NUPI Norwegian Institute of International Affairs

Policy Brief
[5 / 2018]

Cyber Security Capacity Building in Myanmar

Lars Gjesvik and Niels Nagelhus Schia

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.

Introduction
Digitalization is creating both opportunities and threats globally, that have the potential to both foster and hinder the development of states. 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. 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.

To harness the benefits of digitalization and mitigate the threats, assisting developing countries in building their ability to respond to and prevent harmful online activity will grow in importance in the coming years. This idea of Cyber Security Capacity Building (CCB) has been proposed as a framework for assessing and nurturing these abilities.

In this paper, we will use the framework proposed by Klimburg and Zylberberg (2016), taking a broad approach to cyber security that considers the wider economical and societal impacts of digitization.[1]

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]

Benefits of digitalizing: in developing countries and in Myanmar
While there is no consensus regarding how large the potential benefits of digitalizing are for developing nations, some metrics have been developed to identify a connection between growth in Internet connection and growth in GDP. 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] The speed with which ICT is spreading compared with traditional infrastructure is a bonus to the potential benefits.[4]

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, such as the UN sustainable development goals6.[5] A 2016 report from the Global E-Sustainability Initiative (GeSi) 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.[6]

Myanmar's peculiar political history makes it a key case one the importance of cyber security for development. On the one hand, it has recently emerged from decades of oppressive rules at the hand of the military junta, trying at the same time to develop its economy and democratize its political system. At the same time, a country that was isolated from the rest of the world is connecting to the In9ternet at an unprecedented pace. 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%.[7] 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.[8]

For Myanmar, a key area where underdevelopment is sought remedied through ICT is the area of e-commerce and online banking, with banking penetration in Myanmar as low as 10% in urban areas and even lower in rural areas.[9] 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.[10] 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.[11] Myanmar has also, in cooperation with the Asian Development Bank, started mapping the opportunities presented by e-governance for assisting in managing the large and diverse country.[12]

Threats stemming from digitalizing: in developing countries and Myanmar

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. The positive effects of digitalization are dependent on an environment that enables these positive effects to manifest themselves. This in turn rests on several factors, such as building digital infrastructure, making sure that this infrastructure has a sufficient capacity, regulation gaps, and ownership issues, such as monopolies or oligopolies.[13]

- 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 rBackend systems that concentrate information for companies and government. This has been shown to produce great efficiency gains, but also to concentrate information which again makes it a more valuable target.

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

- 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.[14]

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

Recent developments have highlighted the vulnerabilities of developing countries. A notable case is the spread of the "WannaCry" ransomware in May 2017, that spread by using a known vulnerability in the Windows operating system. However, the updates and patches that protected against the malware was phased out for older versions.[15] Generally older versions of operating systems are more common in countries that have less of the required capital needed to upgrade them, which poses an additional risk for developing countries.[16] As developing countries often lack the manpower and the funding to participate in debates on Internet governance their concerns and voices risks not being heard19, and as a consequence not managed properly.[17]

A global trend is for cyber-campaigns 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. 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.[18] However, the tools and skills required to protect from these types of surveillance are widely available for those with the knowledge to find them. Raising awareness in developing societies about both the risks of internet connectivity, and the many cheap and free tools that mitigate these risks are an important step in building a solid civil society. Organizations such as the Tactical Technology Collective even offer these packages in Burmese (SWIA).

As widespread Internet connection is a new phenomenon in Myanmar, there are plenty of 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.[19] We have identified the following key issues in the Cyber Security setup for Myanmar:

Reliance on key commercial actors:

As the Myanmar 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. A key role is thus likely to be played by commercial actors, in particular the two large telecoms-operators in the country: Ooredoo and Telenor.[20] A 2013 Human Rights Watch report stressed the risk that digital 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.[21] While Ooredoo has been criticized for complying with harsh censorship regimes in other parts of the world, Telenor is seen as having one of the more advanced social responsibility policies in the world. Both do, however, have a history of shutting down its services when faced with governmental pressures.[22]

Cybercrime

An important characteristic of 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. Myanmar is one of the countries that have been identified as such a country in the South-Eastern Asian region.[23] 29More 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.[24] 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.[25]

Social issues

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.25 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. A field study made by the SWIA revealed that most of 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.[26]

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. In the run-up to 2010 elections Myanmar was on the receiving end of what was at the time one of the largest Distributed Denial Of Service-attacks (DDoS) ever recorded.[27] 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.[28] While blocking and denying access to websites have stopped, there are concerns over 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 some way positive to the country's Muslim minority.[29]

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. Operations against Vietnam that coincided with rulings unfavorable to China on South China Sea issues shows that data is being politicized in the region. 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.[30] A similar pattern vas evident in the 2015 Arbor Networks investigation into the "Trochilus"-campaign.[31] 42While both reports are hesitant at attributing China directly, other experts have hinted toward China being the likely culprit. As long as Myanmar was a pariah-state globally its relationship with its giant northern neighbor resembled that of a client state. However, the recent democratization has changed the relationship between the two countries, with Myanmar backpedaling on former agreements.[32]

The state of Cyber Security 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. The infrastructure in Myanmar is disproportionately based on mobile broadband access and not fixed broadband. 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.[34] Slower speeds again raises the vulnerability to attacks like DDOS-ing. Sub-par connection speeds also undermine the ability to use newer technologies that could potentially help development, one prominent example being the Blockchain technology.[35]

Myanmar is 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 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.[36]

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.[37] 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.[38] 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.[39]

A subdivision of the political and regulatory capacity is a country's participation in international fora's 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 (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.[40] 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.[41]

Conclusion

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.

Endnotes

1) (Klimburg, Zylberberg, 2016).
2) Ibid
3) (ITU, 2012).
4) http://systemtransformation-sdg.gesi.org/160608_GeSI_SystemTransformation.pdf
5) Schia, Niels Nagelhus. 2017. "The Cyber Frontier and digital pitfalls in the Global South". Third World Quarterly.
6) (http://systemtransformation-sdg.gesi.org/160608_GeSI_SystemTransformation.pdf)
7) (Calderaro).
8) (http://www.ictworks.org/2015/09/30/wow-myanmar-is-going-straight-to-smartphones/)
9) (SWIA).
10) Ibid
11) (https://www.wavemoney.com.mm/about-us/).
12) https://www.adb.org/sites/default/files/project-document/161546/47158-001-tacr-01.pdf
13) (Klimburg, Zylberberg, 2016).
14) Ibid
15) (https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs).
16) (https://www.unodc.org/unodc/en/frontpage/2017/May/in-wake-of-wannacry-attacks--un-cybersecurity-expert-discusses-internet-safety.html).
17) (Klimburg, Zylberberg).
18) (Citizen Lab, https://targetedthreats.net/).
19) (Calderaro
20) (Calderaro).
21) (https://www.hrw.org/report/2013/05/19/reforming-telecommunications-burma/human-rights-and-responsible-investment-mobile).
22) (Calderaro).
23) (ASPI, 2016).
24) (BMI research, 2016).
25) (SWIA).
26) (SWIA).
27) SWIA
28) Arbor Networks
29) (https://rsf.org/en/news/stop-cyber-attacks-against-independent-burmese-media).
30) (http://foreignpolicy.com/2016/04/01/the-perils-of-burmas-internet-craze/)
31) (https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf)
32) (https://www.scmagazineuk.com/trochilus-rat-targets-government-of-myanmar/article/531356/)
33) (ASPI, 2016)
34) (WDR 2016: 208).
35) Kshetri – third world quarterly
36) (ASPI, 2016)
37) (ASPI, 2016).
38) (SWIA).
39) (ASPI).
40) (ASPI, 2016)
41) Ibid.

NUPI
Norwegian Institute
of International
Affairs

NUPI
Norwegian Institute of International Affairs
C.J. Hambros plass 2D
PO Box 8159 Dep. NO-0033 Oslo, Norway
www.nupi.no | post@nupi.no

Established in 1959, the Norwegian Institute of International Affairs [NUPI] is a leading independent research institute on international politics and areas of relevance to Norwegian foreign policy. Formally under the Ministry of Education and Research, NUPI nevertheless operates as an independent, non-political instance in all its professional activities. Research undertaken at NUPI ranges from short-term applied research to more long-term basic research.

About the Authors:

Lars Gjesvik is a research assistant in the Research group for Security and Defence, working mainly on cybersecurity.

Niels Nagelhus Schia is a senior research fellow at NUPI and head of NUPI's Cyber Security Centre