Nov 14th, 1:10 PM - 1:30 PM

Cybercrime in the Developing World

David A. Ghelerter
University of North Georgia, daghel6896@ung.edu

John E. Wilson
University of North Georgia, JEWILS3068@ung.edu

Noah L. Welch
University of North Georgia, NLWELC4209@ung.edu

John-David Rusk
University of North Georgia, jdrusk@ung.edu

Abstract

This paper attempts to discover the reasons behind the increase in cybercrime in developing nations over the past two decades. It discusses many examples and cases of projects to increase internet access in developing countries and how they enabled cybercrime. This paper examines how nations where many cybercrimes occurred, did not have the necessary resources or neglected to react appropriately. The other primary focus is how cybercrimes are not viewed the same as other crimes in many of these countries and how this perception allows cybercriminals to do as they please with no stigma from their neighbors. It concludes that laws and law enforcement, fund distribution, and ethics of these developing countries need to change to reduce the amount of cybercrime.

Disciplines

Business Law, Public Responsibility, and Ethics | Information Security | Management Information Systems | Technology and Innovation

Cybercrime in the Developing World

1st David A. Ghelerter
Department of Computer Science and Information Systems
University of North Georgia
Dahlonega, Georgia, USA
daghel6896@ung.edu

2nd John E. Wilson
Department of Computer Science and Information Systems
University of North Georgia
Dahlonega, Georgia, USA
jewils3068@ung.edu

3rd Noah L. Welch
Department of Computer Science and Information Systems
University of North Georgia
Dahlonega, Georgia, USA
nlwelc4209@ung.edu

4th John-David Rusk
Department of Computer Science and Information Systems
University of North Georgia
Dahlonega, Georgia, USA
ORCiD:0000-0002-8001-2436
jdrusk@ung.edu

***Abstract*—This paper attempts to discover the reasons behind the increase in cybercrime in developing nations over the past two decades. It discusses many examples and cases of projects to increase internet access in developing countries and how they enabled cybercrime. This paper examines how nations, where many cybercrimes occurred, did not have the necessary resources or neglected to react appropriately. The other primary focus is how cybercrimes are not viewed the same as other crimes in many of these countries and how this perception allows cybercriminals to do as they please with no stigma from their neighbors. It concludes that laws and law enforcement, fund distribution, and ethics of these developing countries need to change to reduce the amount of cybercrime.**

Keywords—cybercrime, developing nations, formatting, style, styling, insert

I. Introduction

The specter of cybercrime looms large over the developing world and is prefaced by socioeconomic and technical factors. Developing nations are advancing at a rapid rate, with the number of internet users growing steadily at four percent per year [1]. This growth rate is no accident. It is fueled by global aid and private companies seeking to grow profits. This increase in the "connected population" creates new targets for cybercriminals and new cybercriminals. Unfortunately, the developing world has not yet caught up to the developed world regarding security. The financial consequences of this technology lag have been crippling.

Developing nations need to address the problem of cybercrime in three ways: legally, technically, and morally. Laws need to adequately address the problem and be up to date with cybercriminal activities. On the front end, frameworks are needed for distributing aid funds and negotiating with foreign companies offering technological goods and services. Law enforcement must get up to speed technically on modern cybersecurity techniques. Finally, local culture needs to recognize cybercrime as real crime and appropriately incorporate it into their moral codes. Cybercrime is an enormous and growing problem in the developing world. If it is not addressed appropriately and quickly, it has the potential to inhibit future growth that has the potential to lift millions out of poverty.

II. More Internet Users Mean More Cyber Attacks

Increased access to the Internet has primarily been viewed as positive. The World Bank, included within its Social Development Goal, sought to develop affordable broadband in at least 35 land-locked, fragile, and small island nations. The statement was as follows:

> Strive to provide universal and affordable access to the Internet in the least developed countries by 2020. An affordable entry-level broadband subscription would cost less than five percent of average per-capita income [2].

Accomplishing this goal involved assistance in three key areas. The first was Sector Policy and regulatory reforms that encouraged both government and the private sector to create broadband access for low-income populations. Second, they allocated $1.2 billion for Loans and Grants to develop broadband access. Lastly, they became directly involved in partnerships to expand broadband access to provide technical and business expertise. Most of these funds went to nations in Africa.

The World Bank's motives were undoubtedly noble. They viewed the Internet as a powerful tool for delivering education and healthcare, economic improvement of marginalized people, and greater transparency in local government. However, this grand plan focused on the economic aspects of enhanced broadband access. World Bank paid insufficient attention to potential problems it could create, particularly regarding security.

As a result of the World Bank's actions and other economic drivers, developing countries have seen a rise in the proportion of the population with access to the Internet, and now even in the lowest-income nations, as much as half the population has access to the Internet. And, more specifically, broadband. The fact that US-based computers are always powered on and broadband-connected makes them so attractive as targets for cybercriminals. This is becoming increasingly true in the developed world. One tragic example was in Kenya, where in 2009, they laid the first broadband submarine cable, dramatically increasing both access to and speed of the Internet. In the following year, there were, on average, 50,000 bot attacks per day, up from 800 per day on the previous satellite-based network [3]. With this rise in connectivity, there has been a corresponding diffusion of the tools of cybercrime, which have been taken up by individuals and organized criminal societies.

Moreover, one of the World Bank's most cherished goals, Government Transparency and Accountability, has become increasingly negated because of Cybercriminal activities. In many parts of the developing world, governments are autocratic and capricious. The economic development that has taken place in the developing world over the last few decades has created a

new, aspirational middle class in many nations. This economic class has significantly more resources than generations past but lacks the funds to wield the influence over the society that an autocrat or oligarchy can. Naturally, this situation can lead to social friction between rulers and the ruled, often manifested as activism. Increasingly, autocratic governments are using the tools of cybercrime against their citizens.

In 2017 the Government of Azerbaijan launched a coordinated "Spear phishing" attack against human rights activists, journalists, and political dissenters. This attack used email messages and Facebook chats to access personal information and private communications. This allowed the Azeri government to identify and target even mild criticism. Many of these targets were imprisoned or intimidated [4].

In 2021, in Vietnam, an ally of the United States, a hacking group connected to the Vietnamese government called Ocean Lotus initiated a spyware attack against the country's human rights activists. As in the case of Azerbaijan, a phishing email campaign targeted activists, including several livings abroad. These attacks attempted to gain personal information, subsequently used to intimidate activists [5].

These are two examples of the government being the prime actor in Cyberattacks. Of course, the government is not the only perpetrator of cybercrime. Citizen cybercriminals have begun a booming trade targeting their people for financial gain. Hacking has been a known phenomenon since the 1990s, long before developing the World Bank's broadband development initiatives [6]. It is reasonable to say that they should have known this could happen and failed miserably in addressing it.

III. How the connected population grows

There are many challenges to increasing internet access in the developing world, including inadequate infrastructure for a local population, unforgiving geography, insufficient funds, and, of course, the rise of cybercrime. Nevertheless, the connected population is growing steadily. Primarily this is related to programs to aid the development that grew from World Bank initiatives. For example, the One Laptop Per Child (OLPC) program provided low-income children with low-cost, Linux-based laptops. The program began with Nicholas Negraponte at the Massachusetts Institute of Technology (MIT). He developed what was called the "$100 Laptop". It had all the features of a typical computer but required so little electricity that it could be powered with a hand-crank generator. It received rave reviews from the aid community, including UN Secretary-General Kofi Annan. It was reported that this device would change the world [7]. Once again, optimism trumped practical reality. Soon, people who possessed these laptops could connect them to the Internet. In theory, the Linux security system, BitFrost, is supposed to prevent the spread of viruses. However, there is always the opportunity for zero-day exploits, which have not yet been found.

Furthermore, in this case, much more sophisticated users could target people who have never used or perhaps even seen a computer. In one particularly notorious case, a user of a low-cost computer developed the "Love Bug" virus, which targeted other such computers [6]. Regrettably, for this reason and others, the OLPC program is now viewed mainly as a failure.

Admittedly, Intel did not have altruistic intentions, they were motivated by potential profit. The environment created by global aid money was creating a new market, and they wanted to exploit it. Intel also decided to jump into what it viewed as a massive market of low-income users [7]. It developed a low-cost computer called the Classmate with a scaled-down version of Windows. They claim to have distributed "tens of thousands" of these computers. The Classmate did make a nod to security and offered an antivirus package. However, this came with an additional cost, which most buyers could not afford, leaving users vulnerable to attack from the plethora of Windows-centered Cybercrime attack vectors.

Undoubtedly, these income-appropriate options provide children in developing nations with a valuable learning experience. Nevertheless, as with World Bank initiatives, there was little or no focus on security. It was either practically non-existent in the case of OLPC or too expensive in the case of the Intel Classmate.

IV. A problem with many facets

Cybercrime in the developing world is markedly different from the developed world in terms of targets, ingredients, and sources. The quality of cybercrime tools, such as hardware and infrastructure, is often inferior to those in the developed world [8]. However primitive the tools, they are becoming increasingly ubiquitous. The technological deficit with developing nations may make it more difficult for a developing world cybercriminal to attack modern infrastructure. However, it is undoubtedly sufficient to attack local targets lacking appropriate defenses. Also, the developing world lacks the institutions and legal framework to address cybercrime appropriately. The most prominent cybercrime actors in the developing world are organized criminal actors, who often influence the society they victimize [9]. So, many developing countries struggle to develop effective means of defense against cybercrime. For example, in Tanzania and Uganda, it took several years for cybercrime to reach parliamentary debate and be recognized as a criminal activity in bills.

Even when a developing country can create laws designed to target cyber criminals, they often lack the means to enforce these laws. Judges, lawyers, and law enforcement are rarely up to speed on the fundamentals needed to understand cybercrime. For example, out of 40,000 licensed attorneys in Malaysia, only four were familiar with cybercrime [1]. Even in cases where the criminal is brought to justice, the law codes often lack the specificity to make the charge stick. In India, an IT Act was passed in 2000 to address cybercrime, but it lacked provisions to deal with phishing, cyber-stalking, or online harassment [8]. The law was amended in 2008 but was again behind the times. This go round, provisions were lacking to handle wi-fi hacking, child pornography, and cyber-terrorism. The problem persists, and the lag time in legal mechanisms allows cybercrime to flourish. Indonesia, Brazil, and Romania also suffer similar problems, where hackers cannot be charged for distributing viruses or even illegally obtaining credit card information. Conviction rates hover around 2% [8]. Naturally, this leads to problems within these nations but also encourages local cybercriminals to engage in jurisdictional arbitrage, where they initiate attacks on foreign targets from weak jurisdictions.

For this reason, 92% of trojan horse programs originate in the developing world. A classic example is from the town of Ramnicu Valcea, Romania. In 2005, two local police officers dealt with over 200 reports of eBay fraud using a nine-year-old computer and no internet connection [8]. Not only was it practically impossible for them to adequately investigate cybercrimes, but even attempting to do so would inhibit them from any other activity.

The lack of appropriate laws or enforcement mechanisms has greatly emboldened cybercriminals. In Brazil, gangs of cybercriminals, when attempting to attack US-based computers, do not even use masking techniques to hide their identity [8]. They are perfectly aware that there are no consequences for their actions. Moreover, there is little to no social stigma attached to cybercrime in the developing world, as would be applied to a conventional thief or con artist. So, the moral framework is often as weak as the legal one. Countries like Iran, Algeria, and Bangladesh have the most relaxed cybersecurity laws. In Iran, 30.29% of mobile devices are infected with malware [10]. This is alarming because their Internet is not secure, making it easier for hackers online to steal their information. It is also because of the lack of cyber-education in these countries. The poverty rate in Iran is 14%, so most kids are not taught the proper things to look up on the Internet and do not have the same knowledge as we do [11]. Outdated software is also a big problem in these countries because many people do not have the funds to buy the latest Apple or Microsoft device. Newer versions of Microsoft Windows have built-in antivirus and cyberattack protection that alert to instances of tracking software or malware found on a computer. Lower-income communities run into the problem of using older versions of Windows lacking these features, making hackers' jobs a lot easier.

Another regrettable impact of cybercrime on the developing world is targeting remittances from overseas workers. In March 2018, Europol, the European Agency for Law Enforcement, arrested the suspected leader of a cybercrime syndicate targeting financial transfers and ATMs in over 40 countries. The reported losses from these attacks were over one billion dollars [8]. This type of cybercrime is particularly nefarious because most of the nations targeted do not have deposit insurance schemes like the FDIC in the United States, which guarantees deposits up to $250,000. So, once the money is stolen, it is gone, and the recipient gets nothing. In countries such as Guatemala, remittances make up half of the country's GDP. So, attacks like this are devastating to the local population and the local economy.

V. Conclusion

The problem of cybercrime in the developing world is not going away soon. This problem was foisted upon the developing world by insufficiently planned aid projects and profit-seeking by western companies. The enormous amount of money poured into expanding broadband and increasing access to computers has dramatically proliferated internet use. Global Digital Insight reports that the global population with access to the Internet grows by four percent annually. In real terms, this means that yearly, two hundred and eighty million people connect to the Internet. Most of these new users rely on public computers or lost-cost laptops. Regretfully, this exposes all these new users to a cyberattack, potentially devastating financial loss, or repression by the local government.

Protecting all of these people, their data, and their money will require an enormous change in how cybercrime is understood and prosecuted, how aid funds are distributed, and the available utilities in computers sold by foreign companies. Lawmakers and law enforcement must get up to speed on cybersecurity trends. The laws need to reflect what is current, and the enforcers need to be able to execute what is legislated. However, there also needs to be an incentive for cultural change in the developing world that connects existing moral codes to what happens online. Using a computer to steal millions or billions of dollars is no different from walking into a bank with a firearm. The unauthorized use of personal information by private or government actors is no different than more established and frowned upon forms of espionage. The average person needs to understand this and incorporate it into whatever belief system they hold. Furthermore, given the vast pool of money supporting increased internet access and the resulting immense growth in new internet users every year, this will have to happen fast.

References

[1] Goel, Shresth. "Cyber-crime in Developing Countries." Volume 1 (Issue 4), Journal For Law Students and Researchers, 22 Aug. 2020

[2] "Connecting for Inclusion: Broadband Access for All." The World Bank, www.worldbank.org/en/topic/digitaldevelopment/brief/connecting-for-inclusion-broadband-access-for-all.

[3] Ksherti, Nir. "Diffusion and Effects of Cybercrime in Developing Economies." Volume 31 (Issue 7), Third World Quarterly, November 2010

[4] "Azerbaijan: Activists targeted by 'government-sponsored' cyber attack." Amnesty International, 10 Mar. 2017, www.amnesty.org/en/latest/news/2017/03/azerbaijan-activists-targeted-by-government-sponsored-cyber-attack.

[5] "Vietnamese activists targeted by notorious hacking group." Amnesty International, 24 Feb. 2021, www.amnesty.org/en/latest/news/2021/02/viet-nam-hacking-group-targets-activist.

[6] Warren, Pete. "Crime fears as cheap PCs head for Africa." The Guardian, 6 Feb. 2008, www.theguardian.com/technology/2008/feb/07/olpc.security.

[7] Robertson, Adi. "OLPC's $100 Laptop was going to change the World – Then it all went wrong." The Verge, 16 Apr. 2018, www.theverge.com/2018/4/16/17233946/olpcs-100-laptop-education-where-is-it-now.

[8] Peters, Allison and Jordan, Amy. "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime." Third Way, 2 Oct. 2019, www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime.

[9] Swiatkowska, Joanna (2020). "Tackling cybercrime to unleash developing countries digital potential." (Report No. 33), Oxford University, pathwayscommission.bsg.ox.ac.uk/sites/default/files/2020-01/tackling_cybercrime_to_unleash_developing_countries_digital_potential.pdf.

[10] Bischoff, Paul. "Which countries have the worst (and best) cybersecurity?" Comparitech, 21, Sept. 2021, www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country.

[11] "Iran Poverty Rate 1986-2022." Macrotrends, https://www.macrotrends.net/countries/IRN/iran/poverty-rate