CYBERLAW

by CIJIC

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente.***

CYBERLAW

by CIJIC

EDIÇÃO N.º IX – MARÇO DE 2020

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

CYBERLAW

by CIJIC

CYBERLAW by CIJIC

EDITOR: NUNO TEIXEIRA CASTRO

SUPORTE EDITORIAL: EUGÉNIO ALVES DA SILVA e AFONSO FREITAS DANTAS

PRESIDENTE DO CIJIC: EDUARDO VERA-CRUZ PINTO

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

CYBERLAW by CIJIC

NOTAS DO EDITOR:

Globalização. Tecnologia e Inteligência artificial. Mobilidade organizacional e individual. Manipulação. A pandemia de Coronavírus. Hoje. O futuro.

Vivemos tempos “*estranhos*”. Acutilantes. Irresolutos. Contingentes. Exigentes. O “tema” que nos capta, quase em exclusivo, a atenção, desde o início do ano de 2020, é a pandemia de coronavírus. Aquela dinâmica, rotineira, até agora tida como “garantida” atravessa momentos de grande indeterminação. Hora a hora somos como que bombardeados com números esmagadores: de taxas mundiais galopantes de infectados, doentes em cuidados intensivos, de mortos. No passar deste tempo, diariamente, deambulámos entre um imoderado e célere na disseminação da infecção *versus* um vagaroso e fleumático passo na demonstração de resultados animadores no seu combate. O racional económico de «custo-benefício» geralmente revelaria a perigosidade associada à extrema cautela. Porém na questão, truncada, do coronavírus é diferente[1]. “*Achatar as curvas*”, “*Proteger os mais idosos e os mais vulneráveis*”, “*Suster a vaga de procura do SNS por forma a dar-lhe tempo para acudir às solicitações*”, mesmo que o custo seja o parar da Economia. Global. Entretanto o tempo continua o seu passo. Assim como a epidemia há-de passar.

[1] Cass Sunstein @ https://www.bloomberg.com/opinion/articles/2020-03-26/coronavirus-lockdowns-look-smart-under-cost-benefit-scrutiny

E, quando aí chegados, a questão resolutiva a colocar não deverá andar muito longe de um: "*Que mundo esperar do pós-covid19*"?

O avanço da tecnologia, combinando melhores recursos de *hardware* com inteligência artificial, aos quais o Homem socorre, permitiram sequenciar o genoma do COVID-19 em menos de um mês. A inteligência artificial, por exemplo, num contexto, global, de recursos exíguos tem sido testada para suprir lacunas críticas nos recursos de saúde, ajudando à racionalidade da decisão política, alavancando centros de inovação em inteligência artificial, robótica e automação em saúde. Na Ásia[2]. Por agora.

O mesmo avanço tecnológico, por sua vez, no actual cenário de "*guerra*" ao vírus, colocou a ponderação das liberdades fundamentais num estádio de confronto titânico. Recuperando o "*achatar a curva*", um pouco por todo o mundo, os governos, democráticos, colocaram os respectivos países em *lockdown*. Sem cautelas. Entre confinamentos e quarentenas obrigatórias, um recurso parece permitir - em face da falta de meios humanos para controlo efectivo de milhões de cidadãos - fiscalizar o cumprimento das directrizes estatais. A tentação executiva por esse controlo, universal, dos cidadãos preclude a fruição de múltiplas liberdades constitucionalmente consagradas. O racional da discussão que vinha sendo tido até agora[3], deslocou-se, por via do perigo abstracto que a pandemia comporta, da questão securitária *versus* liberdades fundamentais para "*saúde pública*" *versus* liberdades fundamentais.

Um pouco por todo o ocidente democrático, a tónica recursiva tem passado pelo uso da "*vigilância digital* estadual[4]". Tal como um pouco por todo o mundo, direitos humanos fundamentais[5] são colocados em teste face à imposição destas regras "excepcionais". O Estado de emergência tende a permitir, justificando múltiplas

[2] Eficiência, especialidade, racionalidade, sistemas capacitativos e colaborativos público-privados. O trabalho dos dados ao serviço dos povos. https://www.technologyreview.com/s/614555/ai-in-health-care-capacity-capability-and-a-future-of-active-health-in-asia/

[3] « Tribunal Constitucional chumba acesso das secretas a registos de comunicações», @ https://rr.sapo.pt/2019/09/19/politica/tribunal-constitucional-chumba-acesso-das-secretas-a-registos-de-comunicacoes/noticia/165164/

[4] Por exemplo: https://www.wsj.com/articles/europe-tracks-residents-phones-for-coronavirus-research-11585301401

[5] Por exemplo, no contexto da América do Sul, «Sociedade civil pede que tecnologias usadas devido à pandemia respeitem os Direitos Humanos», @ https://idec.org.br/noticia/sociedade-civil-pede-governos-da-america-latina-e-caribe-que-tecnologias-digitais-aplicadas

intrusões como *adequadas*[6], *necessárias e proporcionais*[7]. A questão, sendo excepcional e de carácter limitada no tempo, deveria ser pacificamente tolerada pelos cidadãos. Afinal, sob o manto de um fundamento como o "*interesse público*" [8] e salvaguarda da "*saúde pública*" até a limitação do escopo de protecção, desde logo, da privacidade de dados pessoais sensíveis claudica[9].

[6] No parecer 32/2020, a CNPD, delimitando geograficamente a aplicação de videovigilância por drones ao concelho de Ovar, dada a excepcionalidade da cerca sanitária entretanto imposta, reitera que "(…)as restrições aos direitos fundamentais devem limitar-se ao estritamente necessário às finalidades visadas com este sistema de videovigilância ", recomendando, adicionalmente, "que se garanta que a captação de imagens assim realizada salvaguarde a privacidade daqueles que se encontrem nas respectivas habitações", e, "que se garanta o direito de acesso às imagens gravadas , nos termos legalmente previstos", bem como que se adoptem "medidas adequadas a garantir a integridade das imagens gravadas no processo de transferência dos registos(…) para o "contentor de informação encriptado"" . @ https://www.cnpd.pt/home/decisoes/Par/PAR_2020_32.pdf

[7] Por exemplo, em Espanha, a AEPD: «(…)*Los fundamentos que legitiman/hacen posible dichos tratamientos son la necesidad de atender las misiones realizadas en interés público, así como la de garantizar los intereses vitales de los propios afectados o de terceras personas.* ***Las finalidades para las que pueden tratarse los datos son, únicamente, las relacionadas con el control de la epidemia****, entre ellas, las de ofrecer información sobre el uso de las aplicaciones de autoevaluación realizadas por las administraciones públicas o la obtención de estadísticas con datos de geolocalización agregados para ofrecer mapas que informen sobre áreas de mayor o menor riesgo.* ***Los datos que pueden obtenerse y utilizarse han de ser los que las autoridades públicas competentes consideren proporcionados/necesarios para cumplir con dichas finalidades.*** *Estos datos sólo podrán ser facilitados por quienes sean mayores de 16 años. En el caso de tratar datos de menores de 16 años, se requeriría de la autorización de sus padres o representantes legales.* ***Únicamente podrán tratar dichos datos las autoridades públicas competentes para actuar conforme a la declaración del estado de alarma****, es decir, el Ministerio de Sanidad y las Consejerías de Sanidad de las Comunidades Autónomas, que podrán cederse datos entre ellas, y a los profesionales sanitarios que traten a los pacientes o que intervengan en el control de la epidemia.****Las entidades privadas que colaboren con dichas autoridades sólo podrán utilizar los datos conforme a las instrucciones de estas y, en ningún caso, para fines distintos de los autorizados.»*** @ https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-apps-webs-autoevaluacion-coronavirus-privacidad

[8] A limitação ao tratamento de dados sensíveis, por exemplo, de saúde sucumbe ante "*razões de interesse público nos domínios da saúde pública*", desde que «(…)***Tais atividades de tratamento de dados sobre a saúde autorizadas por motivos de interesse público não deverão ter por resultado que os dados sejam tratados para outros fins por terceiros, como os empregadores ou as companhias de seguros e entidades bancárias»*** (Considerando 54 in fine) .

Considerando *(54) « O tratamento de categorias especiais de dados pessoais pode ser necessário por razões de interesse público nos domínios da saúde pública, sem o consentimento do titular dos dados. Esse tratamento deverá ser objeto de medidas adequadas e específicas, a fim de defender os direitos e liberdades das pessoas singulares. Neste contexto, a noção de «saúde pública» deverá ser interpretada segundo a definição constante do Regulamento (CE) n.o 1338/2008 do Parlamento Europeu e do Conselho (11), ou seja, todos os elementos relacionados com a saúde, a saber, o estado de saúde, incluindo a morbilidade e a incapacidade, as determinantes desse estado de saúde, as necessidades de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o acesso universal aos mesmos, assim como as despesas e o financiamento dos cuidados de saúde, e as causas de mortalidade(...)***».***

[9] Confirmando o Considerando (54), ainda, da leitura conjunta **das alíneas g) e i) do Art.o 9, n.º2, RGPD**: «**G)** *Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados*;», e**, i)** « *Se o tratamento for* ***necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde*** *ou para assegurar um elevado nível de qualidade e de*

Mas há um "*senão*". O receio de que a excepcionalidade vire regra é real[10]. Com efeito, é inegável que, neste momento, os receios de Yuval Harari [11], criador de *Homo Deus*, sejam partilhados por muitos de nós. Tal como as considerações de Joel P. Trachtman, quanto aos benefícios de um mundo global[12]: benéfico se mais cooperativo, com capacidades regulatórias internacionais reforçadas ao nível da saúde, cibersegurança, proteção ambiental e crises financeiras.

Ambos convergem na necessidade de compromisso, de partilha, cooperação e solidariedade global. O que se conclui espontaneamente dos apontamentos citados, através de um silogismo categórico: ameaça sobre todos os países, ameaça global, logo, resposta de todos os países, global. Não obstante, será que hoje temos líderes políticos mundiais à altura dos desafios[13] pungentes que se nos colocam nestes termos?

E no futuro?

segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional;». @ https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

[10] Yuval Harari:«(…) *Many short-term emergency measures will become a fixture of life. That is the nature of emergencies. They fast-forward historical processes. Decisions that in normal times could take years of deliberation are passed in a matter of hours. Immature and even dangerous technologies are pressed into service, because the risks of doing nothing are bigger.",* @ https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

[11] Harari: «(…) *In this moment of crisis, the crucial struggle takes place within humanity itself. If this epidemic results in greater disunity and mistrust among humans, it will be the virus's greatest victory. When humans squabble – viruses double. In contrast, if the epidemic results in closer global cooperation, it will be a victory not only against the coronavirus, but against all future pathogens*.», @ https://time.com/5803225/yuval-noah-harari-coronavirus-humanity-leadership/

[12] Joel P. Trachtman, «(…) *Not all global problems result from globalization. For those that do, globalization itself can ameliorate them to some extent. Furthermore, we can establish international laws and institutions to minimize those problems that do arise from globalization: globalized governance to respond to globalization-induced problems. This is smart globalization, and once we do it this way, it is likely that globalization should be retained because, on net, it will make us better off*.", @ https://www.bostonglobe.com/2020/03/30/opinion/not-all-global-problems-result-globalization/

[13] Ainda Harari: «(…)*Today humanity faces an acute crisis not only due to the coronavirus, but also due to the lack of trust between humans. To defeat an epidemic, people need to trust scientific experts, citizens need to trust public authorities, and countries need to trust each other. Over the last few years, irresponsible politicians have deliberately undermined trust in science, in public authorities and in international cooperation. As a result, we are now facing this crisis bereft of global leaders that can inspire, organize and finance a coordinated global response*.», *idem*.

Gerd Leonhard, num exercício curioso reproduzido no Diário de Notícias, destaca dois aspectos cruciais. Circunscrevendo-nos à tecnologia, esta *"tornou-se a nova religião". "Estamos a entrar num novo Renascimento". O próximo passo será regulamentá-la de forma mais apertada com o objetivo de que humanos e o próprio planeta beneficiem do progresso tecnológico.* Não obstante, esta relação acabará seduzir-se ante uma *vigilância estatal por meios tecnológicos* (que) *irá tornar-se o novo normal após as medidas extraordinárias que foram tomadas para controlar esta pandemia*[14].

E como já vai longo, para concluir, convocamos, novamente, a questão fundamental: "*Que mundo esperar do pós-covid19*"?

A provocação desconcertante e acutilante que se impõe, inclusive politicamente, não poderia ser outra: «*Of course, even if we disappear, it will not be the end of the world. Something will survive us. Perhaps the rats will eventually take over and rebuild civilization. Perhaps, then, the rats will learn from our mistakes. But I very much hope we can rely on the leaders assembled here, and not on the rats.*» [15]

Nesta nova edição da «Cyberlaw by CIJIC», procuramos sustentar o crescimento paralelo que o Mestrado de Segurança da Informação e Direito do Ciberespaço[16] vai granjeando. É pois, com orgulho, que passaremos a destacar produção deste, com maior regularidade. Afinal, este é um desígnio da própria criação da revista. Provavelmente, num futuro não muito distante, estará na calha a edição em papel de futuras edições. Se há questão que se nos colocou com o teletrabalho foi: qual a redundância digital? *Ie*, sem acesso à internet, ou sem eletricidade/bateria, como é que seria possível aceder

[14] «Não haverá normal: futuristas preveem mudanças permanentes pós-coronavírus», @ https://www.dn.pt/dinheiro/nao-havera-normal-futuristas-preveem-mudancas-permanentes-pos-coronavirus-11987179.html

[15] Yuval Harari: «Yuval Harari's blistering warning to Davos», @ https://www.weforum.org/agenda/2020/01/yuval-hararis-warning-davos-speech-future-predications/

[16] Mais informações @ : https://fenix.tecnico.ulisboa.pt/cursos/msidc

a conteúdos para efeitos de estudo? Como ler(aceder) nestas circunstâncias? Como mitigar a "info-exclusão" quando o sistema não é propriamente redundante na acessibilidade[17]?

Reavendo, nesta edição, incorporando conteúdo em inglês escrito, por força de deveres de participação, cooperação e colaboração internacional[18] que muito nos orgulha, procuramos revisitar temas como cibersegurança em contexto marítimo, dados pessoais e dados não pessoais, monitorização de trabalhadores em contexto laboral, a regulação jurídica do ciberespaço - mutação do paradigma à luz do acórdão James Elliot, *Phishing*, redes sociais e manipulação da opinião pública, o problema da mobilidade em contexto organizacional, e, os desafios da cibersegurança forense de *smartphones* no continente africano. Os temas são oportunos. São, igualmente, desafiantes. São, finalmente, abertos a colaboração múltipla, participada.

Resta-me agradecer a todos quantos contribuíram para mais uma edição da Revista, pelo esforço, pela disponibilidade, pela obra, endereçando a todos, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um justíssimo: - Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 29 de Março de 2020

Nuno Teixeira Castro

[17] Por exemplo, «Ministro Siza Vieira admite aulas por canais "estilo youtube" ou TV por cabo.», @ https://observador.pt/2020/03/29/ministro-siza-vieira-admite-aulas-por-canais-estilo-youtube-ou-tv-por-cabo/
Mas, sem acesso internet, ou sem cabo – até porque a cobertura não é de 100%, há, pelo menos, cerca de 20% de famílias sem acesso ao Cabo – como é que as crianças e adolescentes que se encontrem nesta situação se integram? Como é que se combate esta exclusão digital?

[18] Um trabalho colaborativo ímpar. @ https://networkofcenters.net/center/cyberlaw-research-centre-university-lisbon-school-law-cijic

CYBERLAW by CIJIC

DOUTRINA

THE CHALLENGES OF SMARTPHONE FORENSICS IN SUB-SAHARAN AFRICA

RICARDO J.G.N. DOS SANTOS [1]

[1] Master Student of Information Security and Cyber Law Instituto Superior Técnico – Portugal Contact: rjgndossantos@gmail.com.

ABSTRACT

The modernization of public and private services in sub-Saharan Africa has been challenging to the region, due to a massive adoption of information and communication technologies, such as mobile-centric solutions connected or not to overseas Cloud computing services, putting an overwhelming pressure on security forces and the judicial apparatus of these countries to deal accordingly with new criminal phenomena of cyberspace. As a result, building sustainable Smartphone Forensics capacity presents itself as the way forward, despite budgetary, legal and even political constraints that ultimately determine its effectiveness, in parallel with the obligation to comply with cyberspace security standards, some of them already in force, as a consequence of international treaties that bilaterally or regionally bind many of these countries.

Keywords: *Sub-Saharan Africa; Cyber security; Cybercrime; Law Enforcement; Smartphone; Forensics; Challenges*

1.FOREWORD

The information age has been a more constant presence in our daily lives, due to not only the speed and technological innovation it brings, but also with the almost near extinction of some activities that used to be part of modern societies, such as postal services, landline telephones, neighbourhood groceries and corner stores.

Not to mention services, both in private and government sectors, that have been replaced by e-mail, VoIP, e-commerce and many more, which, due to the immaterial nature of cyberspace, require security measures to be adjusted to this new reality.

Paving the way for the Fourth Industrial Revolution of real time, lower costs, modularity, and large-scale integration done by Cloud Computing[1], IoT[2], and other paradigms, the information age presents itself as a kind of unblocked expanding snowball, throughout cyberspace, giving way to new forms of social, economic and even political way of living, especially in countries with a considerable digitization rate of public and government services.

Sub-Saharan Africa is not apart from this global trend, precisely because of the great transformations it has witnessed over the last decade. Nevertheless, it remains a big unknown in the information age, due to great challenges it still has to deal with organized crime, terrorism and other vicious behaviours, which are increasing today in cyberspace.

In addition, sub-Saharan Africa has yet to create technological infrastructure and capacity to absorb the potential of information age technologies. Even having considerable digital mobile network coverage, this part of the African continent still has a low level of

[1] See: https://www.ibm.com/cloud/learn/cloud-computing (accessed on 27/12/2019)
[2] See: https://www.iotforall.com/what-is-iot-simple-explanation/ (accessed on 27/12/2019)

consumption of state-of-the-art computer services and solutions compared to other regions of the world, which in part defines the general characteristics of criminal behaviour there.

However, due to the phenomenon of globalization, knowledge exchange with global criminal networks is already a reality, which puts pressure on sub-Saharan African governments to respond diligently to this global scale threat by strengthening police cooperation mechanisms, both within Interpol and the regional economic blocs, with Europol being of particular note.

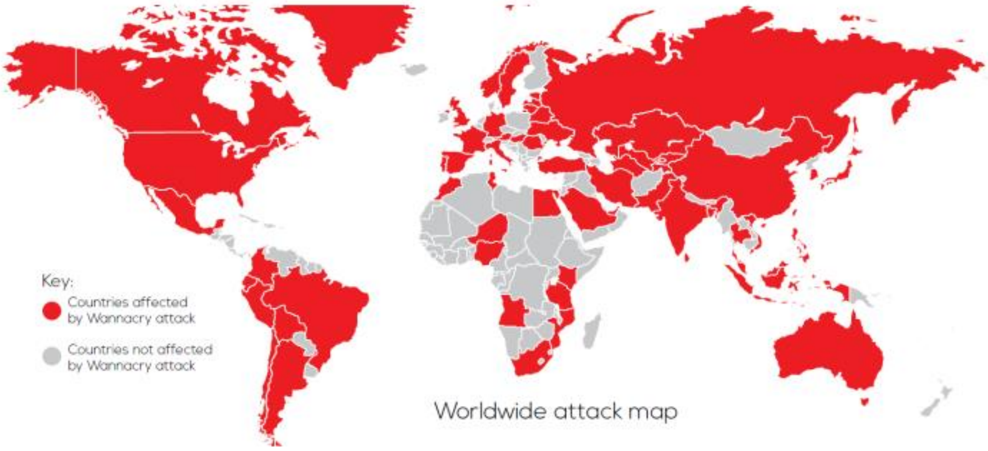
Thus, bearing in mind the particular characteristics of cybercrime in sub-Saharan Africa, building sustainable Smartphone Forensics capacity presents itself as the way forward, despite budgetary, legal and even political constraints that ultimately determine its effectiveness, in parallel with the obligation to comply with cyberspace security standards, some of them already in force, as a consequence of international treaties that bilaterally or regionally bind many of these countries.

2. GLOBAL OVERVIEW OF ORGANIZED INTERNET CRIME

A recent report [1] points out data as the key element on the security agenda of organizations and citizens as well, by strengthening data protection legislation, to tackle attacks such as ransomware. In effect, despite experiencing a decrease in global occurrences, ransomware has become more selective and focused on people and organizations.

For instance, in 2019 most visible attacks were against local governments, specifically in the United States. This trend had commenced earlier in 2018, when an attack paralysed the city of Atlanta for several weeks and only proved to be the tip of the iceberg. After that, more than half a dozen cities and public services across the US fell victim to ransomware, on a near-monthly basis, and in the most extreme situations, a state of emergency was declared[3].

Although spotted only in the US, these ransomware attacks have underscored the need for strengthening law enforcement international cooperation.


Key:
● Countries affected by Wannacry attack
● Countries not affected by Wannacry attack
Worldwide attack map

Source: Serianu, 2018 [2]

Figure 1 – A global overview of ransomware attacks in 2018

[3] See: https://www.cpomagazine.com/cyber-security/top-10-ransomware-stories-of-2019/ (accessed on 27/12/2019)

Indeed, in January 2019, authorities from several US agencies, along with police and prosecutors from Belgium and Ukraine, as part of a Joint Investigation Teams assisted by Eurojust, seized the *xDedic marketplace* in an operation also supported by the German Federal Criminal Police Office and Europol, exposing more than EUR 60 million in fraud[4].

Another clear and growing concern are Supply Chain Attacks [1], i.e. the use of compromised third parties as a means to infiltrate networks affecting suppliers of third-party software or hardware, but also other business services.

For instance, large companies, which may have a multitude of third-party suppliers, some with a high degree of connectivity, bringing each one its own risk. Such risks are similarly incurred when a larger company acquires a smaller company which may have lower cyber security maturity[5].

Moreover, many companies are becoming increasingly reliant on third-party services such as the cloud, where malicious software, even signed with legitimate digital certificates, can appear to be an authentic software update[6]. These attacks have also affected large parts of business, resulting in costly production stoppages in Europe[7] and the USA.

Amongst them [1] are Distributed Denial of Service (DDoS) attacks, whose purpose resembles the previous ones, since the main element that drives them is extortion, particularly crypto currency. Besides, DDoS attacks are often linked to so-called hacktivism[8], which presents itself one of the greatest security challenges of democratic countries, since it acts, most of the time, as a faceless force with no explicit ideological alignment, but often linked to covert acts of sovereign states or hostile organizations.

[4] See: https://www.europol.europa.eu/newsroom/news/xdedic-marketplace-shut-down-in-international-operation (accessed on 27/12/2019)
[5] See: https://www.theguardian.com/business/2019/jul/09/marriott-fined-over-gdpr-breach-ico (accessed on 27/12/2019)
[6] See: https://securelist.com/operation-shadowhammer/89992/ (accessed on 27/12/2019)
[7] See: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/lockergoga-ransomware-family-used-in-targeted-attacks/ (accessed on 27/12/2019)
[8] See: https://www.checkpoint.com/definitions/what-is-hacktivism/(accessed on 27/12/2019)

It poses challenges on law enforcement agencies to gather digital evidence to determine the root cause of these criminal acts before they can be presented in Court, especially because of the massive use of sophisticated encryption and obfuscation methods.

Likewise, in spite of a noted decline[9], DDoS attacks remain one of the most prominent threats reported by the private sector [1], superseded only by *phishing* and other social engineering attacks, resulting in the interruption of online bank services, creating more of a public impact rather than direct financial damage.

Such attacks typically originate from low-capability actors, who can still leverage easily accessible DDoS-for-hire services[10] that exploit booters/ stressers. While most attacks can be successfully mitigated, emerging DDoS techniques, which may be significantly harder to defend against, such as memcached[11] amplified attacks remain a concern for the financial sector.

In 2018[12] and 2019[13], respectively, two large DDoS attacks using this technique were spotted. Notice that social networks and other content providers commonly use a memcached approach, which is likely to expose their servers to UDP based reflection attacks[14].

In turn [1], there was also an accentuation of the recording of criminal sexual phenomena such as child pornography[15], which now is boosting[16], and related explicit content material[17], largely due to the popularization of smartphone use by minors, but also, raising

[9] See: https://gbhackers.com/ddos-for-hire-service/(accessed on 27/12/2019)
[10] See: https://www.csoonline.com/article/3180246/hire-a-ddos-service-to-take-down-your-enemies.html (accessed on 27/12/2019)
[11] See: https://www.tutorialspoint.com/memcached/index.htm(accessed on 27/12/2019)
[12] See: https://thehackernews.com/2018/03/biggest-ddos-attack-github.html(accessed on 27/12/2019)
[13] See: https://www.imperva.com/blog/imperva-blocks-our-largest-ddos-l7-brute-force-attack-ever-peaking-at-292000-rps/(accessed on 27/12/2019)
[14] See: https://www.imperva.com/learn/application-security/udp-flood/ (accessed on 27/12/2019)
[15] See: https://www.europol.europa.eu/newsroom/news/14-arrests-in-takedown-of-massive-child-sexual-abuse-platform (accessed on 27/12/2019)
[16] See: https://globalnews.ca/news/4153203/swedish-man-guilty-online-rape-convictions-upgraded/ (accessed on 27/12/2019)
[17] See: https://www.nationalcrimeagency.gov.uk/news/five-years-in-jail-and-worldwide-travel-ban-for-british-teacher-who-wanted-to-abuse-young-filipino-children (accessed on 27/12/2019)

additional concerns about the Darknet[18]. In effect, it is in these prolific web places where smuggling-related transactions[19], narcotics, scamming money and terrorism[20] have found a safe haven

In a word, Darknet remains the key online propeller for trade in an extensive range of criminal products and services and a priority threat for law enforcement [1], even with coordinated law enforcement reaction, combined with extensive DDoS counter-attacks that have generated distrust in the Tor[21] environment.

Even so, it seems existing market varieties and customer-base on Tor are making a full migration to new platforms, which have increased the number of single-vendor shops and smaller fragmented markets on Tor, including those catering for specific languages, supported by strong encrypted communication applications, likely to support illicit trade[22].

A final word on enabling factors of the above mentioned organized crime phenomena on the Internet [1]. The first is the wide array of Online Service Providers (OSP) exploited by terrorist groups, which presents a significant challenge to any disruption efforts, since they are exploiting emerging platforms for their online communication and distribution strategies associated, in some cases, to hacktivism.

These terrorist attacks can rapidly turn viral before any OSP or law enforcement can react, exemplified here not only with the remarkable cases in Iraq and Syria[23], but also in New Zealand[24] and Nigeria[25], which are certainly not isolated events.

[18] See: https://www.darkowl.com/what-is-the-darknet(accessed on 27/12/2019)

[19] See: https://www.nytimes.com/2019/06/11/technology/online-dark-web-drug-markets.html (accessed on 27/12/2019)

[20] See: https://www.counterextremism.com/press/extremist-content-online-isis-utilizes-dark-web-remain-online (accessed on 27/12/2019)

[21] See: https://www.torproject.org/ (accessed on 27/12/2019)

[22] See: https://www.theguardian.com/world/2019/may/03/german-police-close-down-dark-web-marketplace (accessed on 27/12/2019)

[23] See: https://www.project-syndicate.org/commentary/america-islamic-state-information-war-by-anne-marie-slaughter-and-asha-c-castleberry-2019-09?barrier=accesspaylog (accessed on 27/12/2019)

[24] See: https://www.nytimes.com/spotlight/christchurch-attack-new-zealand (accessed on 27/12/2019)

[25] See: https://www.ict.org.il/UserFiles/Cyber%20Report%203.pdf

A second enabling factor is *phishing*[26], which remains an important tool in the cybercriminals arsenal, inducing victims to withdraw money[27] from their bank accounts. The big news currently is the inclusion of crypto currencies to propel these criminal acts, giving rise to *cyber mules*, which, like their narcotics counterparts, are used to traffic crypto currency.

In 2018, over the course of three months, law enforcement and private sector partners from over 30 countries participated in the fourth European Money Mule Action (EMMA) which ended up with the tracking of over 1.500 *cyber mules* and 140 *cyber mule's* organisers, resulting in 168 arrests. Financial sector participants reported 26,376 fraudulent *cyber mules'* transactions, preventing an estimated loss of over EUR 36 million. Two interesting related cases were reported in the United Kingdom[28] and the Netherlands[29].

[26] See: https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html (accessed on 27/12/2019)

[27] See: https://as.com/diarioas/2014/12/16/english/1418723895_163685.html (accessed on 27/12/2019)

[28] See: https://www.europol.europa.eu/newsroom/news/6-arrested-in-uk-and-netherlands-in-%E2%82%AC24-million-cryptocurrency-theft (accessed on 02/01/2020)

[29] See: https://financefeeds.com/europol-dutch-and-luxembourg-authorities-clamp-down-on-crypto-mixing-service-bestmixer-io/ (accessed on 02/01/2020)

3. A BRIEF ON DIGITAL FORENSICS

Digital forensics, or computer forensics, comprises the application of scientific investigatory techniques to digital crimes and attacks. Jason Jordaan, principal forensic scientist at DFIRLABS[30], has a good definition for that,[31] naming it as the identification, preservation, examination, and analysis of digital evidence, using a scientifically accepted and validated process and the ultimate presentation of that evidence in a court of law to answer some legal question.

In current global cyber security status, this poses a major challenge especially for countries that are cyclically lacking human, financial or material capacities, especially if dealing, for example, with Cloud Computing [3], [24].

Besides [4], the nature of the cases in which digital evidence is involved is generally borderless and the offense happens in a split second.

Thus, the findings derived from electronic evidence must therefore follow a standard set of guidelines to ensure it is admissible not only in a specific country's court of law, but also in the international criminal justice system. For that reason, understanding electronic evidence is a challenging process due to the fact the data can be scattered in several physical locations, sometimes across countries or jurisdictional borders effortlessly and in a matter of seconds.

And, of course, being highly volatile, the data are easily altered, overwritten, damaged or destroyed by the single stroke of a key. Therefore, the data can be copied without degradation, so that the lifespan of electronic evidence, unlike any other discipline of forensic evidence, is short before it is rendered useless.

[30] See: https://www.dfirlabs.com/ (accessed on 02/01/2020)

[31] See: https://www.csoonline.com/article/3334396/what-is-digital-forensics-and-how-to-land-a-job-in-this-hot-field.html (accessed on 02/01/2020)

An example of this is a smartphone. After five years, it may not be able to switch on or function properly. Based on these facts, therefore, electronic evidence must be processed and handled with due care.

On the other hand [4], the criteria for the admissibility of electronic evidence may differ from jurisdiction to jurisdiction. Any forensic investigator should always consider, as a basis for starting a case, the following (table 1):

Table 1 - General Criteria for the Admissibility of Electronic Evidence

General Criteria for the Admissibility of Electronic Evidence	
Authenticity	The evidence must establish facts in a way that cannot be disputed and be representative of its original state.
Completeness	The analysis of, or any opinion based on, the evidence must tell the whole history and not be tailored to match a more favourable or desired perspective.
Reliability	There must be nothing about the way in which the evidence was collected and subsequently handled that may cast doubt on its authenticity or veracity.
Convincing	The evidence must be persuasive as to the facts it represents, and must be able to convince the stakeholder of the truth in court.
Proportionality	The methods used to gather evidence must be fair and proportionate to the interests of the justice: the prejudice (i.e. level of intrusion or coercion) caused to the rights of any party should not outweigh the probative value of the evidence (i.e. its value as proof).

Source: Interpol, 2019 [4]

To achieve this purpose [4], a seven-step model is recommended for managing a case (figure 2). Moreover [4], prior to conducting a case, the Digital Forensics Laboratory personnel must ensure it is following and complying with relevant legislation.

One last remark to alert that following standardized guidelines is paramount, but innovations are also encouraged, especially in low-income countries [5]. For this reason, sometimes it is valid relying on low-cost forensics[32], setting up a functional and credible forensic workstation at the cost of a few hundred dollars [6] to create admissible evidence for legal proceedings in Court.

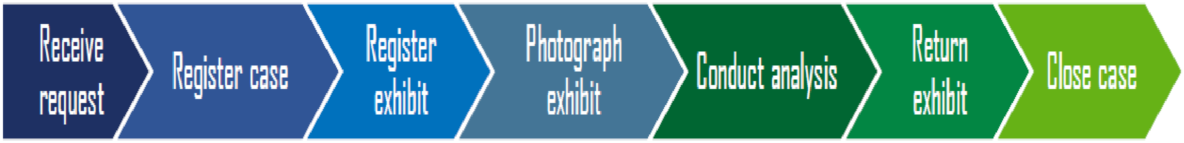


Figure 2 – A recommended model for collecting any electronic evidence
Source: Interpol, 2019 [4]

3.1 Smartphone Forensics

Of particular interest is the process of conducting Digital Forensics examination (figure 3) and analysis on mobile devices[33], where two levels of data acquisition are considered [4], respectively, physical data and logical data acquisitions.

While physical data acquisition includes all raw data, a logical copy typically only includes an allocated subset of those data. Physical data acquisition, at whole disk level, copies all data contained on the disk, including the partition scheme, partitioned area, and not partitioned area. Logical data acquisition on disk level copies only a logical partitioned area. The availability of forensic software tools for mobile devices is considerably different from that of personal computers [7]. While personal computers may differ from mobile devices from a hardware and software perspective, their functionality has become increasingly similar. Although the majority of mobile device operating systems are open source[34], feature phone Operating Systems are typically closed.

[32] See: https://www.digitalforensicshub.com/index.html (accessed on 06/01/2020)
[33] Desktops, Servers and other *fixed* devices
[34] Android Operating System. Further details here: https://www.android.com/ (accessed on 06/01/2020)

This means that interpreting their associated file system and structure become difficult, not to mention a myriad of file system and structure permutations which may create significant challenges for mobile forensic tool manufacturers and forensic investigators.

The types of software available for mobile device examination include commercial and open source forensic tools [7], as well as non-forensic tools intended for device management, testing, and diagnostics. Forensic tools are typically designed to acquire data from the internal memory of handsets and Universal Integrated Circuit Cards[35] without altering their content and to calculate integrity hashes for the acquired data. Whilst non-forensic tools may allow unrestricted two-way flow of information and omit data integrity hash functions. Consequently, mobile device investigators typically assemble a collection of both forensic and non-forensic tools for their toolkit.

It should be noted, however [8], that the proliferation of smartphones on the consumer market caused a high demand for forensic examination of the devices. This could not be met by existing computer forensics techniques.

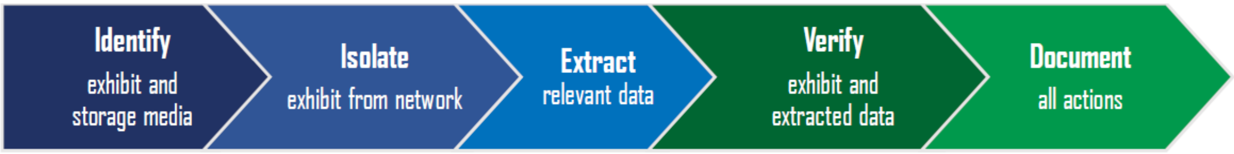


Figure 3 – Electronic data acquisition process in smartphone forensics
Source: Interpol, 2019 [4]

To remain competitive, original equipment manufacturers frequently change mobile phone form factors, operating system file structures, data storage, services, peripherals, and even pin connectors and cables. As a result, forensic examiners must use different forensic processes if compared to usual computer forensics.

[35] See: https://techterms.com/definition/uicc (accessed on 06/01/2020)

A crucial aspect in smartphone forensics is the device isolation [7], since many mobile devices offer the user the ability to perform either a remote lock or remote wipe by simply sending a text message command[36] to the mobile device. Additional reasons for disabling network connectivity include incoming data[37] that may modify the current state of the data stored on the mobile device.

Outgoing data may also be undesirable as the current GPS location may be delivered to an advisory providing the geographic location of the forensic examiner. Therefore, forensic examiners need to be aware and take precautions when securing mobile devices mitigating the chance of data modification. Isolating the mobile device from other devices used for data synchronization is also important [7] to keep new data from contaminating the existing data.

If the device is found in a cradle or connected with a personal computer, pulling the plug from the back of the personal computer eliminates data transfer or synchronization overwrites, thus capturing data should be done by a qualified digital forensics professional. Isolating a mobile device from all radio networks[38] is also important [7] to keep new traffic, such as SMS messages, from overwriting existing data.

Besides, the risk of overwriting potential evidence, the question may arise whether data received on the mobile device after seizure is within the scope of the original authority granted.

[36] For example, a text message.
[37] For example, calls or text messages.
[38] For example, Wi-Fi, Cellular and Bluetooth.

4. BUDAPEST CONVENTION ON CYBERCRIME

Finally, a brief look at the Budapest Convention, which is a comprehensive guiding document drawn up by the Council of Europe[39] in November 2001 and open for signature by its member and non-member States which have participated in its elaboration and for accession by other non-member States.

The Budapest Convention resembles a harmonious triangle whose vertices unfold three broad lines of action [9], respectively: (i) criminal conduct; (ii) tools and procedures and (iii) international cooperation. It is considered one of the most relevant documents on cybercrime and digital forensics.

With regard to criminal conduct, its scope covers illegal access; illegal interception; data interference; system interference; misuse of devices; fraud and forgery; child pornography; and intellectual property offences. About tools and procedures, it covers expedited preservation; search and seizure; production order; and interception of computer data.

Finally, with regard to international cooperation, the Budapest Convention sets out the terms of mutual assistance in criminal matters, covering the areas of extradition, spontaneous information, expedited preservation, and many more.

By March 2018 [9], the Budapest Convention was already explicitly or implicitly present in the cyber laws of 130 countries, of which 57 had already ratified and transposed them into domestic law. The vast majority are OECD countries.

[39] See: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (accessed on 06/01/2020)

5. SUB-SAHARAN AFRICA: OPPORTUNITIES, GEOPOLITICS AND MODERNIZATION

Located below the Sahel,[40] this poorly industrialized part of the African continent, which consists of 46 countries and in 2018 had 1.038.627.178 inhabitants, is now according to UNDP[41] experiencing steady economic growth and macroeconomic stability.

This is also accompanied by a flourishing private investment not only in the agricultural, telecommunications, finance, retail trade, housing and construction sectors, but also in new technologies, which are spreading rapidly across the continent, leading to a considerable progress in the areas of information and communication.

This scenario contrasts with the primary and extractive characteristics of the early stages of its economy, based on raw material exports, along with residual high and medium-income tourism.

This optimism is also shared by the World Bank [10], which points out Sub-Saharan Africa as the region that has been implementing the highest number of reforms every year since 2012. Consequently, the private sector is feeling the impact of these improvements, with the average time and cost to register a business, for example, declining from 59 days and 192% of per capita income in 2006 to 23 days and 40% of per capita income today.

Furthermore, the average paid-in minimum capital has fallen from 212% o to 11% of per capita income in the same period. Still according to the World Bank [10], Kenya and Rwanda are the most represented Sub-Saharan Africa countries in Doing Business 2019, due to growth in digitization, as well as business regulatory reforms. Kenya simplified the process of providing value added tax (VAT) information by enhancing its existing online system, iTax[42].

[40] See: https://www.britannica.com/place/Sahel (accessed on 06/01/2020)
[41] See: https://www.africa.undp.org/content/rba/en/home/regioninfo.html (accessed on 06/01/2020)
[42] See: https://itax.kra.go.ke/KRA-Portal/ (accessed on 06/01/2020)

Furthermore, in Kenya, the Ministry of Lands and Physical Planning implemented an online land rent financial management system on the eCitizen portal[43], enabling property owners to determine the amount owed in land rent, make an online payment and obtain land rates clearance certificates digitally.

On the other hand, Rwanda streamlined the process of starting a business by replacing its electronic billing machine system with new software that allows taxpayers to issue value added tax invoices.

The free software, which is provided by the office of their Revenue Authority, allows taxpayers to issue value added tax invoices from any printer, eliminating the previous requirement to purchase and set up a special billing machine[44] among other recent achievements.

The main reason for this sub-Saharan Africa awakening in the international arena seems to be the remarkable growth[45] of its middle class, which brings with it consumption habits very close to those in the most developed countries in the northern hemisphere.

They have been even often challenged by a Subaltern Globalization[46] carried across the Southern hemisphere by non-governmental organizations and international partnerships with African Diasporas in Europe and America, leading to an informed and better prepared middle class able to understand the geopolitical dynamics worldwide. Indeed, in the context of globalization and the current global financial crisis, new cooperation players are emerging in Africa[47].

[43] See: https://www.ecitizen.go.ke/ (accessed on 06/01/2020)
[44] See: https://www.rra.gov.rw/fileadmin/user_upload/20180328_vsdc_technical_specifications_v.4.pdf (accessed on 06/01/2020)
[45] See: https://www.uhy.com/the-worlds-fastest-growing-middle-class/ (accessed on 06/01/2020)
[46] See: http://www.allacademic.com/meta/p74466_index.html (accessed on 06/01/2020)
[47] See: https://journals.openedition.org/poldev/138 (accessed on 06/01/2020)

These partners loosen financial constraints and conditionality, increase the room for manoeuvre and stimulate commodity markets, namely, substantial technology transfer and an outsourcing of production to Africa, especially with a view to accessing the North American and European markets.

The increase in product quality and production diversification suggests that territorial poles of competition are emerging, while the continent participates both in production segments that are integrated in global technical production and in cognitive processes, especially via multinational firms[48].

On the other hand, they also increase the risks of renewed indebtedness and potentially weaken the coordination of aid policies. Furthermore, Africa is now concerned with many problems that are global in scope, such as climate change, market instability, epidemiological risks, terrorism[49] and political instability[50].

Particularly important in this equation is the role of the People's Republic of China, which bets on a welfare model where the balance of countries' internal affairs is not accountable for mutual cooperation[51]. As a result, this Asian nation became not only the largest creditor in sub-Saharan Africa, but also the largest investor in Africa, often playing this friendly card in debt relief[52].

5.1 Booming Mobile Connectivity

One of the consequences of this new positioning of Sub-Saharan Africa in the world is the expansion of information and communications technologies in a continent traditionally

[48] See: https://journals.openedition.org/poldev/138 (accessed on 06/01/2020)
[49] *Ibidem*
[50] See: https://www.dni.gov/files/images/globalTrends/documents/GT-Africa_Democratization_ForPublishing-WithCovers.pdf (accessed on 06/01/2020)
[51] See:https://www.economist.com/briefing/2019/03/07/africa-is-attracting-ever-more-interest-from-powers-elsewhere (accessed on 06/01/2020)
[52] See: https://beyond-ratings.com/publications/geopolitics-debt-chinafrica-relationship/(accessed on 06/01/2020)

devoid of basic telecommunications and energy infrastructures capable of matching the information age. That is present especially in the hinterland, which created an opportunity for booming mobile connectivity, especially in countries that usually are leading their sub-regions. Indeed, Sub-Saharan Africa mobile network operators are eager today to contribute to the development of a strong information and communication technology industry. The importance of this boom is not only economic, but also, social [11].

Mobile internet connectivity brings about material increases in productivity, providing more efficient ways for consumers, workers and businesses to trade, communicate and access information. Besides and more importantly, the economic impact of mobile technology is also reflected in the industry's contribution to the global economy, which in 2017 amounted to $3.6 trillion or 4.5% of total Gross Domestic Product (GDP).

In many low and middle-income countries, this proportion is even higher – for example, in Sub-Saharan Africa it accounted for 7.1% of total GDP in 2017 [11]. In fact [12], mobile economy in Sub-Saharan Africa has been driven by various consumer needs across the region. Mobiles are not just a communication device but also the primary channel for getting online and a vital tool to access life-enhancing services.

This is particularly true in rural areas, where around half the population lives and where the provision of these services by conventional means is constrained by acute funding, skills and infrastructure gaps. Mobile network assets and services, such as APIs, IoT, mobile money and billing platforms, are enabling sustainable business models for key services across verticals in the region. The number of mobile internet subscribers in the region has quadrupled since the start of this decade; the technology is the only available platform for the majority of the population to get online.

In late 2017, there were 135 live mobile money services across the region, with 122 million active accounts, a figure which is expected to have significantly increased by 2025, when nearly 300 million people is expected to be online, the majority of them connecting via high-speed mobile broadband networks.

On the other hand [12], mobile money continues to flow rapidly across Sub-Saharan Africa. In 2017, the total value and number of mobile money transactions grew by 14.4% and 17.9% to reach $19.9 billion and 1.2 billion, respectively. Although East Africa remains the largest mobile money market, accounting for 56.4% of total users in the region, West and Central Africa have seen rapid uptake in recent years, helped by enabling regulatory policies.

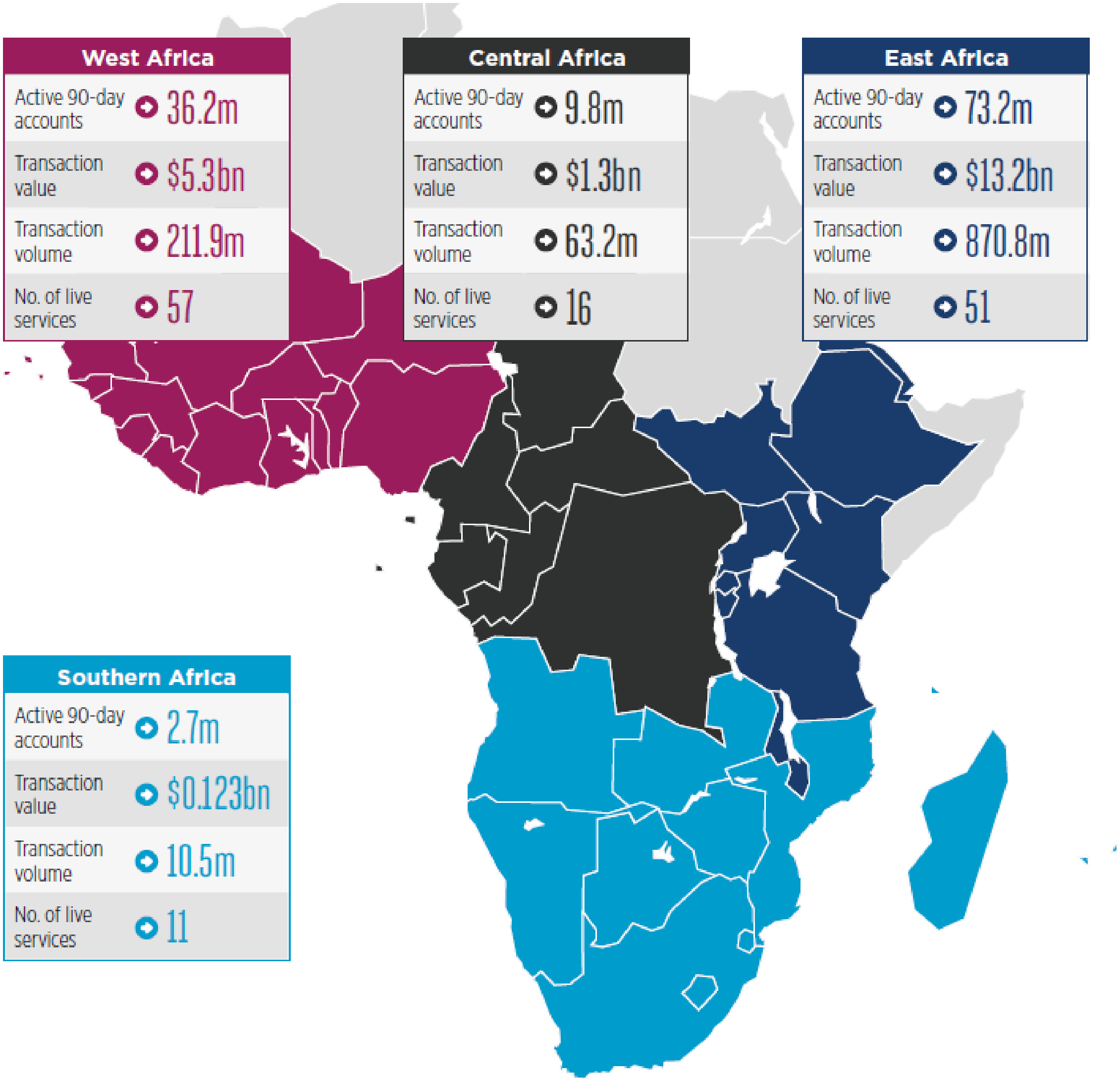
Both sub-regions have seen their share of the mobile money market double to 30.9% and 9.7%, respectively, over the five years to 2017. In addition [11] to the economic impact, mobile internet can drive material improvements in social outcomes (health, education and personal freedoms) and overall quality of life, average life evaluations and net positive emotions. In short, mobile technology has been contributing to the achievement of the UN Sustainable Development Goals.

Moreover [13], mobile internet connectivity will help overcome the traditional barriers of distance and limited access to healthcare, promoting education, innovation and job creation innovation hubs. Not to mention opportunities for established businesses to partner with start-ups and create thriving ecosystems of creativity and enterprises.

It is, ultimately, bringing the informal sector into the mainstream economy, by enabling banks and telecoms providers to reach out to previously unbanked customers with low-cost accessible services[53]. However 4G penetration remains limited, because the Sub-Saharan African mobile telecommunications market is highly dependent on 2G and 3G technologies, it limits operators' ability to monetize value-added services and mobile connectivity, pushing mobile network operators to remain highly dependent on traditional voice and SMS revenues[54].

[53] Note: A successful example is Kenya’s M-PESA

[54] See: https://www.spglobal.com/marketintelligence/en/news-insights/blog/opportunities-and-challenges-for-african-telecommunications-industry-at-africacom-2018(accessed on 06/01/2020)



Source: GSMA, 2018 [12]

Figure 4 – Mobile money financial flow in Sub-Saharan Africa

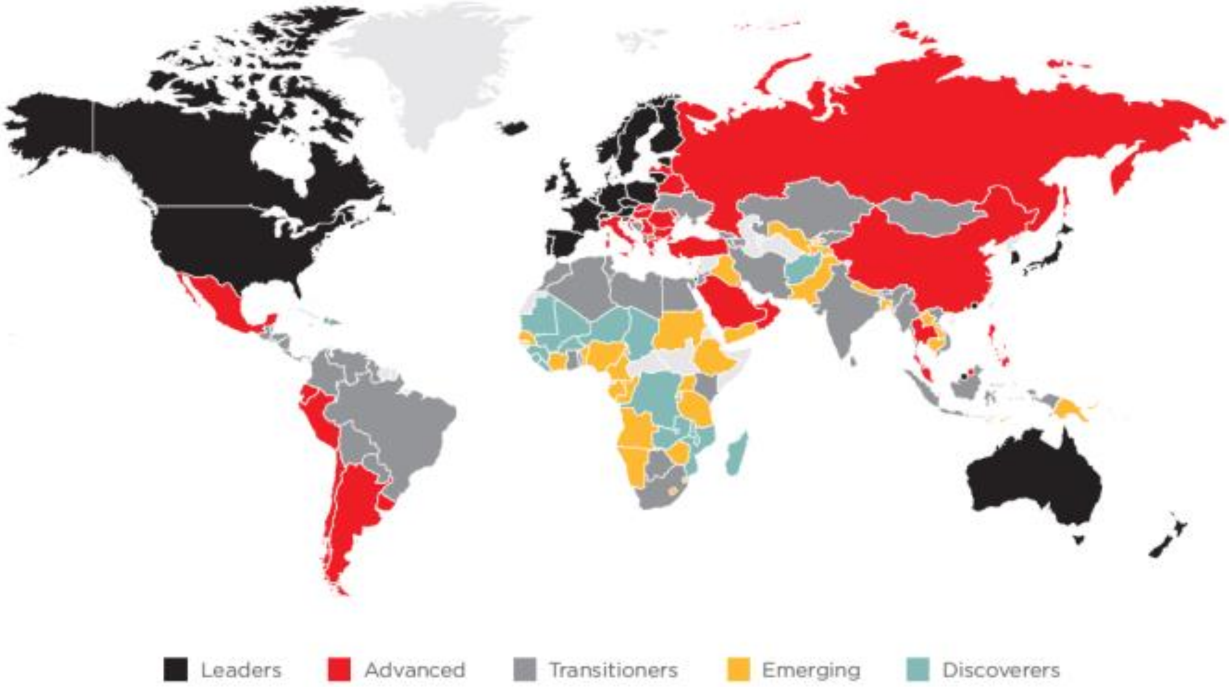
Figure 5 is taken from 2018 GSMA Intelligence report [11] which also states that Sub-Saharan countries have yet to start to reduce the gap on consumer readiness and affordability.

It means that the region will need to maintain its progress in this area while also accelerating improvements in infrastructure and the development of local content and services. Although no country in Sub-Saharan Africa is in the advanced cluster of the mobile connectivity index[55], Mauritius is close to the threshold[56].

[55] Note: The Mobile Connectivity Index measures a number of indicators, scored within a range of 0 to 100, with a higher score representing stronger performance in delivering mobile internet connectivity. For further details see: http://www.mobileconnectivityindex.com/

[56] Note: In fact, Mauritius surpassed this level in 2019

Furthermore, several other countries have been improving their performance since 2014, with four[57] joining the transitioners cluster and 10 moving from the Discoverers to the Emerging cluster. As a result, fewer than half of the countries in the region are now in the Discoverers cluster (compared to two thirds in 2014). In 2018 [14], there was a notable acceleration in network expansion in Sub-Saharan Africa, where coverage reached 70% – a considerable increase from 63% in 2017, and from 52% in 2014.



Source: GSMA, 2018 [11]

Figure 5 – Global mobile connectivity index

More than 80 million people previously unable to access 3G networks are now covered.

Nigeria reached almost 75% coverage, whereas the Democratic Republic of the Congo reached more than 50%. Most of this expansion was driven by a programme of upgrading 2G sites, which were focused on voice and SMS services, to also support mobile internet services.

[57] Cape Verde, Ghana, Botswana and Kenya

The deployment of single Radio Access Network technology and U900[58] has allowed operators to roll out 3G in a more cost-efficient manner. U900 has been particularly effective by enabling the use of low-frequency spectrum bands for 3G, which is less costly than deploying in the 2100 MHz band. While the 900 MHz spectrum has historically been used for voice and SMS services, operators have been responding to the increasing adoption of internet-enabled feature phones and smartphones in the continent.

Between 2014 and 2018 [14], the penetration of smartphone connections in Sub-Saharan Africa increased from 10% to 30% of the population, with more Africans able to use their phones to access data services. It is now more viable for operators to move voice traffic to 3G by *refarming*[59] part of their 900 MHz spectrum, especially as some U900 technologies can easily be deployed through remote software upgrades and allow dynamic spectrum allocation between 3G and legacy services.

With 85% 2G coverage currently in Sub- Saharan Africa, it is expected that operators will continue to upgrade their sites over the next few years, narrowing the gap between 2G and 3G coverage. Moreover, upgrading 2G sites in remote areas will remain a challenge as the incremental costs associated with equipment, backhaul and power may not generate sufficient returns to justify the investment.

For the 150 million individuals in Sub-Saharan Africa that live in areas where there is no pre-existing mobile infrastructure[60], extending networks will remain a significant economic challenge. Given the lack of commercial sustainability in these areas, alternative solutions will be required. Still to close the gap [14] between the usage and drive digital inclusion. This means that mobile data needs to be affordable for even the poorest in society.

However, despite the falling cost of data, unaffordability for the poorest quintile[61] remains significantly higher than the 2% target for all regions. In Sub-Saharan Africa, the

[58] See: http://www.telecomabc.com/u/umts900.html (accessed on 06/01/2020)
[59] See: https://www.gsma.com/spectrum/wp-content/uploads/2017/11/10-Day-2-Session-3-How-to-Implement-Spectrum-Refarming-Shola-Sanni.pdf (accessed on 06/01/2020)
[60] No 2G coverage
[61] Equivalent to 20%

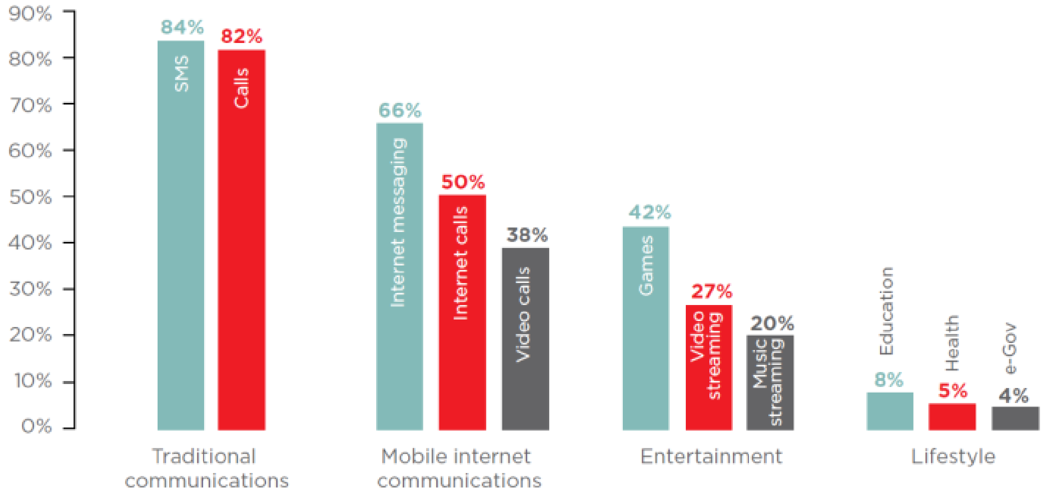
cost of 1 GB of data for the poorest quintile is almost 40% of their monthly income. In South Asia, for instance, the average affordability for that amount of data is only 1.2% of their monthly income.

5.2 Poor 5G Prospects

Concerning to 5G coverage inception in Sub-Saharan Africa [15], it is clear that Sub-Saharan Africa has more of a demand-side than a supply-side problem for mobile broadband. This is evidenced by the significant mismatch between 4G network coverage and 4G adoptions across the region.

Over 800 million people in the region are still unconnected, 62% of which are already covered by a mobile broadband network. The reason for insufficient demand in the region is mainly socio-economic and exogenous to the telecommunications industry. And, most importantly, if the demand problem is still to be addressed, all stakeholders, especially governments, should work together to ensure that broadband usage can be optimised for consumers and businesses.

That is explained due to the fact that beyond the traditional use for making calls, many customers in developing countries use their smartphones for leisure and entertainment, especially watching free online video and playing games. As video overcomes the literacy challenge, its use will continue to grow and will increasingly account for the bulk of network traffic for most operators in the region.



Source: GSMA, 2019 [15]

In terms of regional engagement levels, sub-Saharan Africa is still at the bottom globally, but two aspects are striking [16]. The first is the exponential increase of mobile money relevance in the East African Economic Community doing business, galvanized by Kenya.

The second is the consumer profile in Sub-Saharan countries, which focus mainly on entertainment content or social networking rather than on productivity services or tools, which are also available, in contrast to the consumer profile from Europe, North America and the Far East, which is precisely the opposite.

5.3 Cyber Security Threats Landscape

In 2016 [17], a number of institutions in African countries were targeted by cyber security threats. In one particular case, the attack lasted more than 12 months – spanning from October 2015 until August 2016 - and it relied on a number of weaknesses in the organisations' information and communications technologies infrastructure and processes.

The hackers conspired with malicious insiders to install malicious keylogging[62] and remote desktop software on machines dedicated for the processing of financial transactions.

[62] See: https://techterms.com/definition/keylogger (accessed on 06/01/2020)

The keylogging software was used to capture user keystrokes and send data (user account credentials, customer account information, email and chat messages) to an external cloud infrastructure.

Using these credentials, the attackers accessed the infected computers remotely and processed fraudulent Electronic, Mobile and ATM Funds Transfers. These attacks confirmed the vulnerability of the overall Sub-Saharan Africa networks and infrastructure. In effect, an assessment [17] conducted in various countries and inspection of network traffic in 10 different organisations across Africa determined 3 vectors, namely, BYOD[63], Insider threats, and Phishing Scams. In all organisations, traditional antivirus software could no longer match the new strains of malware targeting African organisations, such as Botnets[64], Ransomware, Spyware[65], Trojans[66] and Worms[67]. Common distribution channels included malicious files and links to malware hosting sites embedded in emails, social media sites, portable drives and BYOD devices.

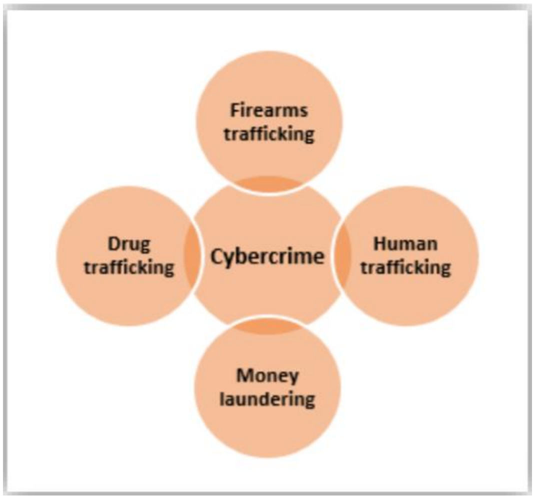
Peer to Peer (P2P)[68] connections have also been widely used for communications between infected machines and botnets. Notice that P2P connections are usually hard to detect and block at the network level using traditional methods. Thus, attackers are using this flaw to weaponise torrent software to deliver malware and enhance private communication capabilities with infected machines.

Some insights [17] revealed that Remote Access[69] software was one of the most commonly used for malicious purposes without the knowledge of the victim, along with other methods used to evade traditional antiviruses and achieve persistency. For example, the use of fileless malware,[70]which hide in locations that are hard to scan. Appendix I displays a summary of cyber security gaps in Sub-Saharan Africa in 2016. Overall [24], the nature of

[63] Stands for *Bring Your Own Device*. For further details see https://www.techopedia.com/definition/29070/bring-your-own-device-byod (accessed on 06/01/2020)
[64] See: https://www.techopedia.com/definition/384/botnet(accessed on 06/01/2020)
[65] See: https://techterms.com/definition/spyware(accessed on 06/01/2020)
[66] See: https://techterms.com/definition/trojanhorse(accessed on 06/01/2020)
[67] See: https://techterms.com/definition/worm(accessed on 06/01/2020)
[68] See: https://techterms.com/definition/p2p(accessed on 06/01/2020)
[69] See: https://techterms.com/definition/remoteaccess (accessed on 06/01/2020)
[70] See: https://us.norton.com/internetsecurity-malware-what-is-fileless-malware..html(accessed on 06/01/2020)

cybercrime cases on the continent are mostly cyber-enabled crimes, and not cybercrimes committed exclusively in cyberspace.

Cyber-enabled crimes are traditional crimes that increase the scale or reach of groups through the use of computers, computer networks, or other forms of information and communication technology.



Source: Interpol, 2019 [24]

Figure 6 – Criminal forms facilitated by cybercrime

6. CURRENT STATUS OF SMARTPHONE FORENSICS IN SUB-SAHARAN AFRICA

The analysis of the current status of digital forensics readiness in sub-Saharan African countries can be stratified into four groups. This includes smartphone forensics, which is one of its specific branches [4], [7].

South Africa, which can also be classified as Advanced[71] at the continental level, stands out for complying with internationally recognized standards and good technological and legal practices [4]. Being totally sovereign in the area, South Africa cooperates either with the European Union, Interpol, or bilaterally with similar police institutions [18]. In effect, the South Africa Police Services has general law enforcement powers to investigate an Incident under Criminal Procedure Act 51 of 1977, which sets out the procedure to be followed by the South African Police when investigating a criminal offence, which includes cyber-related offences. In this case, different agencies work together to facilitate enforcement and compliance[72].

Second, there are the Transitioners countries, composed of Kenya, Nigeria, Rwanda, Mauritius, Ghana and Senegal, which partially comply with internationally recognized technological and legal standards and good practices [4].

Kenya, which operates with M-pesa[73], one of the world's largest mobile money transfer services [18], has made great progress in the area of smartphone forensics, especially in the training of forensic experts. It should be noted that Kenya had, in 2016, the highest number of professionals, with 1,400 cyber experts, which exceeded the figures from other countries in its region, who still had the disadvantage of usually not being trained or receiving *ad-hoc* training when a cyber-incident occurs[74].

[71] Note: for better understanding by the reader, a convention similar to the GSMA report [11] is used

[72] See: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/south-africa (accessed on 13/02/2020)

[73] Note: M-Pesa is a mobile phone-based money transfer, financing and micro financing service, very popular in Kenya, Tanzania, Afghanistan, South Africa, India, and also, in Romania and Albania.

[74] See: https://www.ict.org.il/Article/2275/Cyber_threats_on_African_subjects#gsc.tab=0 (accessed on 13/02/2020)

But despite advances in the area of human resources and in the use of forensic technology[75], a serious conflict between civil society and the government persists after Kenya's president signed to law the contentious Computer Misuse and Cybercrimes Act[76]. This situation forced the suspension of the act and, consequently, the evaporation of the relevance of smartphone forensics for obtaining evidence to be presented in court.

Nigeria, on the other hand, had in 2016 the chilling rate of more than one out of every seven mobile devices in the country infected with mobile malware [18]. With important steps in the technological strengthening of law enforcement agencies, especially from 2015, to respond to this challenge, and the growth of a flourishing private sector in the area of digital forensics[77]. Even so, Nigeria still does not systematically comply with internationally recognized technological and legal standards and good practices [4]. However, Nigeria has given good indications of its intention to comply in the future [78].

In turn, Rwanda established a specialized Police department in charge of digital forensics and works closely with the local CSIRT[79] in case of computer security incidents [18]. That may include collaboration with local CERT[80] and Interpol to locate and identify the perpetrators. The country has achieved encouraging results[81]. The government of Rwanda has also a partnership with global cyber security organization such as IMPACT[82] and other national CERT's [18]. Rwanda well deserves a case study for the effective way it has

[75] See: https://www.cyberdigitalforensics.com/nairobi-digital-forensics (accessed on 13/02/2020)
[76] See: https://techweez.com/2018/06/21/lsk-seeks-enjoined-case-against-cybercrimes-act/ (accessed on 13/02/2020)
[77] See: http://cfinonline.org ; http://firstdigitalforensics.com.ng/our-clients.html ; https://www.premiumtimesng.com/news/more-news/205374-nigeria-police-launch-forensic-lab-abuja.html
[78] See: https://www.vanguardngr.com/2017/05/cybercrimeu-s-support-nigeria-fight-fraud/ (accessed on 13/02/2020)
[79] Note: CSIRT is a Computer Security Incident Response Team that is assigned the responsibility for coordinating and supporting the response to a computer security event or incident.
[80] Note: CERT is a Community Emergency Response Team that deals with the evolution of malware, viruses and other cyber-attacks.
[81] See: https://blog.comodo.com/comodo-news/new-rwandan-cybercrime-law-step-forward-in-african-cybersecurity/ (accessed on 13/02/2020)
[82] See: https://www.impactcybertrust.org/ (accessed on 22/02/2020)

prioritized synergies[83], resources[84] and cooperation programs[85] for technological modernization with tangible results[86], a dynamic that also extends to the legal area[87].

Regarding Mauritius, its Police Force has a capable Cyber Crime Unit, which has received U.S. government training[88]. Organized hacking operations by indigenous criminal groups are very limited[89], but the extent of hacking operations conducted by external actors remains unknown[90].

Regarding Ghana, officially, there has been, until 2016, a relatively low incidence of cyber-crime in the country [18]. However, as of 2017, in line with their objective of dealing effectively with cyber-crime, the Ghana Police added another two cyber-crime units to the existing one at their headquarters in Accra [91]. Though they have not yet focussed on the root causes of cybercrime[92], which have placed Ghana at the top of the sub-Saharan African countries since 2010 [25]. Furthermore, the Ghana Police still rely on conventional crime laws relating to false pretence in the criminal Code Act 29/60 Section 131 and its associate statutes. Therefore, crimes committed under these laws are bailed offences and carry lesser punishments which cannot therefore deter the fraudsters from committing cyber offences [26]. This has been offset by contracting of state-of-the-art forensic investigation services in the private sector [93].

[83] See: https://www.africa.engineering.cmu.edu/(accessed on 06/01/2020)

[84] See: https://www.maastrichtuniversity.nl/news/forensic-training-rwandan-police-officers-succesfully-completed(accessed on 06/01/2020)

[85] See: https://www.interpol.int/ar/1/1/2016/Investigating-cyber-enabled-crimes-focus-of-joint-Rwandan-and-INTERPOL-exercise(accessed on 06/01/2020)

[86] See: https://www.ktpress.rw/2018/06/new-forensic-lab-opened/(accessed on 06/01/2020)

[87] See: https://www.rwandabar.org.rw/a-forensic-evidence-cybercrimes-electronic-evidence-and-data-protection-workshop/(accessed on 06/01/2020)

[88] https://www.osac.gov/Country/Mauritius/Content/Detail/Report/e248beb4-219e-4708-a774-15f4aed12f9e

[89] See: https://www.slideshare.net/curiousEngine/cybercrime-and-computer-misuse-cases-presentation ; http://www.elandsys.com/~sm/cybercrime-facebook-mauritius.html(accessed on 13/02/2020)

[90] See: https://www.osac.gov/Country/Mauritius/Content/Detail/Report/e248beb4-219e-4708-a774-15f4aed12f9e

[91] See: https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Cybercrime-Ghana-police-to-set-up-two-cyber-crime-units-751378 (accessed on 14/02/2020)

[92] See: https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Police-Cybercrime-Unit-warns-Ghanaians-to-stop-watching-porn-with-office-computers-792082 (accessed on 14/02/2020)

[93] See: https://e-crimebureau.com/cyber-forensics/ (accessed on 14/02/2020)

In third place are the Emerging Countries, namely Senegal, Togo, Côte d'Ivoire, Mali and Republic of Congo[94]. Despite partially complying with internationally recognized technological standards and good practices [4], their Police departments do not have clear scope and legal competences in relation to cyber-crime units. They are believed to support the fight against the most common criminal forms facilitated by cyber-crime [24]. This group of French-speaking countries has capacity-building programs in digital forensics, particularly with the European Union and Interpol[95], but also, bilaterally with France under the *Francophonie*[96].

Senegal maintains a division to investigate cyber-crimes within the Interior Ministry National Police [18], called Cell Investigations Cyber Crime Unit, which has recently been equipped with new technological means[97]. Notice that cybercrime is a relatively recent issue in Senegal's judicial system[98]. Other major stakeholders concerned include the Intelligence Agency, a specialized branch within the National Police that focuses on cyber-crime [18].

In Togo, the government maintains a division specially tasked to investigate cyber-crimes within the Information and Communication Technologies Agency that is under the Ministry of Security and Civil Protection [18]. Although the legal framework has been adopted only recently in this country[99], the combined action of the judicial police and the prosecutor's office has already culminated in some cases in court[100].

In turn, Cote d'Ivoire signed a Microsoft partnership agreement for the establishment of an authorized IT Academy, which provides training to officers of the national police [18].

[94] Also known as Congo-Brazzaville

[95] See: https://www.interpol.int/en/News-and-Events/News/2019/Nigeria-and-INTERPOL-formalize-West-African-Police-Information-System-cooperation

[96] See: https://www.francophonie.org

[97] See: https://africabusinessagency.com/senegal-police-emploie-grands-moyens-cybersecurite/ (accessed on 14/02/2020)

[98] See: https://www.snap221.info/cybercriminalite-la-justice-senegalaise-et-les-effets-pervers-dinternet/ (accessed on 14/02/2020)

[99] See: https://www.togofirst.com/fr/tic/0712-2164-togo-adoption-de-la-loi-sur-la-cybersecurite-et-la-lutte-contre-la-cybercriminalite (accessed on 14/02/2020)

[100] See: https://lexpressiondz.com/info-en-continu/relizane-93-affaires-de-cybercriminalite-traites-en-2019-320353

Despite this, national police performance is still quite limited[101] in view of the intricate ramifications of this country[102] with Internet Organized Crime [1].

Regarding Mali, this country, which has been experiencing a prolonged separatist conflict with the Tuareg community, maintains a division specially tasked to investigate cyber-crimes known as the Judicial Investigation Brigade[103], even though there are currently no specific laws governing cyber-security [18]. Indeed, only in the Criminal Code can any vague reference to cyber-crime be found[104].

For its part, Republic of the Congo maintains a unit within the National Police, tasked with investigating cyber-crimes, with all cyber security issues directly supervised by the Ministry of the Interior [18]. This unit uses an approach to repress citizens' deviant behaviours[105], a trademark of *Francophonie* countries.

Finally, the Discoverers, which are countries that do not formally have police units specialized in the combat and forensic investigation of cyber-crimes. However, they are frequently requesting outsourcing from Israel, France, USA, China, Russia, or regional[106] and global[107] companies. These countries generally do not comply with internationally recognized legal standards and good practices.[4] Capacity-building programs in digital forensics, particularly with the European Union and Interpol, are irregular or practically non-existent.

[101] https://www.aljazeera.com/news/africa/2014/08/cracking-down-cybercrime-ivory-coast-20148279503515697.html (accessed on 13/02/2020)

[102] See: https://observers.france24.com/en/20090728-online-money-scammers-ivory-coast-fraud-crime (accessed on 13/02/2020)

[103] See: http://bamada.net/cybercriminalite-au-mali-la-brigade-dinvestigation-judiciaire-demantele-un-reseau-de-fraudeurs (accessed on 13/02/2020)

[104] Articles 264 and 271.

[105] See: https://feministescongo.wordpress.com/tag/cybercriminalite/ (accessed on 13/02/2020)

[106] See: https://mybroadband.co.za/news/security/119280-interception-of-communications-in-sa-you-should-be-worried.html (accessed on 13/02/2020)

[107] See: https://globalvoices.org/2016/05/16/the-government-of-mozambique-is-spying-on-its-citizens-according-to-verdade/ (accessed on 13/02/2020)

6.1 Malabo Convention Issues

In 2014, the Organization of African Unity adopted the Malabo Convention on Cyber security and Protection of Personal Data[108], which despite its breadth and relevance in the information age, has so far been ratified[109] by only 4 out of 46 sub-Saharan African countries respectively, Ghana, Guinea, Mauritius and Namibia.

In fact, a 2016 report [18] presented an overview of the 46 countries of Sub-Saharan Africa in terms of specific criminal law provisions on cybercrime and electronic evidence, showing that 11 countries seemed to have basic substantive and procedural law provisions in place[110] although implementing regulations may still be missing in some of these countries.

While 12 other countries seemed to have substantive and procedural law provisions partially in place [111], a significant part of Sub-Saharan Africa countries had neither specific legal provisions on cyber-crime nor electronic evidence in force, even having drafted laws or amendments to existing legislation that reportedly had been prepared in at least 15 countries[112].

In some instances, bills had been presented to national parliaments. In others, the fate of draft laws is uncertain. Therefore [18], [19] the state of legislation on cybercrime and electronic evidence in Africa is not satisfactory (fig.7), since 20% of the countries seemed to have the minimum legislation in place.

[108] See: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed on 06/01/2020)

[109] https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf (accessed on 06/01/2020)

[110] Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia

[111] Benin, Gambia, Kenya, Madagascar, Morocco, Mozambique, Rwanda, South Africa and Zimbabwe

[112] Burkina Faso, Djibouti, Ethiopia, Guinea, Kenya, Lesotho, Mali, Namibia, Niger, South Africa, Swaziland (e-Swatini), Togo, Tunisia, and Zimbabwe

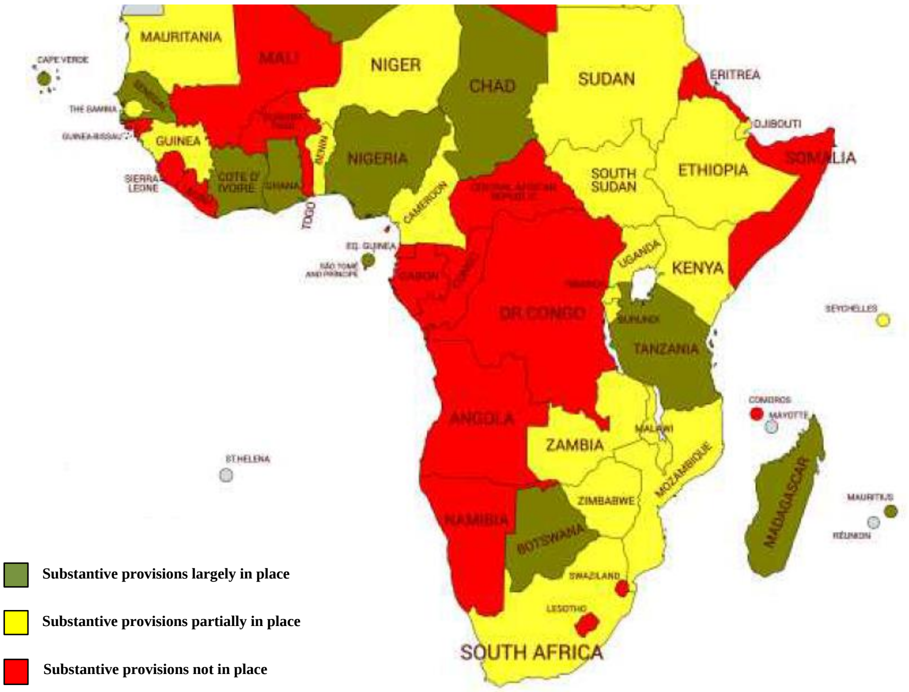
Some other key findings arose as well, for example, from the strong focus on personal data protection issues, which is often confused with over criminalisation, particularly with regard to content and speech.

The slowness of member states in transposing the Malabo Convention into local law contrasts with the influx of foreign investment and the forward thinking of some Transitioners states, which are heavily, committed to information and communication technologies, such as Nigeria and Rwanda[113].

A comparative analysis [9] of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime suggests that Malabo is broader than the Budapest Convention in regard to electronic transactions; personal data protection and cyber security and cybercrime. Furthermore [9], the Malabo Convention unites different aspects related to information technology law, also including certain non-digital and non-criminal justice issues.

With regard to these three broad lines of action of the Budapest Convention, there is an almost complete alignment with the Malabo Convention on criminal conduct and tools and procedures. On the other hand, there is almost no alignment with respect to specific provisions and the legal basis for international cooperation in cyber-crimes and obtaining electronic evidence.

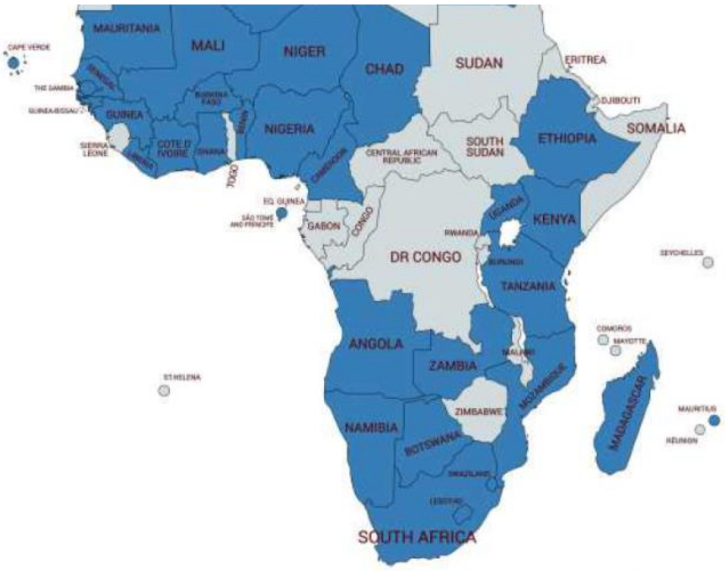
[113] https://busa.org.za/wp-content/uploads/2018/03/Public-7-Continental-Free-Trade-Agreement-Establishment-10-03-2018.pdf(accessed on 06/01/2020)



Source: Lucchetti, 2018 [9]

Figure 7 – Current status of Malabo Convention in Sub-Saharan African countries

Another point [9] that also draws attention is the high adoption rate (fig. 8) of the Budapest Convention as a reference model for the elaboration of local cyber laws, which contrasts with that of the Malabo Convention.



Source: Lucchetti, 2018 [9]

Figure 8 - Adoption rate of the Budapest Convention in Sub-Saharan Africa

6.2 Extrajudicial Surveillance

It seems that Sub-Saharan governments are more prone to *deploy sophisticated network eavesdropping tools against their citizens, kicking out any hopes of duly endorsing the* African Union Convention on Cyber Security and Personal Data Protection [114].

Supported mostly by US, French and Israeli expertise and technology [115], in most cases **spying on dissidents [116] living in the country and abroad is the main agenda, if not the only one, of an overwhelming part of** Sub-Saharan security forces. The situation has gotten prompt reaction from civil society[117], claiming, among others, against those restrictions.

As a result, the transposition of the Malabo Convention into local law should preserve the viability and usability of the internet as a platform for communications in Africa, in order to enhance its effectiveness as a driver of commerce, education, health, and development generally.

It should be emphasized that improving digital security is crucial to this effort, helping to expand global access to information and communications technologies. However, improving cyber security also entails protecting human rights [118].

[114] See: https://www.cybersecurityintelligence.com/blog/african-states-quick-to-adopt-network-surveillance--738.html(accessed on 06/01/2020)

[115] See: https://www.theafricareport.com/22841/inside-africas-increasingly-lucrative-surveillance-market/(accessed on 12/02/2020)

[116] See: https://www.cybersecurityintelligence.com/blog/ethiopian-cyber-spies-left-clues-behind-3011.html(accessed on 06/01/2020)

[117] See: https://techweez.com/2018/06/21/lsk-seeks-enjoined-case-against-cybercrimes-act/ (accessed on 12/02/2020)

[118] See: https://www.accessnow.org/access-now-brief-african-countries-can-shape-cybercrime-laws-protect-rights/(accessed on 06/01/2020)

7. DISCUSSION

The selectivity and financial damage that comes from cyber-attacks [1], particularly in countries that have already ratified the Budapest Convention, suggests that, from the perspective of criminals, the risk pays off.

On the other hand [1], the great difficulty in decoupling these attacks from the most varied forms of cyber activism is also evident, which may come from political or religious extremism, as well as from anti-establishment movements.

Other evidence [1] is the great difficulty that law enforcement agencies are facing in containing the cybercrime phenomenon, even at the regional or community level, largely because of the persistence of Darknet, whose monitoring, control and possible eradication could be achieved by, for example, more robust Online Service Provider control mechanisms. Nevertheless, this issue is particularly complex in Europe, where the process of balancing individual rights and freedoms is critical[119].

As a recent criminal phenomenon [1], cyber mules have helped to make phishing more sophisticate, which is the most relevant form of cybercrime in sub-Saharan Africa [2], [17], [18]. In order to manage this situation and other types of attacks against victims located in this region, it seems undisputable that Open-Source software still presents itself as an alternative [6] to circumvent these countries' chronic budget deficit in terms of information security, not only as isolated initiatives[120], but as long-term programs.

That does not contradict recommendations of reference bodies [4], [7] in the sense that a study of similar solutions in other regions of the world, with socioeconomic characteristics very similar to the reality of sub-Saharan Africa, is justified.

[119] See: https://ec.europa.eu/info/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_en(accessed on 06/01/2020)

[120] See: https://linux4afrika.de/en/ (accessed on 06/02/2020)

An objective analysis [9] of the state of transposition of both the Budapest Convention and the Malabo Convention into the legislation of sub-Saharan African countries shows the dual nature of the problem facing their governments.

While there are answers to the questions of local socio-economic development, the aggressive nature of neoliberal globalization, embodied in multinational corporations and related services [13], as well as the UN technical and financial assistance bodies [10],[20], cannot be ignored. That has resulted in the widening, in many cases, of the structural disparities and social inequity inherited from colonialism. **However, opting for simplistic crack-down approaches on whistle-blowers, or spying on dissidents living domestically and abroad, does not seem to be the best answer to their challenge. At worst, this can only mean a transposition of every day's reality into cyberspace.**

It also seems [9] **that the Malabo Convention was nothing more than an imperfect imitation of the Budapest Convention, with some political folklore, which copies the uncertainties and insecurities of African governments regarding the information age. The standard is that, when in doubt, the alternative is to refer to the Budapest Convention - which explains its higher adoption rate if compared to Malabo's.**

To be sure what could be expected was a greater investment in institutional capacity building of the judiciary, keeping the actions initiated long before the Malabo Summit [20]. The good news is that Sub-Saharan Law Societies appear to be up-to-date with the latest developments in cyber law[121].

Notable too, are many contributions of African scholars, who remain committed to creating a legally sustainable digital forensics, such as the University of Pretoria in South Africa [21], a country which has been experiencing particularly sophisticated ransomware attacks[122] and the University of Lagos in Nigeria [22], [23], considered today the African superpower of smartphones.

[121] See: https://www.lexafrica.com/cyber-law-block-chain-technology/(accessed on 06/01/2020)
[122] See: https://www.bbc.com/news/technology-49125853(accessed on 06/01/2020)

In conclusion, in that same reasoning, it is confirmed that the booming mobile connectivity [11], [12], [15], [16] currently taking place in sub-Saharan Africa is still dictated by the market of neoliberal globalization. In fact, since the Washington Consensus[123], the relocation of the means of production and financial transactions has become the *modus operandi* of a large number of companies in the OECD countries.

They will be the largest providers of these *quasi* low-cost services, once installed in sub-Saharan Africa, in spite of a remarkable lack of digital literacy and financial ability to pay for them nowadays. That is a very interesting aspect, since usually most consumers in sub-Saharan Africa have opted to spend their money on entertainment-related content [15]. Therefore, some of the rare success stories in the countries of the region, such as the mobile money penetration in East Africa, galvanized by Kenya, need to be studied very carefully, as well as the cyber security gaps presented here [2], [17], [18], which should also be framed in the same perspective.

Lastly, the analysis of the current status of smartphone forensics in sub-Saharan African countries shows that almost all of them do not fully comply with internationally recognized standards and good technological and legal practices [4]. Even with large investments or capacity-building programs in human resources, forensic facilities and tools from the European Union and Interpol [18], [20], mistrust persists between law societies and the governments.

Furthermore, in most of the countries, there is no well-defined structure regarding the powers and attributions of cyber-crime units within the Police departments, which often overlap with intelligence services. Thus, combined with the absence of cyber legislation in most of the countries [9], the digital evidence obtained this way does not proceed in court.

[123] See: https://www.gsid.nagoya-u.ac.jp/sotsubo/Washington%20Consensus.pdf (accessed on 06/01/2020)

8. CONCLUSION

Three important aspects can be highlighted from this discussion.

First, unlike countries in the northern hemisphere, the nature of cybercrime cases on the African continent are mostly cyber-enabled crimes, and not cybercrimes committed exclusively in cyberspace. Consequently, cyber units are shaped to act more as ancillary services to the police departments and not to coordinate across specialized cyber security areas, such as combating and preventing cyber terrorism, cybercrime, cyber espionage and cyber activism. This scenario puts them in a position of subordination, which removes the effectiveness of the response and prevention of crimes with ramifications to Organized Internet Crime.

Secondly, with mobile technology being the most widely used technology standard for accessing digital services and solutions in sub-Saharan Africa, in-depth knowledge of smartphone forensics should be at the top of the European Union and Interpol's capacity-building programs priorities. However, that has not been happening, since these bodies have a Eurocentric perspective of containing cyber-enabled crimes, namely the Darknet's African connections with the international drug, people and arms trafficking and money laundering, which are also at the top of the OECD countries' security agenda.

Thirdly, the recognition of the duality of criteria, in general, in the application of the law in Sub-Saharan Africa, which gives priority to the crime of opinion or public morality, and not to the eradication of criminal forms that are much more serious and harmful to this region of the African continent, such as *Cyber Sakawa* and many more.

Particular attention is drawn to the duplicity which the vast majority of signatory countries to the Budapest Convention deal with this repressive stance in Sub-Saharan Africa. On the one hand, they are supporting capacity-building programs for the adoption of internationally recognized legal standards and good practices. On the other hand, provide the means and technological knowledge for extrajudicial surveillance, compromising the consolidation of the rule of law. Therefore, realistic conditions should be created globally for Sub-Saharan governments to return to their traditional role of facilitators to address the current challenges of the smartphone forensics in Sub-Saharan Africa. *Dixit*.

9.REFERENCES

[1] EC3 - European Cybercrime Centre. *Internet Organised Crime Threat Assessment (Iocta) 2019*. Europol. 2019 Available for download here: https://www.europol.europa.eu/iocta-report

[2] Serianu. *Africa Cybersecurity Report 2017. Demystifying Africa's Cyber Security Poverty Line*. 2017. Available for download here: https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

[3] Ben Martini, Kim-Kwang Raymond Choo. *An Integrated Conceptual Digital Forensic Framework For Cloud Computing*. Digital Investigation 9 (2012) 71–80. Elsevier. 2012. Available for download here: https://www.sciencedirect.com/science/article/pii/S174228761200059X

[4] INTERPOL. *Global Guidelines For Digital Forensics Laboratories*. INTERPOL Global Complex for Innovation. 2019. Available for download here: https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf

[5] Naing Linn Htun & Mie Mie Su Thwin. *Proposed Workable Process Flow with Analysis Framework for Android Forensics in Cyber-Crime Investigation*. The International Journal Of Engineering And Science (IJES) || Volume || 6 || Issue || 1 || Pages || PP 82-92|| 2017 ||ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805. Available for download here: https://www.researchgate.net/publication/313049731_Proposed_Workable_Process_Flow_with_Analysis_Framework_for_Android_Forensics_in_Cyber-Crime_Investigation

[6] Matthew McMillon. Building a Low Cost Forensics Workstation. SANS Institute. 2003. Available for download here: https://www.sans.org/reading-room/whitepapers/incident/building-cost-forensics-workstation-895

[7] Rick Ayers, Sam Brothers and Wayne Jansen. Guidelines on Mobile Device Forensics. NIST Special Publication 800-101 Revision 1. 2014. Available for download here: https://csrc.nist.gov/publications/detail/sp/800-101/rev-1/final

[8] Bijoy Boban. *An Analysis on Iphone and Smart Phone Forensics*. Cyber Law and Computer Forensics. Lovely Professional University, Phagwara, Punjab, India. 2014. Available for download here:

https://www.academia.edu/6716305/AN_ANALYSIS_ON_iPHONE_AND_SMART_PHONE_FORENSICS

[9] Matteo Lucchetti. *Cybercrime Legislation in Africa Regional and International Standards*. GLACY+. Cybercrime Pogramme Office of the Council of Europe (C-PROC). 2018. Available for download here: https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-05.pres_cybercrime_legislation_in_africa_12apr2018_matteo_l.pdf

[10] World Bank. *Doing Business 2019. Training for Reform*. 2019. Available for download here: https://www.doingbusiness.org/content/dam/doingBusiness/media/Annual-Reports/English/DB2019-report_web-version.pdf

[11] Kalvin Bahia. *State of Mobile Internet Connectivity 2018*. GSM Association. 2018. Available for download here: https://www.gsmaintelligence.com/research/?file=c0bcc185be555f77478a8fdf986ea318&download

[12] GSM Association. *Sub-Saharan Africa. The Mobile Economy 2018*. 2018. Available for download here: https://www.gsmaintelligence.com/research/?file=809c442550e5487f3b1d025fdc70e23b&download

[13] PriceWaterHouseCoopers. *Disrupting Africa: Riding the Wave of the Digital Revolution*. 2017. Available for download here: https://www.pwc.com/gx/en/issues/high-growth-markets/assets/disrupting-africa-riding-the-wave-of-the-digital-revolution.pdf

[14] Kalvin Bahia & Stefano Suardi. *The State of Mobile Internet Connectivity 2019*. GSM Association. 2019. Available for download here: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/07/GSMA-State-of-Mobile-Internet-Connectivity-Report-2019.pdf

[15] Kenechi Okeleke, David George and Emeka Obiodu. *5G in Sub-Saharan Africa: Laying the Foundations*. GSM Association. 2019. Available for download here: https://www.gsmaintelligence.com/research/?file=7d4569ab4c1f69b82e9ad8f179ba92ef&download

[16] Jan Stryjak & Michael Meyer. *Evaluating Mobile Engagement*. GSM Association. 2018. Available for download here:

https://www.gsmaintelligence.com/research/?file=e608440880a26e2d36bd073a1245d26c&download

[17] Paula Musuva-Kigen, Martin Ekpeke, Emmanuel Inkoom,Beatrice Inkoom,Dadi Masesa,Brencil Kaimba,Kevin Kimani,Martin Mwangi,Barbara Munyendo,Faith Mueni,Daniel Ndegwa, Stephen Wanjuki, Nabihah Rishad, Samuel Keige, Jeff Karanja, Hilary Soita, Andrew Njuguna Ngari,Bryan Mutethia Nturibi,Denzel Ndegwa,Edward Owino,Gloria Gesicho,Ian Omondi Bwana,James Waiharo, Joylyn Chepkurui Kirui and Kenneth Mbae. *Africa Cyber Security Report 2016*. Serianu. Available for download here: https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf

[18] Symantech. *Cyber Crime & Cyber Security Trends in Africa*. 2016. Available for download here: https://www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf

[19] Lewis C. Bande. *Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities.* International Journal of Cyber Criminology Vol 12 Issue 1 January – June 2018. 2018.Available for download here: https://www.cybercrimejournal.com/BandeVol12Issue1IJCC2018.pdf

[20] UNCTAD. *Harmonizing Cyberlaws and Regulations. Experience of the East Africa Community.* 2012. Available for download here: https://unctad.org/en/PublicationsLibrary/dtlstict2012d4_en.pdf

[21] Michael Kohn, JHP Eloff and MS Olivier. *Framework for a Digital Forensic Investigation*. Information and Computer Security Architectures Research Group (ICSA). Department of Computer Science University of Pretoria. 2006. Available for download here: https://www.researchgate.net/publication/220803284_Framework_for_a_Digital_Forensic_Investigation

[22] Ajetunmobi, Rukayat A, Uwadia, Charles O, and Oladeji, Florence A. *A Survey and Critique of Digital Forensic Investigative Models*. International Journal of Computer Science and Information Security (IJCSIS),Vol. 14, No. 12, December 2016.Available for download here: https://www.academia.edu/31243408/A_Survey_and_Critique_of_Digital_Forensic_investigative_Models

[23] Rukayat A. Ajetunmobi, Charles O. Uwadia, Florence A. Oladeji.Computer *Forensic Guidelines: A Requirement for fighting Cyber Crime in Nigeria now?* Department of Computer Sciences, University of Lagos. 2016. Available for download here: https://www.academia.edu/31328029/Cybercrime_-_A_Case_for_Computer_Forensic_Guidelines_in_nigeria

[24] George Grispos, Tim Storer, William Bradley Glisson. *Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics*. University of Nebraska. 2012. Available for download here: https://www.academia.edu/2777260/CalmBefore_the_Storm_The_Challenges_of_Cloud_Computing_in_Digital_Forensics

[24] Interpol. *Overview of Serious and Organized Crime in Africa. Analytical Report*. ENACT (Enhancing Africa's response to transnational organized crime). 2018. Available for download here: https://www.interpol.int/content/download/12850/file/Overview%20of%20Serious%20and%20Organized%20crime%20in%20Africa-EN.pdf

[25] Warner, J. *Understanding Cyber-Crime in Ghana: A View from Below*. International Journal of Cyber Criminology (IJCC), Vol. 5 (1): 736–749. 2011. Available for download here: https://www.ripandscam.com/pdf/Cyber-crime-in-Ghana.pdf

[26] Boateng, R. Longe, O.B. Mbarika, W.A.V. Avevor, I. Isabalija, S.R. *Cyber Sakawa - Cybercrime and Criminality in Ghana*. Journal of Information Technology Impact. Vol. 11, No. 2, pp. 85-100. 2011. Available for download here: https://www.researchgate.net/publication/220889824_Cyber_Crime_and_Criminality_in_Ghana_Its_Forms_and_Implications

Appendix I
Table 2 – Cyber security gaps in Sub-Saharan Africa in 2016

Theme	Scenario	Consequence	Mitigation	Identified Gaps
Understanding of Cybercrime	Perceptions are different on what is an act of Cybercrime.	No standard definition. No collaboration between countries to fight cybercrime	Clear-cut definitions of cybercrime and cross-border co-operation to improve legal sanctions	How African companies can collaborate and share information on cybercrime
Monetary investments in cyber security solutions	Limited or no investments in cyber security solutions	Organisations are losing money through cybercrime	Cater for cyber security during Annual budgets. Proactive Investments in analysis and incident response.	Metrics to determine minimum budgetary allocations for cyber security for different industries
BYOD	High BYOD usage with low rates of best practice policies	Acceptable usage of company resources not defined. High risks associated with such devices	Define BYOD policies. Compliance within the workplace. Effective measures in place	Policies and best practices for the workplace
Cyber Security Management	In-house management of cyber security. Cyber security roles combined with other IT roles	Individuals assigned cyber security roles in organisations are more often overloaded with other tasks within the organisation and/or lack the necessary skill set to handle cyber incidents.	Develop in-house CSIRT, defined Information Security Departments or managed security services.	Developing, operating and maintaining cyber security functions at the work place.
Information Security	Few individuals with	Company employees lack	More training on different	Training more information

Theme	Scenario	Consequence	Mitigation	Identified Gaps
Certification & **Technical Training**	sufficient security technical training	basic information about information security foundation principles, best practices, important tools and latest technologies.	Information Security standards. Acquire information security certifications.	Security professionals
Employee Training	Employee training done mainly after a cyber security incident	Sharing information with unknown entities. Poor internet practice. Lack of preparedness after an incident assessment	Conduct regular people based risk. Develop an employee security awareness program	Developing and running and effective security awareness programs
Reporting of Cyber **Crimes**	High number of cybercrime is not reported to police, and for those that are reported, very few are followed through to prosecution.	Immature cyber security bills, laws and processes. Lack of user awareness	Adopt more mature processes for cybercrime prosecution. Involve more sectors during development of cyber laws. Universities, local groups, organisations and cyber security specialists. Raise awareness to citizens on reporting of cybercrimes	Escalation matrix for country wide cybercrime reporting.
External Threat **Analysis**	Publicly accessible IP infrastructure has unnecessary services enabled, including content	Unauthorized access to critical systems. High increase of widespread	Monitoring the latest security vulnerabilities published.	Standard configuration for systems. Continuous testing and monitoring

Theme	Scenario	Consequence	Mitigation	Identified Gaps
	management and remote administration. Misconfigured SSL certificates and encryption settings.	attacks leveraging vulnerable infrastructure	Updating the security configuration guideline	
Internal Cyber **Threat Analysis**	Use of obsolete systems and apps. Use of clear text and insecure protocols. Server misconfiguration. Use of default Credentials	Unauthorized access to critical systems. Vulnerable systems	Configuring all security mechanisms. Turning off all unused services. Setting up roles, permissions, and accounts, including disabling all default accounts or changing their passwords. Applying the latest security patches. Regular vulnerability scanning from both internal and external perspectives	Password management and best practice. Patch management best practice. Emergency patch management practices
Internal Traffic Analysis	Malware on systems. Botnets in private Infrastructures	Undetected malware on systems. Delayed incidence response	Continuous monitoring Incident response plan	Managing 24X7 monitoring. Traffic monitoring and analysis

Source: Serianu, 2017 [17]