highly insufficient for responding to rapidly evolving digital threats. Beyond the actual legal framework, the implementation of existing laws is also lacking, as there are limited resources, competencies, and abilities to investigate and prosecute cybercrime both in the police and the judiciary. Some initiatives have been taken, such as the Cybercrime Division at the National Police Criminal Investigation Department, but also here, the unit suffer from limited capacity. Very few cybercrime cases have been brought to court. Prosecutors and judges need training on cybercrime and how to make use of digital evidence.

One of the institutions that has been established is a national Computer Emergency Response Team (CERT), with mmCERT (Myanmar Computer Emergency Response Team) being established as early as 2004 by e-National Task Force. The CERT's mission is to do incident handling, public awareness in security, to provide cyber security advice to Myanmar Internet users, and to prevent cyberattacks. It is also nrmCERT's responsibility to function as a coordinator of incident responses with other teams, organizations, security experts, and law enforcement agencies nationally and internationally. In 2010

mmCERT came under the responsibility of Myanmar's Ministry of Transport and Communications. This ministry also has its own cyber security unit aiming to enhance the cyber security capacity in the country. The CERT is also an operational member of the Asia Pacific Computer Emergency Response Team (APCERT) and the International Multilateral Partnership Against Cyber Threats (IMPACT). While it's ostensibly providing technical assistance, cataloguing incidents, collaborating with international partners, and assisting police and other agencies its limited resources significantly hamper its ability to deliver on its mandate. The lack of financial resources available for mmCERT results in insufficient technical equipment, lack of human resources, and limited ability to operate as intended. And outside of its international affiliations, private companies and stakeholders in Myanmar hold that mmCERT is not adequately capable of addressing cyber security' threats in Myanmar (Myanmar Centre for Responsible Business, 2015). In addition, there is little awareness of the role and functions of mmCERT, resulting in a lack of information being shared with the organization. While the leading companies, particularly the international ones, have capacities to manage incidents, the cooperation between government and private actors are minimal, further limiting the ability of mmCERT to work as intended.[6]

When it comes to regional collaborations these are limited. Among the more effective collaborations described by' interviewees during fieldwork in 2016 and 2017, was the engagement with Interpol. This was pointed at as an important channel for cross-border collaboration and information sharing. Interpol, ITU, and ASEAN deliver capacity' building programs to the cybercrime unit at the national police, although not on a regular basis. Regional initiatives through ASEAN intend to develop better, more accessible, and more affordable IT infrastructure. These goals have been established and endorsed in an ASEAN broadband corridor study that also identified key drivers for broadband rollout and recommendations for government initiatives (ASEAN, 2016) as well as improved capacities, knowledge and awareness (ASEAN, 2015). Some regional measures have also been taken to mitigate possible bullet-proof hosting, weak links, and havens of vulnerable ICT architectures in the CLMV countries — Cambodia, Laos, My'anmar, and Vietnam (Heinl, 2014). The collaboration with other ASEAN

member states on mutual legal assistance treaty in criminal matters has not been ratified to include cases concerning cybercrime, and My'anmar has not signed the Budapest Convention or any other multilateral or regional cybercrime agreement.

Cultural and societal factors

Cy'ber security is provisioned by' a multitude of actors frequently described as an “assemblage” of private, public, and private citizens (Collier, 2018). To fully' comprehend the work on maintaining a safe and reliable cy'berspace for citizens one needs to broaden the view to include not only the government initiatives but also the leading private companies and individual citizens. For My'anmar there is a widespread lack of attention being afforded to the security implications of rapid digitalization. This holds true for both public and private sector employees as well as the general public at large. It can be seen through widespread usage of pirated software and unsecured mail accounts for employees, as well as a limited level of awareness on the security issues modern societies face. The most problematic account however related to the understanding of cyber security dangers in the public at large. Taking a broad understanding of cyber security, including such concerns as the dissemination of fake news, there was a noted lack of skepticism surrounding claims made online. Furthermore, there is little to no awareness about the dangers of handing out private data or sensitive information online among the general public, providing an ample breeding ground for cybercrime.[7] Seen in correlation with the incitement towards ethnic violence mentioned above, the lack of awareness and competencies when it comes to navigating digital media is troubling.

The main exceptions to the rule of low awareness about cyber security is an issue in the private sector, and most notably among the two leading telecommunication operators in the country. After a 2012 licensing-round, licenses were awarded to Qatari telecoms operator Ooredoo and Norwegian operator Telenor (Calderaro, 2014). In Myanmar, there has been a shared responsibility for the development of the telecommunications sector: while the government is focused on developing laws and regulations extending connectivity has fallen into the hands of foreign companies. A large part of the task is thus dependent on the

companies doing so in a manner that highlights their corporate social responsibility. A 2013 Human Rights Watch report underlined the potential positive impacts of the Internet and digitalization in societies such as Myanmar. However, the report also stressed the risk that this technology would be used by the regime to crack down on dissent, used for illegal surveillance, and as a way to enforce censorship. The call was for companies involved in improving the ICT-

infrastructure in Myanmar to refrain from cooperating with the government on matters that would undermine the rights of its citizens (HRW, 2013).

Whether the companies do so is up for debate. The smaller of the companies is Ooredoo, which has no clear published guidelines and a spotty record on protecting the rights of its users. The company in fact has a history of accepting censorship by the Qatari government and installing filters in accordance with the wishes of autocratic regimes (Calderaro, 2014). Telenor on the other hand is widely regarded as having one of the more advanced policies on social responsibility, however there are some concerns raised over its shutting down of its services at the behest of the Thai military junta in 2014. There are also some uncertainties over the extent to which telephone operators are willing to pass information over to the government and whether these policies are clearly enough formulated to withstand potential pressures (Calderaro, 2014).

The way forward

When addressing the question of Myanmar's preparedness and development on the issue of cyber security, a starting point is mapping the landscape of digital infrastructure and its trajectory. The infrastructure in Myanmar is disproportionately based on mobile broadband access and not fixed broadband, which translates into lower speeds and worse service. Myanmar is thus a typical case of early stage Internet development, while there has been an immense growth in spreading internet coverage nationally, the underlying structure and backbone of the Internet remains weak. This is important as most websites, both foreign and domestic, are based on servers outside the borders of Myanmar. A stable connection to the outside world is thus important to gain access to most of the

websites that residents want to access. Up until very recently Myanmar was served by a single submarine cable, creating both large vulnerabilities in the infrastructure and a slow connection (Telegeography, 2020).

In general Myanmar's cyber security "maturity" is at the start-up level, very few actions, other than some initial discussions on this topic, have been taken. There are however some indications on clear progress towards a more formative level in the education sector, the legal and regulatory framework, and on establishing better standards. Nevertheless, Myanmar remains among the countries in the Asia-Pacific region with the least attention to cyber security. Reports have pointed to large issues and gaps in the approach to the issue. Beyond the military aspect of cyber security Myanmar is among the lowest scoring countries in all categories in a comparison between Asian countries, highlighting a long list of issues that needs to be addressed (ASPI, 2017). A shortage in skilled labor is one of the main issues, as the 1CT sector is regulated and run by a small group of public employees tasked with managing the rapid transition. The digital transformation, coupled with the democratic transition, is dependent on the development of a long list of technical standards and regulation, as well as reinventing the educational system to meet new demands. On top of this, the interconnected nature of the ICT sector, and the fact that Myanmar has already become entangled with foreign actors after years of isolation, points to the scope of the challenge Myanmar is facing to make the transition run smoothly (Myanmar Centre for Responsible Business, 2015). Moreover, while the government drafted a master plan for telecommunications in 2015 its implementation has been severely postponed and uneven, undermining the efforts at creating a sound political environment. This is mirrored in the regulatory sector wherein the existing rules and regulations are aimed at control and censorship, and not on cybercrime and related issues (ASPI, 2017).

A subdivision of the political and regulatory capacity is a country's participation in international foras and programs. This is an area of particular importance in cyberspace, where the government challenges are often global in nature. One of the main ways for countries with less-developed cyber security maturity is to

engage in cooperation between Computer Emergency Response Teams (CERTs). There are some regional initiatives enabling this, such as the APCERT which covers the Asia-Pacific Region and where Myanmar is a member. This is a positive, both for the development of capabilities within countries and to foster cooperation and information-sharing between countries and national CERTs. While Myanmar participates in APCERT, as well as some bilateral capacity building programs with India and Singapore, among others, the country has not so far engaged other countries beyond capacity-building programs (ASPI, 2017).

In the midst of a democratic transition, Myanmar is trying to utilize ICT and digital technologies to jump-start its development. The potential for ICT to do so is great, but so are the risks inherent in connecting to the Internet. Due to its fragile political state, turbulent regional politics, and fraught social cohesion, Myanmar faces a set of unique challenges. Building cyber security is paramount to avoid a scenario wherein digital technologies act as a catalyst of destructive forces, and not as a vehicle for development. Expanding and developing cyber security capabilities should therefore be a priority as key financial and governmental functions are moved online, otherwise the digitalization of Myanmar risks being a curse disguised as a blessing.

Notes

1 This chapter builds on fieldwork in Myanmar in 2016 and 2017 and further develops findings from a NUPI-policy brief and working paper: Managing a digital revolution — Cyber Security Capacity Building in Myanmar (2018).

2 In wireless and household Internet penetration.

3 Rogue states and countries in the Global South become hosts to outlaw servers, so-called “bulletproof hosting.” The hosts of these servers operate beyond the reach of most law enforcers, and make cybercrime possible elsewhere (Schia, 2018: 826).

4 For more about this see, www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-assessments- around-world, and

www.nupi.no/en/About-NUPI/Projects-centres-and-programmes/Cybersecurity-Capacity-Building-2.0-Bridging-the-digital-divide-and-strengthening-sustainable-development

5 This was confirmed by several officials from various ministries in Myanmar during fieldwork and interviews in 2016 and 2017.

6 This was confirmed by several officials from various ministries in Myanmar during fieldwork and interviews in Nay Pyi Taw and Yangon in 2016 and 2017.

7 Field assessment findings, fieldwork in Myanmar 2016 and 2017.

Suggested reading

Chang, L. Y. C. (2017). "Cybercrime and Cyber Security in ASEAN," in J. Liu, M. Travers & L. Chang (eds.), *Comparative Criminology in Asia* (pp. 135—148). Cham: Springer.

Clark, D. B. (2017, September 28). "Myanmar's Internet Disrupted Society - And Fueled Extremists," *WIRED,* www.wired.com/story/myanmar-internet-disrupted-society-extremism/

Myanmar Centre for Responsible Business. (2019). "Policy Brief: Cyber Security and Cyber Crime: Issues or Myanmar." www.myanmar-responsiblebusiness.org/pdf/2019-Policy-Brief-Cyber-Secur ity-and-Cyber-Crime_en.pdf

Singh, R. (2019, July 5). "Myanmar's March Towards a Digital Future," *Internet Society,* www.internetso ciety.org/blog/2019/07/myanmars-march-towards-a-digital-future/

Unleash Research Labs. (2016). "Unleashed: Unveiling Cyberwar in Myanmar." http://unleashed.blin khackergroup.org/op-its-time/3/

References

ASEAN. (2015). “ASEAN ICT Masterplan 2015.” www.asean.org/storage/images/2015/December/ telmin/ASEAN per cent201CT per cent20Completion per cent20Report.pdf ASEAN. (2016). “Masterplan on ASEAN Connectivity 2025,” https://asean.org/wp-content/uploads/ 2016/09/Master-Plan-on-ASEAN-Connectivity-20251 .pdf Calderaro, A. (2014). “Digitalizing Myanmar — Connectivity Developments in Political Transitition,”

Center for Global Communication Studies, https://global.asc.upenn.edu/publications/ digitalizing-myan mar-connectivity-developments-in-political-transitions/

Calderaro, A. (2015). “Internet Governance Capacity Building in Post-Authoritarian Contexts,” *Internet Policy Observatory,* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2686095 Chan, S. (2016, February 2). “First Freely Eleceted Parliament after Decades of Military' Rule Opens in Myanmar,” *'lhe New York Times,* www.nytimes.com/2016/02/02/world/asia/first-freely-elected-par liament-after-decades-of-military-rule-opens-in-myanmar.html?_r=0 Collier, J. (2018). “Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision,” *Politics and Governance, 6(2):* 13-21.

Electronic Transactions Law. (State Peace and Development Council Law No 5/.2004, http://unpanl.

un.org/intradoc/groups/public/documents/un-dpadm/unpan041197.pdf (accessed 31 October 2018) FireEye. (2015). “APT30 and the Mechanics of a Long-Running Cyber Espionage Operation.” www2. fireeye.com/rs/fireye/images/ rpt-apt.30.pdf

Heinl, C. H. (2014).“Regional Cybersecurity: Moving Towards a Resilient ASEAN Cybersecurity Regime,” *Asia Policy, IS:* 131—159.

Hindstrom, H. A. (2016a). “The Perils of Burma’s Internet Craze,” for *Foreign Policy.* 01. 04.2016, http://foreignpolicy.com/2016/04/01/the-perils-of-bunnas-internet-craze/

Hindstrom, H. B. (2016b): "Is Myanmar's Military Behind Shadowy Cyber Attacks?" for *The Diplomat,* 27. 02.2016 https://thediplomat.eom/2016/02/was-myanmars-military-behind-shadowy-cyber- attacks/

HRW. (2013, May 19). "Reforming Telecommunications in Burma." www.hrw.org/report/2013/05/ 19/reforming-telecommunications-bunna/human-

rights-and-responsible-investment-mobile Labovitz, C. (2010, November 3): "Attack Severs Burma Internet," *ASERT.* https://asert.arbornet works.com/attac-severs-myanmar-internet/

Maini, T. S. & Sachdeva, S. (2017, November 14). "China Faces Increasing Competition in Myanmar," *The Diplomat,* https://thediplomat.com/2017/ll/china-faces-increasing-competition-in-myanmar/ Metzger, M. (2016, January 13). "'Trochilus' RAT Targets Government of Myanmar," *SC Media.* www.scmagazineuk.com/trochilus-rat-targets-government-myanmar/article/1477758

Myanmar Centre for Responsible Business. (2015, September 24). "Sector-Wide Impact Assesment of Myanmar's ICT Sector." www.myanmar-responsiblebusiness.org/swia/ict.html

Nizza, M. (2007, September 28). "Burmese Government Clamps down on Internet," *The New York Times,* https://thelede.blogs.nytimes.com/2007/09/28/burmese-government-clamps-down-on- internet/

Reporters Without Borders. (2010, May 10). "Stop Cyber Attacks on Independent Burmese Media." https://rsf.org/en/news/stop-cyber-attacks-against-independent-burmese-media

Rod, E. G. & Weidmann, N. B. (2015). "Empowering Activists or Autocrats? The Internet in Authoritarian Regimes," *Journal of Pence Research*, 52(3): 338-351.

Schia, N. N. (2018). "The Cyber Frontier and Digital Pitfalls in the Global South,"

Third World Quarterly, 59(5): 821-837.

Stecklow, W. (2018, August 15). “Why Facebook Is Losing the War on Hate Speech in Myanmar. www.reuters.com/investigates/special-report/myanmar-facebook-hate/

Telegeography. (2020, August 14). “Submarine Cable Map.” https://www.submarinecablemap.eom/#/

Threat Metrix. (2016). “Q1 Cybercrime Report.” www.threatmetrix.com/wp-content/uploads/2017/ 04/cybercrime-2016-qt-1492588964.pdf?_ga=2.203348887.767081945.1493862414-973637201. 1493760913

Unleashed. (2015). “Unleashed — Unveiling Cyberwar in Myanmar.” http://unleashed.blinkhackergroup. org/

Vota, W. (2015, September 30). “Wow! Myanmar Is Going Straight to Smartphones,” *ICT Works.* www.ictworks.org/2015/09/30/wow-myannrar-is-going-straight-to-smartphones/