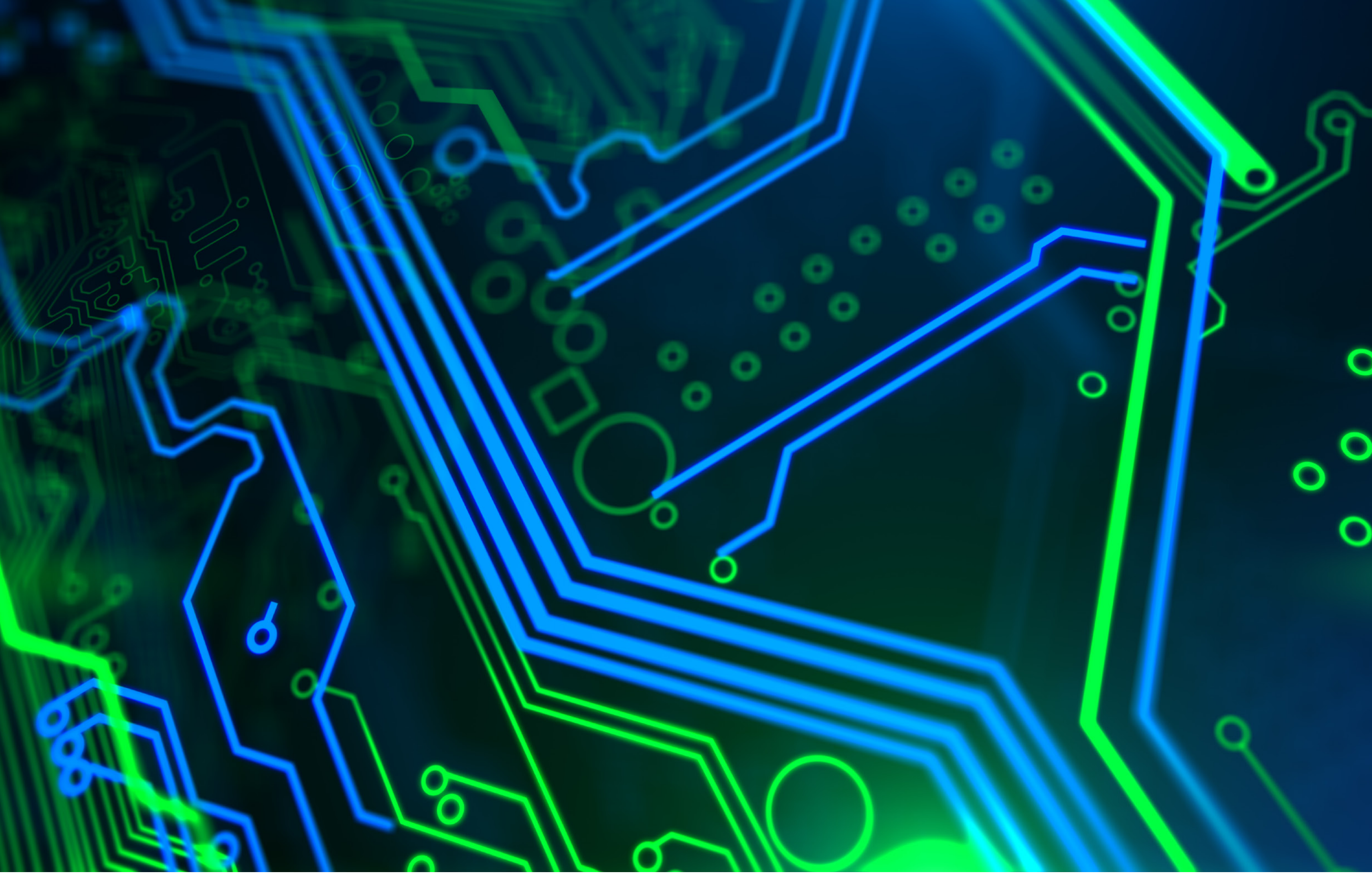


# Tackling cybercrime to unleash developing countries' digital potential

Background Paper

Dr Joanna Świątkowska

BLAVATNIK SCHOOL OF GOVERNMENT
UNIVERSITY OF OXFORD

Pathways for Prosperity Commission
Technology & Inclusive Development

Dr Joanna Świątkowska
The European Cybersecurity Forum - CYBERSEC *and* AGH University of Science and Technology

Background Paper 33
January 2020

The Pathways for Prosperity Commission on Technology and Inclusive Development is proud to work with a talented and diverse group of commissioners who are global leaders from government, the private sector and academia. Hosted and managed by Oxford University's Blavatnik School of Government, the Commission collaborates with international development partners, developing country governments, private sector leaders, emerging entrepreneurs and civil society. It aims to catalyse new conversations and to encourage the co-design of country-level solutions aimed at making frontier technologies work for the benefit of the world's poorest and most marginalised men and women.

This paper is part of a series of background papers on technological change and inclusive development, bringing together evidence, ideas and research to feed into the commission's thinking. The views and positions expressed in this paper are those of the author and do not represent the commission.

Citation:
Świątkowska, J. (2020) *Tackling cybercrime to unleash developing countries' digital potential*. Pathways for Prosperity Commission Background Paper Series; no. 33. Oxford, United Kingdom.

www.pathwayscommission.bsg.ox.ac.uk
@P4PCommission
#PathwaysCommission

Cover image © Shutterstock

BLAVATNIK SCHOOL OF GOVERNMENT
UNIVERSITY OF OXFORD

Pathways for Prosperity Commission
Technology & Inclusive Development

## Abstract

This paper provides an analysis of the cybercrime landscape in developing countries and focuses particularly on threats to their economic well-being. It highlights current trends in cybercrime activities and discusses various challenges faced by entities engaged in cybersecurity. The main goal of the paper is to strengthen the position of developing countries, providing multidimensional recommendations – especially for political leaders and policymakers – on how to build a secure digital future. To do this, the paper examines two approaches towards cybersecurity: 'digital optimism' and 'digital realism' and the lessons that can be learnt from these approaches. The paper suggests moving towards a new era of 'digital pragmatism' – an approach that can help to build a solid and secure foundation for the digital revolution.

## Acknowledgements

I would like to thank Mr Michael Bem and Ms Karine Szotowski for their expert advice throughout the preparation of the paper. Any possible mistakes and inaccuracies are mine alone.

# Table of Contents

# Introduction

## The digital revolution

Over the years, the internet has undeniably facilitated positive change for individuals, societies and businesses alike: by empowering people, strengthening and spreading democratic values, fostering innovation, and contributing to economic growth. However, the digital revolution has two sides, bringing both tremendous opportunities and significant threats to societies, economies and national security.

This paper argues that two distinct approaches to digital development have predominated since the invention of the internet, starting with 'digital optimism' and shifting into 'digital realism' (Schia 2017). Each approach demonstrates a different level of trust towards new technologies, and different decisions about how to implement security measures. These postures have had strong implications for how cybercrime threats have been handled, specifically at the governance level.

Through the early years of digital adoption, in the era referred to as one of 'digital optimism', countries perceived cybersecurity mainly as a technical issue rather than a strategic challenge.[1] As a consequence, decisive governmental actions were missing. Fragmented, ad-hoc approaches were prevalent, as opposed to a holistic vision. This period was also characterised by over-optimistic trust in new technologies and their positive impact on the world. Their wide implementation was not accompanied by proper security measures. Attitudes only started to change with the advent of the first truly significant cyber incidents, like the 2007 cyberattacks on Estonia and the Stuxnet worm attack uncovered in 2010. Following such incidents, the world entered the phase of 'digital realism' – an approach characterised by the conviction that digital development must be built on stronger security foundations – that were technological and strategic in nature. Digital realism also brought greater distrust in new technologies in general.

## Technology and developing countries

The main thesis of this paper is that developing countries need not be encumbered by limitations and mistakes that early adopters of technology fell prey to. These countries can better design and build their digital futures, greatly enhancing their economic growth. To achieve this, they will need to transition to an attitude of 'digital pragmatism', which constitutes an enhanced version of digital realism. Digital pragmatism is characterised by the implementation of 'secure by design' decisions and actions, at both the technical level and the strategic level. This approach allows for effective management of the risks inherent in digitalisation. It requires better situational awareness of both the threats and the opportunities related to digitalisation, which in turn allows for the implementation of targeted and efficient solutions. The effectiveness of cybersecurity countermeasures can be significantly increased and amplified by new technologies – for instance, artificial intelligence (AI) may be used to help solve many cybersecurity problems. The 'digital pragmatism' approach also

[1] Rough assessments can be made to provide a time frame for these two areas: digital optimism started with the wide-spread use of the internet (mid-90s) and lasted until the end of the first decade of the 21st century. Digital realism started at that point and continues.

calls for more co-ordinated and more effective international efforts to deal with the cybercrime problem, and for greater support for developing countries that are starting to develop digitalisation. Implementing such an approach may help to maintain trust in new technologies and therefore support the global digital revolution.[2]

## The Digital Single Market

This introduction provides a brief overview of the evolution of security approaches and the history of widespread internet adoption to help improve understanding of these concepts. It is difficult to assess the impact of new technologies on the global economy, as ICT is no longer a specific sector, but pervades all modern economic systems (European Commission 2015, p. 3). Nevertheless, selected estimates provide interesting insights. In some economies, the internet is thought to contribute up to 8% of GDP, powering growth and creating jobs (BCG 2012, p. 3). The Digital Single Market completion in the EU could amount to €415 billion per year to the EU's GDP (McKinsey Global Institute 2016). Gartner Research experts anticipate that product and service providers for the Internet of Things (IoT) will produce incremental revenue exceeding US$300 billion in 2020, translating into US$1.9 trillion in global economic value-add through sales to end markets (Middleton, Tully, and Kjeldsen 2013).

The economic benefits are undeniable. Yet, for years, in the era of 'digital optimism', governments, public entities, technology users, vendors, developers and other stakeholders were virtually blinded by the opportunities that ICT yields. Focusing mostly on the advantages behind the inventions, the importance of implementing appropriate safeguards was disproportionately downplayed.[3] While ICT systems have become omnipresent and indispensable across almost all spheres of daily life – critical infrastructures included – cyberthreats and their plausible consequences were underestimated. The following examples illustrate the problem and show the overly light approach taken by technology and governance entities in the cybersecurity area.

As ICT systems – predominantly the internet – became widespread, vendors and service providers were driven by the desire to feed the market with new products, solutions and functionalities as fast as possible. 'Technical debt', a term introduced by software programmer Ward Cunningham, describes the shipment of rough products to clients, with the intent to make amendments at a later stage (Chong 2013; Hoog 2015). Digital optimism introduced a problem that some label as 'technical security debt' – meaning that developers and vendors have often put unsecure products on the market, posing significant risks (Hoog 2015). According to estimations given by Carnegie Mellon University's CyLab Sustainable Computing Consortium, the average commercial off-the-shelf software contains 20 to 30 bugs for every 1,000 lines of code (Wired 2004).[4] At the same time, having processed data from 40 million security scans, cloud security and compliance company Qualys found that just 10% of vulnerabilities are responsible for 90% of all cybersecurity exposures (2006). This means that, very often, individuals, companies and governments adopt

[2] Chapter 3 includes recommendations on how to pragmatically introduce cybersecurity in developing countries.

[3] Understood broadly: technological, organisational, institutional, and so on.

[4] To gain a sense of perspective, Windows XP contains at least 40 million lines of code.

flawed technologies, entrusting them with essential aspects of their activity. Moreover, they tend to ignore basic security measures, such as updating software and operating systems, which would significantly strengthen their security posture and mitigate potential risks. Alarming discoveries confirm this thesis: in a 2015 study, hackers relied on flaws that have been known since 2002 in nearly 90% of cases (Harrison, Pagliery 2015).

## The need for cybersecurity

The presumption that digital development brings mostly advantages was not only reflected in poor technical security standards – similar mistakes were made by governments and international organisations at the strategic level. National cybersecurity strategies only started to be widely implemented at the turn of the first and second decade of the 21st century. Before this date, such legal frameworks were only a sporadic phenomenon, developed by pioneer countries.[5]

For years, the 'dark side' of the internet manifested itself in multiple shapes and forms: from seemingly harmless cases of unauthorised access, to disinformation spread through digital communications channels, online fraud, scams, and illegal trade, as well as other forms of organised crime, attacks on critical infrastructure aimed at causing massive disruption, political and industrial espionage, and terrorist activity co-ordinated through the internet – to list just a few examples. Over the years, such crimes became the new norm. An increasing proliferation of hostile actors has also been noticed: from individual hackers to organised crime groups, terrorists and state actors.[6] Each was driven by different motives and made use of different strategies and methods – all of which makes cybersecurity an even more difficult and challenging domain.

Cyberthreats eventually became so severe that the international community could no longer ignore the consequences. Incidents such as the massive cyberattacks targeting Estonia in 2007 – the infamous Stuxnet malicious computer worm which crippled the Iranian nuclear facilities – and the 2015 cyberattack on the Ukrainian power grid all served as wake-up calls for the general population and decision-makers in particular. Today, even the World Wide Web inventor, Sir Timothy Berners-Lee, calls for fixing the internet, stating that 'it has been hijacked for nefarious purposes' (Phys.org 2019). The international community finally ceased naively trusting technologies, entering a period of more prudent 'digital realism'. Characterised by the growing conviction that cybersecurity must be treated as an important element of all digital endeavours, this approach has been associated with governance, regulatory, technological, institutional, and organisational actions at both domestic and international levels. Key global actors such as Interpol, NATO, the

[5] In 2003, only two countries had a National Cybersecurity Strategy (NCSS), in 2010–11, in 2011–21. Now 97 countries have an NCSS. Disclaimer about calculation: To prepare this calculation, data from the indicated sources (ITU, National Cybersecurity Strategies Repository; ENISA, NCSSs Map; CCDCOE Cybersecurity strategies) as well as the author's research, were used. It is important to notice that sometimes a subjective assessment was made of whether the particular documents qualified as a NCSS. It happened that general national security strategies were qualified as NCSS, which, according to the author, was not justified. Since the sources and the research may not be exhaustive, it is likely that the actual numbers of strategies deviate from those mentioned above.

[6] More on the evolution of cybercrime can be found in the article written by Criminal Lawyer Group, available from: https://www.criminallawyergroup.com/the-evolution-of-cybercrime-from-past-to-the-present

UN, the EU, the African Union and others put cybersecurity at the top of their agenda. Countries extensively built their cybersecurity ecosystems.[7] Groundbreaking legislation such as the Network and Information Security (NIS) Directive are being adopted. Some of them, like the General Data Protection Regulation (GDPR) and the EU Cybersecurity Act, even have the ambition to influence technical standards (by introducing certification of ICT products and services).

All those processes have the potential to strategically change the cybersecurity landscape, yet seem collectively insufficient. This is why another distinctive feature of digital realism manifests in diminished trust in digital technologies. This distrust may, in the most radical scenario, negatively impact on further digital revolution – slowing it down, and leading to the fragmentation of digital economies. For instance, cybersecurity concerns were given as justification to propose barriers and limitations on the deployment of 5G networks using Chinese infrastructure components. Such actions have a huge impact on global supply chains and may even lead to the 'decoupling' of tech ecosystems (Woo, Volz 2019). Discussions about more advanced actions, such as national and international governance and regulations to improve cybersecurity, are triggered by eroding trust and the insufficient positive outcomes of cybersecurity measures. This has the potential to bring structural changes to the technological and geopolitical state of play, influencing developing states (Świątkowska, Albrycht 2019).

In other words, much has changed since the early days of the internet. The American essayist, philosopher, and poet Ralph Waldo Emerson once said that 'our distrust is very expensive'. This is not necessarily obvious in the context of cyberspace. On the one hand, trust is indeed essential for developing a digital economy, making life-changing inventions, and ultimately, changing the world. In that sense, missed opportunity costs associated with lack of trust can be significant. Trust, however, requires solid foundations, as otherwise losses may quickly outweigh benefits. It is therefore crucial to discuss and establish an adequate level of trust when taking actions that will enable further digital innovation – an undertaking in which governments and the international multi-stakeholder community must play an active role. Digital pragmatism is needed to overcome many of those challenges.

### Research covered by this report

This report's analysis is limited to discussing cybercrime and its impact on economic development. The first chapter looks at general trends and statistics related to the cybercrime landscape, but also examines the difficulties in combating threats.

The second chapter analyses digital vulnerabilities across developing countries. It takes a closer look at selected structural factors present in developing countries that strongly impact on the cybercrime landscape and the ways of addressing these factors. This chapter provides context to improve decision-makers' understanding of the actions that must be taken to increase their cybersecurity.

[7] Involving such bodies as Computer Emergency Response Teams, dedicated public authorities (even in the rank of Ministries), law enforcement agencies, military units and so forth.

The third chapter considers governance decisions taken at national and international level and sets out recommendations on how to deal with the cybercrime problem in developing countries. Future action and pragmatic solutions are proposed in light of the lessons learnt by early adopters in the eras of ‘digital optimism’ and ‘digital realism’.

# 1. The cybercrime landscape

## 1.1 Definition of cybercrime

For many years, cybersecurity was perceived as mostly a technical problem. This approach imposed tech-orientated language, with early definitions explaining cybersecurity through the three key security attributes: confidentiality, availability, and integrity of data and services provided by network and information systems.[8] Yet, over time, various actors came to realise that cybersecurity is not just a topic of ICT conversation. As cyberspace increasingly pervades everyday life, business, and national security, the understanding of the phenomenon must be broader, and encompass wider areas of intervention with governance actions, institutional set-up and regulatory decisions at its core. This paper proposes the following definition:

> Cybersecurity is the optimal state where users can function securely and achieve their goals in the cyberspace domain by effectively managing risks posed by multidimensional threats.

As cyberthreats pose different challenges to different actors, countermeasures must be tailored accordingly. Therefore, to achieve optimal results, actors must play distinct roles and fulfil various responsibilities.[9] Governments and state apparatus ought to co-ordinate many key endeavours – for example, providing strategic objectives and priorities on cybersecurity at a national level, and building a favourable environment for other actors' engagement. In most cases, actions designed to protect technical components (devices, systems, networks, and so on) will undeniably serve as a foundation for broader cybersecurity. However, plenty of additional capabilities will be required to holistically ensure cybersecurity.

There are many ingredients essential to the enhancement of cybersecurity: goal-derived strategies, executive sponsorship, risk management, legal and compliance frameworks, organisational architectures, human resources and others. Fundamentally, all actions aimed at tackling cybercrime should constitute a subset of wider cybersecurity-relevant activities. Implementation of those elements is very complicated and often requires significant financial resources, therefore the process can cause difficulties.

We also need to consider the meaning of 'cybercrime' itself. Unsurprisingly, there is no single, universally accepted definition. From a close analysis of proposed approaches, however, several common denominators can be extrapolated. First and foremost, technology is at the core of most cybercrime definitions, for instance: the EU defines the phenomenon as 'a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target' (European Commission 2013, p. 3). Second, a specific duality in understandings of cybercrime can be observed. This boils down to the differentiation between two

[8] Or 'security of network and information systems' – terms often used interchangeably (EU Directive 2016/1148, 3).

[9] With differing tasks while combating different hostile activities, eg cyberespionage, cybercrime, etc.

– often interrelated – forms of criminal activity: *cyber-dependent* crimes – which can be committed only with the use of ICT systems, for example, Distributed-Denial-of-Service (DDoS) attacks – and *cyber-enabled* crimes (traditional illegal acts that are transformed and scaled up by ICT, such as online fraud and data theft) (Interpol, HM Government 2016, p. 17). Currently, most 'offline' crimes at some point also include 'cyber' components.

## 1.2 The cost of cybercrime

It is difficult to accurately estimate the cost of cybercrime. With so many variables, unknowns, and complexities (Scott 2016), all approximations must be taken with scepticism. Nevertheless, estimations reflect the severity of the problem. One of the best-known calculations is provided by McAfee and CSIS; the latest edition of their report asserts that cyber incidents may cost the global economy as much as US$600 billion, or 0.8% of global GDP (CSIS, McAfee 2018, p. 6).[10 ´ 11]

Table 1 provides estimates of financial losses related to cybercrime, broken down by region. This shows the potential of cybercrime's negative impact on economic growth.

[10] Another way to understand the magnitude of cybercrime is to compare it to the internet economy as a whole. Boston Consulting Group estimated that the value of the latter was approximately US$4.2 trillion (BCG 2012). This essentially means that cybercrime can be viewed as a 14% tax on growth (CSIS, McAfee 2018, 19). Other estimates claim that cybercrime costs the global economy US$2.9 million per minute (RiskIQ 2019).

[11] Even computing losses caused by cybercrime may be difficult to calculate. The methodology used in Table 1 offers a good example of how to deal with this issue. Aspects considered included: the loss of intellectual property and business confidential information, online fraud and financial crimes, financial manipulation (using stolen sensitive information on potential mergers, among others), the cost of securing networks, buying cyberinsurance, paying for recovery from cyber-attack, reputational damage and liability risk for the hacked company and its brand (including temporary damage to stock value), opportunity costs (including disruption in production or services), and reduced trust for online activities. All these issues could be examined in detail while assessing cybercrime consequences in developing countries.

Table 1. Regional Distribution of Cybercrime 2017

| **Region** | **Income level** | **No. of countries** | **Region GDP (US$, trillions)** | **Cybercrime cost (US$, billions)** | **Cybercrime loss (% GDP)** |
|---|---|---|---|---|---|
| **East Asia & Pacific** | | **36** | **22.5** | **120 to 200** | **0.53 to 0.89%** |
| *thereof* | High income | 12 | | | |
| | Developing | 24 | | | |
| **Europe & Central Asia** | | **55** | **20.3** | **160 to 180** | **0.79 to 0.89%** |
| *thereof* | High income | 35 | | | |
| | Developing | 20 | | | |
| **Latin America & Caribbean** | | **38** | **5.3** | **15 to 30** | **0.28 to 0.57%** |
| *thereof* | High income | 13 | | | |
| | Developing | 25 | | | |
| **Middle East & North Africa** | | **21** | **3.1** | **2 to 5** | **0.06 to 0.16%** |
| *thereof* | High income | 8 | | | |
| | Developing | 13 | | | |
| **North America** | | **3** | **20.2** | **140 to 175** | **0.69 to 0.87%** |
| *thereof* | High income | 3 | | | |
| **South Asia** | | **8** | **2.9** | **7 to 15** | **0.24 to 0.52%** |
| *thereof* | Developing | 8 | | | |
| **Sub-Saharan Africa** | | **48** | **1.5** | **1 to 3** | **0.07 to 0.20%** |
| *thereof* | High income | 1 | | | |
| | Developing | 47 | | | |
| Total | | 209 | | | |

Source: Own elaboration based on CSIS, McAfee 2018 and the World Bank's countries classification 2019.

As Table 1 shows, developing countries lose much less money to cybercrime than developed countries. At first glance, this may downplay the importance of the problem. However, in societies very often touched by abject poverty, every efflux of money is tremendously notable; it can be a truly burning problem for economic well-being at an individual level. Table 1 also suggests that cybercrime losses increase alongside income levels and internet penetration. Given the increase of internet use in developing countries, the cybercrime landscape may quickly expand and broaden its impact.

Economic consequences, as indicated, are not limited to the losses directly sustained by developing countries. At times, additional and more severe consequences manifest: these tend to be long term and much more difficult to resolve. Poorly secured infrastructure that weakens the entire global system, skillset shortages, untrustworthy strategic and legal systems, and the growing strength of organized criminal groups  – to name a few – significantly impede economic conditions and the relative position of developing countries in the international arena. A lack of confidence that developing countries are reliable business partners often hinders investments and knowledge exchange, leading to their partial exclusion from the global economic system. All of this has an obvious impact on economic growth.

There are several reasons why cybercrime is on the rise. Some of them – such as relative anonymity (which decreases the chance of being caught) – derive strictly from the architecture of the internet. Others, like scalability, are related to different circumstances – for instance, they may be the result of new technology development and automation. In general, cybercrime is low-cost, highly profitable, and increasingly easy to commit. Cyberattacks-as-a-service, enabled by illegal marketplaces hosted within the Darknet,[12] contribute to the easy accessibility of tools that enable hostile actors to commit cybercrimes, even where they lack technical knowledge. Offenders no longer need sophisticated knowledge or skills to commit crimes, as they can purchase the necessary tools and tutorials online. Ransomware toolkits, for instance, cost only a few dollars, with more sophisticated versions available for US$3,000 (McAfee 2018, p. 11).

Automation exponentially increases the scale of the problem, as it allows the same illicit activities to be repeatedly carried out with minimal effort. Malware development itself has also been automated: systems can identify vulnerable devices and prepare appropriate payloads.[13] According to McAfee, one major internet service provider reported observing 80 billion malicious scans a day (McAfee 2018, p. 4). All of this makes cybercrime an attractive and lucrative type of illegal businesses. Cybercrime has evolved into a complex economy, a system composed of various intertwined economic actors, which generate and maintain large criminal revenues (McGuire 2018, p. 12).

Cybercrime is no longer the domain of individual actors or 'lone wolves'. It is a complex undertaking, conducted to a large extent by organized criminal groups . Upwards of 80% of cybercrime acts are estimated to originate in some form of organised activity (UNODC 2013, p. XVII). As the complexity of cybercrime increases, advanced governance actions co-ordinated between national and international partners are increasingly necessary.

[12] Darknet can be defined as 'a network built on top of the internet — which has been designed specifically for anonymity' (Sabarinath 2019). Darknet is often used for illegal activities.

[13] A payload is the component of the cyberattack which causes harm to the victim (Cloudflare).

## 1.3 The main types of cybercrime

Countless types of cybercrime contribute to these losses. It would be impossible to discuss in detail all the methods adopted by criminals to commit offences, especially as they constantly evolve and adapt. Yet, analysing the trends and factors that have led to the unprecedented scale of the problem can help to understand the cybercrime landscape.

This section summarises several prominent categories of hostile and illegal activities in cyberspace, as emphasised in recent reports by specialised agencies and private security companies. Due to the scope of this paper, the selection has been limited to those types of cybercrime that have a significant economic impact and are important in the context of developing countries – being either financially driven or generating noteworthy financial consequences.

### 1.3.1 Malware and ransomware

With its destructive nature and potential for real financial impact, ransomware is one of the key types of cybercrime. The term refers to a type of malware that surreptitiously encrypts victim data and demands payment be made – usually in cryptocurrency[14] – to restore access (Fruhlinger 2018). The potential for ransomware to hamper the economy and financial well-being of a victim is significant. For example, in May 2017, WannaCry ransomware affected around 300,000 victims (Europol 2018, p. 16), shutting down computers with outdated Windows operating systems.[15] The UK health sector was particularly adversely affected – a report from the UK Department of Health stated that it had cost the British National Health Service £92 million (Field 2018) – but the attack had impacts on a range of sectors in more than 150 countries. Overall, the global economy lost approximately US$4 billion due to the attack (Berr 2017).

A month later, NotPetya ransomware paralysed some of the largest businesses in the world. One of its victims, the Danish shipping company Maersk, which moves about one-fifth of the world's freight, lost between US$200 and US$300 million (Mathews 2017). The Maersk case is particularly interesting, as it captures the comprehensive nature of cyberattacks and their cascading impact on the economy: the malware interrupted operations at Maersk's terminals in four different countries, causing week-long delays, with repercussions for other industries that relied on timely delivery of their products and manufacturing components. In total, the global damages caused by NotPetya amounted to more than US$10 billion (Greenberg 2018).

The effects of ransomware and attacks are not only confined to the economy: they can also cripple critical infrastructure. For example, in South Africa, some residents of Johannesburg were cut off from electrical power due to a ransomware attack (BBC 2019). Chapter 2 will discuss the cyberthreats landscape in developing countries in more detail.

[14] Making law enforcement attempts to trace the funds more difficult.

[15] It is important to highlight that patches for affected systems existed but were not applied. Microsoft had originally released them in March – almost two months before the incident, and again on the day of the attack.

Banking malware represents another specific type of cyberthreat. The rise of online banking has rendered this threat increasingly substantial (Europol 2018, p. 18). Banking Trojans – types of software designed to illegally access banking details – are gaining the most traction in this arena (Batt 2018). It is suggested that one of the key reasons is the increased use of mobile banking applications. The software provider Check Point  found that the number of threats against mobile devices in the first half of 2019 had risen by 50% compared to the previous year (Palmer 2019).

### 1.3.2 Credit card fraud

Online transactions – the backbone of e-commerce industry – have seen a rise in 'card-not-present' (CNP) fraud, in line with the general growth of digital commerce (Europol 2018, p. 43). CNP scams occur because the buyer is not required to physically present the card to the retailer to complete the purchase, allowing criminals to make a fraudulent transaction. These crimes require the victim's information (names, card numbers and passwords) that can be acquired in a number of ways, including 'phishing' and purchasing data on the online black market. For instance, the amount of credit card data available on the Darknet has increased by 153% over the past year (Stuppy 2019).

### 1.3.3 Data breaches

Data breaches are closely tied to malware and fraud. A breach is defined as: 'an incident that results in the confirmed disclosure… of data to an unauthorized party' (Verizon 2018, p. 2). There are numerous reasons why acquiring access to individual and organisational data is at the forefront of criminal activities. Attaining information can be an end in itself – for example, as part of a cyberespionage campaign, which can give the instigator valuable, strategic knowledge and an associated advantage over the competitor. Such data can also be monetised, for instance, through sale on the Darknet, or through extortion (such as blackmailing the victim). The data can be used to commit further illicit activities, for instance to steal financial resources. Some assessments have shown that 76% of analysed breaches were financially motivated (Verizon 2018, p. 5).

Data breaches may lead to further, indirect consequences. For example, the breach that affected more than three billion Yahoo! customers, compromised names, dates of birth, email addresses and passwords. The incident introduced severe risk for the direct victims, but also reduced Yahoo's sale price by an estimated US$350 million (Armerding 2018), as it was in the process of being acquired by Verizon.

### 1.3.4 Cross-cutting factors and cryptocurrencies

Cross-cutting crime factors are those that impact, facilitate, or otherwise contribute to multiple crimes (Europol 2018, p. 54). Social engineering – particularly phishing – is by far the most prevalent in this group.[16] Conducted at a large scale, it can have significant financial consequences. In 2018, for example, an international organized crime group stole the credentials of hundreds of banking institutions' customers, and subsequently stole €1 million in funds (Europol 2018, p. 55).

While not a direct cyberthreat, cryptocurrencies bring intriguing novelties to an analysis of cybercrime and play a pivotal role in many digital crimes. They have been used as a 'cross-cutting factor' (see above) and also as a target for cybercrime. Due to their pseudonymisation and decentralised infrastructure, cryptocurrencies continue to be the mainstay of illicit online transactions and enable the commissioning, perpetration, and monetisation of cybercrime (Europol 2018, p. 58, p. 59). As the value of Bitcoin, Ethereum, or Monero increases, their users and facilitators – for instance, currency exchangers, mining services, and wallet holders – are becoming common targets of crime (Europol 2018, p. 63). Two new growing trends are worth noting: cryptojacking – exploiting internet users' bandwidth and processing power to mine cryptocurrencies (Europol 2018) – and  initial coin-offering scams.

## 1.4 New cybercrime frontiers

Implementing successful cybercrime countermeasures requires us to consider current threats, and also to anticipate what the future will bring. Several technologies and methods are expected to significantly influence the cybersecurity landscape (in negative and positive ways). Debates on cybersecurity measures should also consider the broader trends related to digitalisation, as they bring new circumstances that change the cybersecurity landscape. Some selected examples include:

**Fourth Industrial Revolution (4IR):** 4IR will transform many forms of cybercrime, mostly by increasing the gravity of their consequences. As digital solutions begin to 'blur the lines between the physical, digital, and biological spheres' (Schwab 2016), more components of everyday life will increasingly rely on digital technologies. As a result, current paradigms of production, management, and governance will be revolutionised. In this new environment, new avenues for cybercrime will appear. For example, 5G will serve as an important building block for 4IR. Its capacity for increased data transfer rate, lower latency, and higher throughput may herald a new era of artificial intelligence (AI), telemedicine, autonomous transport, and the Internet of Things (IoT), to name but a few technologies. At the same time, it may hinder law enforcement activities, making it harder to identify and locate users. As Europol warned, it will allow users 'to download

[16] Social engineering is understood in this context as psychological manipulation to trick users into making security mistakes or giving away sensitive information, which enables criminals to, for instance, overtake the victim's device.

data from multiple sources simultaneously, making the investigation of communication events increasingly complex' (Europol 2018). Also, while previous generations of mobile networks made use of unique identifiers assigned to each individual device, 5G will rely on temporary identifiers, further complicating the attribution process (Europol 2018).[17]

**Internet of Things (IoT):** In the era of 4IR, the IoT is likely to become omnipresent. The avenues for cyberattacks will exponentially increase, and the cyberattacks themselves will undoubtedly evolve. Distributed Denial-of-Service (DDoS) attacks contextualise the potential importance of the problem. Some predict that, in 2020, there will be 20 billion connected devices worldwide. If as poorly secured as they are today (Hung 2017), they will serve as powerful tools, supporting criminal activities. Weak passwords, poor configuration, and unpatched technical vulnerabilities will allow criminals to control devices to carry out unprecedented DDoS attacks. Examples of such attacks have already been seen. For example, in October 2016, the world witnessed one of the most infamous DDoS attacks, which leveraged malware dubbed Mirai. Offenders used automated tools to scan the internet for connected devices and used 60 default usernames and password combinations to gain access (Batt 2019). The machines were then infected with the malware and became part of a remotely controlled botnet – a network of hundreds of thousands of hijacked IoT devices, used to launch large-scale attacks – that brought down the domain registration services provider, Dyn, for several hours.[18] As a consequence, a large number of services and websites in the US and Western Europe were also suspended. In the age of countless, omnipresent, interconnected devices, similar attacks will pose a great challenge.

**Artificial Intelligence (AI):** The benefits associated with the development of AI are widely discussed, but AI will also revolutionise the cybercrime scene. The core of the problem lies in AI's enabling power, which will significantly enhance numerous hostile activities conducted in cyberspace – for instance, improving malware development or social engineering attacks. The ability of computers to communicate in natural languages may mean that automated messages will hardly be distinguishable from a human-authored text (Gladyshev 2018). AI can also be used for automated malicious payload creation, helping to adapt this process to avoid detection, and drastically decreasing effective anti-malware countermeasures.

AI is also likely to be used for more sophisticated attacks, as it learns from the data it is fed and adjusts outcomes accordingly. Abuse of that process – for example, through data manipulation – may have unwanted and dangerous consequences. For instance, a bank loan approval or a self-driving car might be manipulated (Gladyshev 2018). By manipulating data that fuels AI, people can influence automated decisions made by the algorithms. Consequences may be multifaceted: people entitled to receive loans could be rejected (influencing their economic well-being) or the functioning of autonomous vehicles could be impacted (leading to dangerous accidents).

[17] Attribution is understood here as the process of ascertaining and assigning responsibility for malicious cyber activity (for more, see Lin 2016).

[18] Botnets can be used for numerous hostile activities: DDoS attacks, sending spam, stealing personal information, hosting malicious sites, and delivering 'payloads' of other malicious etc. (Hogben cited in UNODC 2013).

**Quantum computing:** While still an issue of the future, quantum computing could be another potential game-changer. With its superior computing power, current encryption mechanisms will become obsolete. Ensuring data confidentiality might then be difficult to achieve and will require more advanced methods. Is has been estimated that 'about 99% of online encryption is vulnerable to quantum computers' (Gold 2019). Financial sectors worldwide must foresee challenges related to those issues and start thinking about the transition to quantum-safe cryptography (Ollson 2019).

## 1.5 Difficulties in combating cybercrime

The challenges associated with designing, implementing and operating successful cybercrime countermeasures are multidimensional. Here we divide them into the main categories.

### 1.5.1 Cross-border procedural and legal issues

To sufficiently prevent and combat cybercrime, states must have substantive and procedural legal provisions in place. This is one of the most important tasks that governments must fulfil. It is often a struggle to establish and maintain effective criminalisation.[19] Legal frameworks must remain adaptive and flexible, but putting domestic mechanisms in order is merely a first step. The biggest obstacles and underlying difficulties in combating cybercrime are related to its cross-border nature.[20]

International legal interoperability and effective collaboration lie at the heart of the challenge.[21] In most cases, victims and offenders are located in different legal jurisdictions. Consequently, those cases can be solved only if legal regimes are aligned between countries and effective mechanisms for co-operation exist. Therefore, an intensive international collaboration against cybercrime requires harmonising elements of the domestic criminal laws that refer to cybercrime and building effective procedural powers (World Bank 2017, p. 26). To complicate the issue of co-operation even further, it is becoming obvious that 'traditional' instruments of co-operation, like mutual legal assistance regimes, are ineffective in the digital era, and the international community must therefore look for new assistance mechanisms.

[19] Different strategies were deployed to deal with that. One is to adjust already existing provisions to be applicable to cyberspace. The other is to provide some new measures.

[20] Cybercriminals tend to search for a safe haven and operate from that territory.

[21] International operability derives from cohesive legal frameworks dedicated to cybercrime issues that are adopted in various countries (World Bank 2017, 36).

### 1.5.2 Digital skills and resources

Countering cybercrime often requires skills and resources that national law enforcement agencies do not have. The architecture of the internet – in so far as it enables anonymity, and criminals can often operate behind multiple layers of fake identifies – promotes clandestine actions, as it complicates even basic actions to identify the offender (World Bank 2017, p. 34). The digital environment brings challenges even to the most fundamental procedures such as the collection, preservation, and evaluation of evidence (Grimes 2016).[22] Obstacles related to those processes emerge from the necessity of advanced technical knowledge, but also from the fact that access to evidence will not be possible without co-ordinated international operations (often with the participation of the private sector).

### 1.5.3 Evolving technology

Technological innovation offers countless, constantly evolving tools to commit cybercrime. To keep up with technological changes, law enforcement and the judiciary must constantly perfect their methods and invest in knowledge, equipment, and skills – all of which require the time and resources public bodies often lack – particularly in developing countries. Keeping up with technological advancements causes operational issues and difficulties solving fundamental security problems. Very often the technologies that bring innovation and benefits for society also hamper the efforts of law enforcement agencies. Encryption is a good example – it brings enormous benefits for users, enhancing privacy and confidentiality of data and communication. It serves as an essential element of cybersecurity and a building block for secure solutions that enable the digital economy to thrive (Kelly 2018). At the same time, it creates significant obstacles and challenges for entities responsible for combating cybercrime, as often they are not able to track criminals and have access to important evidence or information. There is currently a vivid global debate on whether or not to introduce 'backdoors' into systems to enable more efficient work of law enforcement agencies. Backdoors are a double-edged sword: while helping police action, they can significantly weaken the security and cause hard-to-predict damages to the security ecosystem.

### 1.5.4 Private sector role

Another barrier to combating cybercrime is linked to the increasing role of the private sector (without whom many cases cannot be solved). In the digital realm, private companies predominate: they own and operate infrastructure, provide products and services to end users, and maintain databases. They often have sole access to the potential evidence and information necessary for an investigation. Law enforcement authorities therefore rely on co-operation with private sector organisations, often of foreign origin. Governments must therefore establish efficient mechanisms for public–private co-operation by instigating, supporting and enhancing international initiatives.

[22] The need for education applies also to prosecutors, judges, and juries.

This is of utmost importance as new technological advancements, applications and emerging technologies bring more complex challenges. Fast and streamlined access to cloud-based digital evidence is an area where public–private co-operation is needed (UNODC 2013, p. XXII; World Bank 2017, p. 105). This issue is currently at the top of the political agenda. For example, the Clarifying Lawful Overseas Use of Data (CLOUD) Act) – the US federal law enacted in 2018 – aims to solve difficulties with data access across borders, where the use of traditional mutual assistance is often not feasible. The key element of the legislation obliges US-based tech companies to provide data to federal law enforcement, even if the servers are located on foreign soil.[23] Several tech giants, including Microsoft, Facebook, Apple and Google supported the creation of the CLOUD Act (Foley 2018).

## 1.5.5 Human rights issues

Most of the issues described in this chapter are multiplied by the need to balance security with the rights and freedoms of citizens, especially the right to privacy and freedom of expression. This domain must be dealt with through solid legal safeguards and standards established and executed by governments (World Bank 2017, p171-177). It is important to underline that, despite popular belief, security measures do not necessarily invade personal freedoms. On the contrary, when implemented properly and with respect to legal safeguards, they may significantly contribute to the protection of those rights. Examples include the implementation of encryption, pseudonymisation, and other elements related to the protection of the confidentiality, integrity, and availability of the data and systems. Indeed, although it is difficult to reconcile security and human rights and freedoms, it is not impossible.

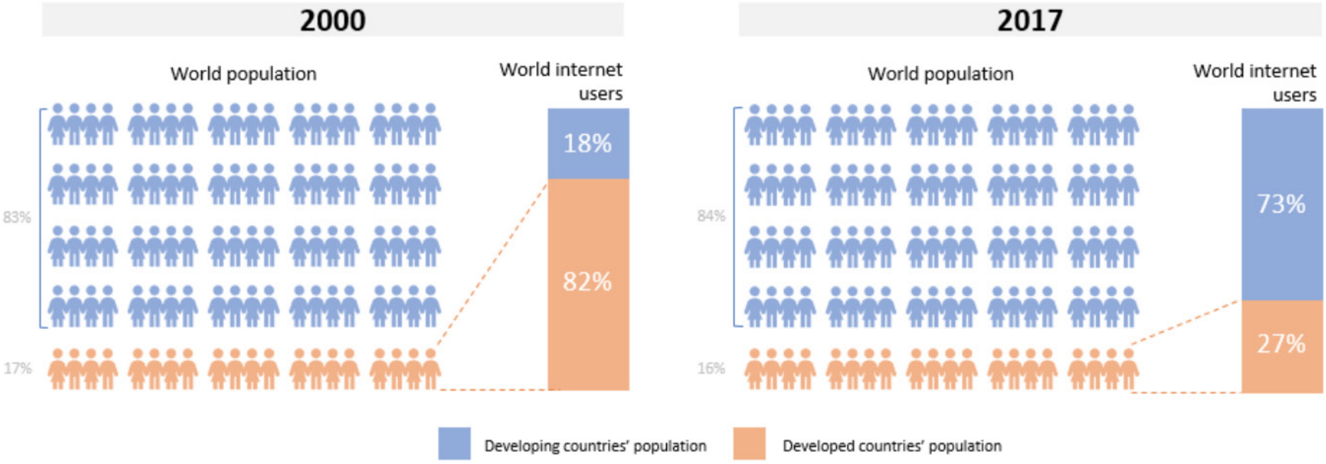
[23] The CLOUD Act applies only  to the most severe crimes.

# 2. Analysing digital vulnerabilities in developing countries

## 2.1 The rolling digital snowball

The International Telecommunication Union (ITU) estimated that more than half of the global population were online at the end of 2018 (ITU 2018).[24] And, in the last 15 years, the demography of internet users has changed dramatically: in 2000, developed countries (17% of world population) represented 82% of the world's internet users; by 2017, developing countries were the biggest group of internet users (73%) and the majority of the world's population (84%).[25] While developed countries are still over-represented among internet users, the gap is closing very fast (World Bank 2019).

Figure 1: Changes in the global distribution of the internet



Source: Own elaboration based on the World Bank's countries classification (2019), the World Bank's World Development Indicators, ITU Country ICT Data.

Internet penetration in developing countries is still relatively low (amounting to 45.3% at the end of 2018), it faces various obstacles (Kshetri 2010, p. 1058), and is unevenly distributed (Pathways for Prosperity Commission 2018). However, it is growing at a rampant rate (ITU 2018). Africa has the lowest number of internet users, but is making the most dynamic progress. The percentage of Africans using the internet has increased from 2% in 2005 to almost 25% in 2018 (ITU 2018). Other regions are also experiencing growth. In the Commonwealth of Independent States (CIS), 71.3% of the population use the internet, while in the Arab States it is 54.7%, and in the Asia-Pacific region, 47% (ITU 2018).[26]

[24] 51.2% of the global population (3.9 billion people).

[25] Upper-middle-income, lower-middle-income and low-income categories are considered for the World Bank's definition of developing countries.

[26] The CIS consists of Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan

Developing countries are also characterised by the significant growth of the number of mobile broadband subscriptions, which is likely to accelerate further. The largest expansion of broadband subscriptions has been observed in the Asia-Pacific region, the Arab States, and Africa (ITU 2018). Notably, countries of the Global South often bypassed fixed-phone infrastructure and invested directly in wireless technology (Schia 2017, p. 4). Dominant mobile digital infrastructure brings specific issues that influence security conditions.

Much has been written about the positive aspects of digitalisation. Indeed, as a precondition of economic well-being, it is an underlying factor for attaining the UN's Sustainable Development Goals (SDGs). Globally, political and business leaders strive to create favourable conditions to make sure that the related benefits, especially in the economic arena, will materialise. National, regional and international mechanisms have sprung up to facilitate the process, due to the widely accepted presumption that only through digitalisation will the global economy be able to achieve its full potential. The Digital African Market was set up with the main goal of unleashing entrepreneurial energy, innovation and economic capabilities of the continent.

Along with digital transformation, developing countries have been facing various cyberthreats that may endanger their economic development and also perturb the global financial system. Even though most developing countries are at the beginning of their digital journey, significant security problems already exist, and these are only likely to increase. For instance, more malicious activities tend to be observed when a country's internet penetration is above a threshold of 10–15% (Reilly 2007). Developing countries have crossed that threshold and so have become an important element of the global cybersecurity landscape.

## 2.2 Developing countries in particular peril

Structural factors in developing countries strongly influence their cybercrime position. During the initial phase of digitalisation, nations experience a phenomenon known as 'hollow diffusion' (Kshetri, 2010, p. 1066). Digitalisation often outpaces the establishment and implementation of cybersecurity technical controls and – often primarily – governance frameworks.[27] Existing weaknesses are exploited by cybercriminals who target victims in developing countries, and also take advantage of the digital infrastructures of those countries to carry out attacks on other territories, including developed states.[28] This trend is expected to increase, and developing countries must act against it. To better understand this complex issue, it is important to analyse common denominators that typify the cybercrime scene in developing countries.

[27] Niels Nagelhus Schia uses the name 'societal hollowness'. Compare to the concept of 'digital optimism' introduced earlier.

[28] The US, UK, and other European states have for a very long time served as main cyberattack originators. The last decade marked a noticeable shift towards emerging economies. For instance, in 2009 seven of the top ten countries for creating Trojans designed to steal passwords were developing countries. They accounted for 92% of such Trojans globally (Kshetri 2010).

### 2.2.1 Technology-related security shortages

Poorly secured, outdated, unlicensed and unmanaged information assets, often relied on in many developing countries, serve as a key facilitating factor for cybercrime:[29]

- As many as 80% of PCs on the African continent are already infected with malware (Akerele 2018). Windows 7, the operating system most vulnerable to the WannaCry attack, holds a 55% market share in Africa (Schia 2017, p. 12).

- About one quarter of African users are using Microsoft Windows XP, an operating system that has lacked support and patches since 2014 (Akerele 2018, p. 24).

- More than 95% of African organisations (in both the private and public sectors) are either operating at or below the 'security poverty line', which means that they cannot effectively manage cyberattacks – mainly because they do not have basic security measures and structures in place and barely invest in security solutions (Serianu 2017, p. 7).

- According to the Global Software Survey, approximately 57% of software used in Africa and the Middle East is unlicensed, which means that upgrades and security patches will not be installed (BSA 2016, p. 8). Entities and individuals from emerging economies often simply cannot afford the latest software and hardware versions and cannot invest in cybersecurity solutions, making them very susceptible to attacks.

This problem has an additional dimension, in that ICT vendors (similarly to vendors in other sectors) tend to adapt to the market demand by adjusting their offer to match clients' capacities or expectations. For many developing countries, high-security products are unaffordable; therefore instead, manufacturers provide low-cost, consequently less secure versions of their products. Such outdated or unprotected systems are easy prey for cybercriminals (Kshetri 2010, p. 1066), serving as targets that can be either directly exploited or weaponised to enable further crimes.

As a consequence, cybersecurity problems in developing countries can have significant implications, not only for those countries, but also globally. Taking the observed trends into account, immensely growing populations in developing countries will be soon be equipped with billions of connected devices. Poorly secured, they are cybercrime targets, but they can also be used as tools to commit further attacks. One possible scenario is that the proliferation of unsecured devices in these markets will create the potential for larger, more damaging botnets. According to cybersecurity author Jeffrey Carr, 'one botnet of one million hosts could conservatively generate enough traffic to take most Fortune 500 companies collectively offline. A botnet of 10 million hosts on the other hand, could easily paralyse the network infrastructure of a major Western nation' (Carr 2009, p. 13).

[29] Understood broadly as both hardware and software at either private or institutional level.

Technology-related problems in developing countries are an important reason why cybercrime is flourishing. The issue can be limited by governance interventions that may, for instance, be focused on enforcing security standards in the critical sectors. Governments can also build a dialogue with technology vendors, so they can provide more secure products and services (these issues are described in section 3.4).

### 2.2.2 Human factor – the centrepiece of cybersecurity

A lack of knowledge and skills – including basic cyberthreat awareness and 'digital hygiene' – is another reason why developing countries have poor cybersecurity (Kshetri 2010, p. 1068). Careless online behaviour is one of the main reasons that users fall victim to cybercrime. The problem is sadly broader, as many developing countries suffer from a shortage of cybersecurity specialists to help enhance cybersecurity.  As we move towards the 4IR, relevant skills will be crucial to safety and security in the digital world.

While the total population of the African continent now exceeds 1.3 billion, the number of certified cybersecurity professionals is merely 10,000 (Serianu 2017, p. 11). Some estimates are even lower: according to ISACA (an independent association of professionals involved in information security), as of mid-2018, Sub-Saharan Africa was home to 5,700 certified cybersecurity professionals. These numbers represent a mere 4% of ISACA-accredited information assurance experts globally (Nduati 2018).

Often no systemic solutions are available to tackle the problem as the educational system fails to offer sufficient courses or research projects in the cybersecurity area (Serianu 2017, p. 19). And in most cases, informal education does not suffice.[30] Arguably, when formal cybersecurity education was nascent or non-existent across the well-established states, individuals gained their knowledge mostly through independent self-study. This strategy is not easily applicable to developing countries, as most people are not fluent in English, a prerequisite for understanding most information security content (Information Today 2008, p. 22 cited in Kshetri 2010, p. 1067).

Education represents one of the most important avenues of governmental intervention. The integration of cybersecurity aspects into educational curricula is the main step. There are numerous examples of international standards and guidelines that can be used to create an educational framework. Tailored courses can be created to increase skills among targeted groups. Equally, non-governmental entities also need to get involved in those endeavours (see section 3.3).

A final human-related problem is associated with poor economic situations, especially where unemployment rates are high and wages are low, or highly unequal. Such conditions can foster cybercrime as a very lucrative source of quick income. Cybercriminal activities may be seen as an attractive occupation, and a solution to financial problems among the poor and marginalised.

[30] Understood as self-teaching, courses, programmes offered outside of the official educational system.

Experts claim that the lack of offers within the legal ICT labour market push those who have acquired elementary skills – or purchased hacking tools on the Darknet – towards illegal activities (Sullivan 2007; World Bank 2017, p. 16). High unemployment and poverty lead to high societal acceptance of cybercrime engagement. In Western African countries, so-called *yahooboys* (Adeniran 2011 cited in UNODC 2013, p. 10) are university students who view online fraud as a means of economic subsistence. Another example is the *sakawa* boys, emerging in Ghana, who engage in internet fraud and frequently justify their activities as the only way to survive in the absence of employment (Warner 2011, p. 746).

### 2.2.3 Insufficient strategic solutions and imperfect legal frameworks

This report has underlined that effective strategic and legal frameworks play an essential role in combating cybercrime. Unfortunately, developing countries suffer visible shortages across those domains. Next to technology and human-oriented challenges, strategic and legal deficiencies pose futher challenges to combatting cybercrime in developing countries.

Many developing countries are yet to adopt national cybersecurity strategies to provide a general governance framework for long-term actions. This hinders efforts to create a well-functioning cybersecurity ecosystem, or to determine key roles and responsibilities. Without strategic guidance, basic mechanisms for co-operation are often missing. Similarly, crucial processes – for instance, related to national risk analysis, information exchange or incident management – are not in place.

More than two-thirds of surveyed countries in Africa, the Americas, Asia and Oceania view their laws related to cybercrime as only partly sufficient, or not sufficient at all (UNODC 2013, p. XVIII). Unrelated research confirms this, pointing out that, in 2016, 30 out of 54 African countries did not have specific legal provisions in force regarding cybercrime and electronic evidence (Symantec 2016, p. 54). There is abundant evidence that organized criminal groups consider a number of factors when making decisions about which geographic location to operate from. One of the most important factors is the strength of the rule of law. Cybercriminals search for 'safe havens', hoping that weak legal frameworks and subpar enforcement will decrease the probability of their apprehension and conviction, as well as the expected penalty (Kshetri 2010, p. 1063). Consequently, cybercrime in developing countries is flourishing. For instance, Brazil is ranked as one of the largest originators of attacks globally, and is the leader in Latin America and the Caribbean (Kessem, Korman 2015). Experts highlight inadequate legislation as a key part of this problem (CSIS, McAfee 2018, p23).

Non-existent or insufficient regulations are not the only obstacles to combatting, investigating and prosecuting cybercrime. Very often, weak enforcement mechanisms are a further problem. This calls for immediate intervention from national governments, which must create national legal frameworks, including appropriate criminal laws and domestic criminal procedural powers that will enable them to fight cybercrime. This must be accompanied by international co-ordination aimed at achieving legal interoperability.

Developing countries often lack capabilities when it comes to law enforcement authorities and jurisdiction. They have few specialised police, with around 0.2 per 100,000 national internet users (UNODC 2013, p. XXIII). UNODC's survey highlights that 70% of dedicated law enforcement officers in emerging nations lack computer skills and equipment, while only half receive training more than once a year. Most countries reported requiring technical assistance, mainly in the area of cybercrime investigative techniques (UNODC 2013, p. XXIII). The survey also shows that unprepared judicial services and prosecutors represent a significant bottleneck in fighting cybercrime (UNODC 2013, p. XXIV).

Apart from legal issues, there is also the risk of additional collateral damage associated with thoughtless cybercrime legislation. Experts warn that many African countries' newly created anti-cybercrime legal solutions threaten freedom of expression and other fundamental human rights – in particular where offences are vaguely defined and safeguards are weak or missing. This brings potential risks to individuals, undermines trust, and hinders international and public–private sector co-operation (Symantec 2016, p. 55). This must serve as a warning for all other developing countries: governance decisions in this area must be rational and bold, as this will be the condition of success for many reforms.

## 2.2.4 Digitalisation of financial services

The increasing role of digital financial services is actively shaping the cybercrime scene. In developing countries, traditional banking and other financial activities are often expensive and inaccessible (especially in rural areas). As a result, most of the poorest live without access to basic services such as bank accounts (Instapay 2018; Pelletier, Khavul, Estrin 2014), significantly hampering chances for economic transformation and exacerbating social exclusion.[31] Digital financial services, often based on mobile phones, however, provide a viable solution for many.

Africa is the world leader in digital finance, with 14% of all Africans receiving money through mobile transfers (Akerele 2018, p. 4). However, the widespread trust in digital solutions for financial resources makes them attractive targets for cybercriminals, increases the threat of banking malware, and poses a real threat to developing countries. For example, of the top 10 countries (by share of users) attacked through banking Trojans, seven were in the Global South (Chebyshev 2019). Asia is one of the regions particularly plagued by mobile malware (Symantec 2018, p. 79), and a similar situation is visible in South Africa, where 47% of smartphone users fell victim to mobile cybercrime in 2013 (Symantec 2016, p. 8).

Cybercrime aimed at financial institutions and digital financial services is one of the greatest concerns in developing countries. Because of  their lower cybersecurity maturity level, banks in developing countries are targets, and they also create weaknesses in the global financial system.

[31] For instance, 70% of Latin Americans do not have a bank account; 60% of transactions made by SMEs are in cash.

Due to their participation in world-wide payment systems such as SWIFT, financial institutions operating in emerging nations can serve as gateways to banks in developed countries. Previously, to get to one of the major western banks, cybercriminals have penetrated institutions in Bangladesh, Vietnam, and Ecuador (CSIS, McAfee 2018, p. 10).

Cyberattacks on banks in the Global South could damage the finances of the banks in question, their customers, and also global finance more broadly. The attacks could cause reluctance among large financial institutions to interoperate with developing country firms which introduce higher risk (Schia 2017, p. 9). Being an outcast in the global financial ecosystem would equal further aggravation of economic problems for a developing country. The gravity of the potential consequences on whole national systems necessitates changes from the respective financial institutions, but also systemic actions in governance to enforce the implementation of the appropriate security standards.

Apart from the immediate financial loss, cybercrime undermines the reputation of the targeted organisation. Customers may lose trust in the bank, but also in the technologies, which may result in slower digital transformation and development delays. Afraid of falling victim one way or the other, clients may choose to withdraw their assets 'and place them under the proverbial mattress, thereby further hurting the global financial system and markets' (World Bank 2017, p. 91). Cyberattacks targeting the client information stored and processed by financial institutions can have an equally devastating impact on economies: for instance, this can lead to lowered credit scores, reduced investment rates in developing countries, and regulatory fines and litigation for businesses (World Bank 2017, p. 91). It can also hamper the development and use of mobile financial services enabled by ICT systems. This can translate into negative consequences for the economic inclusion of the poorest.

### 2.2.5 Digital infrastructure evolution

The evolution of digital infrastructure in developing countries will have a significant impact on security. Older generations of wireless networks, widely used across developing countries, are technically more susceptible to cyberattacks (Shaik; Seifert, et al. 2016).[32] With the shift towards broadband networks, the nature and magnitude of cyberthreats will evolve, keeping pace with technological progression, and facilitating the growth of various forms of abuse (Kshetri 2010, p. 1063), including increased botnet activity. Better network quality translates to more potent attacks, and more attractive and higher value targets, and therefore new opportunities for criminals.

As discussed earlier, technological development will soon bring a large IoT presence. In this context, potential attacks could be devastating for entire economies – and may even have global consequences. Developing countries must strengthen their systems to avoid being used as targets and instruments for attacks on the global digital infrastructure. Some of the problems

[32] For instance according to the GSMA in 2015, 77% of Sub-Saharan Africa's mobile connections were on 2G, 22% were 3G and just 1% was made up of 4G connections (Gilbert 2018).

are surfacing today: China is the home of the highest number of botnet-forming IoT devices, by a large margin (Symantec 2018, p. 80). Recently, Brazil experienced significant botnet activity being used to hijack traffic meant for banks operating in this country (Cimpanu 2018). Challenges related to security standards may require governance negotiations and decisions at the highest political levels.

### 2.2.6 Illicit financial flows and cybercrime

Developing countries' cybercrime and economic problems are intertwined. Any analysis of the economic impact of cybercrime must encompass a discussion on organized criminal groups  and illicit financial flows (IFFs) – the phenomenon described as 'a key development challenge'. IFFs are defined as 'money illegally earned, transferred or used that crosses borders' (World Bank 2017a).

IFFs have negative effects on national economies, especially in developing countries. Some estimates say that about US$1 trillion flows out of emerging markets and developing countries annually, without a trace (Global Financial Integrity 2014), with corruption, crime, and tax evasion being key drivers. The value of IFFs into and out of developing countries represented, on average, more than 20% of developing countries' trade with developed countries between 2006 and 2015. Financial losses are therefore direct, as for every dollar that is illegally transferred to a different country, a proportion could have been gained as tax revenues on imports or exports and related corporate income taxes. This drains public resources that could have otherwise contributed to sustainable economic growth. They might, for instance, have led to jobs creation and inequality and poverty reduction (Global Financial Integrity 2019).

New technologies can significantly influence all activities that fall into the category of IFFs. They are becoming a significant 'cross-cutting factor' that enables other illegal activities. Traditional organized criminal groups, in developing countries and elsewhere, progressively engage in cyber activities and facilitate fraud, corruption, tax evasion, and other crimes.[33] The anonymity, complexity and frequent lack of regulations in the digital space (as observed in the intrinsic features of the Darknet, cryptocurrencies, gambling services, and so on) benefit criminals, enabling money transfer, money laundering, and the trade of illicit goods (Tropina 2016, p. 1). IFFs are becoming inseparably connected with cybercrime, creating a complex and thriving illegal digital economy. Simple countermeasures will not be sufficient to solve such complex, multifaceted issues. Whole-of-government and international strategies must be applied to combat these challenges.

[33] In general, organized criminal groups  show increasing interest in cybercrime, and are also professionalising their activities. West African criminal groups have a long tradition with perpetrating unsophisticated social engineering frauds known as Nigerian email scams, which have now vastly increased in maturity. Phishing campaigns called BEC (Business Email Compromise) are on the rise and, as they target larger organisations, cause significant financial losses. At least US$3 billion have been lost to BEC scams in the past three years, with more than 22,000 victims globally (Trend Micro, Interpol 2017).

# 3. Development by digital pragmatism

## 3.1 From digital optimism to pragmatic actions

Cybersecurity must be treated as a precondition for digital revolution; this is far easier said than done. Security measures, in their broader sense, include not just technical, but also organisational and regulatory efforts. Establishing optimal cybersecurity is a multistakeholder task, but strong governmental engagement is essential. Successful and effective outcomes will also rely on international harmonisation of cybersecurity approaches and co-ordinated actions. If developing countries want to avoid the mistakes made by earlier technology adopters, they need to implement a wide range of actions from the outset.[34]

As discussed in the Introduction, after a period of 'digital optimism' in developed countries during the first decades of internet uptake, many moved towards 'digital realism' defined by increased interest in cybersecurity needs and solutions at a national and international level. While many digital realist endeavours have been successful, others were contaminated with errors and imperfections.

Because developing countries often have very limited resources, cybersecurity initiatives must be as efficient and cost-effective as possible. These countries have a lack of funds for programmes to cover fundamental cybersecurity capabilities. Also, businesses show a limited interest in investing in and implementing cybersecurity measures (Pijnenburg Muller 2015). Security is often not the first choice for expense allocation. Therefore, decisions must be thought out carefully and focus on priority areas. Developing countries cannot afford to waste resources on mechanisms that are inefficient or ineffective, as often observed in developed countries' processes.[35] This is one reason why developing countries should not simply transplant approaches that exist in Western countries, but instead work to tailor solutions to their needs.

An important feature of digital optimism was the almost unlimited trust in the opportunities brought by digital technologies. Digital realism, on the other hand, is much more sceptical and distrustful, which often leads to overly pessimistic assessments (see the Introduction). In the long term, this may slow down digital development and economic growth. In contrast, this chapter proposes a 'digital pragmatism', which promotes a rational awareness of both the opportunities and threats stemming from cyberspace, and judicious usage of new technologies, which can strongly enhance the cybersecurity landscape. All states, societies and economies must make the most of existing and emerging technologies. This can be done if a cybersecurity-by-design approach is applied by all relevant stakeholders, both at the national and international level.

[34] Or in many cases, as their digital revolution has already begun, from the early stages.

[35] Numerous reports, analysis point out that choices regarding the cybersecurity measures should be based on better analysis and risk assessment. See for instance Bradley 2019; Ashford 2019; Ponemon Institute LLC 2017.

## 3.2 National cybersecurity strategies and legal frameworks

Developing countries should build their cybersecurity ecosystem and governance structures on effective national strategies, which put cybercrime countermeasures at the top of the agenda. The development of their strategy should be accelerated and formulated on the basis of the best practices and existing guidelines.[36] This will set the tone for the strategic actions and decisions and send a strong message of determination and decisiveness in fighting cybercrime. A well-prepared and properly implemented strategy will also signal to business partners and international organisations that a country is ready to provide a safe environment for commercial projects and investments.[37]

A national strategy will provide a broad framework for a cybersecurity ecosystem, including governance structures. It should therefore be followed by concrete legal actions and capacity-building initiatives that will lead to actual changes. Legal measures should be established and implemented across criminalisation, procedural powers, jurisdiction, international co-operation, personal data protection. These must be treated as a priority by developing country governments.[38]

Luckily, noteworthy international efforts to establish such methods are underway. These should be drawn from and used as valuable benchmarks. In recent years, numerous national and international legal mechanisms have been developed, which can operate at a global scale. UNODC points out five main legal frameworks to facilitate international co-operation (UNODC 2013, p. XIX):

- Council of Europe Convention on Cybercrime (the Budapest Convention on Cybercrime)

- Commonwealth of Independent States' Agreement on Cooperation in Combating Offences related to Computer Information

- African Union Convention on Cybersecurity and Personal Data

- League of Arab States Convention on Combating Information Technology Offences

- Shanghai Cooperation Organisation Agreement on Cooperation in the Field of International Information Security.

Even though those frameworks have common areas, significant discrepancies can be observed, for instance, regarding the criminalisation of various acts, such as 'spamming'.[39] The distribution of spam emails can be treated as a criminalised act in one country but not in the other. Such fragmentation risks undermining governments' ability to effectively tackle cross-border crimes.

[36] For instance, ITU's Guide to Developing a National Cybersecurity Strategy, ENISA's NCSS Good Practice Guide.

[37] One good recommendation for developing countries is to precede strategic actions and priorities with a solid risk assessment process. This will allow them to deal with the most pressing problems as well as allocate resources in reasonable ways.

[38] Solid legal solutions related to personal data protection may significantly help to combat data-related threats

[39] Apart from fragmentation, lack of universal application poses a significant challenge. Only 82 countries signed one (or more) multilateral documents and therefore entered into international agreements.

For this reason, developing states and the international community must have legal interoperability in mind when creating new solutions or amending existing ones. This is not an easy task, not least because different societies have distinct cultural factors that affect their legal system and approaches to issues such as privacy. It is in the joint interest of all parties to find a consensus and harmonise approaches (UNODC 2013, p. XIX). Many proposals on how to overcome such differences  are worth considering. For instance, one study suggests the creation of international model provisions on criminalising core cybercrimes, investigative powers, jurisdiction, and cross-state co-operation for electronic evidence (UNODC 2013, pp. XIII–XV).

As new legal challenges appear, finding a compromise will be even more important. There are already some burning issues that will certainly become subjects of international negotiations – for example, cross-border access to electronic evidence (European Commission 2018). Some mechanisms to harmonise policies exist in Africa, and these can be extended to cover cybercrime fighting. For instance, the Economic Community of West African States (ECOWAS) conducts an initiative that aims to collaborate on jointly agreed strategies and policies, including development of telecom-related decisions (AU-EU DETF 2019, p. 59). Such projects can cover cybersecurity and anti-crime measures, and be replicated or adapted in other regions.

Negotiations for the alignment of existing cybersecurity solutions, their evolution, or the development of new ones, require a very pragmatic design process. One important factor is that the design should be inclusive from the outset: developing countries must be at the heart of this discussion, shaping outcomes alongside developed states. Involving developing countries in this process increases the chances of wider acceptance and better implementation. Policymakers are more likely to believe in the potential benefits if their country helped to shape the agreement.[40]

While making international cybersecurity efforts, it will also be important to focus on small steps and agree on common points of interest. All-inclusive international agreements will be hard to achieve, so separating the issues into smaller elements may bring better results, at least in the short term. This approach can be applied, for instance, to achieving consensus on norms of responsible state behaviour in cyberspace, currently being discussed at the UN. Agreeing on basic common denominators can be a good starting point for other decisions. Basic 'islands of consensus' can serve as starting point for further successful achievements. That may sound less ambitious than aiming at a holistic solution right from the beginning, but in reality, it is more feasible and thus more likely to yield better results.

While setting the legal framework, neither individual states nor the international community should start from scratch. Actions should be guided by proven and well-functioning examples. Of the international frameworks, the Budapest Convention – the first anti-cybercrime instrument – is considered to be very comprehensive, the only truly 'global' (World Bank 2017, p. 196), and the most useful framework (UNODC 2013, p. XIII). It has had a strong impact on the cybersecurity landscape and can serve as an inspiration for countries seeking their own solutions.[41]

[40] The pro-inclusiveness argument can be used as a political strategy to redesign solutions, or to open up discussion for new instruments that are not necessarily needed (the case of the new resolution adopted by the UN General Assembly which aims to create a new anti-cybercrime treaty).

[41] The Budapest Convention has had an impact on legislation, even in those states that chose not to ratify it. An example of a regulation concerning personal data protection is the EU GDPR.

As mentioned earlier, a lack of inclusiveness while negotiating legal solutions may hamper their acceptance. Many developing countries have been reluctant to sign up to the Budapest Convention: this can be explained, at least in part, by their lack of influence over its terms, along with differing understandings of cybercrime challenges. However, the reluctance of some countries could be overcome by highlighting the benefits of a more harmonised approach, and by offering additional inclusive proposals. Greater inclusiveness can be achieved through wider participation in the evolution of the treaty – for instance, in negotiations of potential additional protocols (Seger 2016).

The discussion on the usability of existing solutions and their inclusiveness is more important than ever: we are at a pivotal moment, where voices favouring the development of new cybersecurity tools are gaining traction. The UN General Assembly recently approved a resolution that aims to create a new anti-cybercrime treaty. The resolution was backed by Russia, a country which – among others – has offered an 'inclusiveness' argument to justify the need for a global treaty. The resolution was supported by many developing countries. Many human rights groups and civil society organisations warn that the creation of a completely new legal solution may have some negative consequences, not least that it may enable governments to maintain stricter control over citizens that go online to exercise their rights, curtailing freedom of speech (Vavra 2019). Others argue that the development of a completely new tool is not needed, and that it would be better to work on existing frameworks to make them more inclusive.

Developing countries must put human rights at the heart of the process of creating legislative measures. Aside from the obvious ethical reasons, respecting human rights is also in a country's interest for pragmatic reasons because developing countries must create a favourable environment for international businesses and investors, as well as a good public image. Solid legal safeguards (for instance, privacy protection) must be built in at various levels, explicitly in relation to the private sector, and most notably, internet service providers.[42] Building transparent, trust-based, and trust-inducing collaboration mechanisms is key.

However, even the most solid legal frameworks will not be a deterrent if there are no resources to effectively execute the provisions. Developing countries must overcome resource and capability constraints among law enforcement authorities, prosecutors and the judiciary. Therefore, capacity-building programmes must be developed and enhanced, both at multilateral and bilateral level (World Bank 2017, pp. 246–249). Transfer of knowledge and skills, training, and technical equipment are essential.[43] This is an area where international support for developing countries is especially necessary. It can have different forms, including financial and logistical support, and providing advice, among others.

### Building resilience

To build resilience and thereby diminish the consequences of cybercrime, a legal framework should go beyond the creation of substantive and procedural legal provisions. Countries should focus on ensuring that the vital elements of their functioning are well protected against hostile cyber incidents, including cybercrime. A good practice here is to focus on critical sectors – identifying the

[42] Internet service providers hold reams of data that can serve as e-evidence and affect attitudes towards privacy.

[43] Especially building capabilities in the field of digital forensics should be treated as priority.

most valuable entities that provide critical services or functions, and making sure that these entities are implementing appropriate cybersecurity measures, according to international standards.[44] This model is currently implemented in the EU. The NIS Directive requires member states to identify operators of essential services, who are obliged to introduce cybersecurity measures according to the outcome of the risk assessment process.[45] The main rationale behind those actions is to make sure that at least the most valuable entities are protecting themselves from cyberthreats. This usually gives public actors corrective instruments that can be used if the operator of the services is not compliant. This approach can be considered by developing countries.

## 3.3 Combatting cybercrime with countermeasures and new technologies

In the face of ever-evolving technological challenges, more flexible and dynamic forms of action must be promoted. For instance, to facilitate the work of law enforcement authorities operating in different countries, it would make sense to further develop and enhance existing networks of 24/7 points of contact; they bring faster response times, greater agility, and contribute to better co-operation and cybercrime problem-solving. Developing countries should actively participate in such initiatives.[46] In terms of government and private sector co-operation, the work of worldwide Information Sharing and Coordination Centres should be put to more extensive use by countries in the Global South (World Bank 2017, pp. 209-215).

Very often, effective anti-cybercrime actions can be significantly better enforced when accompanied by the use of new technologies. The digital pragmatism recommended in this paper promotes the use of smart tactics, targeted at the most pressing problems, to increase the effectiveness of the fight against cybercrime. As we have noted, cybercrime currently facilitates a whole criminal ecosystem, with organized criminal groups  and IFFs at its core. This complex environment consists of actors, relations, services, mechanisms, tools, and markets that interact and influence each other (McGuire 2018, pp. 13-14).

For those with limited resources, interrupting critical chains of the cybercrime economy may be a productive route in tackling cybercrime. Eliminating these critical junctures may strongly affect the whole system. For instance, the three main online criminal markets taken down during an international operation – AlphaBay, RAMP, and Hansa (Europol 2018, p. 47) – accounted for

[44] Many examples of those can be given, for instance: ISO 27001, COBIT, NIST Cybersecurity Framework.

[45] The NIS Directive covers the following sectors: energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

[46] 24/7 points of contacts are designated by various countries to provide constant assistance in case of investigations related to the cybercriminal offences. They are operational 24 hours per day, 7 days per week. Various international initiatives call for the establishment of these points of contact, for instance:  article 35 of the Budapest Convention (see more: 24/7 Points of Contact under the Convention on Cybercrime)  or the G7 24/7 High Tech Crime Network (see more: Ott 2018).

87% of all Darknet activity (Chainalysis 2018, p. 4).[47] Moreover, just a few 'mixers' (services that make cryptocurrency transactions harder to track) and gambling sites accounted for 97% of Bitcoin laundering on these platforms (Fanusie, Robinson 2018, p. 11). These two examples of crime concentration confirm that, if entities involved in combatting cybercrime prioritise strategic avenues, the results can be significant. It is therefore important to conduct multidisciplinary analysis on cybercrime value chains to choose the most effective strategy and tools. This must be done in a co-ordinated manner, with the participation of partners from other countries, academia and international institutions. Having identified critical aspects of the cybercrime chains, it will be possible to implement purpose-built, targeted countermeasures.

Existing and emerging technologies may be very useful in identifying these critical points within the cybercrime ecosystem. For instance, big data analytics (BDA) serve as important and increasingly indispensable mechanisms that enable the detection and disruption of financial crime and, broadly speaking, IFFs (Tropina 2017, p. 47). With the exponential growth of electronic transactions and the increasingly high volumes of unstructured data, BDA is becoming the weapon of choice for those who combat financial crime (Deloitte 2014, p. 5). It provides users with an ability to process huge amounts of data, examine nonlinear datasets, reveal or anticipate crime patterns, and link together seemingly unconnected information (Tropina 2017, p. 47). It also allows users to identify potentially illegal behaviour, understand it better by analysing relationships between parties, and make predictions (Deloitte 2014, p. 5). Interestingly, BDA is also very useful in detecting new types of payment abuse, especially those involving blockchain-based cryptocurrencies. Even though blockchain offers a great degree of anonymity, big data analysis enables tracking and matching of various information to better understand the transactions (Tropina 2017, p. 48). Whenever possible, the implementation of BDA instruments ought to be done in a co-ordinated manner, using international platforms and co-operation programmes, as it significantly increases the effectiveness of those actions.

AI and Machine Learning (ML) can be used to increase the efficiency of BDA, but they also have significant potential to increase other cybersecurity measures. Multimedia analytics and predictive policing are examples given by Europol (Europol 2019).[48] AI and ML can be very helpful in combating for instance spam, identifying vulnerabilities, and suggesting fixes. They can predict new threats and malware on the basis of existing patterns and help to spot insider threats by using behaviour analytics (Zinatullin 2018). In general, AI and ML can significantly contribute to better effectiveness of security teams. In the face of specialist staff shortages, especially in developing countries, those advancements may be very important.

[47] Those successful operations did not solve the problem. Criminals migrate to other markets, as new fora are cropping up constantly and taking place of those seized. Still, this shows that some elements within an ecosystem are pivotal and dealing with them strongly enhances the cybercrime fight.

[48] However it must be underlined that this proactive orientation seems to be a matter of extremely severe ethical and legal concern. See, for instance, The Guardian (2019).

Adding to the discussion on anti-organized criminal groups measures, especially those targeting digital financial services, attention must be paid to the possibilities of leveraging existing aid programmes. International programmes for financial inclusion of developing countries should have cybersecurity aspects embedded into their DNA.[49] This would allow use of these programmes to shape the financial systems in developing countries with cybersecurity by design and by default.

## 3.4 Strengthening the human factor in cybercrime prevention

The best way to deal with cybercrime is to focus on prevention. Many of the problems that foster criminal activities – for instance, social engineering – can be eliminated with human-centric efforts. The human factor is a key element of this strategy and requires the implementation of various educational efforts organised mainly at the governmental level.

Two approaches are particularly relevant for developing countries:

- Protect cybercrime targets by enhancing their security level through knowledge and skills – governments must establish cybersecurity-related programmes as well as weave cybersecurity aspects into the educational system.

- Eliminate the problem by preventing potential offenders from committing cybercrime.

### 3.4.1 Education

It is a widely held conviction that cybersecurity should be mainstreamed into general educational programs – this must be treated as a key task for governmental bodies responsible for setting up educational frameworks (European Commission 2017, p.10; Ghernaouti, Wanner 2018, p. 540). Creating cybersecurity curricula based on well-functioning, globally recognised standards would be a good start for developing countries.[50]

The international community – and especially developed countries with a wealth of experience – should actively support such endeavours. While international expertise will be crucial, these programmes must be tailored to local contexts and language environments. For instance, since

[49] For example, the Financial Inclusion Global Initiative by the World Bank Group, ITU, the Committee on Payments and Market Infrastructure with support of the Bill and Melinda Gates Foundation. It is also worth  paying attention to the activities of the Global Forum for Cyber Expertise.

[50] Various sources include: Cybersecurity Curricula 2017 Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. A Report in the Computing Curricula Series. Prepared by: Joint Task Force on Cybersecurity Education; Cybersecurity Reference Curriculum prepared by Partnership for Peace Consortium Emerging Security Challenges Working Group; Cybersecurity Education Training Assistance Program funded by DHS.

Africa has the lowest average access to higher education, its cybersecurity programmes should be targeted at primary and secondary level (AU-EU DETF 2019, p. 31-33). It should be governments' responsibility to build tailored educational proposals to tackle these priority areas.

Decision-makers must anticipate potential negative trends – for instance, related to gender imbalances – when deploying targeted programmes. Finding solutions to such issues will help to avoid societal problems in the future. For instance, research shows that women in Africa are much less likely to use the internet than men (AU-EU DETF 2019, p. 30). The assumption may be that women should not be prioritised as recipients of cybersecurity programmes. However, the wider picture shows that the digital exclusion of women disrupts society and the economy (Women in Digital 2019; Iclaves, SL. 2018). Female digital inclusion is also important to achieving the SDGs. With little experience of technology, women joining the digital world may become easy targets for criminals. This gender-weighted issue should be addressed by designing educational programmes in a very inclusive way, crafted and directed specifically at target groups.[51] Existing and future national and international educational programmes must treat such inclusive programmes as a priority.

Strained financial situations in developing countries may hamper educational efforts: budgetary limitations often do not allow for the creation of solid educational programmes. Once again, technology may help. Although internet access remains limited in many developing countries, where it is available, e-learning may be a good avenue for skills development, at least for some recipients, such as students living in urban areas. There are several examples of free online study programmes, such as Massive Open Online Courses, the Virtual University of Senegal, and the ITU Academy (AU-EU DETF 2019, p. 34; p. 62; p. 63). Such courses may be further enriched with ICT security topics and offered to local communities. Informal methods of gaining knowledge, for instance courses offered by non-governmental organisations (NGOs), development aid agencies and other initiatives also play a significant role. Cybersecurity workshops can also be provided with the help of private companies: special fiscal incentives offered by governments may help to encourage this (AU-EU DETF 2019, p. 36). While these alternative routes may be helpful in spreading knowledge of cybersecurity, formal educational initiatives will remain crucial to cybersecurity education for the wider population.

### 3.4.2 Prevention

The second human-oriented strategy is the implementation of pragmatic preventive policies designed both at the state level and through bottom-up initiatives. For example, awareness-raising campaigns and prevention programmes are important in fighting cybercrime, to prevent potential offenders from engaging in online criminal activity. The key is to make these programmes effective, shrewdly crafting them to target well-identified and susceptible societal groups. It is possible to create 'typical offender' profiles, which consider parameters such as age, education level, and so on. (UNODC 2013, p. 40; p. 42). Programmes tailored to those groups may be a solution for desirable outcomes, and to help manage limited resources. Decision-makers may initiate programmes that will examine which societal groups are most likely to fall into crime, and prepare preventive programmes accordingly.

[51] Inspirational examples include South Africa (VVOB Education for Development 2016)

## 3.5 Technology providers' responsibilities: secure by design and default

Cybersecurity issues are, to a great extent, caused by technological imperfections. Eliminating or reducing these can lead to very positive and effective  outcomes. ICT vendors should understand that building their products and services in line with the principles of security by design can have significant impacts on the cybersecurity landscape.[52] National and international bodies must strongly call on the industry to make a much greater effort to bring secure products to the market. There is also room for other actors. For instance, universities may strongly contribute to development of new, secure-by-design technologies by specially funded research and development programmes.

Various instruments may be applied: some will support regulatory top-down interventions that would enforce higher levels of cybersecurity; some will support a more voluntary approach (driven from the bottom up). There are helpful precedents. In terms of governance decisions, the EU Cybersecurity Act deserves special attention as it establishes a voluntary EU certification framework for ICT digital products, services and processes, with the potential to increase transparency among customers. It also encourages vendors to provide more secure solutions. As for bottom-up, industry-led efforts, numerous international initiatives have been developed, including the Charter of Trust and the Cybersecurity Tech Accord.

Developing countries may actively contribute to these projects, but they can also influence their ecosystem by simply demanding and choosing secure solutions from their vendors – which need to be provided at affordable prices. Perhaps this may sound unrealistic, but paradoxically, the unprecedented technological rivalry between great powers may actually create a convenient moment for developing countries to negotiate good terms, and boost cybersecurity. As the main players seek to maintain or increase their technology-related influence, this can be used to strengthen the position of developing countries.

Technology providers should be chosen according to their security standards.[53] Ensuring that security measures are locked in from the very beginning of the product life cycle – rather than retrofitting them – can vastly improve the cybersecurity landscape, both in developing countries and across the globe. While negotiating the terms of co-operation also other elements can be taken into the consideration, including important functions such as portability and interoperability.

As many developing countries are at the start of building technological foundations, they can turn these nascent stages of digitalisation into an advantage. For instance, they can build digital infrastructure with more secure solutions from the start. For example, while encryption may

[52] Security by design is an approach applied in every phase of the Software Development Life Cycle, aiming to significantly boost its cybersecurity. The approach minimises the number and severity of vulnerabilities and reduces the attack surface. More information about the process can be found in, for example, the Security-by-Design Framework prepared by the Cyber Security Agency of Singapore. A variety of good practices on the topic exist – for instance, ENISA's recommendations on a secure-by-design IoT (ENISA 2019).

[53] Public procurements in this context serve as a very powerful tool.

hamper law enforcement efforts, it can upgrade cybersecurity for legitimate users, increasing the confidentiality of valuable personal and business data. Encryption protocols may be included as obligatory standards during the upcoming 5G standardisation process (Europol 2019, p.12). For developing countries, these issues can bring opportunities. When building or developing telecommunications infrastructure, they can choose solutions with a higher level of security embedded, helping to eliminate various security problems from the outset. This opportunity was not at the disposal of developed countries some years ago. It will, however, require decisive governance actions at both national and international levels.

Building a healthy digital backbone, demanding security from ICT vendors, setting the rules which promote responsible behaviours – all form a strategy that developing countries ought to apply and that the international community should support. Global determination and co-ordination oriented at setting high cybersecurity standards has a real chance to bring significant results.

## Conclusion: The future of cybersecurity is here

Effectively fighting cybercrime in developing countries is a global, shared responsibility for political, governmental, and business leaders, academia, civil society as well as NGOs. It requires bold, pragmatic, multidimensional decisions and strategic, innovative actions. It is crucial to understand that it is not only the security and well-being of developing countries that is at stake – cybersecurity is a global issue.

Political leaders in developing countries and world-wide must create thriving cybersecurity ecosystems that will enable the efficient prevention and combatting of cybercrime. Secure, inclusive, and accessible cyberspace serves as a very important ingredient for the achievement of the SDGs. Woven into the fabric of developing countries' digital future, cybersecurity must be seen as a precondition of economic success as well.

Developing countries will continue their digital journey, and they will rightly do so according to their own designs and trajectories. Yet, building cybersecurity will be a co-ordinated effort, and partnerships will be necessary. Therefore, it is the Global North's responsibility to support developing countries in their efforts. All development assistance programmes that include digital aspects need to have firmly embedded cybersecurity elements. Moreover, projects directly targeted at cybersecurity must be reinforced. To significantly help to overcome skill shortages in developing countries, these could include cybersecurity training, educational programmes, best practice transfer, technological aid, and other initiatives. Those in the Global North should not underestimate the importance of such projects: the security of the developing world is a prerequisite for the security of the developed world.

The days when security was solely a responsibility of the public sector are long gone. Today, multistakeholder efforts are indispensable and private companies, especially ICT vendors, have an essential role to play. As they provide the backbone infrastructure, products and services, the strength of cybersecurity foundations increasingly depends on them. Their engagement and 'secure-by-design' approach is central to the challenge of enhancing cybersecurity in the contemporary world.

Abraham Lincoln once said, 'you cannot escape the responsibility of tomorrow by evading it today'. Humankind reaps enormous dividends from digital development, and the potential for future benefits is limitless, but to make it last, pragmatic cybersecurity responsibility must be taken today.

# References

Akerele, T. (2018). Cyber threats on African subjects. International Institute for Counter-Terrorism [online] Available at: https://www.ict.org.il/AboutUs.aspx#gsc.tab=0.

Armerding, T. (2018). The 18 biggest data breaches of the 21st century. CSO [online] Available at: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

Ashfordt, W. (2019). Businesses investing blindly in cyber security. [online] Available at: https: //www.computerweekly.com/news/252464501/Businesses-investing-blindly-in-cyber-security.

AU-EU Digital Economy Task Force. (2019). New Africa-Europe Digital Economy Partnership. [online] Available at: https://ec.europa.eu/digital-single-market/en/news/new-africa-europe-digital-economy-partnership-report-eu-au-digital-economy-task-force.

Batt, S. (2018). What Is a "Banking Trojan?" [online] Available at: https://www.maketecheasier.com/what-is-banking-trojan/

Batt, S. (2019). The Rise of IoT Botnets (And How to Protect Your Smart Devices). [online] Available at: https://www.makeuseof.com/tag/internet-of-things-botnets/

BBC. (2019). Ransomware hits Johannesburg electricity supply. [online] Available at: https://www.bbc.com/news/technology-49125853.

BCG. (2012). The Internet economy in the G-20. [online] Available at: http://image-src.bcg.com/Images/The_Internet_Economy_G-20_tcm9-106842.pdf

Beer, J. (2018). "WannaCry" ransomware attack losses could reach $4 billion. CBS News [online] Available at: https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/

Bradley, T. (2019). The Standard Cybersecurity Model Is Fundamentally Broken. Forbes, 7 October, 2019 [online] Available at: https://www.forbes.com/sites/tonybradley/2019/10/07/the-standard-cybersecurity-model-is-fundamentally-broken/#5160901d1189

BSA. (2016). BSA Global Software Survey. [online] Available at: http://globalstudy.bsa.org/2016/index.html

Businesswire. (2019). Juniper Research: Retailers to Lose $130bn Globally in Card-not-Present Fraud Over the Next 5 Years. [online] Available at: https://www.businesswire.com/news/home/20190102005011/en.

Carr, J. (2009). Inside Cyber Warfare: Mapping the Cyber Underworld. The United States of America: O'Reilly Media.

Cimpanu, C. (2018). Gigantic 100,000-strong botnet used to hijack traffic meant for Brazilian banks. ZDNet [online] Available at: https://www.zdnet.com/article/gigantic-100000-strong-botnet-used-to-hijack-traffic-meant-for-brazilian-banks/

CCDCOE. Cyber security strategies. [online] Available at: https://ccdcoe.org/library/strategy-and-governance/?category=cyber-security-strategies&region=europe

Chainalysis. (2018). The changing nature of cryptocrime. [online] Available at: https://blog.chainalysis.com/reports/report-the-changing-nature-of-cryptocrime.

Chebyshev, V. (2019). Mobile malware evolution 2018. Kaspersky [online] Available at: https://securelist.com/mobile-malware-evolution-2018/89689/

Chong, J. (2013). Why Is Our Cybersecurity So Insecure? The New Republic [online] Available at: https://newrepublic.com/article/115145/us-cybersecurity-why-software-so-insecure.

Cloudflare. What Is A Malicious Payload? [online] Available at: https://www.cloudflare.com/learning/security/glossary/malicious-payload/

Convention on Cybercrime (Art. 35) Extract: 24/7 Points of Contact under the Convention on Cybercrime. [online] Available at: https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/24%207%20567%2024-7%20text%20ets_en.pdf

Criminal Lawyer Group. [online] Available at: https://www.criminallawyergroup.com/the-evolution-of-cybercrime-from-past-to-the-present/

CSIS., McAfee. (2018). Economic Impact of Cybercrime – No Slowing Down. CSIS [online] Available at: https://www.csis.org/analysis/economic-impact-cybercrime

Cyber Security Agency of Singapore. (2017). Security-by-Design Framework. Version: 1.0. Singapore: Cyber Security Agency of Singapore.

Deloitte. (2014). Insight on financial crime: Challenges facing financial institutions. Deloitte [online] Available at: https://www2.deloitte.com/sg/en/pages/financial-advisory/articles/our-strategic-approach.html

Department of Homeland Security (2019) National Initiative for Cybersecurity Careers and Studies (NICCS), Cybersecurity in the Classroom. [online] Available at: https://niccs.us-cert.gov/formal-education/integrating-cybersecurity-classroom

ENISA. (2019). Good Practices for Security of IoT. Secure Software Development Lifecycle. ENISA [online] Available at: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

ENISA. National Cyber Security Strategies (NCSSs) Map. [online] Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

European Commission. (2013). Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.

European Commission. (2015). A Digital Single Market Strategy for Europe. COM(2015) 192 final

European Commission. (2017). Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. JOIN (2017) 450 final

European Commission. (2018). Proposal for a Regulation of the European Parliament and of the Council on  European Production and Preservation Orders for electronic evidence in criminal matters. COM(2018) 225 final

European Commission. (2019). Digital Single Market, Women in Digital Policy [online] Available at: https://ec.europa.eu/digital-single-market/en/women-ict

Europol. (2018). IOCTA 2018. [online] Available at:  https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

Europol. (2019). Do Criminals Dream Of Electric Sheep? [online] Available at: https://www.europol.europa.eu/newsroom/news/do-criminals-dream-of-electric-sheep-how-technology-shapes-future-of-crime-and-law-enforcement

Fanusie, Y.J., and Robinson, T. (2018). Bitcoin Laundering: an analysis of illicit flaws into digital currency services. Foundation for Defense of Democracies [online] Available at: https://www.fdd.org/analysis/2018/01/10/bitcoin-laundering-an-analysis-of-illicit-flows-into-digital-currency-services/

Field, M. (2018). WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled. The Telegraph, 11 October, 2018 [online] Available at: https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/

Foley, M. (2018). Microsoft bullish on Congress' inclusion of CLOUD Act in funding bill. ZDNet, 22 March, 2018 [online] Available at: https://www.zdnet.com/article/microsoft-bullish-on-congress-inclusion-of-cloud-act-in-funding-bill/

Fruhlinger, J. (2018). What is ransomware? 4 steps to prevent these file-locking attacks. CSO, 20 December, 2018 [online] Available at: https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

Ghernaouti, S., Wanner, B. (2018). Research and Education as Key Success Factors for developing a Cybersecurity Culture. In: Bartsch, M., Frey, S. ed. (2018). Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden. Germany: Springer Vieweg.

Gilbert, P. (2018). 5G is coming, but 3G set to dominate in Sub-Saharan Africa. IT Web, 11 October, 2018 [online] Available at: https://www.itweb.co.za/content/lwrKxq3JjLbMmg1o

Gladyshev, P. Artificial Intelligence and cybercrime. Eolasmagazine, March 2018. [online] Available at: https://www.eolasmagazine.ie/artificial-intelligence-and-cybercrime/

Global Financial Integrity. (2014). Illicit Financial Flows. Analytical Methodologies Utilized by Global Financial Integrity. [online] Available at: https://www.gfintegrity.org/wp-content/uploads/2014/09/GFI-Analytics.pdf

Global Financial Integrity. (2019).  Illicit Financial Flows to and from 148 Developing Countries: 2006-2015 Illicit Financial Flows. [online] Available at: https://secure servercdn.net/45.40.149.159/34n.8bd.myftpupload.com/wp-content/uploads/2019/01/IFF-Report-2019_11.18.19.pdf?time=1579174517

Gold, J. (2019). Quantum computing will break your encryption in a few years. Network World, 20 March, 2019 [online] Available at: https://www.networkworld.com/article/3373550/quantum-computing-will-break-your-encryption-in-a-few-years.html

Goldberg, R. (2016). Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities. United States Department of Commerce, National Telecommunications and Information Administration [online] Available at: https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities

Greenberg, A. (2018). The Untold Story Of Notpetya, The Most Devastating Cyberattack In History. WIRED, 22 August, 2018 [online] Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Grimes, R.A. (2016). The bad guys are wreaking havoc. Why can't they be brought to justice? CSO, 6 December, 2016 [online] Available at: https://www.csoonline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html

Harrison, V., Pagliery, P. (2015). Nearly 1 million new malware threats released every day. CNN Business, 14 April, 2015 [online] Available at: https://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/index.html

HM Government (2016). National Cyber Security Strategy 2016-2021. [online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Hoog, A. (2015). Security Debt is the New Technical Debt. NowSecure [online] Available at: https://www.nowsecure.com/blog/2015/10/08/security-debt-is-the-new-technical-debt/

Hung, M. (ed) (2017). Leading the IoT. Gartner [online] Available at: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

Iclaves, S.L. and UOC (2018). Women in the Digital Age. SMART 2016/0025. Luxembourg: European Commission. [online] Available at: http://www.media2000.it/wp-content/uploads/2018/03/WomeninDigitalAgeStudy-FinalReport.pdf

Interpol. (no date) Cybercrime. [online] Available at: https://www.interpol.int/Crimes/Cybercrime

ITU. (2018). ITU releases 2018 global and regional ICT estimates. Press release, 7 December, 2018 [online] Available at: https://www.itu.int/en/mediacentre/Pages/2018-PR40.aspx

ITU. (no date) ITU Country ICT Data. [online] Available at: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

ITU. (no date) National Cybersecurity Strategies Repository. [online] Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

Joint Task Force on Cybersecurity Education. (2017) Cybersecurity Curricula 2017 Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. A Report in the Computing Curricula Series. [online] Available at: https://europe.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

Kelly, R. (2018). Encryption Services Hampering Law Enforcement. DIGIT [online] Available at: https://digit.fyi/encryption-services-nca-report/

Kessem. L., Korman. M. (2015). Meet the Pezão Trojan: Brazil's Got Malware. Security Intelligence [online] Available at: https://securityintelligence.com/meet-the-pezao-trojan-brazils-got-malware/

Khan, S., Loo, K-K., Naeem, T., Abrar Khan, M. (2008). Denial of Service Attacks and Challenges in Broadband Wireless Network. International Journal of Computer Science and Network Security. Vol. 8 No. 7

Kotadia, M. (2003). Report: a third of spam spread by RAT-infested PCs. [online] Available at: https://www.cnet.com/news/report-a-third-of-spam-spread-by-rat-infested-pcs/

Kshetri, N. (2010). Diffusion and Effects of Cyber-Crime in Developing Economies. Third World Quarterly. Vol. 31, Issue 7 pp.1057-1079 [online] Available at: https://www.tandfonline.com/doi/abs/10.1080/01436597.2010.518752

Lin, H. (2016). Attribution of Malicious Cyber Incidents. [online] Available at: https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf

Marsh, S. (2019). Ethics committee raises alarm over 'predictive policing' tool. The Guardian, 20 April, 2019 [online] Available at: https://www.theguardian.com/uk-news/2019/apr/20/predictive-policing-tool-could-entrench-bias-ethics-committee-warns

Mathews, L. (2017). NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million. Forbes, 16 August, 2017 [online] Available at: https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#2a60bbf94f9a.

McGuire, M. (2018). Into The Web of Profit. [online] Available at:  https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf.

McKinsey Global Institute. (2016). Digital Europe: Pushing the Frontier, Capturing the Benefits. McKinsey Digital [online] Available at: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-europe-realizing-the-continents-potential

Middleton, P., Tully, J., Kjeldsen, P. (2013). Forecast: The Internet of Things, Worldwide. Gartner Research, 18 November, 2013 [online] Available at: https://www.gartner.com/en/documents/2625419/forecast-the-internet-of-things-worldwide-2013

Nduati, H. (2018). Cybersecurity in Emerging Financial Markets. CCAP. [online] Available at: https://www.findevgateway.org/sites/default/files/publication_files/cybersecurity_in_emerging_markets_06-30_0.pdf

Olsson, E. (2019). Report: FIS warned to prepare for quantum threats. Bobs Guide, 5 December, 2019 [online] Available at: https://www.bobsguide.com/guide/news/2019/Dec/6/report-fis-warned-to-prepare-for-quantum-threats/

Ott, C. (2018). What You Should Know About The 24/7 Cybercrime Network. [online] Available at: https://www.dwt.com/files/uploads/documents/publications/What%20You%20Should%20Know%20About%20The%2024.pdf

Palmer, D. (2019). Mobile malware attacks are booming in 2019: These are the most common threats. ZDNet, 25 July, 2019 [online] Available at: https://www.zdnet.com/article/mobile-malware-attacks-are-booming-in-2019-these-are-the-most-common-threats/

Panda Security. Android devices 50 times more infected with malware compared to iOS. 14 January, 2019 [online] Available at: https://www.pandasecurity.com/mediacenter/mobile-security/android-more-infected-than-ios/

Partnership for Peace Consortium Emerging Security Challenges Working Group. (2016). Cybersecurity Reference Curriculum. [online] Available at: https://pfp-consortium.org/index.php/item/263-new-cybersecurity-curriculum-now-available

Pathways for Prosperity Commission. (2018). Digital Lives: Meaningful Connections for the Next 3 Billion. Oxford, UK: Pathways for Prosperity Commission

Pelletier, A., Khavul, S., Estrin, S. (2014). Mobile payment services in developing countries, Policy brief 89319. IGC. [online] Available at: https://www.theigc.org/wp-content/uploads/2017/08/Pelletier-et-al-2017-policy-brief.pdf

Phys.org. (2019). 30 years later, Berners-Lee sees mission to fix internet's ills. 5 March, 2019 [online] Available at: https://phys.org/news/2019-03-years-berners-lee-mission-internet-ills.html

Pijnenburg Muller, L. (2015). Cyber Security Capacity Building in Developing Countries. Policy Brief [15/20115] Norwegian Institute of International Affairs (NUPI). [online] Available at: https://www.files.ethz.ch/isn/190144/NUPI%20Policy%20Brief-15-15-Muller.pdf

Ponemon Institute LLC. (2017). The Cost of Insecure Endpoints. [online] Available at: https://www.absolute.com/media/1810/ponemon-cost-of-insecure-endpoints.pdf

Qualys. (2006). The Laws of Vulnerabilities: Six Axioms for Understanding Risk. [online] Available at: https://www.qualys.com/docs/laws-of-vulnerabilities.pdf

Reilly, M. (2007). Beware, botnets have your PC in their sights. New Scientist. Volume 196, Issue 2634, 15 December, 2007 [online] Available at: https://doi.org/10.1016/S0262-4079(07)63152-2

RiskIQ. (2019). The Evil Internet Minute 2019. [online] Available at: https://www.riskiq.com/infographic/evil-internet-minute-2019/

Sabarinath. (2019). Darknet Vs Dark Web Vs Deep Web Vs Surface Web — Different Parts Of The World Wide Web. Techlog 360 [online] Available at: https://techlog360.com/darknet-vs-dark-web-vs-deep-web-vs-surface-web/.

Schia, N.N. (2017). The cyber frontier and digital pitfalls in the Global South. Third World Quarterly. Volume 39, 2018 – Issue 5, 11 December 2017

Schwab, K. (2016). The Fourth Industrial Revolution: what it means, how to respond. World Economic Forum [online] Available at: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Scott, P. (2016). How much of a problem is cyber-crime in the UK?, Only 13% of cybercrime is reported. The Telegraph, 1 November, 2016 [online] Available at: https://www.telegraph.co.uk/news/2016/11/01/how-much-of-a-problem-is-cyber-crime-in-the-uk/

Seger, A. (2016). India and the Budapest Convention: why not? Contribution to CyFy 2016, New Delhi, 28 to 30 September 2016 [online] Available at: https://rm.coe.int/16806a6698

Serianu. (2017). Africa Cyber Security Report 2017. [online] Available at: https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

Shaik, A., Seifert, J., Borgaonkar, R., Asokan, N., Niemi, V. (2016). Practical Attacks against Privacy and Availability in 4G/LTE Mobile Communication Systems. In Proceedings of the 23nd Annual Network and Distributed System Security Symposium (NDSS 2016) [online] Available at: https://arxiv.org/pdf/1510.07563.pdf

Stuppy, R. (2019). Card-Not-Present Fraud is On the Rise: 5 Statistics to Prove It. BlueSnap, 14 June, 2019 [online] Available at: https://home.bluesnap.com/snap-center/blog/card-not-present-fraud-statistics/

Sullivan, B. (2007). Who's Behind Criminal "bot" Networks? University of Nebraska- Lincoln [online] Available at: https://www.unl.edu/eskridge/cyberbot3.htm

Świątkowska, J., Albrycht, I. (2019). The Future of 5G or Quo Vadis, Europe? The Kosciuszko Institute [online] Available at: https://ik.org.pl/en/publications/the-future-of-5g-or-quo-vadis-europe/

Symantec. AUC. (2016). Cyber Crime & Cyber Security Trends in Africa. [online] Available at: https://www.thegfce.com/initiatives/cybersecurity-and-cybercrime-trends-in-africa/documents/publications/2017/03/10/report-cyber-trends-in-africa

Symantec. (2018). Facts and figures, Internet Security Threat Report. [online] Available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

Toesland, F. (2015). Will Africa take the lead in the Internet of Things? [online] Available at: http://africanbusinessmagazine.com/sectors/infrastructure/will-africa-take-leadinternet-things/

Trend Micro, Interpol. (2017). Cybercrime in Western Africa: poised for an underground Market. [online] Available at: https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-africa.pdf

Tropina, T. (2016). Do Digital Technologies Facilitate Illicit Financial Flows? The World Development Report 2016. Digital Dividends. Background Paper. [online] Available at: http://pubdocs.worldbank.org/en/396751453906608518/WDR16-BP-Do-Digital-Technologies-Facilitate-Illicit-Financial-Flows-Tropina.pdf

Tropina, T. (2017). Big Data: Tackling Illicit Financial flows. In Atlantic Council & Thomson Reuters (Ed.). Big Data: A Twenty-First Century Arms Race. [online] Available at: https://www.atlanticcouncil.org/wp-content/uploads/2017/06/Big_Data_A_Twenty-First_Century_Arms_Race_web_0627_Chapter_4.pdf

UNODC. (2013). Comprehensive Study on Cybercrime. New York: UN

Vavra, S. (2019). The U.N. passed a resolution that gives Russia greater influence over internet norms. Cyberscoop, 18 November, 2019 [online] Available at: https://www.cyberscoop.com/un-resolution-internet-cybercrime-global-norms/

Verizon. (2018). Data Breach Investigations Report. [online] Available at: https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf. VVOB Education for development. (2016). Gender is an integral part of inclusive education in South Africa. [online] Available at: https://www.vvob.org/en/news/gender-integral-part-inclusive-education-south-africa

Warner, J. (2011). Understanding Cyber-crime in Ghana: A view from Below. International Journal of Cyber Criminology. Vol 5 (1)

Wired. (2014). Linux: Fewer Bugs Than Rivals. WIRED, 14 December, 2004 [online] Available at: https://www.wired.com/2004/12/linux-fewer-bugs-than-rivals/

Woo, S., Volz, S. (2019). U.S. Considers Requiring 5G Equipment for Domestic Use Be Made Outside China. Wall Street Journal, 23 June, 2019 [online] Available at: https://www.wsj.com/articles/u-s-considers-requiring-5g-equipment-for-domestic-use-be-made-outside-china-11561313072

World Bank. (2017). Combatting Cybercrime: Tools and Capacity Building for Emerging Economies. DC: World Bank and United Nations

World Bank. (2017a). Illicit Financial Flows (IFFs). Brief, 7 July, 2017 [online] Available at: https://www.worldbank.org/en/topic/financialsector/brief/illicit-financial-flows-iffs

World Bank. (2019). World Bank Country and Lending Groups. [online] Available at: https://datahelpdesk.worldbank.org/knowledgebase/articles/906519

World Economic Forum. (2017). Executive Briefing: The future of jobs and skills in Africa. Place: Publisher

Zinatullin, L. (2018). Artificial Intelligence and Cybersecurity: Attacking and Defending. Tripwire, 10 December, 2018 [online] Available at: https://www.tripwire.com/state-of-security/featured/artificial-intelligence-cybersecurity-attacking-defending/

BLAVATNIK
SCHOOL OF
GOVERNMENT

UNIVERSITY OF
OXFORD

Pathways
for Prosperity
Commission
*Technology &*
*Inclusive Development*