Publisher: Norwegian Institute of International Affairs

ISBN: 978-82-7002-337-0

Any views expressed in this publication are those of the author. They should not be interpreted as reflecting the views of the Norwegian Institute of International Affairs. The text may not be printed in part or in full without the permission of the author.

Visiting address: C.J. Hambros plass 2d
Address: P.O. Box 8159 Dep.
NO-0033 Oslo, Norway
Internet: www.nupi.no
E-mail: info@nupi.no
Fax: [+ 47] 22 99 40 50

Tel: [+ 47] 22 99 40 00

Managing a digital revolution: Cyber Security Capacity Building in Myanmar[1]

Niels Nagelhus Schia
Lars Gjesvik

[1] Presented at the Norwegian Information Security Conference 2017 (NISK 2017).

Published by the Norwegian Institute of International Affairs

Contents

Summary

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 little or no institutions in place to ensure the transition goes smoothly. Using the framework of Cyber Security Capacity Building (CCB) we examine the risks and potential benefits of Myanmar's embracement of digital technologies.

The potential benefits of digitalization

Through the rapid digitalization of the developing world a plethora of opportunities and pitfalls are evolving before our eyes. The rapid expansion of internet connectivity is connecting ever more people to an international world of business, discourse and entertainment. Thus, 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. As a key part of this the concept of cyber security comes to the fore. As the developed world struggles with how to secure its digital infrastructure and the processes that depend on it, the developing worlds do as well. This has led to an emerging idea of Cyber Security Capacity Building, wherein donor states attempt to strengthen the ability of developing states to govern and protect its cyberspace.

In this paper, we have used the framework of Cyber Security Capacity Building (CCB) proposed by Klimburg and Zylberberg (2016), as it takes a broader approach to cyber security. Other approaches tend to focus more exclusively on national security, while CCB considers the wider economical and societal impacts of digitization. The rationale for this concept is an idea that cyber security impacts states and donors through three underlying mechanisms. In reverse order, they are 1) the ability of digital technologies to promote freedom, by creating spaces for expression of thought and debates that are free from governmental constraints. 2) By using CCB to strengthen the international cyber security architecture. As the Internet is an online arena the security is only as strong as the weakest link, improving developing states will therefore improve the structure globally. And finally, 3) the increasing importance of digitalization and ICT in fostering economic and societal development, and the need for Cyber Security to protect these benefits.[2] It is this final element we will now turn to, and which will be the focus of this

[2] Klimburg, Zylberberg: 2016

paper, by addressing the various ways in which digital technologies are promoting development.

At the most basic level expanding ICT and broadband infrastructure has been linked to growth in GDP. While noting that there might be issues of causality, and there has been varying numbers reported, the most frequently cited number comes from the ITU which states that a 10% increase in Broadband coverage correlates with a 1.38% increase in GDP.[3] As the Internet is a global marketplace, connecting to it improves the ability of developing states to connect consumers, producers, and ordinary citizens. The digital economy contributed an estimated 4 trillion US dollars in 2016, and grew by 10%, a rate of growth that outstrips the overall G20 economy.[4] Even more important is its contribution in developing countries, where a study has suggested that ICT might have contributed as much as a quarter of the growth in developing countries at the start of the millennium.[5]

Compounding the importance of ICT in promoting growth is the speed of diffusion. While ICT is creating possibilities for growth, it is also doing so for more people far faster than traditional expansion of infrastructure. Since the dawn of electricity and the development of electricity grids, over a hundred years ago, only 17% of the population of Sub-Saharan Africa are connected to such a grid. As a contrast about 70% are by now connected to the Internet in some form or another, a mere 23 years after the technology became commercialized.[6] This is of course a simplification, as the degree of coverage varies substantially, but it highlights the great potential of ICT's in developing and transforming economies. The sheer pace of the expansion of Internet are creating new forms of employment and means of communication and exchange, such as mobile banking and mobile money in Sub-Saharan Africa.

[3] (ITU, 2012).

[4] (WEF, 2015).

[5] Ibid

[6] http://systemtransformation-sdg.gesi.org/160608_GeSI_SystemTransformation.pdf

ICT and the Sustainable Development Goals

Another method of measuring potential impact is to move beyond simply economic numbers and look at how ICT relate to development in a larger setting. One such setting is to look at how ICT impact on key benchmark goals for development. The main such goals are the UN sustainable development goals, which consists of 169 targets distributed among 17 "goals". These goals are meant as a continuation of the UN millennial goals, which were claimed as a success in terms of fostering development and improving living conditions globally.[7]

ICT works towards the sustainable development goals through two avenues: on the one hand, it is singled out as one of the 169 "sub targets" and is therefore a development target on its own. Added as a part of the aim to improve industry and infrastructure the issue has been framed in the following manner by the UN Economic and Social Council:

> *71. Infrastructure and economic development also rely on information and Communications technology. Mobile cellular services have spread rapidly around the world, allowing people in previously unconnected areas to join the global information society. By 2015, the percentage of the population living in areas covered by mobile broadband network s stood at 69 per cent globally. In rural areas, the share was only 29 per cent.*[8]

As a result, one the stated targets for the UN goal pertaining to Industry, Innovation and Infrastructure is to "Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020".[9]

While ICT and digitalization is thus an integrated part of the sustainable development goals, the by-effects of digitalization will secure the larger gains. As ICT spreads and societies connect to the Internet there is widespread optimism regarding the possibilities

[7] http://www.un.org/millenniumgoals/mdgmomentum.shtml

[8] http://www.un.org/ga/search/view_doc.asp?symbol=E/2016/75&Lang=E

[9] UN

for developing countries to transform their societies. While ICT and digitalization is tied in to development in a direct manner, the larger perceived value lies in the ability of digitalization to help reach the development goals in other areas as well. The optimism for ICT to transform developing societies is substantial, and theories abound on how it can be done. A 2016 report from the Global E-Sustainability Initiative is markedly bullish about the potential for ICT's to push developed countries further along. Among the drastic transformative effects that are hypothesized are reductions of yearly traffic fatalities by 720.000 globally, of improving healthcare for 1.2 billion people and potential carbon emission reductions by close to 20%. The report also highlights the possibilities ICT offers in terms of education, fostering economic growth, and building smart cities.[10]

The benefits of digitalization in Myanmar

In 2016 the first 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, it has also moved towards a democratization of the society.[11] 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.[12] 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%. The rapid connectivity is part of a government-initiated effort at modernizing the country

[10] (http://systemtransformation-sdg.gesi.org/160608_GeSI_SystemTransformation.pdf

[11] https://www.nytimes.com/2016/02/02/world/asia/first-freely-elected-parliament-after-decades-of-military-rule-opens-in-myanmar.html?_r=0

[12] http://www.ictworks.org/2015/09/30/wow-myanmar-is-going-straight-to-smartphones/

that started in parallel with the democratization in 2011.[13] By the end of 2015 the number of subscribers in the country had ballooned into almost 50%, indicating an increase in internet subscribers of around 300% yearly. The growth has been mostly related to smartphones, which make up around 80% percent of all mobile phones in the country, a share that is higher than in most developed countries.[14] This has in turn lead to a growing number of services that are based upon ICT.

An area that has been noted for its considerable potential in development is e-commerce and online banking, with banking penetration in Myanmar as low as 10% in urban areas and even lower in rural areas.[15] The Central Bank has already taken steps towards ensuring that this can be utilized, publishing a directive in 2013 that allows telecommunication suppliers to provide mobile money solutions as well.[16] One example is Wave Money, a mobile-money operating company raised as a cooperation by the Telenor group and Yoma bank which has started operating in the country.[17] The potential benefits of supplying previously unbanked regions with access to banking is potentially be large, as the existence of safe opportunities for saving and applying for credit could lead to more widespread economic development.

In cooperation with the Asian Development Bank Myanmar has looked at the possibility of utilizing e-governance as a method of overcoming issues stemming from the country's diverse geography, lagging development and diversity. E-government has the potential of enhancing efficiency and transparency, if properly managed and based on a solid foundation, which could have great benefits for any country.[18][19]

[13] Calderaro

[14] http://www.ictworks.org/2015/09/30/wow-myanmar-is-going-straight-to-smartphones/

[15] SWIA

[16] Ibid

[17] https://www.wavemoney.com.mm/about-us/)

[18] https://www.adb.org/sites/default/files/project-document/161546/47158-001-tacr-01.pdf

[19] http://www.moi.gov.mm/moi:eng/?q=news/8/10/2016/id-8661

Digital threats in developing countries

While connecting developing countries is potentially hugely beneficial, and able to unlock large potential for growth, there are a long list of perils involved in digitalization. Some of these are common for all countries, yet other are more unique for developing countries. The positive effects of digitalization are therefore dependent on an environment that enables these positive effects to manifest themselves. This is dependent on several factors, not only building digital infrastructure, but making sure that this infrastructure has a sufficient capacity, ownership issues, such as monopolies or oligopolies and the expansion of networks away from the urban areas where they tend to cluster.[20] Some of the main challenges has been identified, however, and measures to mitigate these are taking form. The aforementioned GeSi-report outlines three main areas of concern for developing countries: lack of political knowledge and appropriate regulation, lack of funding and financial incentives to invest in these technologies and lack of knowledge in the wider population, both in terms of user-skills and expertise.[21]

For developing countries, the issue of cyber security is made more prominent by the fact that the very services that contribute to increased efficiency and economic gains are also the ones that are most vulnerable to attacks and penetrations. Three main areas have been identified that both hold great potential economic gains but also severe security risk:[22]

1: Backend systems that concentrate information for companies and government (e-government). This has been shown

[20] Klimburg, Zylberberg

[21] (http://systemtransformation-sdg.gesi.org/160608_GeSI_SystemTransformation.pdf

[22] Klimburg, Zylberberg

to produce great efficiency gains, but also to concentrate information which again makes it a more valuable target.[23]

2: The potential of leapfrogging and cloud-computing leading to even greater concentration of information, but also new and changing security challenges. [24]

3: Mobile money and e-commerce, which lets underbanked or unbanked areas access money and credit, but which also adds great potential monetary benefits for cybercriminals.[25] This has normally been a more pressing issue in the developed world, but recent cases such as the robbery of the Bangladesh National Bank is a reminder that as capacity develops the issue will move towards less developed regions as well.[26]

The potential harm for unsuccessful digitalization goes beyond mere untapped potential, the lack of stable reliable access can in fact increase the divide between the developing and the developed world. Tabira and Otieno (2017) shows how the development goal of "quality education for all" can be hampered by reliance on ICT for teaching and access. They found that due to uneven connection and power shortages education in Kenya in fact suffered by implementing ICT-based teachings, as contrasted to traditional teaching. An ill-managed switch meant teachers was unable to cope with the environment, and students as a result lost interest. This points to ICT potentially widening the divide between developed and developing, at least in terms of education, as the former has instant access to a wealth of information while the latter gets left behind by insufficient infrastructure.[27] Put in a larger context this might raise some concerning issue on the over reliance on ICT to reach development goals. Some of the issues hampering development, such as bad infrastructure and the need for regulation reform will not go away because of digitalization, in fact they might get worse. This underlines the importance of a wider set of issues, such as cyber security, as an integrated part of

[23] Ibid

[24] Ibid

[25] Ibid

[26] https://www.nytimes.com/2016/05/27/business/dealbook/north-korea-linked-to-digital-thefts-from-global-banks.html?_r=0

[27] http://link.springer.com/article/10.1007%2Fs11625-017-0422-8

a development agenda, as the creation of secure networks is crucial to harvest the potential benefits.

At the same time, recent developments have highlighted the vulnerabilities of developing countries, particularly the spread of the "WannaCry" ransomware in May 2017. The ransomware propagated by utilizing an exposed vulnerability in the Microsoft operating system that had been patched months prior. However, the updates and patches that protected against the malware was phased out for older versions, or not provided altogether for pirated versions. The result was a much larger spread of the ransomware in states like China and Russia, which relied heavily on particularly pirated operating systems.[28] Generally older versions of operating systems are more common in countries that have less of the required capital needed to upgrade them. As an example Windows 7, the operating system that was most vulnerable to the WannaCry attack, enjoys a 55% market share in Africa - being by far the most popular operating system - while it has a market share of around 40% in Europe and trending downwards, also recently being overtaken by windows 10 as the most widely used operating system.[29] This points towards a scenario wherein developing countries get stuck with ageing and increasingly outdated software, which could pose a huge security risk. Without strong institutions and organizations related to cyber security that could step up in the event of a crisis the consequences could potentially be enormous.[30] It is therefore imperative that any move towards digitalization is accompanied by a strong and persistent focus on cyber security to prevent the gains from connecting to the global Internet economy to be outweighed by the security risks.

While the most pressing issue is the emergence of risks within the developing countries, the emergence of ICT in a broader range of countries also raise issues relating to the international

[28] https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs

[29] http://gs.statcounter.com/os-version-market-share/windows/desktop/europe/#monthly-201605-201705

[30] https://www.unodc.org/unodc/en/frontpage/2017/May/in-wake-of-wannacry-attacks--un-cybersecurity-expert-discusses-internet-safety.html

governance-structure. The current management of the Internet is being done by groups of private sector, civil society and government in a model described as Multi-Stakeholder Model (MSM). This model has come under increasing pressure from a coalition of authoritarian and developing countries, led by China and Russia, stressing the importance of state stability over all other concerns. This movement, described as Cyber Sovereignty has resulted in a polarized debate between the two camps.[31] For developing countries an important issue is their limited ability to participate in the existing debates, mainly caused by logistical and financial problems: as the meetings are taken place all over the globe, and include difficult technical questions that necessitate the participation of devoted specialists.[32]

This is linked to the related question of whether the Internet is used to promote freedom of expression and other freedoms, or as a vehicle for repression. This question also stresses the need of adding civil society into the governance of the Internet.[33] These are issues that have been promoted in the EU cyber strategy as well, and are linked to the idea of the Internet as an enabler of liberal democracies.[34] A global trend is for cyber-attacks to not only target industry and governments, but also Civil Society Organizations, who often do not have the resources to defend themselves against these attacks, presenting a large threat against organizations working for human rights and keeping the government responsible. Furthermore, these attacks are often characterized by low degree of technical sophistication, and more advanced social engineering aspects using so-called spear-phishing techniques to obtain information.[35] However, the tools and skills required to protect from these types of surveillance are widely available for those with the knowledge to find them. Organizations such as the Tactical Technology Collective even offer these packages in Burmese.[36] Raising awareness in developing societies about both the risks of internet connectivity, and the many cheap

[31] Klimburg, Zylberberg

[32] Ibid

[33] Ibid

[34] JOIN, 2013

[35] Citizen Lab, https://targetedthreats.net/

[36] SWIA

and free tools that mitigate these risks are an important step in building a solid civil society.

The troubling cyber landscape in Myanmar

As mentioned Myanmar has over the last years seen one of the most rapid and comprehensive extensions in digital coverage ever.[37] It should therefore come as no surprise that the country still has unresolved issues relating to the securing and managing of this transition. A further complicating element is that Myanmar is undergoing this rapid transformation at the same time as the country is undergoing a profound political transition as well. Adding internet connectivity as the same time as the country transitions from being run by its military junta to a more democratic form of governance is heightening the risk that the technology will be used to exert government control and surveillance.[38]

Key actors

As the government is limited in both its capacity and its resources, calls have been made for large international companies to help implement security in the country. As smaller businesses do not have the knowledge or ability to establish sufficiently secure practices this is an area where large Multinational ICT-companies could (and should) help develop capabilities.[39]

A key role is thus likely to be played by commercial actors, in particular the differing telecoms operators that will be included in the process. After a 2012 licensing-round the licenses were awarded to Qatari telecoms-operator Ooredoo and Norwegian operator

[37] Calderaro

[38] Calderaro

[39] SWIA

Telenor.[40] 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.[41]

Whether the companies do so are up for debate. The most concerning of the companies is Ooredoo, which has no clear published guideline/ 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. For Ooredoo another key issue is the fact that the company is Muslim, in a country with increasing ethno-religious tensions between Muslims and Buddhists. So far this has only resulted in smaller incidents, but as tension increases it is an area that is worth watching.[42] 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 also some uncertainties over the extent to which Telenor is willing to pass information over to the government and whether these policies are clearly enough formulated to withstand potential pressures.[43]

[40] Calderaro

[41] https://www.hrw.org/report/2013/05/19/reforming-telecommunications-burma/human-rights-and-responsible-investment-mobile

[42] Calderaro

[43] Ibid

Cybercrime

In the Asia-Pacific region there exists a large and partly sophisticated cybercriminal element, while the national approaches to cybercrime are uneven. In several countries cybercriminal regulation is being used either as a mean to achieve political suppression of dissident voices, or as a mean to prevent unwanted content such as pornography and gambling.[44] As a result, the prosecution and investigation of cyber criminals looking for financial profit is scarce. An important development in cybercrime is the fluid nature of the operations, which tends to move towards the points of least resistance. Countries that have few laws covering cybercrime, or insufficient enforcement of these laws, are being used as staging arenas for attacks on other nations in the region. Cybercrime is therefore emerging as a distinctly transnational issue that needs to be addressed through cooperation and coordination. Myanmar is one of the countries that have been identified as such a country, and there are efforts by countries with more developed capabilities, such as the US, Japan, South Korea and Australia, to develop the cybercrime prevention capabilities in Myanmar.[45]

The global nature of the Internet means that criminals often operate outside of the country they target, and this is being used by foreign actors to set up branches of illegal activity in other countries. This is a novel, if distinct, feature of Asian cyber-politics as both China and North Korea have been accused of staging operations from within other countries. A 2014 Chinese hacking organization was exposed and arrested in Kenya in 2014, apparently having set up an advanced cybercrime operation with up to 80 members in what was described as "military style dormitories".[46] A more recent example is the exposure of North Korean operations from within China, the very same organization that is alleged to be behind the robbery of the Bangladesh Central Bank.[47] This creates issues both in terms of cybercrime prevention

[44] ASPI, 2016

[45] Ibid

[46] http://www.bbc.com/news/world-africa-30327412

[47] http://www.businessinsider.com/r-exclusive-north-koreas-unit-180-the-cyber-warfare-cell-that-worries-the-west-2017-5?r=US&IR=T&IR=T

and international politics, as states stage attacks on each other interests from within third-party states. States with underdeveloped regulation and cyber-capabilities is likely to be attractive spots as such third-party staging grounds.

More concerning for domestic stability in Myanmar is the connection between these cybercriminal elements and various political forces operating in the country. The lack of government provided security, as well as law and order, has resulted in an environment that spurs the growth of criminal gangs, and connects them to the political elite. This creates a hostile environment for legitimate businesses to compete in, hampering growth and development.[48] The government has criminalized hacking, but the law, dating back to 2004, is ill-suited to more recent challenges. At the same time, a new cybercrime law has been in development for some time, yet it is not implemented as of this date.[49]

As Myanmar struggles with an unstable political situation, and therefore limitations with its application of the rule of law, the country is seeing the emergence of a broad range of criminal issues, among them 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. One of the two issues that is singled out in a 2016 report as particularly troubling is cybercrime, along with financial crime.[50] Cybercrime is an existing, and growing, concern in Myanmar. As the growth in cybercrime rapidly outpaces the growth in digital transactions globally 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 with lacking legal frameworks and enforcements like Myanmar is likely to see a disproportional part of this growth. [51]

[48] BMI research 2016

[49] SWIA

[50] BMI research 2016

[51] https://www.threatmetrix.com/wp-content/uploads/2017/04/cybercrime-2016-q1-1492588964.pdf?_ga=2.203348887.767081945.1493862414-973637201.1493760913

Social issues

Myanmar is still struggling to cope with various ethnic conflicts, with separatist insurgencies raging in the country's border regions to the north and the east. While the intensity of the conflicts has been falling over the recent years, there are still minor clashes occurring from time to time.[52] 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.[53] 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.[54] Since then hate speech has continued to spread and is becoming an increasingly pressing problem. A field study made by the SWIA revealed that most of the hate speech was directed towards the Muslim majority, with a significant part of the hate speech including calls for violence and even killing of Muslims.[55] The discrimination is not limited to Muslim minorities, but it remains the most glaring example of persecution in the country.[56]

The socio-political nexus

The cultural and ethnic tensions in cyberspace feeds into existing political fissures. Myanmar has at multiple points in its history seen control over information and access being used politically by actors. Back in 2010 Myanmar was on the receiving end of what was at the time one of the largest Distributed Denial

[52] BMI research 2016

[53] SWIA

[54] Calderaro

[55] SWIA

[56] Ibid

of Service-attacks (DDoS) ever recorded. 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.[57] 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. The connection at the time was so limited that the attack was several hundred times larger than needed to shut down the connection.[58] At the time, political or geopolitical DDoS was a very rare occurrence, and this fact remains true today. There are only a handful of DDoS-attacks that has been knowingly attributed to political actors, with the attacks on Estonia in 2010 and Georgia in 2008 the most famous examples.[59] While the source of the attacks has not been made public to this date, strong suspicion has been directed towards the Burmese military junta that governed the country, particularly as dissident websites hosted outside of Myanmar had been targeted earlier in the year.[60] There were also similar accusations raised at the Burmese military and government following restrictions of access and information in 2007. [61]

Since the democratization these large operations stopping the flow of information altogether has stopped. As the country has connected to the internet they have been allowed access to a wealth of information they did not previously have access to, resulting in a renaissance of sorts for independent media outlets and civil society groups. Despite this apparent positive development there are huge concerns relating to the security of these websites. There are also questions regarding whether stopping dissent has merely taken on another form. The most concerning developments have been the rise of vigilante groups pushing a nationalistic and authoritarian agenda by attacking websites and news outlets that are critical of the government, or in

[57] Arbor Networks

[58] Ibid

[59] Ibid

[60] https://rsf.org/en/news/stop-cyber-attacks-against-independent-burmese-media

[61] https://thelede.blogs.nytimes.com/2007/09/28/burmese-government-clamps-down-on-internet/

some way positive to the country's Muslim minority.[62] The most active of these group has been identified as the "Blink Hacker Group", and has targeted numerous media websites over the last few years. This group has been linked to the Myanmar military by an independent investigation undertaken by research-firm Unleashed. 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, which is evident in its pushing of a ultra-nationalistic agenda.[63] Coupled with the rise of Islamophobia and the use of social media as an instigator of violence between differing ethnic groups, and mainly aimed towards the ethnic Rohingya-minority, there are clear warning signs that cyber security will be crucial towards ensuring free speech and avoiding spiraling ethnic conflicts in the years to come.

If the regulatory framework remains unconvincing some of this responsibility may again fall into the hands of companies running the infrastructure. Using hacking and digital technologies for political gains is not new however, and prevention is tricky. Some ICT-companies have tried to solve the problem, and many more might be forced to. The most widely cited example is the Safaricom-case where the service provider took steps after the 2007 Kenyan election. The election, which was disputed and coloured by a distinct ethnic element, resulted in an eruption of violence leaving over a 1000 dead. Later investigations unearthed that blogs and SMS had played a prominent role in the planning and inciting of violence, and in the runup to the 2013 election there were fears that a similar situation might develop. In the end Safaricom ended up issuing tough guidelines for bulk messaging in order to avoid for its services to be used as a means of organizing violence. While it remains unclear to what extent the effort helped, as most organizing went to other channels such as social media, it shows how companies might take responsibilities for the political messaging taking place on their platforms. [64] [65]

[62] http://foreignpolicy.com/2016/04/01/the-perils-of-burmas-internet-craze/

[63] http://unleashed.blinkhackergroup.org/

[64] http://www.capitalfm.co.ke/news/2012/06/safaricom-issues-tough-rules-on-political-messanging/

International outlook

The trend in the region is like that in the broader world, as data is being used increasingly as a tool for states to promote their interests. What used to be operations for intelligence purposes are now being used more in line with political goals and as means to political ends. While there have not been any cases comparable to the hack of the Democratic National Committee in the US elections, operations against Vietnam that coincided with rulings unfavorable to China on South China Sea issues shows that data is being politicized in Asia as well. This raises important question on how to approach cyber security, particularly as e-government, e-commerce and IoT is likely to be ever more widespread and important.[66]

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 are like those of the Chinese government, the group has not as of yet been definitely linked to any actor.[67] The report also includes mention of attacks on an unnamed "regional customer" undergoing "significant political transition" and postulates that the attack was an attempt to gain knowledge into the degree of instability in the country. This could refer to other countries than Myanmar, but Myanmar is also more specifically referenced as one of the countries where it is likely that APT 30 is operating. [68]

Another intrusion was detected in late 2015, as Arbor Networks investigated what later came to be known as the "Trochilus"-campaign. The tools used, and the scale of the campaign, indicated a sophisticated state-sponsored actor, with Arbor again

[65] https://www.ihrb.org/focus-areas/information-communication-technology/report-digital-dangers-corporate-responses-hate-speech

[66] ASPI 2016

[67] APT 30, FireEye

[68] https://www2.fireeye.com/rs/fireeye/images/rpt-apt30.pdf

suggesting that it was a hacker group known as "Group 27" which also has been tied to China by several experts.[69]

While both reports are hesitant at attributing China directly, the political context and historic relations between the two countries is a strong indicator. When Myanmar was a pariah-state globally its relationship with its giant northern neighbor resembled that of a client state. China has been accused over the years of profiting from illegal trade in timber, gold, and Jade. However, the recent democratization has changed the relationship between the two countries, with Myanmar backpedaling on former agreements. The clearest example is the efforts in Kachin State, where China has had to take on a more active peace-promoting role and claims it is trying to live to its role as a "responsible world power". Some has questioned the sincerity of these efforts, however, claiming that the main goal for China is to remain the dominant foreign influence in the country, and at all cost keep the west away. The northern parts of Myanmar could also potentially become crucial for Chinese regional efforts, such as the "One Belt, One Road"-project. As long as Chinese interests are prevalent in Myanmar, its presence is likely to be felt, and this would by all likelihood translate into the digital domain as well.[70] These examples indicate that a healthy and secure internet might become a prime precondition for Myanmar to enjoy functioning sovereignty, particularly as the fragile political and social situation in the country gives opportunities for exploitation and pressure.

[69] (https://www.scmagazineuk.com/trochilus-rat-targets-government-of-myanmar/article/531356/

[70] http://foreignpolicy.com/2017/04/18/china-is-playing-peacemaker-in-myanmar-but-with-an-ulterior-motive-myitsone-dam-energy/

Cyber vulnerabilities in Myanmar

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. This issue was raised in Australian Strategic Policy Institute report (2016) on cyber security preparedness in the region, namely the problems arising from a lack of understanding of one's own assets and needs. Countries have different structures underpinning the Internet, and different issues needed to be addressed to handle it. An example raised in said report is the difference between a country like China, where almost all services are state-owned, and Australia, where 90% of the infrastructure is in private hands. That these two countries are facing drastically different governmental challenges is clear, and no method can be said to cover both cases. Realizing what one has is the first step towards securing it.[71] For Myanmar, as we shall see, the situation of depending on a limited set of state and private actors in driving the entire telecommunication sector should therefore frame the debate on policy. The first issue is the infrastructure providing internet access for the population.

Infrastructure

For Myanmar, the state of the infrastructure carrying the internet poses some distinct challenges and questions. Utilizing the World Bank's division of infrastructure into three miles one can assess to what degree Myanmar is developing its capabilities. The first mile is where the internet enters the country, the middle is the distribution within the country and the final mile is the part where the coverage reaches the end users. Traditionally the issue for developing states has been the middle mile, as the focus is on

[71] ASPI 2016

entrance points to countries and access in urban areas, while less effort is put into the distribution within countries.[72]

The infrastructure in Myanmar is disproportionately based on mobile broadband access and not fixed broadband.[73] The World Bank has highlighted this as an issue in several developing countries, as wireless alternatives are not a full substitute for fixed-line networks, often being more expensive and slower. This creates a subdivision of the Internet coverage into different leagues, with developing countries stuck with a lower quality coverage.[74] Slower speeds again raise the vulnerability to attacks like DDOS-ing, which Myanmar, as mentioned above, has been the victim of in the past.

Myanmar is a typical case of early-stage internet development, while there has been an immense growth in internet coverage nationally, through the building of mobile towers and mobile internet, the underlying structure and backbone of the Internet remains weak. This is important as most of the 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 residents want to access. Up until very recently Myanmar was served by a single submarine cable, creating both large vulnerabilities in the infrastructure and slow connection.[75]

With regards to the infrastructure servicing Myanmar from abroad the government is in control of the sole Internet Exchange Point (IX) in the country (in fact a faux-IX, but functioning as one nonetheless). This meant that all data traffic moving in and out of the country was in the government's hands, inserting huge risks for privacy and data infiltration.[76] The country was also served by a single submarine cable, which is a glaring vulnerability in any country's cyber security setup as evident in the 2010 DDoS-attack and an accidental severing of the cable in 2007, both instances that

[72] WDR, 2016: 219

[73] ASPI 2016

[74] WDR 2016: 208

[75] ASPI, 2016

[76] Calderaro

left the country without Internet coverage for some time.[77] However recent developments have seen two new connections to the submarine cable network - through the SEA-ME-WE-5 consortium and the Asia Africa Europe (AAE1) connection - in late 2016 and early 2017, mitigating this vulnerability. These new connections will still be under government control however, meaning that the foundation for a secure and open Internet infrastructure is limited at best.[78]

Regulation and politics

In general Myanmar's cyber security "Maturity" is among the worst in the Asia-Pacific region. 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 ASPI-report, highlighting a long list of issues that needs to be addressed.[79] A shortage in skilled labor is one of the main issues, as the ICT 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.[80] 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

[77] SWIA

[78] Calderaro

[79] ASPI, 2016

[80] SWIA

and regulations are aimed at control and censorship, and not on cybercrime and related issues.[81]

This is not particularly surprising, as the country recently was closed off from the rest of the world and with a legal framework aimed at different goals than today. In this context, the twin developments of democratization and digitization are asking a lot of the country, and they are likely to impact and shape the trajectory of each other. The result is often that even when the country follows recommendations from donors in shaping the process, key aspects may be omitted. An example can be taken from the development of the new telecommunications law in 2013, where the Myanmar Government circulated a draft in an open and inclusive process in the lines of the "best practice" approach of multistakeholder-approaches. As the report was written in English, however, it was clear that the intended audience was foreign companies and government, and not Burmese actors.[82] This example illustrates that the recent political history can shape and alter the processes that are supposedly "best", as the underlying logic is not internalized by the actors who are supposed to see the processes through. More disconcerting is the lack of transparency in educating and enabling the population to take part in the reform and understand its implications.[83] Seen in a wider context there is little tradition in Myanmar for inclusive, transparent policy formulation, which is seen as the best practice when formulating digital policies.[84]

As the challenges for the government in formulating a coherent policy from scratch are severe, several experts have pointed towards the international companies operating in Myanmar to take responsibility for the sector. One of the main concerns raised by the ASPI-report was the non-existent cooperation between private companies and the public regulators, which is the opposite of the recommended multi-stakeholder model of governance.[85] For the companies, themselves adopting international standards in the absence of domestic ones has been pointed to as a potential

[81] ASPI, 2016

[82] Calderaro

[83] Ibid

[84] SWIA

[85] ASPI

key factor in promoting sound governance long-term. For this to be done successfully holding companies like Telenor to their own standards abroad, even in challenging contexts, will therefore be of high importance.[86]

International cooperation

A subdivision of the political and regulatory capacity is a country's participation in international fora's and programs. This is an area of importance in cyberspace, where the government challenges are often global in nature. There are large differences in the extent to which countries engage in multilateral and bilateral cooperation in cyberspace. To a large extent a mature cyber policy in general extends to more engagement and cooperation on cyber issues. One of the main ways for countries with less developed cyber security maturity is to engage in cooperation between Computer Emergency Response Teams (CERT's). 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 CERT's.[87]

While Myanmar participates in APCERT, as well as some bilateral capacity building programs with India and Singapore, among other. The country has not so far engaged other countries beyond capacity-building programs.[88]

[86] SWIA

[87] ASPI, 2016

[88] ASPI, 2016

Concluding remarks

Sources

Klimburg, Zylberberg: NUPI report

GeSI-report: http://systemtransformation-sdg.gesi.org/160608_GeSI_SystemTransformation.pdf

FireEye-report, APT 30:https://www2.fireeye.com/WEB-2015RPTAPT30.html / https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

News article on APT 30: https://techcrunch.com/2015/04/12/fireeye-apt-30-southeast-asia-india-report/

News article APT 27 and Trochilus: https://www.scmagazineuk.com/trochilus-rat-targets-government-of-myanmar/article/531356/

On cybercampaign against Myanmar NGO's: https://www.theregister.co.uk/2016/01/12/seven_pointed_dagger_cyberspies/

On Mynamars Militaries offensive capabilities: http://www.atimes.com/atimes/Southeast_Asia/JJ01Ae01.html

On Bangladeshi bank heist and North korea: https://www.nytimes.com/2016/05/27/business/dealbook/north-korea-linked-to-digital-thefts-from-global-banks.html?_r=0

North Korea staging attacks from other countries: http://www.businessinsider.com/r-exclusive-north-koreas-unit-180-the-cyber-warfare-cell-that-worries-the-west-2017-5?r=US&IR=T&IR=T

On Chinese crime network in Kenya: http://www.bbc.com/news/world-africa-30327412

Dalberg report on digitalization in developing countries: http://www.impactoftheinternet.com/

Myanmar Cert - homepage: http://www.mmcert.org.mm/

Myanmar master plan - draft: http://www.mcit.gov.mm/sites/default/files/Draft%20Masterplan%20(summary)English.pdf

Paper on regional cyberissues for ASEAN-countries: https://jsis.washington.edu/news/asean-cybersecurity-profile-finding-path-resilient-regime/

On the 2010 DDos-attack: https://www.infosecurity-magazine.com/news/massive-ddos-attack-knocks-burma-offline/

Human Rights paper on cyber issues in Myanmar: https://www.hrw.org/report/2013/05/19/reforming-telecommunications-burma/human-rights-and-responsible-investment-mobile

Risk analysis by BMI Myanmar: http://store.bmiresearch.com/myanmar-crime-and-security-risk-report.html

ASPI cyber-maturity report: https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2015/Cyber-Maturity-2015.pdf

Sector Wide Impact Analysis Myanmar

Paper on corporate handling of hate-speech: https://www.ihrb.org/focus-areas/information-communication-technology/report-digital-dangers-corporate-responses-hate-speech

Safaricom-ruling in Kenya: http://www.capitalfm.co.ke/news/2012/06/safaricom-issues-tough-rules-on-political-messanging/

Blink Hacker group-report: http://unleashed.blinkhackergroup.org/

More on hacking and social issues: http://foreignpolicy.com/2016/04/01/the-perils-of-burmas-internet-craze/

On hate-crime and ethnic tensions in Myanmar: https://www.crisisgroup.org/search?text=myanmar

More on hate-crime in Myanmar: https://www.crisisgroup.org/asia/south-east-asia/myanmar/myanmar-assassination-shows-urgency-burmese-unity-against-hate-crimes

Myanmar as a hub for spam-campaigns: http://www.esecurityplanet.com/news/article.php/3937751/Myanmar-is-No1-Spammer-Now.htm

http://www.nbcnews.com/id/43929328/ns/technology_and_science-security/t/myanmar-worlds-no-online-attack-traffic/#.WUpRHcY8yUl

On the potential for ecommerce in Myanmar: https://www.techinasia.com/talk/grabbing-ecommerce-horns-golden-land-myanmar

On the digital revolution in Myanmar: https://www.techinasia.com/myanmar-internet-revolution-startups

On Milennium development goals and ICT: http://www.springer.com/gp/book/9781489974389

Cyber Security Education in developing countries (South african case): https://link.springer.com/chapter/10.1007/978-3-642-41178-6_30

Paper on SDG and ICT: https://link.springer.com/chapter/10.1007/978-3-319-44447-5_1

Myanmars tech-revolution: http://www.ictworks.org/2015/09/30/wow-myanmar-is-going-straight-to-smartphones/

On how ICT troubles undermine potential gains, Kenyan case: https://link.springer.com/article/10.1007%2Fs11625-017-0422-8

Paper on ICT's role in development: https://newsroom.accenture.com/news/digital-solutions-can-drive-progress-toward-united-nations-sustainable-development-goals-by-2030-finds-report-from-global-e-sustainability-initiative-produced-with-accenture-strategy.htm

Litterature review of paper on ICT and development: https://link.springer.com/article/10.1007/s11625-017-0426-4

UN memo on SDG mentioning ICT: http://www.un.org/ga/search/view_doc.asp?symbol=E/2016/75&Lang=E

Articles by James Coe, british journalist in Myanmar:
Digital surveillance: http://frontiermyanmar.net/en/features/question-trust-myanmars-shadowy-world-digital-surveillance
Judicial problems, also cyber: http://frontiermyanmar.net/en/broken-justice
On e-banking in Myanmar: http://frontiermyanmar.net/en/business/leapfrogging-the-future

ITU-paper on cybercrime: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf

Guide to Myanmar for companies (some relevant issues): https://www.scribd.com/doc/247079657/Starting-Up-in-Myanmar-A-First-Guide-by-Harald-Friedl-Ruben-D-Hauwers

Myanmar Times on domestic cybercrime: http://www.mmtimes.com/index.php/national-news/4168-email-hacking-exposes-cybercrime-in-myanmar.html

On Myanmar and hacking of foreign governments: http://thediplomat.com/2016/02/was-myanmars-military-behind-shadowy-cyber-attacks/

More on Thai-hacks: http://www.mmbiztoday.com/articles/new-wave-burmese-hackers-behind-thai-website-attacks

Slightly outdated paper on development and ICT (In Mozambique): http://hdr.undp.org/sites/default/files/mozambique_nhdr_2008_ict.pdf

On 2010 campaign against dissidents: https://rsf.org/en/news/stop-cyber-attacks-against-independent-burmese-media

Info on submarine cables and international connections:
http://www.submarinecablemap.com/#/
http://www.aaeone.com/
http://www.smw3.com/
http://www.seamewe5.com/ (expired)

Articles on expanded connectivity:
http://www.mmtimes.com/index.php/business/technology/10205-burma-inks-deal-for-new-subsea-internet-cable.html
http://www.aseanbriefing.com/news/2015/09/23/new-internet-cable-myanmar.html