Assessing Ethiopia's Readiness to Combat Computer-focused Crimes: A Legislative Analysis

Assessing Ethiopia's Readiness to Combat Computer-focused Crimes: A Legislative Analysis.

Molalign Asmare Jemberie: Bahir Dar University Law School, Ethiopia

&Audrey Guinchard: Essex Law School, Essex, UK

Abstract

The rapid digitalisation of Ethiopia's telecommunication services has not only brought important benefits to its economy and society but also some significant challenges, not the least an increasing vulnerability to cybercrime attacks. The Ethiopian government started to criminalise computer-focused offences in the 2004 Criminal Code by including a short list of computer crime provisions, partially completed by the 2012 Telecom Fraud Offence Proclamation. A decade later, the 2016 Computer Crime Proclamation significantly revised these offences and their punishments. Yet, the Ethiopian legislator is contemplating a third set of legislation, with the 2019 draft Computer Crime Proclamation. This article critically analyses these three legislative reforms. It contends that the 2016 Computer Crime Proclamation represents a strong positive step towards a proportionate and adapted response to computer-focused crimes. Ethiopia's current readiness to tackle cybercrime would be, however, strengthened if it were to further improve the 2016 Proclamation's provisions. The 2019 Draft Proclamation is not unfortunately the way forward. As it stands, it would perpetuate the cycle of revisions without being justified by rapid changes in technological advancement or by the specificities of cybercrimes, such as their scale and transnational dimension. For the reform to be effective and long-lasting, the legislator should simultaneously maintain the 2016 Proclamation, which successfully modernised the law, and remedied its deficiencies. Reform should notably consider the specific features of computer-focused crimes and the best experiences from international and regional standards, notably the Budapest Convention, and the AU Malabo Convention. Such an approach would reinforce Ethiopia's adequate criminalisation of computer-focused crimes cognisant of the cybercrime and cybersecurity ecosystem.

Keywords: ***computer-focused crimes, taxonomy, legislative response, gaps, punishment, proportionality***

1. INTRODUCTION

Following late telecom liberalisation in 2020 and digitisation of Ethiopian telecommunication services from the late 1990s onwards,[1] Ethiopia's access to the internet has steadily increased, reaching its peak in 2022 with a 25% internet penetration rate.[2] Despite this penetration rate slowing down to 19.4% in 2024[3] due to non-technical issues,[4] digitised telecommunication services have brought significant benefits to its economy and society.[5] The corollary, of course, has been an increasing vulnerability to cybercrime attacks, also globally on the rise.[6] This article critically analyses Ethiopia's responses to cybercrime, focusing solely on computer-focused crimes.[7] It contends that the Computer Crime Proclamation No.958/2016,[8] represents a significant and positive step towards a proportionate and adapted response to computer-dependent crimes, compared to the initial criminalisation in the 2004 Federal Democratic Republic of Ethiopian (FDRE) Criminal Code.[9] Nevertheless, Ethiopia's readiness to tackle cybercrime would be strengthened if it were to further improve the Proclamation's substantive criminal law provisions on computer-focused crimes. This article argues that the third legislation currently explored, the

[1] Federal Democratic Republic of Ethiopia, *Digital Ethiopia 2025: A Strategy for Ethiopia Inclusive Prosperity*, 51 (2020); Tsicie, Abiie and Feyissa, Cirma., Ethiopia: Past, present, and future, in Eli M. Noam, (ed.) *Telecommunications in Africa*, Oxford University Press, (1999), pp.51-78, spec, pp.53-56.

[2] Data Portal, Digital 2022: Ethiopia, Stage of the Digital in Ethiopia in 2022, https://datareportal.com/reports/digital-2022-ethiopia?rq=ethiopia%202022 (accessed July 30, 2024). From a 1.9% internet penetration reported for 2014, in Kinfe Micheal Yilma and Halefom H. Abraha, The Internet and Regulatory Response in Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media, Mizan Law Review Vol.9: No.1 (2015), 108-153, spec 110

[3] Data Portal, Digital 2024: Ethiopia, State of digital in Ethiopia in 2024, https://datareportal.com/reports/digital-2024-ethiopia (accessed on July 26, 2024).
Digital Watch Observatory, Geneva Internet Platform (digwathch), Ethiopia, https://dig.watch/countries/ethiopia (accessed on July 26, 2024).

[4] Federal Democratic Republic of Ethiopia, State of Emergency Proclamation No 6/2023, *Federal Negarit Gazzete*, (November 2023); A State of Emergency Proclamation No. 5/2021, *Federal Negarit Gazzete*, (November 2021). These Proclamations allowed for communication restrictions in some part of the countries such as Tigray, Afar, Amhara, Western Oromia and so on.

[5] Elvis Melia, *The Impact of Information and Communication Technologies on Jobs in Africa: A Literature Review,* Deutsches Institut für Entwicklungspolitik (giz), 30 (2019); Tsicie and Feyissa *supra* note 1.

[6] For Ethiopia, Kinfe Micheal Yilma, Developments in Cybercrime Law and Practice in Ethiopia, *Computer Law & Security Review* Vol.30: No.6, (2014) p. 720, pp. 720-721; globally, Stein Schjolberg, The Road in Cyberspace to United Nations: A Report on the Development of Global Cyber security Since 2008 and Recommendations for Future Initiatives, 63, 2007-2008 (HLEG, GCA, ITU), (2018) p.1.

[7] Also called computer-dependent crimes, *see* Thomas Holt and Adam Bossler, Introduction, in Thomas Holt and Adam Bossler, *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offences*, Routledge (2015), p.7; Jonathan Clough, *Principles of Cybercrime*, Cambridge University Press, (2015), pp.10-12; *see* discussion infra, II.

[8] A Proclamation to Provide for the Computer Crime, Proclamation No. 958/2016, *Federal Negarit Gazeta*, 22nd Year No. 83, (Addis Ababa 7th July, 2016), Article 5. [hereinafter the 2016 Proclamation]. The text is available on Federal Democratic Republic of Ethiopia, Ministry of Innovation and Technology website at https://mint.gov.et/docs/telecom-fraud-offence-proclamation-no-761-2012/?lang=en (accessed on July 30, 2024).

[9] *See* the Criminal Code of the Federal Democratic Republic of Ethiopia, *Negarit Gazzeta*, Proclamation No.414/2004, 9th of May, Article 706-711, (2004), [hereafter the "2004 Criminal Code"]. Book VI "Crimes against Property," Chapter III "Crimes against Right in Property," Section II "Computer Crimes" from Articles 705-711.

2019 Draft Proclamation, is not the way forward.[10] To be effective and long-lasting, tailored to cybercrime's specificities and able to withstand the rapid technological advancement characteristic of digital technologies, the proposed text should be substantially revised, should the legislator decide to go forward with it.

Introduced in 1894, Ethiopia's telecommunication network struggled to expand and recover from the Italo-Ethiopian wars of the first half of the 20th century.[11] It took a series of market reforms in 1996 to broaden its telecommunication services, offering mobile services by 1999, 3G in 2001, roaming by 2003 and broadband in 2004.[12] With this rise in quality telecommunications, the threat of cybercrimes became an increasing possibility, calling for the newly reintroduced Ethiopian Federal Government to regulate the use of information technology in the country.[13] Ethiopia used the revision of the 1957 Penal Code to introduce a specific chapter on *Computer Crimes* in its 2004 Criminal Code.[14] Multiple sources inspired the drafting of this first cybercrime legislation, notably: the Convention on Cybercrime n. 185[15], despite Ethiopia not being a signatory; and the US and UK legislations.[16] The Ethiopian Government's commitment to tackle cybercrime was later reinforced with the introduction of the 2009 Information and Communication Technology Policy, the 2011 National Information Security Policy, and the 2011 Criminal Justice Policy.[17]

[10] The Draft Proclamation to Provide for the Regulation of Computer Crime, Computer Proclamation No…./2019, at Article 3. [hereinafter the 2019 draft Proclamation].

[11] Tsicie and Feyissa *supra* note 1; ITU, *Internet from the Horn of Africa: Ethiopia Case Study*, Geneva, (July 2002) pp.6-12 available at https://www.itu.int/osg/spu/casestudies/ETH_CS1.pdf (accessed on July 30, 2024). [hereinafter "ITU: Ethiopia Case Study"]; Timothy John Charles Kelly, "Concept Project Information Document (PID)-Ethiopia Digital Foundations Project-P171034." World Bank Group (2019), p.47 – the World Bank Group had financed some of the telecommunication infrastructures; Taye E. Dubale*, Telecommunication in Ethiopia*, in UNTCAD, Multi-Year Expert Meeting on Services, Development and Trade: The Regulatory and Institutional Dimension, (Geneva, 17-19 March 2010) p.2. Can also be consulted The Ethiopian Telecommunications Corporation (ETC), *Birds Eye View of the Ethiopian Telecommunications Corporation in the Past Millennium, Tele Negarit,* 44:1 (2007), pp.40-43.; and *Brief Historical Review of Telecom Sector in Ethiopia*, https://www.ethiotelecom.et/history/ (accessed on July 30, 2024).

[12] Id. Yilma and Abraha, *supra* note 2, pp.114-119.

[13] The federal structure was re-introduced in 1991, followed by a new constitution in 1995, Constitution of the Federal Democratic Republic of Ethiopia (FDRE) Constitution, (21 August, 1995), Article 5 (2). *See* notably Yilma *supra* note 6, pp. 720-721.

[14] For the 2004 Criminal Code, *supra* note 9; the Penal Code of The Empire of Ethiopia 1957, Proclamation No. 158 of 1957, *Negarit Gazeta, Gazette Extraordinary,* 23 July 1957. The technology born crimes was not criminalized in the Penal Code.

[15] Council of Europe, *Convention on Cybercrime*, ETS 185, 23.XI, Budapest, (2001). [hereinafter the "Budapest Convention"].

[16] *See* የኢትዮጵያ ፌዴራላዊ ዲሞክራሲያዊ ሪፐብሊክ የተሻሻለው የወንጀል ሕግ ሐተታ ዘምክንያት (Explanatory Note to the 2004 Criminal Code). [original language was in *Amharic*, translation: mine]. [hereinafter "Explanatory Note to the Criminal Code"]. As stated in the Explanatory Note to the 2004 the Criminal Code, the main sources of national criminal code computer crime provisions are the 1990 Massachusetts "Act to Prevent Computer Crime", the 1994 Texas "Computer Crime Statute," the 1990 UK "Computer Misuse Act", the USA "Fraud and Related Activity in Connection with Computer".

[17] These policies contribute to a country's readiness to fight cybercrime. *See* notably: Marco Gercke, Understanding cybercrime: a guide for developing countries, *International Telecommunications Union* (2009), pp.63-83; Marco Gercke, Understanding cybercrime: Phenomena, challenges and legal response, *International Telecommunication Union* 366 (2012), pp.97-113, 169-280; UNODC, Comprehensive Study on Cybercrime, February 2013; M. Y. Ayenew, Assessment of Cybercrime Governance in Ethiopia Since 2004, *New Media and Mass Communication* Vol.96 (2021) p.1 DOI: 10.7176/nmmc/96-01; Beatrice Brunhöber, *Criminal Law of Global Digitality:*

Nevertheless, the Code suffered from some weaknesses, not least the non-criminalisation of illegal interception.[18] In 2012, the Telecom Fraud Offense Proclamation partly attempted to tackle some of the Code's deficiencies concerning cyberattacks against the telecom critical infrastructures.[19] These inadequacies of the first wave of legislations led to a legislative overhaul barely a decade later, along with further revisions of the above policies.[20] At the heart of this second wave of legislative reforms, is the 2016 Proclamation, which repealed the Computer Crimes chapter of the Code as well as Article 5 of the 2012 Proclamation, followed soon after by a new ICT Policy.[21] The 2016 Proclamation's drafting committee conducted extensive research on cybercrime, identifying prevalent attacks and vulnerabilities, and examining gaps in relevant laws.[22] It also consulted international standards, model laws, and national legislation to align the law with the international aspect of computer crimes. Despite Ethiopia not being a signatory to both, the Budapest Convention and the future Malabo Convention[23] had a noticeable influence on the Ethiopian legislature.[24]

Characteristics and Critique of Cybercrime Law, in Matthias C. Kettemann, Alexander Peukert, and Indra Spiecker gen. Döhmann, *The Law Of Global Digitality,* Routledge (2022) pp223, 245-247. *See* also Michal Choraś, Rafal Kozik, Andrew Churchill, and Artsiom Yautsiukhin, Are We Doing All the Right Things to Counter Cybercrime? *in* Babak Akhgar and Ben Brewster, (eds) *Combatting Cybercrime and Cyberterrorism. Advanced Sciences and Technologies for Security Applications*, Springer, (2016), p. 279.

[18] *See* e.g. Yilma, *supra* note 6; Yilma and Abraha, *supra* note 2.

[19] A Proclamation on Telecom Fraud Offense, Proclamation No.761/2012, Federal *Negrait Gazeta*, (September, 2012). [hereinafter the "2012 Telecom Fraud Proclamation"]. Article 5 of the Proclamation that deals with computer related crimes has been repealed by the 2016 Computer Crime Proclamation.

[20] Kinfe Micheal Yilma, Some Remarks on Ethiopia's New Cybercrime Legislation, *Mizan Law Review* Vol.10: No.2, (2016), pp. 448, 453-454; Kinfe Micheal Yilma, Ethiopia's New Cybercrime Legislation: Some Reflections, *Computer Law& Security Review*, Vol. 33, (2017), p. 250.

[21] Soon after, there are also the Federal Democratic Republic of Ethiopia, National Information and Communication Technology Policy and Strategy, (September, 2017). [hereinafter the 2017 New ICT Policy].

[22] የኮምፒውተር ወንጀል አዋጅ ማብራሪያ (The Explanatory Note to the Computer Crime Proclamation), 2-4 (2016) [original language was in *Amharic*, translation: mine]. [hereinafter "Explanatory Note to Computer Crime Proclamation"].

[23] The Draft African Union (AU) Convention on the Establishment of a Credible Legal Framework for Cyber-security in Africa, AU Draft Version, (2011), and later adopted as the African Union, the *African Union Convention on Cyber Security and Personal Data Protection*, 27 June 2014 (EX.CL/846(XXV)). [hereinafter the "Malabo Convention"].

[24] Notably: ITU, Computer Crime and Cybercrime: Southern African Development Community (SADC) Model Law, Harmonization of ICT Policies in Sub-Saharan Africa (HIPSSA). (2013). [hereinafter the "ITU SADC Model Law"]; United Nations Economic and Social Commission for West Asia (ESCWA) (2007), *Models for Cyber Legislation in ESCWA Member Countries*, E/ESCWA/ ICTD/2007/8, Beirut: ESSWA [hereinafter the ESCWA Model Legislation]; G8 Communiqué, Meeting of Justice and Interior Ministers, December 9–10, 1997, *Communiqué Annex: Principles and Action Plan to Combat High-Tech crime*, available at https://www.justice.gov/sites/default/files/ag/legacy/2004/06/08/97Communique.pdf (last visited on July 31, 2024); and UN General Assembly Resolutions from 1990-2004: The UN General Assembly Resolution 45/121, *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, A/RES/45/121, (14 December 1990); The UN General Assembly Resolution 55/59, *Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century*, A/RES/55/59**,** **(**4 December 2000); The UN General Assembly Resolution 55/63, *Combating the Criminal Misuse of Information Technologies,* A/RES/55/63, (4 December 2000); The UN General Assembly Resolution 56/121, *Combating the Criminal Misuse of Information Technologies,* A/RES/56/121, (19 December 2001); The UN General Assembly Resolution 57/239, *Creation of a Global Culture of Cyber-security,* A/RES/57/239, as annexed, (20 December 2002); and The UN General Assembly Resolution 58/99, *Creation of a Global Culture of Cyber-security and the Protection of Critical Information Infrastructures***,** A/RES/58/199, (23 December 2003).

The 2016 Proclamation's scope is wider than the particular focus of this article. This *lex speciali* created computer-content crimes, including terrorism; and introduced legal mechanisms to prevent, control, investigate, and prosecute computer crimes, and collect evidence.[25] These provisions have been heavily criticised for favouring law enforcement authorities to the detriment of basic protection of human rights, especially freedom of expression.[26] In contrast, its Articles on computer-focused crimes have not attracted comments, whether praises or criticisms, although they represent a significant modernisation of the 2004 offences.[27] Furthermore, the 2019 Draft Proclamation proposes further amendments to the computer-focused offences, in addition to possibly remedying the controversial aspects of the Proclamation.[28]

This frequent cycle of revisions of the criminal law framework raises the question of the legislation's adequacy in tackling computer-focused crimes. Are the revisions justified by the need to update the criminal law to account for new, unforeseeable *modi operandi* and rapid technological advancement? Or are they the symptom of the legislator's difficulty in structuring the criminal law to capture the specificities of cybercrime while remaining technologically neutral? One way to measure this adequacy could be by looking at the number of crime reports, prosecutions and convictions for computer-focused crimes. Yet, reliable national statistics on cybercrimes are notoriously lacking;[29] and there is a 'conspicuous divergence' between reported cybercrimes and successful prosecutions, even in countries where cybercrime legislation is several decades old and statistical tools already exist albeit in need of tweaking as in the UK.[30] Ethiopia is no different in this respect, with only a few reported cases[31] and a paucity of information on cyber-attacks due to poor reporting.[32] A more fruitful approach to evaluate the adequacy of

[25] The 2016 Proclamation, *supra* note 8.

[26] Article 19, Ethiopia*: Computer Crime Proclamation: Leal Analysis,* Free World Center, (2016) pp. 1-32; Dagne Jembere & Alemu Meheretu. (2018). Implications of the Ethiopian Computer Crime Proclamation on Freedom of Expression. *Jimma University Journal of Law*, Vol. 10, (2018) https://doi.org/10.46404/jlaw.v10i0.989; Shishay Abraha Mehari, Implications of the Ethiopian Computer Crime Proclamation on the Enjoyment of Human Rights, *Ijrar- International Journal Of Research And Analytical Reviews* Vol.7: No. 2, (2020) p.110, 116-119. For an overview on freedom of expression, *see* also Freedom House, *Freedom on the Net 2021, Ethiopia*, https://freedomhouse.org/country/ethiopia/freedom-net/2021 (accessed on Sept., 22, 2021).

[27] *See* Yilma *supra* note 20.

[28] The 2019 draft Proclamation, supra note 10, Art. 3; Kinfe Micheal Yilma, Cybercrime Lawmaking and Human Rights in Ethiopia, *Mizan Law Review* Vol. 15: No.1, (2021), pp.73-106.

[29] Gargi Sarkar & Sandeep K. Shukla, Behavioral Analysis of Cybercrime: Paving The Way For Effective Policing Strategies, *Journal Of Economic Criminology* Vol. 2, (2023), p.1*,* 7. On the lack of statistics, Clough, *supra* note 7, pp.15-16; David S. Wall, *Cybercrime : the transformation of crime in the information age*, Polity (2007), pp.25-40; Audrey Guinchard, Between hype and understatement: reassessing cyber risks as a security strategy, *Journal of Strategic Security* Vol. 4: No. 2, (2011), pp. 75-96; Bert-Jaap Koops, The Internet and its opportunities for cybercrime, in M. Herzog-Evans (Ed.), *Transnational Criminology Manual,* Wolf Legal Publishers (2010), pp. 735-754; Alisdair A. Gillespie, *Cybercrime: Key Issues and Debates*, 2nd edition, Routledge, (2019), ch 1; Ian Walden, *Computer Crimes and Digital Investigations,* Second Edition, Oxford University Press, (2016), p. 7; Ian Walden, Crime and Security in Cybercrime, *Cambridge Review Of International Relations* Vol. 18: No.1 (2005), p. 51, 53.

[30] For a summary on the UK for example, see Appendix B, in Criminal Law Reform Now Network, Reforming the Computer Misuse Act 1990, Report, (2020) http://www.clrnn.co.uk/publications-reports/ (accessed on July 27, 2024).

[31] Yilma, *supra* note 28.

[32] For an unofficially sanctioned survey, *see* the work of Hailu, Halefom, The state of cybercrime governance in Ethiopia. *Article published on ResearchGate, available at https://www. researchgate. com* (2015); *see* also the Ethiopian Monitor, *INSA Thwarts 787 Cyber-Attacks on Ethiopia in 2019/20 FY*, https://ethiopianmonitor.com/2020/08/24/insa-thwarts-787-cyber-attacks-on-ethiopia-in-2019-20-fy/ (accessed on July 2, 2024).

substantive criminal law is to analyse the structure of the offences and their penalties by reference to existing international legal instruments, notably the Budapest Convention, even though a country such as Ethiopia has not ratified the Convention. The specificities of cybercrimes, especially their large-scale and transnational nature, call indeed for national legislators to establish a common legal ground for the criminalisation and punishment of computer-focused crimes. This allows for their country to avoid becoming a safe haven where cybercriminals cannot be prosecuted simply based on deficiencies in the criminalisation of the relevant offences.[33]

This article therefore has adopted a doctrinal approach to examine the criminalisation of computer-focused behaviours. It argues that the 2016 Proclamation, compared with the 2004 Code, significantly improved the criminalisation of computer-focused offences and their punishment. Further improvements can still be sought, not because of technological advancement justifying a third reform, but because of the Proclamation's deficiencies in articulating some aspects of cybercrime offences and their penalties. This article will thus start with section 2 on the contextualisation of Ethiopia's cybercrime legislative response, to critically review the current taxonomies in cybercrime legal instruments and scholarly work and sketch the conceptual framework on proportionate penalties. It will then analyse how the 2016 Proclamation has articulated the computer-focused offences (section 3), and their penalties (section 4), both by reference to the 2004 Code and in anticipation of the third revision, i.e. the 2019 Draft Proclamation. It then concludes in section 5 that the 2019 Draft Proclamation would need important revisions to adequately complement the current 2016 Proclamation and provide Ethiopia with a fully adequate substantive criminal law framework.

2. CONTEXTUALISING ETHIOPIA'S LEGISLATIVE RESPONSES TO CYBERCRIMES

Due to the frequently large-scale nature and transnational dimension of cyberattacks, the fight against cybercrime calls for a baseline, a common denominator, which for substantive criminal law, means establishing a taxonomy of offences to inform their criminalisation as much as their punishment.[34]

2.1 Defining cybercrimes: taxonomies to inform criminalisation

The term cybercrime may have become a familiar occurrence, but it remains ill-defined, often used interchangeably with other expressions such as *computer crime, e-crime, internet crime, digital*

[33] The Council of Europe, Committee of Experts on Crime in Cyber-Space, *Explanatory Report to the Convention on Cybercrime*, Explanatory Report–ETS 185–Cybercrime (Convention), Budapest, 23.XI.2001, (2001). [hereinafter the "Explanatory Report to the Budapest Convention"]; UNODC, *supra* note 17; Helena Carrapico & Benjamin Farrand, Cybercrime as a Fragmented Policy Field in the Context of the Area of Freedom, Security and Justice, in Ariadna Ripoll Servent and Florian Trauner, (eds), *The Routledge Handbook Of Justice And Home Affairs Research*, Routledge, (2017), pp. 146-156, 148; Wang Qianyum, *A Comparative Study of Cybercrime in Criminal Law: China, United States, England, Singapore and The Council of Europe,* PhD Thesis, Erasmus University: Rotterdam, unpublished, 342-353 (2016).

[34] Jeremy Horder, *Ashworth's Principles of Criminal Law*, 10th edition, Oxford University Press, (2022), ch. 4; Jeremy Horder, The Classification of Crimes and the Special Part of the Criminal Law, in Robin Antony Duff and Stuart Green, *Defining Crimes: Essays on the Special Part of the Criminal Law*, Oxford University Press (2005), p.21; Andrew P. Simester and Andreas Von Hirsch, *Crimes, harms, and wrongs: On the principles of criminalisation*, Bloomsbury Publishing, (2011), pp 202-208; George P. Fletcher, *The Grammar of Criminal Law: American, Comparative, And International: Volume One: Foundations*. Oxford University Press, 2007, pp 69-80; similarly, Ian Walden, (2016), *supra* note 29, p. 26.

crime, online crime, virtual crime, techno-crime, and *networked crime*.[35] The legal field has indeed no accepted definition for the term cybercrime. At the international level, neither the Budapest Convention nor the Malabo Convention, nor for that matter, the UN Draft Convention, have defined the term. [36] The meaning of 'cybercrime' can be derived from the broad range of offences the texts criminalise. These offences widely differ in their constitutive elements and rationale, ranging from hacking to unauthorised interference, fraud, child pornography and, for the Budapest Convention only, copyright infringements. At a national level, Ethiopia's 2016 Proclamation chose a different approach, also adopted by the 2019 Draft Proclamation. Its Article 2 expressly defines 'computer crime' by means of three categories of offences: those 'against a computer, computer system, data or network'; the 'conventional crime[s] committed by means' of digital technologies, such as fraud; and the content-related crimes, such as child pornography. At the policy level, the 2021 Draft National Cybersecurity Policy and Strategy of Ethiopia adopts a similarly broad definition of cybercrime as a crime committed by using information and communication technologies and networks, particularly the Internet.[37]

In the absence of an accepted legal definition of cybercrime, scholars of non-legal disciplines have proposed various classifications, noting the difficulties in establishing relevant taxonomies, with some authors adapting over time their proposed categories to better account for the cyber

[35] For example, in the law literature, Clough, supra note 7, ch. 1; Walden, *supra* note 29, ch 2; Marc D. Goodman and Susan W. Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, *International Journal of Law & Information Technology,* Vol.10 No.2 (2002), pp.139-223.; Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, and Sapna Tyagi, *Cybercrime, Digital Forensics and Jurisdiction*, Vol. 593. Springer, (2015), ch 1; in criminology, Wall supra note 29, ch 2; Michael McGuire, It Ain't What It Is, It's The Way That They Do It? Why We Still Don't Understand Cybercrime, in Leukfeldt Rutger and Thomas J. Holt, (eds) *The Human Factor of Cybercrime*, Routledge (2019), 3-28, 8. Matthew David, *Networked Crime. Does the Digital Make the Difference?* Bristol University Press 2023, ch 1; Ravinder Barn & Balbir Barn, An Ontological Representation of a Taxonomy for Cybercrime, Research Papers. 45, *in* 24TH European Conference on Information Systems (ECIS 2016) 1, (2016), https://aisel.aisnet.org/ecis2016_rp/45 (accessed July 30, 2024).

[36] UN draft Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, A/AC.291/22/Rev.3 (Reconvened concluding session of the Ad Hoc Committee (July 29 – August 9, 2024) https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_reconvened_concluding_session/main (accessed July 30, 2024).

[37] The Federal Democratic Republic of Ethiopia National Cyber-security Policy and Strategy, draft 1.0, Addis Ababa, 2 (February, 2021), at iii. [hereinafter "the 2021 Draft Cyber Security Policy," original document in Amharic, translation: mine].

behaviours.[38] Legal scholars have been less adventurous,[39] mostly following the classification of the international legal instruments[40] used by international organisations.[41] The consensus on the taxonomy of cybercrimes in law is thus to classify them into three categories, computer-focused crimes or computer-dependent crimes, computer-related crimes, and content-related crimes, the last two sets pre-existing the emergence of digital technologies, albeit at times needing some adaptations.[42] The fourth and last category of copyright-related offences present in the Budapest Convention has not been widely adopted. This article concerns only the first category, which the Budapest Convention has defined by reference to the computer-science-based triad of confidentiality, integrity and availability.[43] Sometimes nicknamed "true" cybercrimes,[44] these offences were created to palliate the weaknesses of the traditional criminal law offences which could not capture the relevant cyber-behaviours. There are thus five offences: *illegal access*, *illegal interception*, *data interference*, *system interference*, and *misuse of devices*.[45]

Behind these debates on taxonomy is at stake the ability of the law to criminalise cyber-behaviours without depending on a particular digital technology while still accounting for the relevant specificities of cybercrimes. Therefore, two questions, at this stage, matter: what are the characteristics specific to computer-focused crimes and to what extent the criminal law can and

[38] In criminology, notably Wall, *supra* note 29; David S. Wall, The Internet as a Conduit for Criminals, in April Pattavina (ed.) *Information Technology and the Criminal Justice System*, Sage (2005), pp.77-98, 82 (2005) as revised in 2015; Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar. *Cybercrime and digital forensics: An introduction*. *An Introduction,* Routledge, (2022), ch. 1; in psychology and criminology, Kirsty Phillips, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele, and Mary P. Aiken, Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies, *Forensic Sciences*, Vol. 2: No. 2 (2022), p.379, 383-389; Douglas Thomas and Brian Loader, Introduction, in Douglas Thoms and Brian Loader, (eds), *Cybercrime: Law Enforcement, Security And Surveillance In The Information Age*, Psychology Press (2003), p3.; in computer science and business studies, Charlette Donalds and Kweku-Muata Osei-Bryson, Toward a cybercrime classification ontology: A knowledge-based approach, *Computers in Human Behavior,* Vol 92 (2019), p.403; in computer science alone, *see* Sarah Gordon and Richard Ford, *On the definition and classification of cybercrime*, Journal In Computer Virology, Vol. 13: No. 2, (2006) 14; George Tsakalidis, Kostas Vergidis, and Michael Madas, Cybercrime offences: Identification, classification and adaptive response, in 2018 5th International Conference On Control, Decision And Information Technologies, IEEE, (2018), p.470.

[39] For e.g., Walden (2016), *supra* note 29, ch 2; Clough, *supra* note 7, p.17; Gillespie, *supra* note 29, pp. 3-7; Goodman and Brenner, *supra* note 35.

[40] The Budapest Convention, *supra* note 15; Malabo Convention, *supra* note 23; Commonwealth of Independent States, Agreement on Cooperation in Combating Offences related to Computer Information, (2001); ITU-SADC Model Law, *supra* note 19.

[41] From early on: Council of Europe, Computer-related crime : recommendation no. R. (89) 9 on computer-related crime and final report of the European Committee on Crime Problems, (1990), p.12-14; [hereinafter the "Bequai Report Council of Europe R(89)9"]; OECD Information Computer Communications Policy, *Computer-related Crime: analysis of legal policy*, 1986) ch 1; United Nations, United Nations Manual on the Prevention and Control of Computer-Related Crime; United Nations: New York, NY, USA, (1994); UN draft Convention, *supra* note 40.

[42] Goodman and Brenner, *supra* note 35.

[43] The Budapest Convention, *supra* note 15, Section 1, Title 1, Art. 2-6; on the triad, ENISA, *Guidelines for SMEs on the security of personal data processing*, December 2016, p.10 at https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing (accessed on July 27, 2024); Jeroen Van Der Ham, Toward a Better Understanding of 'Cybersecurity, *Digital Threats: Research and Practice*, Vol. 2: No. 3, (2021) pp 1–3

[44] Wall, *supra* note 29, ch 4; *see* also David S. Wall, *What are Cybercrimes?*, Crime And Justice Studies, No 58 (2004/05) 20, https://www.crimeandjustice.org.uk/sites/crimeandjustice.org.uk/files/09627250408553239.pdf (accessed July 30, 2024)

[45] The Budapest Convention, *supra* note 15, Articles 2-6.

should account for them when shaping its response? International legal instruments as well as scholars agree on the positive and adverse impacts that digital technologies have on our daily lives, usually citing as characteristics of cybercrime: the absence of a physical crime scene, including the intangibility of data and offender's relative anonymity; the scale and the transnational dimension of the crimes; as well as the speed and technical nature of cybercrimes, with rapid technical advancement fuelling the impact of the other characteristics.[46] These specificities undoubtedly affect the procedural response, creating new challenges for victims to report crimes and for investigators to meet the standards of evidence in criminal law and collaborate in transnational investigations.[47]

For substantive criminal law purposes, which is the sole focus of this article, these elements are less prominent. Computer-focused crimes have arisen as a response to the difficulties of traditional criminal law to account for behaviours created using technologies. Nevertheless, these new offences also need to be broadly defined to encompass a diversity of situations, targets and means to commit them. Consequently, while the law cannot ignore the specific characteristics of cybercrime, it has to be, paradoxically, technologically neutral to anticipate technological innovations. Legislators also have to balance the need for the law to be specific enough to avoid a challenge of vagueness, while not being too narrow to avoid becoming outdated by technological advancement.[48] Criminal law has long been familiar with this balancing act. For example, the constitutive elements of fraud, a traditional offence pre-existing the digital technologies, include the offender's misrepresentation of reality with their intention for their victim to depart with property, instead of describing the myriads of ways and technologies constitutive of the misrepresentation.[49] Computer-focused crimes are no different in that respect.[50] International legal instruments have strived to define these offences in the most technologically neutral way so that they do not need constant updating.[51] In that respect, it is probably a testimony to the quality and pervasive influence of the Budapest Convention that the multiple drafts of the UN Convention have adopted definitions of computer-focused crimes that are similar, if not identical, to those of

[46] *See* the Bequai Report Council of Europe R(89)9, *supra* note 41, pp.18-20; Preambles of the Budapest and Malabo Conventions, *supra* note 15 and 23, and UN draft Convention, *supra* note 36; UNODC, *supra* note 17. For scholarly work, *see* notably Gillespie, *supra* note 29, ch. 1; Clough, *supra* note 7, p219; Wall, *supra* note 29, ch. 2; Maryke Silalahi Nuth, Taking Advantage of New Technologies: For and Against Crime, *Computer Law & Security Report*, Vol. 24, No. 5, (2008) p. 437; Goodman & Brenner, *supra* note 35; *see* also Holt, Bossler and Seifried-Spellar, *supra* note 41, ch. 12-14; Marc Rogers, Natalie D. Smoak, and Jia Liu, Self-Reported Deviant Computer Behavior: A Big-5, Moral Choice, And Manipulative Exploitive Behavior Analysis, *Deviant behavior* Vol. 27, No. 3, (2006), p. 245.

[47] Gillespie, *supra* note 29, p. 9; Walden (2016), *supra* note 29, ch. 6 and 7; *see* notably, for non-Western countries, Sarika Kader and Anthony Minnaar, Cybercrime Investigations: Cyber-Processes for Detecting of Cybercriminal Activities, Cyber-Intelligence and Evidence Gathering, *Acta Criminologica: African Journal of Criminology & Victimology,* No.5, (2015) p. 67, 71.

[48] As noted as far back as 1989, the Bequai Report Council of Europe R(89)9, *supra* note 41, pp.22-24.

[49] Again as noted very early on, R(89) Report Bequai, pp22-24; for a more modern, specific, comment, *see* for example, John Price, *Dealing with fraud: A regulator's perspective*, Australian Securities & Investments Commission (Speech delivered at the Association of Certified Fraud Examiners Melbourne Chapter annual seminar, Melbourne, 10 (November 2015).

[50] *Id.*

[51] *See,* for example, the definition of data, without any reference to a possible technology other than the most basic and neutral words indicative of the digital component, i.e. a computer system and program, Budapest Convention, Art. 2.

the Budapest Convention.[52] The taxonomy in these international legal instruments becomes therefore a crucial point of reference, providing national legislators with a framework to define the offences so that their criminal law can pass the test of time, without multiple revisions, even when they have not been ratified, as it is the case of Ethiopia.[53] Taxonomy also represents a crucial first step for the law to then identify the degree of seriousness each of the criminalised behaviours reveals, so that the criminal law's response remains proportionate and dissuasive, with corresponding punishment.

2.2 Defining cybercrimes: taxonomies to establish proportionate penalties

Prevalent in punishment theories, the proportionality principle states that the severity of punishments should be proportionate to the severity of the offence.[54] The academic literature on proportionality in punishment is vast and often includes not only the legislative process of choosing and grading penalties but also the sentencing stage whereby the judge will take into account other considerations than just the ordinal proportionality that the legislator stated for a particular crime.[55] Giving the paucity of reported cybercrime cases, this article will focus solely on the choices the Ethiopian legislator made in terms of ordinal proportionality. Therefore, it will analyse how the legislator scaled penalties based on the comparative seriousness of computer-focused crimes.[56]

Ordinal proportionality involves two sub-requirements: *parity* and *rank-ordering.* Parity allows for differences in punishments only if they reflect variations in the degree of blameworthiness of the conduct. Similar crimes should receive a similar assessment of severity unless special circumstances are identified. Rank-ordering requires punishments to be ordered on a scale that reflects the seriousness rankings of the crimes involved.[57] This restricts internal variation for crime prevention purposes, such as imposing exemplary penalties for a specific offence, outside the scale established and with no valid justification. The language of criminal law has evolved to ascertain offences' respective degree of seriousness along three central concepts, which are reflected in the general part of the 2004 Criminal Code: the criminal pathway that runs from the thought process (the least serious) up to achieving the result, itself an indicator of the harm to be avoided; culpability (intention or negligence); and circumstances surrounding the commission of the

[52] *See* UN draft Convention, *supra* note 36, Chapter 2. In that sense, before the writing of the UN draft Convention, Jonathan Clough, A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation, *Monash University Law Review*, Vol. 40, No. 3, (2014), p. 698, 729.

[53] *See* notably Clough, *supra* note 7, p. 27; Walden (2016), *supra* note 29, p. 19.

[54] Horder (2022), *supra* note 34, ch 1; Fletcher, *supra* note 34, ch 6; Lucia Zedner, *Criminal Justice*, Clarendon Law Series, OUP (2004) ch 3. The life-long work of Andrew von Hirsch dominates modern criminal law. *See* notably: Andrew von Hirsch, Proportionality in the Philosophy of Punishment, *Crime and Justice*, Vol. 16, (1992), p.55; and Andrew von Hirsch and Andrew Ashworth, *Proportionate Sentencing: Exploring the Principles*, Oxford University Press, (2005).

[55] Matt Matravers, The Place of Proportionality in Penal Theory, in Michael Tornry (ed.), *Of One-Eyed And Toothless Miscreants: Making The Punishment Fit The Crime?,* Oxford University Press, (2019), p.76, 77-78.

[56] On legal pluralism in Ethiopian criminal law, Jean Graven, The Penal Code of the Empire of Ethiopia, *Journal of Ethiopian Law* Vol. 1, No. 2, (1964), p. 267; Dolores A. Donovan and Getachew Assefa, Homicide in Ethiopia: Human Rights, Federalism, and Legal Pluralism, *American Journal of Comparative Law,* Vol. 51, No. 3, (Summer 2003), p. 505.

[57] Von Hirsch*, Proportionality in the Philosophy of Punishment, supra* note 57*,* pp.81-82; Jesper Ryberg, *The Ethics of Proportionate Punishment: A Critical Investigation*, Kluwer Academic Publishers, (2004), pp. 59-99.

offence which are not constitutive of the offence's basic structure but can usually aggravate the seriousness of the crime. [58]

The challenge is of course how to assess the seriousness of computer-focused offences and grade them accordingly. The Budapest and Malabo Conventions may both insist on their signatories to establish proportionate and dissuasive penalties, but none is explicit on how to achieve this. The consensus though is that the five computer-focused offences have various degrees of seriousness when their respective *modi operandi* and criminal pathway are considered. The misuse of tools offence is considered less serious than the offence of illegal access. The latter is also described as the frequent first step of a cybercriminal before s/he undertakes illegal data and/or system interferences or illegal interception. In addition, none of the two texts indicates the ordinal proportionality of penalties; and the Budapest Convention does not mention aggravating circumstances such as the targeting of critical infrastructures, particularly relevant given the scale and transnational dimensions of many cyber-attacks. Only the regional Directive 2013/40/EU requires a minimum threshold for imprisonment as a penalty but remains silent regarding fines.[59] All five offences are required to attract 'at least' two years imprisonment; for illegal data and system interferences, this is aggravated to three years when a hacking tool is used, to five years when the target is a critical infrastructure when organised crime is involved, or there is serious damage; and when illegal interference concerns personal data, Member States are required to establish aggravating circumstances, without the Directive specifying more.[60] This paucity of information on ordinal proportionality for computer-focused offences should not however act as a deterrent to critically evaluate the Ethiopian legislator's approach to the punishment of its computer-focused crimes. The degree of seriousness of the offences is now established, and the Budapest Convention's approach has become the international standard of reference. This taxonomy gives a framework to label and critically analyse Ethiopia's criminal law response.

3. THE CRIMINALISATION OF COMPUTER-FOCUSED OFFENCES

Relying on international and regional standards, the 2016 Proclamation took care to define each of the base offences, clearly distinguished from their aggravated forms. It also innovated with Article 2 which provides further definitions of terms used across the legislation. The Proclamation is not however without some gaps,[61] although the nature of the deficiencies varies according to the base offence considered.

3.1. Illegal access: an improved, more coherent, definition.

The 2004 Criminal Code criminalised mere unauthorised access to computer services and aggravated unauthorised access to commit further crimes.[62] These offences, committed negligently or intentionally, could apply concurrently to the other offences relevant to further crimes, such as fraud.[63] Eight years later, the 2012 Telecom Fraud Proclamation added illegal access to a telecom

[58] Fletcher, *supra* note 34; *see* the 2004 Criminal Code, *supra* note 9, Title III on the 'conditions of liability to punishment in respect of crimes.'
[59] Directive 2013/40/EU, of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.
[60] Id. Art. 9.
[61] These gaps are recapped in section 3.7.
[62] *See* the 2004 Criminal Code, *supra* note 9, respectively Art. 706(1) and 706(2).
[63] *Id.*, Art. 711.

system, effectively criminalising illegal access that targeted a particular set of critical infrastructures. In that sense, it remedied the Code's weakness of not differentiating between the types of targeted computer systems.[64] Nevertheless, the two offences potentially overlapped, depending on how a computer network was to be interpreted, compared to a telecom system and internet service. Indeed, the 2012 Proclamation did not articulate the scope of either offence, despite a definition of 'telecom service' and 'telecom equipment'.[65]

The 2016 Proclamation brings these different offences into one provision, repealing both Article 5(2) of the 2012 Proclamation, and Article 706 Criminal Code.[66] At first sight, the structure of the offence of illegal access in the 2016 Proclamation remains the same as in the Code and the 2012 Proclamation. The base offence is still about securing access to a computer system, data, or network, and without authorisation. Yet, the 2016 Proclamation brings some significant, positive, changes: it clarifies the scope of the base offence and brings coherence to the legislative choices for criminalisation.

The first main difficulty with the initial offences was the Code's absence of definitions of the key elements (access, authorisation, computer system or data), leading to important uncertainties in terms of the offences' scope and their potential overlap with that of the 2012 Proclamation. By contrast, the 2016 Proclamation specifies that the target can be as much the 'whole' or 'any part of the computer system, data, or network. Thus, it leaves no ambiguity as to whether accessing just one part of a system would be criminalised.[67] It also defines the terms 'computer or computer system', 'computer data', 'network' and 'access' in techno-neutral language, thus future-proofing the legislation against technological improvements or changes.[68] Most importantly, the Proclamation refers to 'in excess of authorization' alongside 'without authorization', with examples of employees and computer crime investigator officers exceeding their authorisation in the Proclamation's Explanatory Note.[69] This accounts for the various *modi operandi* of the crime while remaining techno-neutral. The criminalisation is thus not dependent on the use of a particular technology to commit illegal access. The precision brought to authorisation therefore lifts any ambiguity that existed in the Code and the 2012 Proclamation as to this key criminalising element of the offence.

The other significant weakness in the Code's provision was its criminalisation of negligent illegal access, leading the criminal law to overreach and criminalise an individual who was simply careless, and not even reckless, in their access to a computer system or data.[70] This overbroad legislative choice was in contradiction to the 2012 Proclamation's approach to criminalise only intentional, not negligent, access to telecom networks. The 2016 Proclamation radically departed from the Code, eliminating the possibility of committing illegal access negligently.[71] Ethiopia is thus in line with the Budapest Convention's requirement for the intention to restrict the mental

[64] The 2012 Telecom Fraud Proclamation, *supra* note 19, Art. 5(2).
[65] *Id*., at Art. 2(1).
[66] The 2016 Computer Crime Proclamation, *supra* note 8, Art. 3.
[67] *Id*., Art. 3(1).
[68] *Id*., respectively, Art. 2(2), 2(3), 2(7) and 2(9).
[69] *Id.*, Art. 3(1); the Explanatory Note to Computer Crime Proclamation, *supra* note 23, p.10.
[70] The Criminal Code, *supra* note 9, Art. 706(3)
[71] The 2016 Computer Crime Proclamation, *supra* note 8, Art. 3(1).

element of the offence.[72] This choice reflects a balance between the need to capture the specificities of cybercrimes and the necessity not to over-criminalise. Trespass in criminal law is generally not a crime, but its criminalisation was here required given that accessing a computer system or data is often a first step towards immediately committing a more serious crime. Yet it cannot become the door to an overreach of the criminal law, hence the requirement of intent for illegal access.[73]

To summarise, while the Code's criminalisation of illegal access could only be welcomed, the 2012 Telecom Fraud Proclamation did not remedy the initial weaknesses of the legislation. The initial legislative choices as to the scope of the offences, the absence of definitions for the key terms and the lack of proportionality between the offences called for further reform. The 2016 Proclamation presents a balanced response in terms of the structure of the offence of illegal access.

3.2. Illegal data 'interference': a better-articulated offence despite its name of "causing damage to computer data"

As for illegal access, the 2016 Proclamation brought together into one base offence the various iterations of the offence present in the Code and the 2012 Proclamation.[74] In doing so, it clarified four main aspects of the initial base offences which were problematic. Firstly, the 2016 legislator removed the possibility of negligently committing the offence, avoiding the criminalisation of simple mistakes employees could make, such as data deletion.[75] In that sense, it implicitly reaffirms that the criminal law should be used only as a last resort.[76] Secondly, it specifies that interference could be caused not just "without authorization", but also "in excess of authorization", such as when an employee intentionally deletes data in their employer's computer system.

Thirdly, the 2016 Proclamation criminalised separately those computer-focused crimes and the computer-related crimes,[77] instead of combining the two as in the Code.[78] This welcome move reinstates the coherence of the criminal law and respects the *modi operandi* of most cybercriminals, since theft, forgery, and fraud, are usually facilitated by illegal access without necessarily leading to illegal data interference. A fraudster does not want to damage the personal data of their victim, but to use it to defraud their target.

Finally, the 2016 Proclamation clarified the concept of interference in two ways. It clearly differentiates interference from access, by dropping the Code's reference to access when the latter defined its aggravated offence of data interference with intent to commit further crimes.[79] Thus, the change eliminated the overlap that potentially existed between the two sets of offences (access and data interference), reinstating a clearly delineated taxonomy of cybercrimes attuned to the boundaries in the Budapest Convention and the Malabo Convention.[80]

The second way the Proclamation clarified the meaning of interference is by rewriting the description of the results to be achieved in the base offence. Initially, the 2004 offence was about

[72] The Budapest Convention, *supra* note 15, Art. 2.
[73] The Explanatory Report to the Budapest Convention, *supra* note 33, para. 44-50; Clough, *supra* note 7, pp. 68-69.
[74] The 2016 Computer Crime Proclamation, *supra* note 8, Art. 6(1).
[75] The 2004 Criminal Code, *supra* note 9, Art. 707(3).
[76] Horder (2022), *supra* note 34, pp. 79-81.
[77] The 2016 Computer Crime Proclamation, *supra* note 8, Art. 6, 9-11.
[78] The 2004 Criminal Code, *supra* note 9, Art. 707(2).
[79] Id., Art. 707(2) & 706(2).
[80] Phillips, Davidson, Farr, Burkhardt, Caneppele, and Aiken, *supra* note 38, p. 386.

intentionally causing damage by adding, altering, deleting, or destroying data.[81] Despite the four verbs not being defined, their use seemed to indicate the aim of protecting the confidentiality and integrity of computer data, but not its availability. The problem is that in computer science, data interference can include data becoming unavailable without its integrity or confidentiality being compromised. In other words, data interference is not just damage to data. The Budapest Convention recognised the specificity of this cybercrime by including in its definition the word 'suppression', which its Explanatory Report described by reference to data being unavailable but not altered.[82] Despite the Budapest Convention being available for reference, the drafters of the Ethiopian Criminal Code did not contextualise by referring to this standard concerning suppressing computer data.[83] Consequently, this omission brought an ambiguity as to whether the Ethiopian provision included all scenarios of interfering with data, including interfering with its availability, or whether the drafters meant to discard availability as a protected value. The 2012 Proclamation added to this confusion. Its definition of the offence against telecom infrastructure seems to have included the protection against unavailability, Article 5(3) using 'intercept' in addition to 'alter, destroy or otherwise damage' and Article 5(1) referring to the 'obstruct[ion] with any telecom network, service or system'.

The 2016 Proclamation puts an end to any uncertainty as to the meaning of interference and thus as to the scope of the offence. Of course, it continues to indicate the altering and deleting of data, taking away 'adding', arguably captured by 'altering'. More importantly, instead of 'destroying', it uses the expression of 'rendering it meaningless, useless or inaccessible', thus clearly referring to the underpinning values of integrity and availability. The choice of terms also future-proves the offence of data interference. It is not just a response to the crime of the day, where the drafters claimed to tackle the incoming wave of ransomware attacks rendering their victims' data unavailable without the encryption key.[84] Moreover, the legislator's choice of techno-neutral language shifts the focus away from the conduct towards a description of the result achieved -the destruction and unavailability- independently of the technology used to commit the conduct. In that sense, it could be regretted that the legislator kept the title of 'causing damage to computer data' when the new definition of the offence protects data availability, and not just data integrity (damage). On the positive side, the reform puts Ethiopia in line with the Budapest Convention and the Malabo Convention, it was inspired by.

3.3 System Interference: still an imperfect criminalisation

The two waves of Ethiopian legislative response to cybercrime have struggled, in different ways, to fully and coherently criminalise system interference in line with the Budapest and Malabo Conventions.

The 2016 Proclamation certainly remedies two of the weaknesses of the Code's offence. As for illegal access and data interference, it lifts the ambiguity as to whether such crimes could be

[81] The 2004 Criminal Code, *supra* note 9, Art.707 (1).
[82] The Budapest Convention, *supra* note 15, Art. 4; the Explanatory Report to the Budapest Convention, *supra* note 33, para.61.
[83] The 2004 Criminal Code, *supra* note 9, Art. 707(1).
[84] The Explanatory Note to Computer Crime Proclamation, *supra* note 22, para. 17; Lena Y.Connolly and David S. Wall, The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures, *Computers & Security*, Vol. 87, (2019), 101568.

committed when exceeding authorisation.[85] It also broadened the scope of the offence to reflect the various *modi operandi* of cybercriminals interfering with computer systems or networks. The initial offence in the Code used solely the verb 'disrupting'.[86] This would of course capture several behaviours and techniques, notably denial-of-service attacks (DoS attacks), a typical example of system interference that harms the system's availability. Nevertheless, the Code's choice of the word 'disrupting' may have unduly restricted the scope of the offence, when contrasted with the use of 'hindering' in the Budapest Convention,[87] 'disruption' was featured only twice in the Convention's Explanatory Report.[88] Indeed the term "hinder" covers a broader set of behaviours including keeping back, delaying, or preventing; whereas "disrupt" implies a narrower scope where behaviours are limited to those of impeding or interrupting.[89] The 2016 Proclamation better reflects the multiple variations in the *modi operandi* of cybercriminals interfering with a system or network. Indeed, it now refers to both hindering and disrupting, as well as adding 'impairing' and 'interrupting', a language that remains techno-neutral, thus future-proofing the offence against technological advancement.

Despite these improvements, the 2016 Proclamation does not fully criminalise system interference. As data interference, system interference can affect the integrity as well as the availability of the computer system or network. The 2004 Criminal Code split these two aspects into two separate offences. Damage affecting the integrity of the computer system or network was captured via the offence of data interference, which expressly referred to data and computer system and network; whereas harm to the system's availability was a separate offence, defined as intentionally disrupting the use of computer services by an unauthorised user.[90] The 2016 Proclamation does not fully reinstate the coherence of the cybercrime taxonomy. Certainly, it takes away the reference to computer systems and networks in the illegal data interference offence; but it does not bring the criminalisation of these behaviours within the scope of the offence of system interference. Indeed, the offence does not incorporate terms such as "damaging," "deteriorating," and "suppressing" as found in the Budapest Convention.[91] Thus it is unclear as to whether the new definition of the offence includes these aspects of system interference.

Moreover, it does not require hindering to be 'serious', keeping this element as an aggravating factor, -without definition-, rather than as constitutive of the offence as in the Budapest Convention.[92] Obviously by repealing the negligent mental element of the base offence, the Proclamation reinstates a certain degree of seriousness. Yet, by not specifying that hindering must be serious, the scope of the offence remains broad, in line with the Malabo Convention, but in contrast with the more restrictive approach of the Budapest Convention.[93] By requiring 'hindering' to be serious, the drafters of the latter aimed to avoid the criminalisation of system interference when its form, size or frequency causes little to no damage to integrity or availability, such as when a former employee acts out of revenge against the employer who fired them but without causing damage; or when the size or frequency is more of a nuisance, such as spam, calling for the

[85] The 2016 Computer Crime Proclamation, *supra* note 8, Art. 5.
[86] The Criminal Code, *supra* note 9, Art. 708(1).
[87] The Budapest Convention, *supra* note 15, Art. 5.
[88] The Explanatory Report to the Budapest Convention, *supra* note 33, para. 148 & 155.
[89] *Id.*
[90] The 2004 Criminal Code, *supra* note 9, Art. 708.
[91] *Id*.
[92] The 2016 Computer Crime Proclamation, *supra* note 8, Art. 5 (1) (2) (b).
[93] The Budapest Convention, *supra* note 15, Art. 5.

use of other regulatory means rather than criminal law.[94] The requirement of serious hindering is thus a means to comply with the principle of subsidiarity, whereby criminal law is of last resort and should not be used just because the crime involves digital technologies.[95] It is the approach that should be preferred so that the criminal law also complies with human rights principles. That the Proclamation requires 'serious hindering' for the aggravated offence when committed against critical infrastructure does not alleviate the fact that the offence has an overreach.[96] It is a deficiency that strikes at the heart of the specificities of this particular cybercrime and would thus require remedying in a future reform.

3.4. Illegal interception: a delayed criminalisation

Data interception and data interference are distinct in that data interception impacts data during transmission, while data interference affects data once it is stored.[97] Therefore, there are two separate offences in the Budapest Convention, and later, in the Malabo Convention. Yet, the 2004 Criminal Code chose not to criminalise illegal interception, either as a separate offence or via data interference (which would have been controversial anyway). The 2012 Proclamation partially addressed this gap, having introduced the offences of unauthorised interception in any telecom system and the interception of personal information of subscribers.[98] The scope of these offences remained however limited. Any illegal interception of computer systems or data not transmitted via Ethiopia's telecom system was not criminalised.

It fell on the 2016 Proclamation to at last criminalise intentional interception of "non-public computer data or data processing service',[99] without limiting it to the telecom system or data as in the 2012 Proclamation. In addition, the 2016 Proclamation provides the first definition in Ethiopia's criminal law of interception: the real-time surveillance, recording, listening, acquisition, viewing, controlling, or any other similar act of data processing service or computer data.[100] Expanding on this, the Explanatory Note to the Computer Crime Proclamation adds examples of the act of directly monitoring, listening to, taking, viewing, controlling, or using content, traffic, customer information, computer programs, or similar data without permission during communication, data transfer, or internet activities.[101] Technological advancements will create new opportunities to commit illegal interception, opportunities that the Explanatory Note may not have mentioned. Nevertheless, the techno-neutral language of the Proclamation should ensure that the definition is future-proof.

At odd with this aim of facilitating the interpretation of the offence through carefully techno-neutral definitions, the Proclamation does not explain whether the term 'non-public' refers to the nature of the transmission process or the data transferred. It falls on the Explanatory Note to guide the interpreter, despite 'non-public' being a key constitutive element of the offence. The offence

[94] The Explanatory Report to the Budapest Convention, *supra* note 33, para 67-69.
[95] Horder (2022), *supra* note 34, section 4.4; R A Duff and Stuart P Green, Introduction: The special part and its problems, in Duff and Green, *supra* note 34, pp. 4-5.
[96] The 2016 Computer Crime Proclamation, *supra* note 8, Art. 5 (1) (2) (b).
[97] *See* notably, 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, No. 1, (2018), p. 9, 17.
[98] The 2012 Telecom Fraud Proclamation, *supra* note 19, Article 5(3).
[99] The 2016 Computer Crime Proclamation, *supra* note 8, Art. 4(1).
[100] Id., Art. 2(12).
[101] The Explanatory Note to Computer Crime Proclamation, *supra* note 22, p. 14.

covers non-public computer data transmissions, which refer to the communication mechanism used for transmission rather than the material being transferred.[102] Thus, individuals could still commit illegal interception for example when recording conversations or data in a public space, which they wish to keep private. Rather than leaving it to the Explanatory Note, it would be preferable though for the offence to define 'non-public' in line with, generally, the laudable definitional effort of the 2016 Proclamation.

3.5. The criminalisation of the Misuse of tools offence: from too simple to too complex?

The 2004 Criminal Code's provision on the offence called "criminal acts related to usage of computer devices and data" was not adequately articulated but it had the merit of being short and simple to understand and apply, despite its broad scope potentially leading to some ambiguities. By contrast, the new version of the offence in the 2016 Proclamation shines by its length and complexity, although it better aligns with the Budapest Convention's provisions.[103]

3.5.1 The initial criminalisation of the misuse of tools

The 2004 Criminal Code, inspired by the other national jurisdictions and the Budapest Convention, criminalised the misuse of 'instruments, secret codes or passwords' to deter those who facilitate the commission of computer crimes.[104] Its choice of conducts aligns well with that of the Budapest Convention, although the latter also added 'buying and receiving'. Liability stems from intentionally importing, producing, selling, offering for sale, distributing, or possessing these tools with the intent of committing computer crimes, making the offence a possessory crime. The aim of making the conduct an offence was clearly to address the black market that facilitates the sale or transfer of software used to gain unauthorised access or to impair the availability of computer systems and networks.[105]

The offence's brevity though raised questions about its scope. While the term passwords created no issue of interpretation, the other terms of 'instruments' and 'secret codes' remained undefined and unspecified. By contrast, the Budapest Convention restricted the scope of its offence to the tools 'primarily designed' for crime purposes to alleviate the concerns of the cybersecurity industry about the criminalisation of the legitimate cybersecurity tools they use to protect against cyberattacks. Thus, the Code's silence as to the nature of the tools potentially left the door open to the criminalisation of a wide range of software and hardware, including legitimate cybersecurity tools used in the fight against cybercrimes.[106] Paradoxically, Ethiopia aligned, on this issue, with other national cybercrime legislations, even among signatories of the Convention, as they failed to integrate this important restriction.[107]

---

[102] *Id*., at 15; the Explanatory Note to the Budapest Convention, *supra* note 33, para 54.
[103] The 2016 Computer Crime Proclamation, *supra* note 8, Art. 7.
[104] The Code, *supra* note 9, Art. 709; the Budapest Convention, *supra* note 15, Art. 6.
[105] The Explanatory Report to the Budapest Convention, *supra* note 33, para 71.
[106] *See* Audrey Guinchard, The Criminalisation of Tools Under the Computer Misuse Act 1990: The Need to Rethink Cybercrime Offences to Effectively Protect Legitimate Activities and Deter Cybercriminals, in Tim Owen and Jessica Marshall (eds), *Rethinking Cybercrime: Critical Debates*, Palgrave McMillan (2021), p. 41.
[107] Apart from France, *see* Audrey Guinchard, Better cybersecurity, better democracy? The public interest case for amending the Convention on cybercrime n.185 and the Directive 2013/40/EU on attacks against information systems, in Ricardo Pereira, Annegret Engel & Samuli Miettinen (eds), *The Governance of Criminal Justice in the European*

The 2012 Proclamation did not tackle any of these issues. It created an offence for manufacturing, assembling, important, or offering for sale 'any telecom equipment' and using or holding the equipment but on the condition that the person had not 'obtained a prior permit'. Thus, a defendant who obtains a permit but thereafter uses the equipment for the wrong purposes would not be liable under the 2012 Proclamation. The initial offence was thus in serious need of revisions.

3.5.2 A revised offence: too complex, too broad?

The 2016 Proclamation organises the Article 7 offence into five sub-articles, with sub-article 3 being a possessory offence to sub-articles 1 and 2, and sub-article 5 criminalising sub-section 4 when committed negligently. The overall objective of the offence is to criminalise preparatory acts that are left outside the scope of attempted illegal access or attempted illegal data interference for example, but which, if tackled at an early stage, have the potential to quell the tide of cybercrimes. Its complexity stems from the difficulty in achieving its legitimate objectives without criminalising the cybersecurity industry, and from the difficulty in understanding the *modi operandi* of cybercriminals on the black market for tools.

Regarding the first two Article 7 offences, i.e. the conduct of distributing computer programs, the Proclamation distinguishes between transmitting a computer program (Article 7(1)), and importing, producing, offering for sale, distributing, and making available either the program or the computer device (Article 7(2)). It seems that the legislator had two scenarios in mind. In Article 7(1), the aim is to criminalise defendants who distribute malware without checking if the recipient intends to use it for nefarious purposes. In Article 7(2), it criminalises defendants acting as intermediaries with the knowledge that their customers intend to use the malware for cybercrime offences. The apparent negligent behaviour of the first attracts a lesser punishment: five years of simple imprisonment, and a fine of 30,000 Birr, compared to five years of rigorous imprisonment, and a fine of between 10,000 to 50,000 Birr. The problem is that the two offences arguably create an artificial difference among cybercriminal behaviours. Most cybercriminals distribute problematic computer programs on the black market, not on legitimate markets. Given the context, most will not enquire about the specific objectives of each of their customers, not by negligence, but because their customers may not be particularly forthcoming about their intention to commit cybercrimes.[108] They are in practice as culpable as those who enquire about their customers' intentions. The legal provisions, therefore, do not seem to adequately reflect the *modi operandi* of cybercriminals, offering a lower punishment to cybercriminals under Article 7(1) when culpability is the same in both scenarios. In addition, the distinction unnecessarily complicates the task of the prosecution having to choose between Article 7(1) and Article 7(2).

This criticism should not mask the laudable and successful effort of the legislator to structure the two offences of Article 7(1) and (2), as well as that of Article 7(3) of possessing a tool, to protect legitimate security research activities. The three offences work on the basis that the tool at stake, whether a computer program or computer device, has been 'exclusively designed or adapted for the purpose' of causing damage or committing a computer-dependent crime under Articles 3 to

Union: Transnationalism, localism, and public participation in an evolving constitutional order, Edward Elgar 2020, p148.

[108] Thomas J. Holt and Eric Lampke, Exploring stolen data markets online: products and market forces, *Criminal Justice Studies* Vol. 23, No. 1 (2010), p. 33; Thomas J. Holt, Examining the Forces Shaping Cybercrime Markets Online, *Social Science Computer Review*, Vol. 31, No. 2, (2013), p.165.

6.[109] The use of 'exclusively' has the merit of keeping all dual-use hacking tools outside the scope of the offence, directly avoiding the broad scope of the initial 2004 offence.[110] It has the corresponding merit of protecting the security industry from any accusation of creating or designing cybersecurity tools to commit illegal access when searching for vulnerabilities or Criminal Code failures enabling illegal access. This is a welcome development, very much in line with the spirit of the Budapest Convention. Importantly, it places Ethiopia amongst the extremely few countries which have structured their misuse of tools offence to protect legitimate security researchers from criminal law.[111]

Finally, the provision criminalises the disclosure or transfer of computer programs, secret codes, keys, passwords, or similar data to gain access to a computer system, data, or network, either intentionally or negligently,[112] without authorisation or exceeding authorisation. The objective is to address poor and negligent cybersecurity practices, such as leaving passwords open or poorly implemented security measures leading to unintentional disclosure. Article 7(5) may therefore criminalise many IT administrators who are negligent and do not strictly adhere to security standards. It raises important questions as to whether criminal law should be used to tackle poor cybersecurity practices, or whether regulatory measures would be better suited to encourage the adoption of state-of-the-art cybersecurity practices. The principle of subsidiarity, which promotes a minimalist approach, requires using criminal law as a last resort, protecting legal interests by other means, such as tort law, administrative law or sectoral codes of guidance.[113] Awareness of this requirement not to overcriminalise in this field dates back to 1989. Three decades later, the argument remains valid and underpins the EU efforts to enact the Cyber Resilience Act to create civil law duties to implement cybersecurity standards throughout the lifecycle of a product be it hardware or software.[114] In this instance, the use of criminal law is unlikely to be the most adequate means to deal with poor or absent cybersecurity measures.

3.6. Attempts and accessorial liability of computer-focused crimes

Through its general provisions, the 2004 Criminal Code punished attempts, distinguished from preparatory acts and defined as a crime committed intentionally without achieving the necessary outcome.[115] These general provisions automatically apply to all crimes, including the computer crime provisions. Consequently, the attempt of any computer crime offence in the Code was criminalised and attracted the same punishment as if the offence had been completed.[116] A similar pattern can be observed for accessorial liability, where the Criminal Code criminalised accessories in its general provisions, when the offenders provide information, advice, or assist the principal(s)

---

[109] The 2016 Computer Crime Proclamation, *supra* note 8, Art. 7(1)(2).
[110] The Explanatory Note to the Computer Crime, *supra* note 22, pp.18-19.
[111] Guinchard, *supra* note 95.
[112] The 2016 Computer Crime Proclamation, *supra* note 8, Art. 7(4) & (5).
[113] The Bequai Report Council of Europe R(89)9, *supra* note 41, pp. 24-26; Horder (2022) *supra* note 34, section 4.4; Duff and Green, *supra* note 95, pp. 4-5.
[114] EU Cyber Resilience Act, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0454 (accessed on July 27, 2024); *see* notably the works of Michael D. Scott, Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?, *Maryland Law Review*, Vol. 67, (2007-2008), p. 425, and Susan W. Brenner and Leo L. Clarke, Distributed Security: Preventing Cybercrime, *John Marshall Journal of Information Technology & Privacy Law*, Vol. 23, (2005), p. 659; *see* also Brunhöber, *super* note 17.
[115] The Criminal Code, *supra* note 9, Art. 27 (1) and 26.
[116] *Id*., Art. 27(2).

before, during, or after the commission of the offence so long as the later assisting was agreed beforehand.[117]

By contrast, the 2016 Proclamation is entirely silent on attempts and accessorial liability, raising the question as to whether it implicitly criminalises them or whether it has, surprisingly, left them outside the scope of the statute. A few indicators point towards their indirect criminalisation. Firstly, the Proclamation in Article 29(2) provides that unless otherwise stated, the general part or provisions of the Criminal Code apply. The slight confusion stems from the location of this provision: it is under the procedural Part of the statute, rather than under the substantial law provisions of the statute.[118] It would have been far clearer to introduce this reference to the Criminal Code either before any other provisions or under both the substantial law and procedural Parts of the statute. Nevertheless, the Criminal Code also states that, unless otherwise clearly specified, the general principles included in the Criminal Code apply to other penal legislation, which of course includes computer crime laws such as the 2016 Proclamation.[119] The general criminal code principles concerning attempt and accessorial liability, therefore, help establishing criminal responsibility for attempts and accessories in the 2016 Proclamation.

The problem though pertains to the scope of the criminalisation of attempts, a problem which the 2016 Proclamation perpetuated by not specifying which computer-focused crime could be attempted or not. The Budapest Convention has rejected the criminalisation of attempted illegal access and attempted misuse of tools on the basis that it is 'conceptually difficult to attempt'. For the misuse of tools, it is understandable: the offence itself criminalises preparatory acts. Criminalising its attempts (such as attempted possession of tools) would amount to criminalising the thought process, in violation of human rights principles.[120] For illegal access, the attempted conduct, for example inputting a password, may not indicate a sufficient criminal state of mind.[121] Conversely when it does, for example via the use of a tool to check at speed passwords, the offence would not be attempted illegal access but that of the completed offence of misuse of tools. There is therefore no possibility of criminalising attempted misuse of tools without an overreach of the criminal law. Therefore, instead of the current blanket criminalisation of attempts, the Proclamation should specify which computer-focused crimes could be attempted and exclude attempted illegal access and misuse of tools offences. There is also value in articulating how their attempts could be defined to account in a techno-neutral language for the *modi operandi* of the cybercriminals.[122] Unlike attempts though, the scope of this criminalisation is unlikely to be questionable and in that sense, the silence of the Proclamation is not problematic.[123] The only source of possible confusion pertains to accessorial liability in the transmission of harmful content

[117] *Id*., respectively, Art. 37 and 40.
[118] The 2016 Computer Crime Proclamation, *supra* note 8, Art. 22 (2).
[119] The 2004 Criminal Code, *supra* note 9, Art. 3. On this general principle, *see* Simeneh Kiros and Chernet Hordofa, Over-Criminalisation: A Review of Special Penal Legislation and Administrative Penal Provisions in Ethiopia, *Journal of Ethiopian Law,* Vol. 29, (2017), p.49.
[120] Horder (2022), *supra* note 34, ch. 4. (Criminal Conduct: Actus Reus, Causation, and Permissions).
[121] The Explanatory Report to the Budapest Convention, *supra* note 33, paras. 118-122; *see* the Budapest Convention, *supra* note 15, Art. 11.
[122] Generally, in the theory of criminal law, Horder (2022), *supra* note 34, ch. 13.
[123] Chawki, Darwish and Khan, *supra* note 35, pp. 49-50.

data or malicious code through internet service providers, but the Proclamation addressed it expressly, conditioning their liability to the requirement of criminal intent.[124]

3.7 Criminalisation gaps to be addressed in the 2019 Draft Proclamation and beyond

The 2016 Proclamation's modernisation of computer misuse offences has resulted in a more complete range of offences. Its terms defined in Article 2 in techno-neutral language also allow for the application of laws to both current and future technologies.[125] Nevertheless, some deficiencies remain, which the 2019 Draft Proclamation allegedly aims to tackle. The 2019 Draft certainly does not propose amending the base offence of illegal access, a welcomed approach since the offence's structure is well established in the 2016 Proclamation.[126]

Regarding illegal data interference, the only minor criticism made of the 2016 Proclamation is that of a title not representative of the scope of the offence. The use of 'damage' is associated with attacks against the integrity of the data, whereas the offence now clearly captures attacks against availability. The 2019 Draft proposes a change in title and the elements of the offence but does not remedy this slight discrepancy. Instead, it would more than likely create an additional problem by extending the offence to computer devices, -without defining the term either- to incorporate what seems to be physical damage to machines as done before the rise of digital technologies and thus unrelated to the taxonomy of computer-focused crimes.[127] The reform is not in that sense the way forward.

Concerning illegal system interference, the 2016 Proclamation suffers from ambiguity as to the scope of the offence, whether the offence protects the integrity of the system as well as its availability. The 2019 draft not only failed to clarify this but by adding 'computer data' to its title, it would create further confusion: the offence of system interference would overlap with that of data interference.[128] Furthermore, it would not restrict the offence to 'serious hindering', again not reflecting the specific *modi operandi* of system interference, in addition to the concept being left undefined. On a positive note, though, it proposes a new definition of a computer system to differentiate between a computer as a standalone and an interconnected device, thus clarifying the term, in line with the Budapest Convention.

For illegal interception, the only flaw is that of not defining 'non-public' in the statute, which the 2019 Draft leaves intact.[129] At present, this is remedied by the Explanatory Notes to the 2016 Proclamation, and thus it could be argued that the law should remain untouched. Yet, the transmission of data can still occur without encryption and yet not meant to be openly accessed,

[124] The 2016 Computer Crime Proclamation, *supra* note 8, Art. 16; and the Explanatory Note the 2016 Computer Crime Proclamation, *supra* note 22, pp. 28-30. *See* also the Budapest Convention *supra* note 15, Art. 11; the Explanatory Report to the Budapest Convention, *supra* note 33, paras. 118-122.
[125] The Explanatory Note to Computer Crime Proclamation, *supra* note 23, pp. 4-5*;* the Explanatory Report to the Budapest Convention, *supra* note 33, para. 36.
[126] The 2019 draft Proclamation, *supra* note 10, Art. 3; the 2016 Computer Crime Proclamation, *supra* note 8, Art. 3.
[127] The 2019 draft Proclamation, *supra* note 10, Art. 6.
[128] The 2016 Computer Crime Proclamation, *supra* note 8, Art. 5; the 2019 draft Proclamation, *supra* note 10, Art. 5;
[129] *Id*., at Art. 4; the 2016 Computer Crime Proclamation, *supra* note 8, Art. 4.

so should a reform be proposed, the criminal law would benefit from defining in the statute a key constitutive element of the offence.[130]

By contrast, for the misuse of tools offence, the draft 2019 Proclamation proposes some welcome changes, addressing one of the identified weaknesses, without creating new deficiencies. It would remove the provision that currently criminalises negligent misuse of devices and excludes from the scope of the offence the tools legally obtained from personal or commercial computer devices, data, and programs used for authorised training, testing, or protection of computer systems.[131] Therefore, the draft Proclamation would reinforce Ethiopia's strong position as being one of the few countries having provided a safe haven for security researchers to legitimately test systems and networks for vulnerabilities to improve cybersecurity and resilience to cybercrime attacks. The artificial distinction between Article 7(1) and (2) of the 2016 Computer Crime Proclamation remains unchanged in the draft 2019 Proclamation.

Finally, regarding attempts and accessorial liabilities, the 2019 Draft remains entirely silent.

To summarise, the 2016 Proclamation places Ethiopia in a solid position to tackle the rise of cybercrimes with a substantive criminal law, which is mostly cognisant of the taxonomy of computer-focused crimes as defined in the Budapest Convention. There are some deficiencies though, and the 2019 Draft only addresses the one on the misuse of tools offence committed by negligence. Worse it creates further difficulties by introducing some overlaps between the various offences which cannot be justified by technological advancement and cybercrimes' specificities. The reform is certainly not the way forward. Does a similar conclusion apply to the punishment of these offences?

4. THE PUNISHMENT OF COMPUTER-FOCUSED OFFENCES

In line with the caveat explained in section 2.2, proportionality can be appreciated in two ways: by the legislative use of aggravating factors, and by its tailoring of ordinal proportionality to the taxonomy of cybercrimes and its grading of the offences' seriousness. Another aspect that needs to be looked at is the proportionality of punishment when the offender is a juridical person.

4.1. A wider use of aggravating factors

Ordinal proportionality when aggravating factors exist depends on the degree of seriousness attributed to these factors. Their choice is thus an important part of the taxonomy of cybercrimes.

4.1.1 A consistent choice of aggravating factors

The 2004 Criminal Code recognised one aggravating factor, i.e. the further intent to steal, defraud, or extort, but not others such as the targeting of critical infrastructures.[132] This gap was only partially tackled by the 2012 Proclamation with its creation of the same offences when the targeted critical infrastructure was the telecom networks. In addition, the Code's use of its sole aggravating factor was not entirely consistent. Only the base offences of illegal access and data interference were aggravated. The offence of system interference was not, even though it could be used, for example, as a first step to blackmail a victim. The omission was not consistent with the cybercrime

[130] Woodrow Hartzog, The Public Information Fallacy, Boston University Law Review, Vol. 99, (2019), p. 459, 479-480.
[131] The 2019 draft Proclamation, *supra* note 10, Art. 9.
[132] The 2004 Criminal Code, *supra* note 9, Art. 706-709.

ecosystem already existing at the time. Certainly, crypto-ransomware only became dominant around the 2010s,[133] after the Criminal Code's enactment, but other forms of ransomware, using for example Trojan horse programs, were already widely circulating as far back as 1989.[134] The Criminal Code was therefore not future-proof.

Paradoxically, that the Criminal Code did not aggravate the misuse of tools offence with further intent to commit crimes reflected a stronger awareness of the specificities of cybercrime. Indeed, the offence is preparatory, removed from the circumstances that would reveal a further intent to steal or extort; thus, proving the existence of the aggravating factors would mostly be impossible and may well amount to criminalising a thought process rather than a conduct reflecting intent based on tangible elements. In that sense, it is welcome that the 2016 Proclamation adopted the same approach as the 2004 Criminal Code, not aggravating the misuse of tools offence while remedying the latter's other weaknesses in its choice of aggravating factors.

The 2016 Proclamation indeed establishes consistent aggravating factors across all computer-focused offences except the misuse of tools offence. The first two concern targeting computer data or systems 'exclusively destined for the use of a legal person' and targeting critical infrastructure, a term it defines by reference to an attack that 'would have considerable damage on public safety and the national interest'[135] and which is therefore not restricted to a telecom network as with the 2012 Proclamation. The other two aggravating factors consist of targeting computer data, systems or networks classified as top secret for military purposes or intentional relations (Article 8(a)), and when the country is in a state of emergency (Article 8(b)).

This range of aggravating factors has the merit to cover most circumstances that demonstrate additional seriousness in the commission of cybercrimes. The only lacunae could be the legislator's choice to abandon further intent to commit crimes as an aggravating factor, despite further intent being a common occurrence in cybercrime. Article 19 of the Proclamation however seems to indirectly tackle the situation as it allows for the computer-focused offences to apply concurrently to the offences punishable in the Criminal Code. So, for example, illegal access with intent to commit fraud can be punished as illegal access and attempted fraud. There is, however, an argument to be made as to whether the concurrence of the two would suffice to capture all circumstances that a specific aggravated offence with further intent would cover. Indeed, the aggravated factor can include the criminalisation of behaviours at the preparatory stage of committing, for example, fraud, where obtaining illegal access demonstrates the offender's criminal mental element before the offender engages in the process of defrauding their victim. In that sense, the 2016 Proclamation introduces a gap that ignores the taxonomy of cybercrimes that the two main international Conventions – the Budapest one and the Malabo legal instrument- have established. Reinstating this aggravated offence would be a welcome step forward.

Overall, the reform represents a graduated response that reflects the legislator's strong awareness of the cybercrime ecosystem. Ethiopia has a dissuasive legal framework, ahead of some other, yet older, cybercrime legal frameworks such as the UK Computer Misuse Act 1990 known for its

[133] Connolly and Wall, *supra* note 84.
[134] Samar Kamil, Huda S. A. S. Norul, Ahmad Firdaus and Opeyemi L. Usman, The Rise of Ransomware: A Review of Attacks, Detection Techniques, and Future Challenges, in 2022 *International Conference on Business Analytics for Technology and Security (ICBATS)* 16-17 Feb. 2022, ieee, pp. 1-7 DOI: 10.1109/ICBATS54253.2022.9759000
[135] The 2016 Computer Crime Proclamation, *supra* note 8, Art. 2(11).

proportionality inconsistencies.[136] Furthermore, Ethiopia's choices mostly align with international approaches, which should facilitate Ethiopia's ratification of the Budapest Convention and/or the Malabo Convention should it wish to do so.[137]

4.1.2. Proportionality of punishment between each base offence and their aggravated forms

Proportionality between the base offence and its aggravated forms requires the use of lesser sentences for the base offence. This question concerns all offences, except that of the misuse of tools, which has not been aggravated whether in 2004 or 2016.

The 2004 Criminal Code partially recognised the need for proportionality. Its base offences of illegal access and data interference, where committed with *negligence*, attracted a fine of 2,000 Birr or 3 months simple imprisonment,[138] whereas their aggravated (intentional) form would be punished by a fine of 20,000 Birr and five years of rigorous imprisonment.[139] Nevertheless, the punishment for both base offences, when committed, this time, intentionally, was disproportionate to their aggravated form. Both base offences attracted an unlimited fine, with no established maximum, whereas their aggravated forms had a maximum both for the fine and the imprisonment.[140] It could be argued that the Criminal Code's general part provided the courts with constraints to exercise their discretionary sentencing power and sentence offenders to the commission of these two base offences.[141] The vagueness of the provisions however offered little direction for the courts to ascertain what a proportionate punishment would be, especially in the absence of any sentencing guidelines for cybercrimes until 2013.[142] The other weakness in the 2004 Criminal Code was, as stated, the absence of aggravating factors for system interference.

The 2016 Proclamation reinstates proportionality in the punishment of these base offences and their aggravated forms, as well as for illegal system interference. It also applies the same principles to the new offence of illegal interception. The four base offences therefore have a maximum threshold, and their punishment is gradually increased: the first factor of targeting a legal person attracts a lesser sentence than the second factor of targeting a critical infrastructure. So, for example, mere illegal access now attracts 'simple imprisonment' of no more than three years or/and a fine between 30,000 and 50,000 Birr. It is thus punished more severely than before,[143] with a penalty of imprisonment, instead of just a fine, but with a maximum threshold for the fine, instead of leaving it to judicial discretion as in the 2004 Criminal Code. The Proclamation increases the imprisonment to rigorous imprisonment of five years, when the target computer system, data, or network 'is exclusively destined for the use of a legal person'.[144] It increases the imprisonment even further, up to ten years, as well as the fine (50,000 to 100,000 Birr) when the target is a critical

[136] Criminal Law Reform Now Network, *supra* note 30, chapter 5, para 2.28, and Appendix C p159.
[137] The Malabo Convention, *supra* note 23, preamble, para 1; Art. 25.
[138] The 2004 Criminal Code, *supra* note 9, Art. 706(3) & 707 (3).
[139] Id., Art. 706 (2) & 707(2).
[140] Id., Art. 706 (1) & (2) & 707(1).
[141] Id., Art. 90(2).
[142] የኢትዮጵያ ዲሞክራሲያዊ ፌዴራላዊ ሪፐብሊክ ፌዴራል ጠቅላይ ፍርድ ቤት፣ የተሻሻለው ወንጀል ቅጣት አወሳሰን መመሪያ ቁጥር 2/2006፤ 10(2006)/ Federal Democratic Republic of Ethiopia, Federal Supreme Court, *Revised Sentencing Manual* No. 2/2013, 10 (2013). [The original document is in Amharic language, translation is mine].
[143] The 2004 Criminal Code, *supra* note 9, Art. 706.
[144] The 2016 Computer Crime Proclamation, *supra* note 8, Art. 3(2)(a).

infrastructure.[145] The same pattern can be seen for illegal data and system interferences and illegal interception.[146]

Two criticisms can be nonetheless formulated. The first relates to the fine for the base offence of illegal access, which is not increased when the first aggravating factor applies. The second pertains to system interference, with the fine for the second aggravated factor remaining the same as for the first aggravated factor. The justification probably lies in the legislator's increasing the imprisonment to mark the increased seriousness. For illegal access, it obliges the court to sentence the offender to both a fine and more severe imprisonment, rather than the alternative for the base offence. And for system interference, imprisonment is noticeably more severe for targeting a critical infrastructure (fifteen to twenty years) than for targeting a legal person (five to ten years). Nevertheless, this appreciation of the fine's seriousness of these two aggravated offences could still be argued as problematic. For example, illegal system interference with legal persons' computer data, especially for example in the financial sector, is notoriously more harmful than the base offence against individuals' computer data as the harm will affect the targeted legal persons as well as their customers. Accounting for this difference in the fine, not just concerning the imprisonment, would be welcome. In that sense, the 2016 Proclamation struggled to completely account for the specific harms that the aggravating factors of all cybercrime offences create.

4.2. The need for punishment to better mirror the taxonomy of cybercrimes

Computer-focused crimes are not equal in their seriousness. The misuse of tools offence for example is considered to be preparatory to the other four offences of illegal access, data and system interferences, and illegal interception. Similarly, illegal access often is the first step towards committing other offences of data and system interferences and illegal interception. Conversely, data and system interferences can have very similar harmful consequences for their victims, with or without illegal access having been committed. It can also be argued that at times data interference is more harmful than system interference, since crypto-ransomware (data interference) leads the victim to lose their data, rather than having their data made temporarily unavailable as with a DDOS attack (system interference). The question therefore is whether the current legislation mirrors these subtle differences in the seriousness of each set of offences. The answer is globally positive and a noticeable change to the previous 2004 Criminal Code's approach. Yet some improvements are needed, notably to maintain ordinal proportionality between offences.

Before the 2016 reform indeed, all base intentional offences and the misuse of tools offence had an unlimited fine, leaving it to the courts to establish any proportionality in the absence of any sentencing guidelines until 2013. And where aggravated (illegal access and data interference), the offences attracted identical maximums of 20,000 Birr and five years of rigorous imprisonment, even though illegal access tends to be less serious than data interference. With the 2016 Proclamation, proportionality between the different base offences is partially, but not fully, reinstated, depending on whether we consider their associated fine, imprisonment, or the combination of the two. For example, the base offence of illegal access attracts a 30,000 to 50,000 Birr fine, whereas the base offence of data interference, despite being more harmful, attracts a lower fine of 30,000 Birr maximum. It could be argued that the severity of the punishment for data interference is marked by the use of rigorous imprisonment of three years, instead of a three years simple imprisonment for mere illegal access, in addition to the fact the fine and imprisonment are

[145] *Id*., Art. 3(2)(b).
[146] *Id.,* at Art. 3(2)(b), 4(2) (b), 5(2)(1)(b), & 6(2)(b).

cumulative for data interference but alternative or cumulative for illegal access, a decision left to the courts.[147] Yet, if a fine exists to reflect the harm done, then the choice of a lower fine for the base offence of data interference is questionable, as data interference is more harmful than mere illegal access. The authors would recommend increasing the fine for data interference, as the legislator did for system interference. Punishment for the base offence of system interference is indeed commensurate to the more severe harm the base offence creates, compared to mere illegal access. It leads to a higher maximum of 50,000 Birr and three to five years of rigorous imprisonment; similarly, interception – which can be less harmful than system interference but more serious than illegal access- attracts a fine between 10,000 Birr to 50,000 Birr, with up to five years of rigorous imprisonment.

Another discrepancy in the punishment's proportionality concerns again illegal access and data interference, but this time in their aggravated forms. Both sets of aggravating factors lead to the same fines and imprisonments: 30,000 to 50,000 Birr and three to five years rigorous imprisonment for targeting a legal person; and 50, 000 to 100,000 Birr, with five to ten years rigorous imprisonment for targeting critical infrastructure. The reform thus, failed to account for the difference in the seriousness of the harms that the offences aim to protect against. In that sense, the revised punishments ignore the taxonomy of cybercrimes. Paradoxically the taxonomy is better reflected in the structure of the offences since the Proclamation deleted any reference to access in the constitutive elements of illegal data interference.

Regarding the Article 7 misuse of tools offence, it is more difficult to be assertive as to whether there is or not a lack of proportionality. If we consider the preparatory nature of the offence, the punishment for the possession offence is proportionate. Possession of a tool attracts between a 5,000 to 30,000 Birr fine, or three years simple imprisonment, a lower maximum than for the others. It truly reflects the fact that the offender possessing the tools demonstrates less culpability: s/he has not yet undertaken any step towards committing any of the other offences, whether illegal access, illegal interferences or illegal interception, or distributing the tools in the black market as per Articles 7(1) and (2). Putting the possession offence aside though, the maximums chosen for Article 7(1), (2) and (4) appear disproportionate. Their maximum of 50,000 Birr and 5 years imprisonment (simple for Article 7(1), rigorous for the other two) is undeniably equal to or higher than the punishment for the other completed offences. If we consider these offences to be preparatory to the completed offences of, for example, illegal access or interference, then their punishment is disproportionate. Nevertheless, the higher punishment for these preparatory offences may also reflect the harm done by the growth in the hacking tools black markets. It also accounts for the fact that those making money in the creation and distribution of the tools may never commit themselves further offences, while still helping the principal offenders committing these offences. After all, in general criminal law, the accessory helping the principal (here the offender selling the tool) would be subjected to the same penalties as the principal they are helping (here the offenders who commit illegal access and/or interference).[148] Nevertheless, except for explaining the liabilities of the offender in each sub-article,[149] the Explanatory Note to the Computer Crime Proclamation (maybe legislator) has not helped to interpret the provisions.

[147] *Id*., Art. 3(1).
[148] The 2004 Criminal Code, *supra* note 9, Art. 37(4).
[149] *See* the Explanatory Note to the Computer Crime Proclamation, *supra* note 22, pp.17-19.

4.3. The need for a consistent ratio of imprisonment to fine

The 2004 Criminal Code was logical and consistent in its ratio of imprisonment to fine; yet there was no discernible pattern as to why three months of simple imprisonment equated to 2,000 Birr and five years of rigorous imprisonment to 20,000 Birr. By contrast, the 2016 Proclamation has a noticeable pattern of one year in prison equating to a 10, 000 Birr fine, with the choice between simple and rigorous imprisonment depending on the seriousness of the considered base or aggravated offence.

Nevertheless, the Proclamation is not fully consistent, and without discernible explanations for it. For illegal access, the maximum imprisonment is three years of simple imprisonment, but the maximum fine is 50,000 Birr, instead of an expected 30,000 Birr.[150] It is difficult to understand why. Has the legislator considered increasing the maximum fine to allow the courts to reflect an offender's culpability for example if they demonstrate further intent to commit other offences but have not yet committed these offences? If it is so, it would be a legitimate concern and justification, but then the way forward is to be more explicit about this and expressly create an aggravating factor of further intent, as already indicated.

For system interference and data interception when the second aggravating circumstance is present, the punishment does not follow the general ratio, with 15 to 20 years equating to 50,000 to 100,000 Birr, instead of 150,000 to 200,000 Birr; and 10 to 15 years equating 100,000 to 200,000 Birr instead of 100,000 Birr to 150,000 Birr. These provision punishments of the Criminal Code were not covered in the Sentencing Guidelines.

4.4. The need for proportionality between physical and juridical persons

The Criminal Code allowed juridical persons to be held liable for crimes committed by their officials or employees, excluding state administrative bodies.[151] The fines could be complemented with additional penalties if necessary.[152] The system was complex, with its main characteristic being that the maximum fine threshold remained the same for individuals and juridical persons, ignoring the financial resources that juridical persons may have to pay a fine. For instance, a fine of 50,000 Birr (around USD 870)[153] may represent much less than a percentage of an Ethiopian company's turnover, while an individual's fine could represent an entire year's salary.[154] A system that tailors fines based on income would ensure that every person experiences a proportional penalty when they break the law, promoting equal treatment and punishment for all offenders.[155] The lack of special and proportionate provisions to punish juridical persons committing cybercrimes suggests that they were unlikely to be deterred from committing computer crimes. At least, in the 2012 Proclamation, the maximum fine was equal to ten times the stipulated fine for an

[150] It is the same amount as for juridical persons, Art. 20(2)(a).
[151] *Id*., Art. 34.
[152] *Id*., Art. 90(3) & (4).
[153] *See* National Bank of Ethiopia, Commercial Bank Exchange Rates, https://nbe.gov.et/exchange/banks-exchange-rates/ (accessed on March 3, 2024).
[154] *See* Federal Civil Servants Position Rating, Grading and Salary Scale Council of Ministers Regulation No.455/2019, *Federal Negarit Gazette*, Civil Servant Salary Scale Anex, (2019). For instance, the base salary for Grade-VIII government employee is 3934 Birr (before tax), which 47,208 Birr annually.
[155] Alec Schierenbeck, The constitutionality of income-based fines, The University of Chicago Law Review, Vol. 85, No. 5 (2018), p. 1869, 1871-1872.

individual, although it remained the same whichever offence was considered, thus not reflecting the seriousness of the offence considered.[156]

The 2016 Proclamation addresses the gap by setting a maximum fine threshold for juridical persons.[157] This threshold is determined by whether an individual can be sentenced to a fine only, or imprisonment and a fine.[158] For simple imprisonment up to 5 years, the fine reaches 100,000 Birr, while for rigorous imprisonment above 10 years, it reaches 500,000 Birr.[159] The increase in fines for juridical persons between the base and aggravated offences seems to reflect the rise in punishment for physical cybercriminals. It also differentiates between individuals and juridical persons for all offences, except for the base offence of illegal access. Article 3(1) sets a maximum fine of 50,000 Birr for individuals and juridical persons when the fine is for individuals a year's salary whereas for juridical persons it may be a quarter's profit. To be proportional, the fine for a juridical person committing the base offence of illegal access should be twice the amount.

4.5. The difficult proportionality of punishments in the 2019 Draft Proclamation

The 2016 Proclamation establishes mostly proportionate punishments, whether these are considered: the base offences compared to their aggravating factors; the difference in seriousness between the different base offences; the ratio imprisonment to fine; and the difference between juridical persons and individuals. It would benefit from some of its deficiencies to be remedied, so that proportionality is entirely consistent across the offences and their aggravated forms. The 2019 Draft unfortunately does not address any of these deficiencies. Worse, its provisions would be more disproportional, particularly for illegal access, illegal interception, and system interference. The draft law would reduce the maximum simple imprisonment for illegal access crimes from 3 years to 2 years and increase the maximum fine from Birr 50,000 to 60,000, distorting the ratio imprisonment-fine even more.[160] It would also reduce the maximum rigorous imprisonment for illegal interception from 10 to 8 years.[161] The increase in the fine for illegal access could be a means of recognising the serious harm that mere illegal access can cause;[162] but the decrease in imprisonment, where imprisonment is a good deterrent, seems odd with the increase of the fine.[163] Similarly, the draft law would reduce the imprisonment for aggravated offences, respectively from 10 to 7 years,[164] and from 15 to 10 years.[165] In serious cases, 20 years of rigorous imprisonment under the existing law[166] would be reduced to 15 years under the draft law.[167] Furthermore, the current proportionality between imprisonment for serious cases of illegal data interference and the scenarios of a state of emergency would be lost, both being of a maximum of fifteen years.[168]

---

[156]The 2012 Telecom Fraud Proclamation, *supra* note 19, Art. 11.
[157]The 2016 Computer Crime Proclamation, *supra* note 8, Art. 20.
[158]*Id*., Art. 20(1).
[159]*Id*., Art. 20(2)(c)(d)(e).
[160]*Id*., Art. 3(1).
[161]*Id*., Art. 3(2) (b).
[162] Ryberg, *supra* note 57.
[163]The 2019 draft Proclamation, *supra* note 10, Art. 3 (1) & 2 (a) ((b); the 2016 Computer Crime Proclamation, *supra* note 8, Art. 3 (1) & 2 (a) ((b).
[164] The 2019 draft Proclamation, *supra* note 10, Art. 5(2)(a).
[165] *Id*., Art. 5(2)(b).
[166] The 2016 Computer Crime Proclamation, *supra* note 8, Art. 5(2)(b).
[167] The 2019 draft Proclamation, *supra* note 10, Art. 5(2)(b).
[168] *Id*., Art. 8(b).

In that sense, the draft Proclamation would represent a return to a disproportionate punishment approach for cybercrimes. It is hard to see how the changes could be justified. They ignore the gradation in seriousness between base and aggravated offences, as well as between the different offences, thus negating the taxonomy established for computer-focused offences. And for juridical persons, the fines would become far less of a deterrent than they currently are! The 2019 draft reform is again not the way forward. Instead, it is recommended that the existing punishment for illegal access should be reduced to a fine not exceeding 30,000 Birr, with the reference to 50,000 Birr deleted, so that the ration imprisonment-to-fine used throughout the 2016 Proclamation remains adhered to.

5. CONCLUSION

With the digitisation of Ethiopia's telecommunication services since the 1990s, and broadband becoming available in 2004, the Ethiopian federal government had to grapple with the increasing threats of cybercrimes. In the space of two decades, Ethiopia experienced two sets of legislative responses: the first criminalisation of computer-focused crimes in the 2004 Criminal Code, complemented by the 2012 Proclamation for telecom infrastructures; and the modernisation of these crimes in the 2016 Proclamation which aimed to palliate the deficiencies of the first set. The dust has not yet settled on the latter that the Ethiopian legislator emphasised the inadequacy of the current Proclamation to justify its proposal of a new draft law in 2019.

To critically evaluate Ethiopia's successive legislative responses to computer-focused crimes, we reviewed the taxonomy that the legal community has agreed upon since the Budapest Convention. This taxonomy captures in techno-neutral language the different *modi operandi* of cybercriminals in five offences, from the least serious (misuse of tools, including possession) to the serious (illegal access) and most serious (system and data interferences; data interception). To be proportionate punishments would need to reflect this taxonomy and its implicit degree of seriousness.

The Code was a pioneer in criminalising computer-focused crimes but had some significant weaknesses. It notably did not criminalise illegal data interception and did not articulate well the constitutive elements of the system interference and misuse of tools offences. From inception, the legislator experienced difficulties in drafting a set of offences and their correlative penalties cognisant of the taxonomy of cybercrimes. The law needed future-proofing, not because of technological advancement, but because of the initial difficulty in conceptualising computer-focused crimes with regard to their specific features and the existing international standards. In contrast, the 2016 Proclamation represents a welcome step forward. It significantly improves the structure of the offences to clarify their scope; and it establishes coherence in the proportionality of the penalties between the offences and with their aggravated forms, including with a consistent ratio between imprisonment and fines. Despite some gaps, the Proclamation demonstrates Ethiopia's legislative readiness concerning its substantive criminal law. There remains the need, of course, for adequate provisions in criminal procedure, such as trained professionals to prevent, investigate and prosecute cybercrimes in compliance with human rights. Nevertheless, the Proclamation has put Ethiopia in a strong position to fight cybercrimes over the coming decades.

The 2019 draft Proclamation would be introducing far fewer sweeping changes than the 2016 Proclamation did. Yet, these changes deserve careful consideration should the draft Proclamation be enacted. Too frequent changes in criminal law can be disruptive to the fight against cybercrime, unless this 2019 draft helps develop an even more sustainable response to cybercrimes, bridging

the gaps highlighted in the 2016 Proclamation. The proposed reform addresses one of these gaps, by offering to repeal the misuse of tools offence when committed by negligence, thus protecting IT administrators from making mistakes. It also reinforces the strong protection currently offered to legitimate security researchers using dual-use hacking tools, a protection rarely implemented by other countries.

Besides these provisions, the 2019 Draft does not establish a future-proof legal framework for computer-focused crimes. It leaves intact the existing ambiguities as to the scope of the illegal system interference offence, as well as the over broad reach of the criminal law regarding attempts and illegal system interference. Worse, it creates further difficulties by introducing overlaps between the various offences, overlaps which cannot be justified by technological advancement and cybercrimes' specificities. Its proposal for punishments also represents an unwelcome return to the disproportionate approach that existed in the Code.

To bring sustainability to this anticipated third reform, the authors recommend that the legislator keep unchanged the positive elements of the current 2016 Proclamation and remedy the latter's weaknesses. For the reform not to create new gaps, the legislator, especially the drafting committee, should adopt an approach consistently tailored to the specificities of computer-focused crimes and the best experiences from international and regional standards. Coherence in the structure of the offences and strong proportionate punishments should be a priority to provide a more effective and long-lasting response to the challenges inherent to the field. Consequently, our most important recommendations are summarised as follows. Regarding the offences, firstly, the current offences of illegal access and illegally causing damage to data in the 2016 Proclamation should remain intact in their constitutive elements, except for a change of title to reflect the fact that the offence of causing damage criminalises more than damage and is, actually, illegal interference. Secondly, the 2016 Proclamation could be amended to: 1) clarify the offence of system interference to protect the availability of systems; 2) stop the artificial distinction existing between Article 7(1) and (2) on misuse of tools; and 3) exclude attempted illegal access and misuse of tools which represents a criminalisation of the thought process expressly rejected at international level. Thirdly, articles 5 and 6 in the current 2019 Draft Proclamation should be abandoned, notably those that create overlaps between the two offences of data and system interferences. Conversely, the proposal to abolish negligent misuse of tools (current Article 7(5) 2016 Proclamation) should be adopted. It remedies the current gap in the 2016 Proclamation and promotes the use of tort law and regulatory measures on cybersecurity which are more effective than criminal law in pushing for better cybersecurity practices among IT professionals.

Regarding punishments, the authors would particularly recommend adding further intent as an aggravating factor to illegal access, for the courts to account for the increased culpability of those who commit illegal access with intent to commit further crimes, especially fraud. The reform should also ensure that ordinal proportionality applies to all fines, without exceptions, whether between a base offence and its aggravated forms, across the different base offences, or across their aggravated forms. Finally, it should ensure that the financial means of juridical persons, compared with those of individuals, inform the proportionality between the two.

By respecting the taxonomy of cybercrimes expressed in all international legal instruments, these recommendations aim to further strengthen Ethiopia's readiness to fight cybercrime. Their implementation would send a strong deterrent signal to cyber criminals while creating a space for

good cybersecurity to help fight cybercrime. It would also facilitate Ethiopia's ratification of the Malabo Convention and the serious consultation of the Budapest Convention, should the country wish to do so.