

**Kínai álom, afrikai álom:
A Digitális Selyemút projekt hatása afrikai országok kiberbiztonságára¹**

Jelige: QXL349

Dolgozat lezárásának dátuma: 2021. november 8.

¹ A pályamunka jelentős része tartalmilag megegyezik a szerző azonos című, 2022 áprilisában elkészült diplomamunkájával.

TARTALOMJEGYZÉK

1. BEVEZETÉS	3
1.1. A kutatás relevanciája	3
1.2. Kutatási kérdés	4
1.3. A kutatás esettanulmánya	4
1.4. Az esettanulmány kiválasztása	5
1.5. A dolgozat felépítése	7
2. ELMÉLETI HÁTTÉR: A DIGITÁLIS NEOKOLONIZÁCIÓ	8
2.1. A kiberbiztonságról röviden	8
2.2. Kolonizációs elméletek a múltban	9
2.3. A kolonizációs folyamatok digitálissá válása	10
3. ESETTANULMÁNY: KELET-AFRIKAI ORSZÁGOK A KIBERTÉRBEN	13
3.1. Miért éppen Tanzánia?	13
3.1.1. Tanzánia a kibertérben - A béke és biztonság nevében	13
3.2. Miért éppen Etiópia?	16
3.2.1. Etiópia a kibertérben – Korlátok közé szorítva	17
3.3. Összefoglalás - Nehézségek a digitális fejlődésben	19
4. KÍNA HATÁSA A KELET-AFRIKAI ORSZÁGOK KIBERBIZTONSÁGÁRA	20
4.1. Mit tudunk a Digitális Selyemút tervről?	20
4.2. Technológiai fejlődés Kína segítségével	21
4.2.1. Kockázatok	22
4.3. Digitális diplomácia – Az internetszuverenitás modellje	24
4.3.1. Kockázatok	27
4.4. Összefoglalás - A Digitális Selyemút projekt és a digitális gyarmatosítás	29
5. KÖVETKEZTETÉSEK	31
5.1. Előnyök és hátrányok mérlegelése	31
5.1.1. Következmények a résztvevők szintjén	32
5.1.2. Következmények globális szinten	34
5.2. Konklúzió - Mire számíthatunk a jövőben?	35
6. BIBLIOGRÁFIA	36

1. BEVEZETÉS

Napjainkban egyre nagyobb figyelem irányul a kiberbiztonsági kockázatokra, legyen szó államok vagy egyéni szereplők elleni támadásokról. A legnépszerűbb témák közé tartoznak az orosz hackercsapatok munkássága vagy az adatvédelmi problémák a közösségi médiában. Azonban a szegényebb, fejlődő országok helyzetéről jóval kevesebbet hallunk a hírekben. Az afrikai kontinensen Kína térnyerése egyre nagyobb mértéket ölt, erre jó példa a Digitális Selyemút kiépítésének terve (Shen, 2018). A projekt keretében erős befolyásra tesznek szert Afrikában, a gazdasági és politikai szektoron kívül a kibertérben is. Ahogyan Hszi Csin-ping, a kínai elnök fogalmazott 2013-ban, a kezdeményezés bejelentésekor, elköteleződnek Afrika fejlődésének elősegítése iránt. Így válik a „nagy kínai álom” egyben „afrikai álommal is” (Anthony, 2013). Mit kapunk, ha keresztezzük az újdonsült szuperhatalomtól kapott hiteleket egy kontinensnyi fejlődő, instabil rendszerű országgal? Mire számíthatunk, ha kiépítjük a 4G hálózatot és Huawei telefonokat adunk el olyan társadalmaknak, akiknek még a fejlett országokhoz képest kevés tapasztalatuk van a digitalizáció terén és nem ismerik a modern, digitális világ kiberbiztonsági kihívásait? Mi Kína célja? Vajon egy újfajta, digitális gyarmatosítási folyamatnak lehetünk tanúi? Melyik fél milyen módon és milyen mértékben profitál ebből a kapcsolatból?

1.1. A kutatás relevanciája

Kína tagadhatatlanul a XXI. századi világpolitika egyik főszereplőjévé nőtte ki magát. Ez az ellentmondásos szereplő sokak szerint az Egyesült Államok hegemoniáját veszélyezteti (Layne, 2008), valamint reális esélyét látják annak, hogy néhány éven vagy évtizeden belül át is veszi a vezető pozíciót, mind gazdasági, mind politikai befolyás terén. Az ázsiai ország az utóbbi évtizedek alatt elérte, hogy ne a nyugati vállalatok által épített infrastruktúrára kelljen támaszkodnia: mára a tenger alatti optikai kábelek negyedik legnagyobb gyártójává vált (Hillman, 2021, p. 17). Amennyiben Afrika, a világ legszegényebb és legfejletlenebb kontinense ennek az új szuperhatalomnak az árnyékába kerül, annak feltevéseim szerint komoly következményei lehetnek a helyi és a globális közösségre nézve. A kontinens országai újra alárendelt szerepbe kerülhetnek, ezzel esetlegesen hátráltatva az afrikai társadalmak fejlődését. Továbbá, amennyiben Kína hozzásegíti a fejlődő országokat a kibertérhez való csatlakozáshoz, ezzel nem csupán új szövetségeket szerez magának, hanem a rengeteg új szereplő megjelenésével esetlegesen növelheti is a kiberbiztonsági kockázatok számát. Ezek a kockázatok lehetnek nemzeti szintűek, de a kibertér határok nélküli természetéből adódóan más országokat is érinthetnek, legyen szó egy újfajta kártevő szoftver (*malware*) terjedéséről vagy

egy új, afrikai hackergeneráció feltörekvéséről. Amennyiben Kína befolyásszerzése Afrika kiberterében nem ütközik akadályokba és sikeresen teljesítik projektjüket, a globális közösségnek tisztában kell lennie a lehetséges következményekkel, vagyis az esetleges további terjeszkedéssel újabb és újabb földrészekben. A kibertérben jelenleg is egy folyamatos harc zajlik. Egyet nem értés alakult ki globális szinten abban a kérdésben, hogy milyen módon szükséges szabályozni az internetet (Shen, 2016, p. 1). Kína ebben a harcban előnyhöz juthat, amennyiben megszerzi további országok támogatását, például hazai vállalatok megjelenésével új térségekben (Arsène, 2012, p. 11). Az Egyesült Államoknak, mint Kína legfőbb vetélytársának, illetve szövetségeseinek megfelelően fel kell tudnia mérnie az új szuperhatalom „kibererejét”, valamint a befolyásolt országok gyengeségeit. Kína és Afrika ICT szektoron (*Information and Communication Technology*, magyarul Információs és Kommunikációs Technológia) belüli összekapcsolódásának vizsgálatából továbbá megtudhatjuk, hogy mitől válnak a keleti hitelek ennyire vonzóvá a nyugatiakkal szemben. Ez a gondolatmenet pedig elvezethet minket egy további kutatásra érdemes területhez, vagyis ahhoz az elhanyagolt kérdéshez, hogy a Nyugat mit tehet másképp a jövőben.

1.2. Kutatási kérdés

Dolgozatom célja tehát mindezen okokból, hogy két afrikai ország, Tanzánia és Etiópia esettanulmány keresztül feltárjam Kína, mint legfőbb kereskedelmi partner, illetve hitelező hatását e fejlődő országok ICT szektorában. Kutatásom fő kérdése, hogy vajon Kína újfajta kolonizációs stratégiája milyen hatással van a kijelölt két ország kibertérhez való viszonyára, illetve milyen sajátos módszerekkel igyekszik befolyását növelni a térségben. Célom, hogy a kutatásom végén - a kiberbiztonság területére koncentrálnak - egyértelműen ismertessem ennek az együttműködésnek az előnyeit és hátrányait, ezzel együtt pedig megfogalmazzam a fő kockázatokat a jövőre nézve.

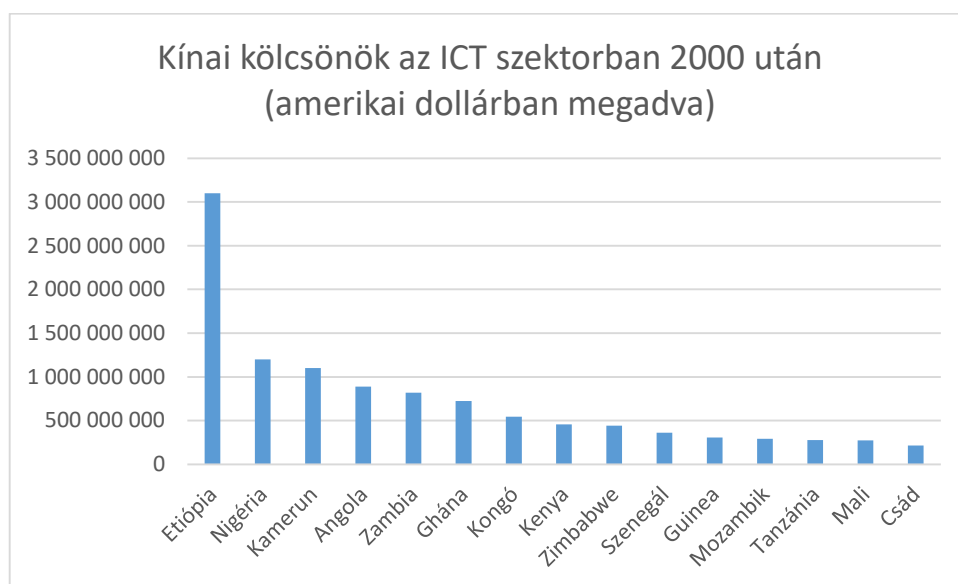
1.3. A kutatás esettanulmánya

Ahhoz, hogy ezt a kérdést megválaszoljuk, elsősorban definiálnunk kell, mit jelent pontosan a digitális neokolonizáció, vagyis az újfajta gyarmatosítási stratégia, amivel Kína megjelent az afrikai kontinensen a 2000-es években (Gravett, 2020). Ebből kiindulva tisztán láthatjuk majd, hogy Kína milyen céllal igyekszik befolyását növelni az elmaradott afrikai országok körében, illetve, hogy miért pont a kibertéren keresztül teszi azt. Megvizsgáljuk, hogy hogyan helyezkedik el a Digitális Selyemút projekt ebben a folyamatban, illetve kik a pontos szereplők.

Kutatásomban két afrikai ország Kínával való kapcsolatának elemzésén keresztül keresem a választ kérdéseimre.

1.4. Az esettanulmány kiválasztása

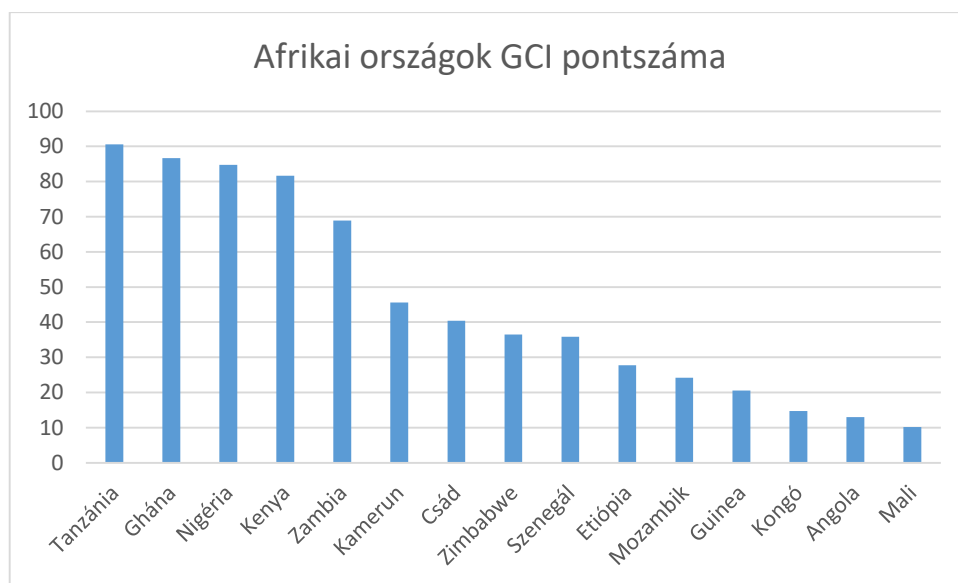
A dolgozatomban bemutatott esettanulmányok kiválasztásakor két szempontot vettem figyelembe. Egyrészt a Kínától kapott hitelek összegét, amiből kiderül, a szuperhatalom mely országok pénzügyi támogatását tartotta legfontosabbnak. Másrészt megvizsgáltam a legnagyobb mértékben támogatott afrikai államok Global Cybersecurity Index szerinti rangsorban elfoglalt helyét, amiből kibebiztonsági fejlettségükre következtethetünk.



1. ábra Kínától kapott hitelek összege az ICT szektorban (Forrás: China Africa Research Initiative, Chinese Loans To Africa Database)

Kína számos afrikai ország számára nyújtott kölcsönöket az ICT szektor fejlesztésének céljából, már az ezredfordulótól kezdve. Az 1. számú ábrán a 15 legnagyobb összeget kapott államok szerepelnek. Jól látható, hogy Etiópiának Kína kiemelkedően magas összegű hiteleket nyújtott, 3,5 milliárd dollár értékben, míg Tanzánia csupán 277 millió dolláros kölcsönben részesült (China Africa Research Initiative, 2021). A hitelek mérete mellett érdemes megfigyelnünk, hogy ezek az államok hol helyezkednek el a Nemzetközi Távközlési Egyesület (International Telecommunication Union, továbbiakban: ITU) által készített Global Cybersecurity Index 2020-as rangsora szerint. Az ITU, vagyis az ENSZ egyik szakosodott szervezetének kezdeményezésében öt különböző szempont alapján készítik el a vizsgált országok kibebiztonsági profilját. Elsőként vizsgálják az adott állam kibertérre vonatkozó jogszabályainak meglétét, ezen belül pedig az adatvédelem és a kritikus infrastruktúra védelmének szabályozását. Ezen kívül figyelembe veszik a technikai és szervezeti

képességeket, vagyis a kiberbiztonsági veszélyhelyzeteket kezelő mechanizmusok, intézmények, munkacsoportok hatékony működését. Végül a kutatásom szempontjából kiemelten fontosnak számító a kapacitásfejlesztési és kooperációs képességek jelennek meg a GCI rangsorban. Ez előbbi szempont a kiberbiztonsági tudatosságra vonatkozik, vagyis azt méri, hogy az adott országban elegendő figyelmet fordítanak-e a felhasználói tudatosság növelésére, például kampányokon, oktatási programokon, tréningeken keresztül. Az utóbbi szempont pedig az együttműködési képességeket veszi figyelembe, akár a köz – és magánszektor közötti vagy más államokkal kötött bilaterális és multilaterális egyezmények alapján (ITU, 2021).



2. ábra Jelentős kínai hitelt felvevő afrikai országok GCI pontszáma (Forrás: ITU, Global Cybersecurity Index 2020)

A 2. ábrán az 1. ábra 15 országa szerepel, ezúttal a GCI pontszámaik alapján rangsorolva. Tanzánia egy figyelemre méltó, 90 feletti pontszámmal szerepel a listán. Míg Etiópia a legnagyobb összegeket kapta Kínától és rendkívül rosszul teljesít a GCI szerint, addig Tanzánia viszonylag kevés segítséggel úgy tűnik, magas fejlettségű kiberbiztonsággal rendelkezik. Etiópia a jogi szabályozás területén teljesít legjobban, habár más országokhoz képest ezen a téren is fejletlennek számít. Tanzánia erősségének a kooperációs képességek számítanak (ITU, 2021). Mindezen adatok alapján arra számítunk, hogy a Kínával való együttműködés során jelentős különbségeket vélünk majd felfedezni a két állam között. E két afrikai ország tehát különböző szempontok miatt, de egyaránt kiemelt figyelmet érdemelnek. Kutatásomban Tanzánia és Etiópia esetére fókuszálok, hogy két, kiberbiztonság terén elméletileg különböző fejlettségi szintű országban is bemutathassam Kína hatását.

1.5. A dolgozat felépítése

Hogy kielégítő választ tudjak adni a kutatásom céljával megfogalmazott kérdésekre, az alábbi szempontok szerint foglalkozom a vizsgált országokkal. Legelőször bemutatom, a szakirodalomban eddig mely szempontok alapján vizsgálták a neokolonializmust, és annak digitális formáját. Ezt követően megindoklom, miért pont Tanzánia és Etiópia érdemelnek kiemelt figyelmet kutatási kérdésem szempontjából. Bemutatom, hogy ezek az afrikai országok milyen kapcsolatban álltak Kínával az ICT szektort illetően és milyen támogatást kaptak a szuperhatalomtól a Digitális Selyemút projekt bejelentését megelőzően. Korábbi kutatások alapján felmérem, ezek a támogatott államok milyen szinten állnak kiberbiztonság terén, illetve milyen viszonyban állnak a modern technológiával. Ezután meg kell vizsgálnunk, mit tudunk a nagyszabású kínai terv célkitűzéseiről és azok gyakorlati megvalósulásáról. A projekt két komponensével foglalkozom részletesen: az új technológiák átadásával, továbbá az internetszuverenitás modelljének meghonosításával az afrikai kontinensen. Feltérképezem a nyilvános projekteket, amelyek Kína és Tanzánia, illetve Etiópia együttműködésével valósultak meg. Mindezek alapján megfogalmazom a kijelölt afrikai országok és Kína kapcsolatából származó legfőbb kiberbiztonsági kockázatokat. Az eredmények alapján bemutatom, Kína cselekedetei hogyan támasztják alá a digitális neokolonializmusról szóló elméletet. Kutatásom végeredményét pedig egy táblázatban összesítem, amelyben felsorakoztatom a vizsgált kapcsolat előnyeit és hátrányait az afrikai országok szempontjából. Ebből kiderül, hogy milyen mértékben profitálnak a felek az együttműködésből, illetve, hogy az melyikük számára jelent nagyobb előnyt. A konklúzió alapján további kutatásra érdemes kérdéseket fogalmazok meg, valamint rövid kitekintésben felvetem azt a kérdést, hogy miért jelent ez a projekt veszélyt az Afrikán túli világra is.

2. ELMÉLETI HÁTTÉR: A DIGITÁLIS NEOKOLONIZÁCIÓ

2.1. A kiberbiztonságról röviden

Kutatásom szempontjából kiemelten fontos tudatosítanom, hogy amikor kiberbiztonsági kockázatokról beszélünk, nem csupán az interneten tárolt információk védelmére kell gondolnunk (Craig et al., 2014). A Digitális Selyemút projekt és a digitális neokolonizáció folyamatában számos tényező a világhálót létrehozó és működtető, fizikai valójában is létező infrastruktúra védelméhez kapcsolódik.

Az internet működése egy jóval bonyolultabb folyamat annál, mint amennyit dolgozatom keretei közt alkalmam nyílik bemutatni. Azonban azt rendkívül fontosnak tartom tudatosítani kutatásom szempontjából, hogy az internet, vagyis a határokon átívelő hálózatok összességének működtetéséhez komoly fizikai infrastruktúra, ezáltal gépek, eszközök (például szerverek, kábelek) és képzett szakemberek szükségesek (Tsagourias, 2015, p. 15). A kibertér a legtöbb szerző több, egymással kölcsönhatásban álló rétegre osztja. Douzet (2014, pp. 4-5) négy réteget különböztet meg, amiből az első a fizikai infrastruktúrát jelenti, vagyis a tenger alatti kábeleket, számítógépeket és minden egyéb felszerelést. A szerző felhívja a figyelmet e réteg sérülékenységeire. Ez az infrastruktúra a szabad információáramlás céljából épült, viszont a kiépítések során nem fordítottak elég figyelmet biztonságának garantálására (Douzet, 2014, p. 4). A hiedelemmel ellentétben nem a műholdakon, hanem a már említett tenger alatti kábeleken keresztül zajlik a nemzetközi adatforgalom 95%-a (Hillman, 2021, p. 3). Ez a réteg bármely állam által kiegészíthető, építhető, vagy akár megsemmisíthető. A második és harmadik réteg a logikai infrastruktúrát, az IP címeket, *domain* neveket, weblapokat illetve az alkalmazásokat, programokat tartalmazza, vagyis mindazt a már megfoghatatlan területet a világhálón, amelyek lehetővé teszik a felhasználók számára az információcserét. Ez utóbbi komponens már a kibertér negyedik rétegét alkotja, amely az első réteggel közösen kiemelt figyelmet érdemel kutatásom szempontjából.

A fejlettebb országok a különböző rétegek védelme érdekében kiberbiztonsági stratégiákkal rendelkeznek, továbbá külön törvényeket alkotnak a világhálón zajló adatforgalom szabályozására (lásd: GDPR rendelet). A fejlődő országokban, köztük az afrikai térség államaiban azonban sok esetben csak később, a 2010-es évek elején kezdett elterjedni az internethasználat (ITU, 2019) és közel sem olyan mértékben, mint Európában vagy Észak-Amerikában. Dolgozatomban problémafelvetése szerint előfordulhat, hogy ezek az elmaradottabb régiók még nem rendelkeznek a megfelelő szaktudással és eszközökkel a kiberbiztonsági

kérdések tudatosításához, ezáltal nem jutnak el a megfelelő jogi szabályozás létrehozásához sem. A kutatásom alapjául szolgáló Digitális Selyemút projekt ezeknek az országoknak az ICT szektorát célozza meg, vagyis egy kulcsfontosságúvá vált infrastruktúra fejlesztését segíti elő (Shen, 2018, p. 2684).

Dolgozatomban kiberbiztonsági kockázatok alatt minden olyan fenyegetést értek, amelyek ezt az infrastruktúrát és a rajta keresztülmenő információkat érhetik. Ezek a fenyegetések jelenthetnek adathalászatot, az információáramlás manipulációját és korlátozását, a fizikai infrastruktúra kisajátítását, felügyeletét vagy hackertámadásokat. Mindez megjelenhet egyéni vagy állami szinten, amelyeket érdemes együtt kezelni, mivel ezek a szintek folyamatos kölcsönhatásban vannak egymással. A támogatott országok digitális terébe való beavatkozás az alább tárgyalt digitális neokolonizáció jelenségével függhet össze.

2.2. Kolonizációs elméletek a múltban

A kolonizáció kérdése egy igen széles körben kutatott elmélet. Az afrikai kontinensen a XIX. században jelentek meg először brit gyarmatosítók, dekolonizációs folyamatokról pedig csak a második világháború végétől kezdve beszélhetünk. Césaire (1950) *Discourse on Colonialism* című írása a posztkolonializmus irodalmának alpműve, amelyben megfogalmazza, hogy a gyarmatosítási folyamatok valójában sohasem a gyarmatok fejlődését szolgálták. A kolonizáció egyértelműen negatív következményekkel jár a harmadik világbéli országok számára, hiszen azok gazdaságát súlyosan károsítják a kizsákmányoló nagyhatalmak (Kohn & Reddy, 2017). Ezek a hatások nem múltak egy nyomtalanul, ráadásul új típusú gyarmatosító államok is megjelentek a nemzetközi szinten a XXI. században (Coleman, 2019). Ezekben az új folyamatokban szintén meghatározó az alá – és fölérendeltségi viszony, azonban a XX. század második felében felgyorsult technológiai fejlődésnek köszönhetően teljesen új módszerekkel biztosítják a gyarmatosítók saját erőfölényüket a fejlődő országokkal szemben.

A digitális neokolonizáció egy viszonylag új, kevésbé kutatott gyarmatosítási folyamat, ami a modern telekommunikációs eszközök segítségével zajlik. A neokolonizáció, mint jelenség elsőként Kwame Nkrumah ghánai származású politikus 1965-ös írásában jelent meg. A megbecsült és befolyásos Nkrumah a neokolonizációról úgy írt, mint az „imperializmus utolsó fázisáról” (Nkrumah, 1965). Az 1960-as évek dekolonizációs hulláma nem hozta el azt a változást számos ország számára, amelyben korábban reménykedtek. A gyarmatosítás, mint a nagyhatalmak kedvelt befolyásnövelő módszere nem tűnt el a nemzetközi színterről. Ezt az újfajta gyarmatosítást úgy definiáljuk, mint azt a jelenséget, aminek célja a hivatalosan már

nem gyarmati státuszban lévő országok közvetett módon történő befolyásolása (Nkrumah, 1965, p. 1). Célja a XX. században az volt, hogy a volt gyarmattartó nagyhatalmak továbbra is élvezhessék az olcsó munkaerő és kiapadhatatlannak tűnő nyersanyag készlet adta előnyöket egy harmadik világbéli országból. Nkrumah szerint a módszerek különbözőek lehetnek, ezek közül a két legnépszerűbb a katonai és a gazdasági befolyásolás (Nkrumah, 1965, p. 2). Az előbbi arra a jelenségre vonatkozik, mikor a gyarmatosító ország fegyveres védelmet kínál a gyarmatnak, ezzel biztosítva katonai jelenlétét az adott államban. Az utóbbi módszer ezzel szemben pénzbeli kölcsönöket ad a „támogatott” országnak, így gazdaságilag teszi függővé a gyarmatot. A volt gyarmattartók azért tehetik meg könnyen ezeket a lépéseket, mivel a gyarmati státuszból éppen csak kikerült országokban még nem alakultak ki olyan stabil politikai rendszerek, amelyek képesek lennének önállóan újjáépíteni és átalakítani országuk működését. A gyarmati idők öröksége tehát nem múlt el nyomtalanul, a ma is tapasztalható egyenlőtlenség a fejlett és fejlődő országok között részben erre a folyamatra vezethető vissza (Loomba, 2002, p. 12).

2.3. A kolonizációs folyamatok digitálissá válása

A neokolonializmus tehát egyáltalán nem új jelenség, hanem a régi típusú gyarmatosítás közvetlen folytatásaként is értelmezhetjük. De mitől lesz ez a folyamat „digitális”? A digitális neokolonizáció már a XXI. század találmánya, hiszen a modern telekommunikációs eszközök, legfőképpen a mobiltelefonok és a világháló teszik lehetővé. A Nyugat befolyására is tekinthetünk ilyen típusú gyarmatosítási folyamatként, hiszen a fejlődő államok – megfelelő technológiai fejlettség híján – kénytelenek elfogadni a legfejlettebb országok által felállított rendet a kibertérben (Arsène, 2016, p. 29). Ezen a területen is számos befolyásolási módszer áll a nagyhatalmak rendelkezésére. Mint azt már tudjuk, a modern kor egyik, ha nem a legértékesebb „nyersanyaga” az információ (Coleman, 2019, p. 424). A digitális eszközök által ez az óriási „nyersanyagkészlet” válik elérhetővé a befolyásukat növelni vágyó államok számára.

Az egyik legegységesebb, leghétköznapiabb módszer, amellyel ma már az internetfelhasználók egy bizonyos rétege tisztában van, az a mérhetetlen adatgyűjtési folyamat, ami többek között a közösségi média oldalakon zajlik. Minden személyes adatunk, nevünk, lakcímünk, születési helyünk, munkahelyünk, végzettségeink, pontos mozgásunk GPS koordinátái valamilyen formában dokumentálásra kerülnek a világhálón. Ez egy olyan visszafordíthatatlan folyamat, amely már sok évvel ezelőtt elkezdődött. Coleman (2019) foglalkozott ezzel a jelenséggel, mint a digitális neokolonizáció egyik módszerével. Mivel a fejlődő országokban az internetezők

kevésbé tájékozottak az adatvédelmi kockázatokat illetően, ezért a digitális gyarmatosító könnyedén tud információhoz jutni rajtuk keresztül. Ezen kívül a szabályozás részleges, vagy teljes hiányát is kihasználhatják a nagyhatalmak. Ha egy kevésbé fejlett országban nem számít bűncselekménynek például a személyes adatok jogtalan felhasználása, vagy egyszerűen nincs jogorvoslat, akkor ezek az államok igen vonzó célpontokká válhatnak. Tehát egy digitális gyarmatosító hatalom egyik fő célja az lehet, hogy a minél erősebb befolyásszerzés érdekében, az interneten keresztül a lehető legtöbb adathoz jusson hozzá, vagyis hogy minél jobban kiismerje a gyarmatosított ország társadalmát.

Az adatgyűjtésnek, mint a digitális gyarmatosítás egyik fő céljának azonban az az alapvető feltétele, hogy a lakosság lehető legnagyobb százaléka rendelkezzen internetelérhetőséggel. Dolgozatomban erre a folyamatra fókuszálok, hiszen Kína ezt a stratégiát alkalmazza jelenleg az afrikai kontinensen. A neokolonizáció Nkrumah által is említett módszere, a pénzbeli kölcsön ebben a folyamatban is megjelenik. A vizsgált esetben Kína, mint potenciális digitális gyarmatosító kölcsönöket ad a legtöbb afrikai országnak, ezáltal segítenek az infrastruktúrafejlesztésben, valamint az internethálózat kiépítésében is. Ez a Digitális Selyemút projekt egyik fő célja (Shen, 2018, p. 2684). Ez a stratégia abból a szempontból figyelemre méltó, hogy ötvözi a régi módszert (gazdasági befolyásolás hitelezéssel) a modern eszközökkel (internethálózat kiterjesztése). A volt gyarmatok a fejlődés, gazdasági előnyök vagy egyéb politikai célok reményében engednek a nagyhatalmaknak és szívesen elfogadják a segítségüket. De mitől válik számukra ilyen vonzóvá egy digitális gyarmatosító hatalom, jelen esetben Kína ajánlata? Az elmaradott országok vezetői szemében a kínai internetszuverenitás modell egy optimális megoldásnak tűnhet, állampolgárainak korlátozása céljából. Mivel a digitális gyarmatosító hatalom közvetett vagy közvetlen módon részt vesz az internethálózat kiépítésében, ezért beleszólása van abba is, hogy milyen típusú internetmodellt kíván elterjeszteni a befolyásolni kívánt országokban. A kínai modell elveti a korlátok nélküli böngészést a világhálón, a vezetők képesek befolyásolni, hogy mely weboldalakhoz férhetnek hozzá az országban élők (Gravett, 2020, pp. 128-129). Ez a modell kulcsfontosságú eleme kutatásomnak, ugyanis ez lehet a leghatásosabb, legkönnyebb megoldás Kína szempontjából, amennyiben kontrolljuk alá akarják vonni Afrika digitálisan fejletlen országait.

Az internetszuverenitás modellje szemben áll a Nyugat által hirdetett és elfogadott szabad világháló elmélettel. Ahogyan Ursula von der Leyen, az Európai Bizottság elnöke fogalmazott 2020-ban, az internetnek „a szabadság, kifejezés és innováció nyílt terének” kell lennie (Európai Bizottság, 2020). Használata egy „új emberi jog”, azonban bizonyos korlátokat kell

szabni, hogy más jogaink se sérüljenek, vagyis meg kell találni egy egyensúlyi állapotot. A fejlett országokban ez a paradigma uralkodik, azonban a világ számos részén egyre népszerűbbé válik a Kína által hirdetett modell. Az internetszuverenitás fogalma a 2010 júniusában kiadott, *Az internet Kínában* című fehér könyvben jelent meg elsőként. Ebben az írásban Kína kijelenti, hogy „határain belül az internet kínai szuverenitás alatt áll”, amit „tisztelni és védeni” szükséges (The Internet in China, 2010). Ez a modell számos autoriter államnak nyújthat megoldást, azonban a világháló nyugati percepciójával teljesen összeférhetetlennek bizonyul. Ahogyan Gravett (2020, p. 128) is felhívja rá a figyelmet, a kínai internetszuverenitás „felügyeletet és kontrollt” jelent, semmint szabadságjogokat. Hszi Csin-ping egy 2015-ös beszédében kijelentette, hogy szerinte a kibertér szuverenitása ugyanúgy, mint a nemzetközi kapcsolatok többi területe, sérthetetlen (Tiezzi, 2015). Tehát a kínai álláspont szerint az internetszuverenitás nem más, mint egy a nemzetközi közösség által is elismert alapelv megnyilvánulása a digitális térben. Fontos megjegyeznünk, hogy Kínán belül is vitatott a szakértők körében a modell pontos definíciója, valamint a gyakorlatba ültetés módja, hiszen a politikai vezetés kommunikációja sem mindig világos (Zeng et al., 2017, p. 436). Mindezek ellenére tisztán láthatjuk, hogy ez az új internetfelfogás a világ elmaradottabb térségeiben nagy népszerűségnek örvend. Úgy tűnik, hogy az általam vizsgált afrikai országok vezetői számára Kína imponál egy új, korlátozottabb, manipulálható internethálózat ígéretével.

Ezek alapján tehát azt láthatjuk, hogy Kína a digitális neokolonializmus elvei alapján igyekszik minél nagyobb befolyást szerezni, legfőképpen az afrikai kontinensen. Érdekesség, hogy ebben az esetben nem egy volt gyarmattartó, például Franciaország vagy Hollandia tér vissza a gyarmatokhoz és igyekszik újból befolyást szerezni a térségben, hanem egy új szereplő lép színre Afrikában. Tehát kijelenthetjük, hogy a digitális neokolonizáció nem csak a múltbéli gyarmati kapcsolatokat képes újjáéleszteni, hanem eddig még sosem látott, új befolyásolási módszerekhez folyamodva épít hidakat egymástól földrajzilag és fejlettségi szintben is távol álló államok között.

A korábbi szakirodalom külön-külön foglalkozott a gyarmatosítási folyamatokkal, a Kínából Afrikába áramló forrásokkal, illetve azok kiberbiztonsági vonzataival, mindezen jelenségeket pedig ritkán vetik össze a kutatók. Dolgozatom többek közt ezt a hiányt hivatott pótolni, az összefüggések vizsgálatával és a kínai-afrikai együttműködés előnyeinek és hátrányainak bemutatásával.

3. ESETTANULMÁNY: KELET-AFRIKAI ORSZÁGOK A KIBERTÉRBEN

Tanzánia és Etiópia a világ legszegényebb régiójában, vagyis a Szubszaharai Afrikában helyezkednek el. 2020-ban Tanzánia lakossága a 60 milliót, Etiópiáé pedig a 115 millió főt közelíti (Világbank, 2020). Míg 2005 és 2008 közt az internethasználók aránya a 2%-ot sem érte el, addig a múlt évtizedben elképesztő mértékű növekedést produkált ez a két elmaradott afrikai ország. 2019-re Tanzániában a népesség 20%-a, Etiópiában pedig már a 25%-a használta az internetet (ITU, 2019). Kétségtelen, hogy ez a növekedés nagyrészt Kína színrelépésének, vagyis a nagy összegű hiteleknek köszönhető: a Szubszaharai Afrika a Kínával szemben leginkább eladósodott térségek között szerepel (Gandhi, 2019). Ebben a fejezetben legelőször megindoklom, hogy miért Etiópiát és Tanzániát érdemes vizsgálni Kína Afrikára gyakorolt hatásának kérdésében. Bemutatom, hogy ezek között az államok közt milyen kapcsolatok szövődtek az ICT szektoron belül, még a Digitális Selyemút projekt kezdete előtt. Ezután megvizsgálom, hogyan viszonyulnak a kiberbiztonság kérdéséhez. Mielőtt a projekt hatásáról szólnék, fontosnak tartom felmérni, hogy ez a két állam a XXI. század elejétől milyen változáson ment keresztül, milyen mértékű fejlődést produkált az ICT szektorban, illetve, hogy ezt milyen külső segítségekkel sikerült elérnie.

3.1. *Miért éppen Tanzánia?*

Tanzániának már az 1970-es évek óta kiemelten fontos kereskedelmi partnere volt Kína. Ennek a kapcsolatnak a gyümölcse többek között a TAZARA vasútvonal, amely Zambiával köti össze a tanzániai főváros kikötőjét (Kinyondo, 2019, p. 9). A projekt nagyrészt pozitív eredményekkel zárult, ezáltal megalapozta a Kína iránti bizalmat. Ezt a bizalmat a tanzániaiak az ICT szektorban is megszavazták Kína számára, leginkább a Huawei nevű vállalat közreműködésével (Alkhawajah, 2019). Ahogyan később is látni fogjuk, Kína valójában már jóval a Digitális Selyemút projekt előtt is nagy befolyással volt Tanzánia információs technológiai fejlődésére. A kelet-afrikai ország csupán a 14. legnagyobb összegű hitelt kapta a szuperhatalomtól az ICT szektorban, azonban térségében kiemelkedő eredményt ért el a Global Cybersecurity Index szerinti 2020-as rangsorban. A továbbiakban bemutatom, hogy mi jellemzi Tanzánia kibertérhez való viszonyát és ezáltal azt is, hogy vajon van-e valóságalapja a GCI indexnek.

3.1.1. *Tanzánia a kibertérben - A béke és biztonság nevében*

Habár az afrikai kontinensen egy bizonyos rétegnek már volt lehetősége csatlakozni a világhálózathoz az 1990-es években, a nagyütemű növekedés időben eltolódott a világ fejlettebb

régióihoz képest (ITU, 2019). Kelet-Afrika, a Föld egyik legutolsó lakott régiójaként, csupán 2009-ben csatlakozott a kontinenseket összekötő hálózathoz, a kínai Hengtong Group vállalat által épített PEACE (*Pakistan & East Africa Connecting Europe*) nevű tenger alatti száloptikai internetskábelén keresztül (Hillman, 2021, p. 18). Ekkor kezdett jelentősen növekedni az internet – és mobiltelefon használat, többek között Etiópiában és Tanzániában is (Furuholt & Sæbø, 2018).

A fejlődő országokra egyébként is jellemző korszerűtlen oktatási rendszerek és a tájékozottság hiánya megnehezítette a tanzániaiak helyzetét. Tanzániában sokáig az úgynevezett Nyilvános Internetelérési Pontok (*Public Internet Access Point*, PIAP) jelentették az egyetlen lehetőséget az online térhez való csatlakozásra, főként vidéken (Furuholt & Sæbø, 2018, p. 2). Mivel az ország lakosságának még ma is csak a harmada lakik városokban (Világbank, 2020), ezért a legtöbb tanzániai sokáig az Európában is ismert, de már idejétmúlt internetskávézókhoz hasonló létesítményekben tudott élni az internet adta lehetőségekkel. A vidéki térségben számos tényező nehezítette az információáramlást, például a nem megfelelően működő digitális infrastruktúra vagy a szakemberek hiánya (Mtega & Benard, 2013, p. 66). Ezért volt nagy jelentőségük a PIAP-oknak, ahol kényelmesen, online lehetett tanulmányi, vagy egyéb hivatalos ügyeket intézni anélkül, hogy a nem túl fejlett infrastruktúra miatt hosszú órákat kellett volna utazniuk a vidéki lakosoknak a legközelebbi nagyvárosba.

Az úgynevezett ICT4RD (ICT For Rural Development) projekt a vidéki térséget volt hivatott felzárkóztatni az információs technológiák használata terén. A 2000-es években indult kezdeményezés néhány résztvevőjével készült interjúkból kiderült, hogy a források nagyrésze a helyi kormányzati hivatalokhoz került, ahol bőséggel rendelkezésre állt minden informatikai felszerelés, az ott dolgozók pedig továbbképzésben is részesültek. Mindeközben 2011-ben még mindig súlyos gondok voltak az országban elérhető internet sebességével. Az egyik interjúban résztvevő személy úgy fogalmazott, hogy ez a projekt „a kormánytól a kormánynak készült, nem a közösségnek” (Furuholt & Sæbø, 2018, p. 8). Egy 2011-ben publikált felmérésből kiderült, hogy a nyilvános internetezők szolgáltatásait nagyrészt csak egy bizonyos demográfiai réteg, fiatalok, férfiak, illetve magasabb végzettséggel rendelkezők vették igénybe (Mtega & Benard, 2013, p. 68). Ebből arra következtethetünk, hogy a projekt során nem sikerült minél szélesebb körben elérhetővé tenni a modern információs technológiákat.

Azonban egy másik felmérésből kiderült, hogy nem csak a PIAP-ok felhasználói és üzemeltetői, hanem az állami szektorban dolgozók körében sem ismert a kiberbűnözés fogalma (Mambile & Mbogoro, 2020, p. 120). Amennyiben egy országban azok a dolgozók, akik felelősek a többi

állampolgár hivatalos ügyeiért, nincsenek tudatában annak, hogy külön jogszabályok vonatkoznak az online térre, egyértelműen veszélyt jelentenek nem csak önmagukra, hanem a közösség többi tagjára is. Fontos megjegyezni, hogy nem csak az ellenük irányuló kiberbűncselekményekkel, hanem azokkal az illegális online tevékenységekkel sincsenek tisztában, amit akár ők maguk is elkövethetnek. Ilyen bűncselekmény például személyes adatokkal való visszaélés, rágalmozás, pornográf tartalmak megosztása, jogvédett tartalmak le – és feltöltése a világhálóra, vagy akár a *cyberslacking*, vagyis a munka közbeni böngészés a weben. Ahogyan Furuholt és Sæbø írásából kiderült, a tanzániaiaknak fontos, hogy online tudják intézni hivatalos ügyeiket. Mivel sem az ügyfelek, sem az állami szférában dolgozók nem képesek felismerni a kiberbiztonsági kockázatokat, illetve nincsenek tisztában az őket illető jogokkal sem, felmerülhet a kérdés, hogy vajon érzékelhető lenne-e számukra egy harmadik fél túlzott befolyása országuk ICT szektorában. Ahogyan azt már korábban megállapítottam, az adatvédelem egy olyan terület, amelyet a potenciális digitális gyarmatosítók szívesen kihasználnak ahhoz, hogy közelebb férközzenek egy bizonyos államhoz. Tanzánia esetében az előbb felsorolt indokok miatt ez a veszély kifejezetten relevánsnak tűnik, hiszen az internetezők nagy része nem is tud az adatvédelem fontosságáról.

A tanzániai állam ezek alapján nem tartja fontosnak, hogy felhívja a figyelmet a tudatos internethasználat fontosságára az állampolgárok körében. Ezt napjainkban alátámasztja továbbá a közösségi médiára vonatkozó szabályozás, amely szintén inkább az állam érdekeit védi, a felhasználókkal szemben (Cross, 2021). Tanzániában a szomszédos államokban zajló polgárháborúk miatt mindig is elsőbbséget élvezett a békés, stabil és biztonságos rend fenntartása, még akkor is, ha ez a demokratikus fejlődést hátráltatta. Az Afrobarometer 2016 és 2018 között készített felmérése szerint a tanzániaiak 64%-a elfogadja, hogy a kormány megfigyelheti az állampolgárok közti kommunikációt, ha ezzel erőszakos eseményeket képes megakadályozni (Afrobarometer, 2016/2018). Az eredmény jól mutatja, hogy a tanzániaiak többsége számára az adatvédelem és privátszféra fontosságát felülírja a nemzetbiztonsági kockázatok elhárítása.

A GCI felmérés szerint Tanzánia rendkívül jól teljesít a nemzetközi kooperáció területén, ezáltal elkötelezettnek mutatkozik az ország kiberbiztonságának megerősítése iránt (ITU, 2021). Érdekesség, hogy amíg az ITU 2015-ös GCI beszámolójában részletesen olvashatunk a vizsgált államok eredményeiről, addig a legújabb verzióban már csak a végső pontszámok jelennek meg. Az említett korábbi verzióban a Kínával való együttműködésről nem esik szó, a 2020-as felmérésből pedig csak sejthetjük, hogy ebben a magas pontszámban éppen a

későbbiekben tárgyalt Digitális Selyemút projekt jelenik meg. Ennek ellenére az állampolgárok biztonsága a kibertérben nem garantált, legfőképpen az általános tájékoztatlanságból kifolyólag. Ugyanakkor Tanzánia már 2016-ban azon kevés afrikai országok közé tartozott, amelyeknek külön törvényeik és módszereik voltak az elektronikus bizonyítékok kezelésére (Kshetri, 2019), tehát ebből a szempontból kiemelkedő teljesítményt nyújt. Ez az ellentmondás különös helyzetet teremt Tanzániában, amiért kifejezetten érdekesnek találom Kína hatásának vizsgálatát az országban.

A Tanzániában végzett felmérésekből kiderült, hogy kiemelten fontosnak számít a vidék helyzete, ahol még mindig nagyon sokan nem kapcsolódtak a világhálózathoz. Akik pedig olyan közalkalmazotti pozícióban dolgoznak, hogy kénytelenek használni az internetet, azok sem rendelkeznek megfelelő tudással ezeknek az új technológiáknak a biztonságos alkalmazásához. Ez a kép egyértelműen ellentmond a Global Cybersecurity Index szerinti rangsorban elért kiemelkedő helyezésnek. Az ország láthatólag törekszik egy modern kiberbiztonsági szabályozás megalkotására, azonban a fejletlenebb területeken élő tanzániaiak védelméhez, az információk biztonságosok kezeléséhez és a kiberbűnözés megelőzéséhez ez még nem elegendő. Sokkal inkább azt láthatjuk, hogy a tanzániai kormány a béke és biztonság fenntartása érdekében hajlandó korlátozni az állampolgárok jogait a kibertérben, különböző megfigyelési módszerekkel, vagy bizonyos tartalmak korlátozásával (Cross, 2021). Hogy ebben a kérdésben Kínának mekkora szerepe van és mennyire egyeztethető össze a tanzániai internetmodell a kínai megfelelőjével, azt a későbbiekben részletesen vizsgálom.

3.2. Miért éppen Etiópia?

Etiópia, Tanzániához hasonlóan viszonylag későn csatlakozott a kibertérhez. Az előbbi állam kivételes helyzetben volt a többi gyarmatosított afrikai országhoz képest, hiszen már a második világháború után sikerült helyreállítania függetlenségét, rövid ideig tartó megszállás után. Kínával az 1990-es években fűzte szorosabbra viszonyát (Cabestan, 2012, p. 54), éppen az internet elterjedésének időszakában. Etiópia Kína számára egyértelműen egy kiemelt projekt, ugyanis 3,1 milliárd dollár összegben kapott kölcsönöket az ICT szektor fejlesztésére. Ezeknek a hiteleknek a nagyrészt már a Digitális Selyemút tervének bejelentése előtt kapta, a Huawei és ZTE vállalatok közreműködésével (Tugendhat & Voo, 2021, p. 18; Horne & Wong, 2014). Etiópia már 2006-ban megállapodott a ZTE-vel, amely a Huawei mellett a második legnagyobb távközlési cég Kínában, valamint napjainkban már a világ egyik legnagyobb mobiltelefongyártója. A legnagyobb etióp internet – és telefonszolgáltató, az ETC (Ethiopian Telecommunications Corporation, napjainkban: Ethio Telecom) 2006-ban kötötte első

szerződését a ZTE-vel, amelyben megállapodtak egy 1,5 milliárd dolláros kölcsönben (Gagliardone & Golooba-Mutebi, 2016, p. 14). Célja, hogy kiterjesszék Etiópia telekommunikációs hálózatát egy 2000 km hosszú kábelhálózattal, ami a 13 legnagyobb várost kötné össze. További célként szerepelt még a vidéki szolgáltatások fejlesztése, valamint egy 20 millió mobilfelhasználót is kiszolgáló hálózat létrehozása. Etiópia ICT szektorában tehát már a kezdetektől megjelent Kína és hamar kialakult az alá – fölérendeltségi viszony az államok közt. A hatalmas összegű kölcsönöknek köszönhetően az etióp állam függővé vált a szuperhatalomtól, amely nélkül valószínűleg nehezen, vagy egyáltalán nem lett volna képes kiterjeszteni internethálózatát és telekommunikációs infrastruktúráját.

3.2.1. Etiópia a kibertérben – Korlátok közé szorítva

Etiópia, Afrika egyik leggyorsabban fejlődő országa erőszakos polgárháborút élt át, ahol ma is rendkívül erős állami befolyás figyelhető meg minden területen (Gagliardone & Golooba-Mutebi, 2016, p. 1). 2019-ben csupán a teljes lakosság 25 %-a használt internetet, azonban nem szabad megfeledkeznünk arról, hogy Etiópia a földrész második legnépesebb országa. Ez azt jelenti, hogy legalább 28 millió internetfelhasználóval rendelkezik. Ebbe a számba beletartoznak az otthoni internetelérhetőséggel rendelkezők, illetve a mobilinternetet használó előfizetők is (ITU, 2019).

Tanzániával ellentétben, az etióp internetezők kiberbiztonságról való tájékozottságáról keveset tudunk. Azonban a szakirodalom jelentős része szól az állam befolyásáról és sajátos módszereiről. Az etióp állam mindig erős befolyásra törekedett a kibertérben is, tehát már a Digitális Selyemút projekt megszületése előtt elindult egy kontrollálható internetmodell bevezetése az országban (Gagliardone & Golooba-Mutebi, 2016, p. 9). Etiópiában a kommunikációt megkönnyítő technológiai fejlődés az éppen hatalmon lévő párt szemében inkább számított fenyegetésnek, mint a társadalom javát szolgáló folyamatnak (Horne & Wong, 2014). Éppen ezért az új technológiák – részben a megfelelő jogi szabályozás hiánya miatt – az állampolgárok megfigyelésének eszközévé váltak. Ez a stratégia már 2001 óta működik, egészen pontosan Meles Zenawi volt miniszterelnök hatalomra kerülése óta, aki felismerte az internet használatának fontosságát politikai stratégiájában. Ebben az időszakban Etiópiában is indult a tanzániai ICT4RD projekthez hasonlóan egy olyan kezdeményezés, amivel az ország telekommunikációs fejlődését segítették elő (Gagliardone & Golooba-Mutebi, 2016, p. 12). A Woredanet nevű projekt keretében létrehoztak egy hálózatot, amely a különböző közigazgatási területeket összeköti Addisz-Abebával, a fővárossal. A hálózatot nem a szabad információáramlás céljából építették ki. A fővárosból maga a miniszterelnök és más vezető

politikusok tartottak tréningeket, küldtek utasításokat a vidéki hivatalnokok számára. A projekt keretében kiosztott plazmatévéket oktatási célokra is használták vidéki iskolákban. Ezzel biztosította az etióp kormány, hogy csak olyan információk jussanak el a fővárostól távoleső régiókba, amik az ő érdeküket szolgálják. Ez a modell rendkívül hasonló a kínai modellhez, hiszen Etiópiában is igyekeznek kiszorítani a kormány nézeteivel ellentétes véleményeket. Mindezek alapján kijelenthetjük, hogy az etióp államtól már a 2000-es évek elején sem állt távol egy korlátok közé szorított internet gondolata, ehhez pedig külső segítséget is igénybe vett. A megfigyelésre alkalmas infrastruktúra természetesen külföldi partnerektől érkezett, kínai és európai vállalatoktól egyaránt (Horne & Wong, 2014).

Meles Zenawi úgy fogalmazott, hogy „felismerték, míg az ICT luxusnak számít a gazdagok körében, számukra – a szegény országok számára – ez egy létfontosságú és alapvetően szükséges eszköz a szegénység elleni harcban” (Gagliardone & Golooba-Mutebi, 2016, p. 5). Úgy tűnik, Etiópia időben felismerte az internet, valamint a kibertér jelentőségét, azonban képtelenek voltak az ebből eredő problémák megfelelő kezelésére. 2011-ben készült el a National Information Security Policy, amelyben már ismert problémaként szerepelt a szakemberek és a megfelelő technológiai tudás hiánya (Eboibi, 2020, p. 11). A következő évben létrehozták az ETHIO-CERT-et, a kiberbiztonsági vészhelyzeteket elhárító csapatot, amely egy fontos lépésnek bizonyult volna a megfelelő kiberstratégia kialakításában. Mindezek ellenére Etiópiában még mindig nincsenek külön kiberbűnözéssel foglalkozó alakulatai a rendfenntartó egységeknek, nincs különálló bíróság, ahol ezekkel az ügyekkel foglalkoznának. Ahogyan a legtöbb fejlődő, afrikai országban, még mindig konvencionális bűnüldözési módszereket használnak (Eboibi, 2020, p. 10), holott ez a kibertérben ritkán vezet eredményre. Ezen túl az etióp állami intézmények 87,4%-ának nincsen jogi szabályozása kibertámadások megelőzésére (Adene, 2020). Ez a jelenség egyértelműen tükröződik Etiópia GCI szerinti alacsony pontszámában. Az ITU felmérésében Etiópia kooperációs képességei a nullával egyenlők, tehát éles ellentétben áll Tanzánia képességeivel. Az ország a felmérés korábban ismertetett öt szempontja közül a jogi szabályozásban teljesít legjobban, azonban ahogyan láthattuk, ez még közel sem elegendő egy hatékony kiberbiztonsági stratégia kialakításához vagy a kiberbűnözés megfelelő kezeléséhez.

3.3. Összefoglalás - Nehézségek a digitális fejlődésben

Összességében elmondhatjuk, hogy Tanzániához hasonlóan Etiópiában is növekszik az internetfelhasználók száma, azonban nem találnak megoldást a folyamattal járó problémák orvoslására. Tanzániában a kiberbiztonság fogalma sokak számára teljesen ismeretlen, ezáltal képtelen felkészülni az online tér veszélyeire. Az előbbieket alapján úgy tűnik, mindkét ország vezetői igyekeznek a saját javukra fordítani az ICT szektor fejlődéséből adódó előnyöket. Tanzániában a kormányzati hivatalok kapták a megfelelő felszerelést és oktatást, Etiópiában pedig a kormány igyekszik szűk kontroll alatt tartani az információáramlást, ezzel saját érdekeit szolgálva. Etiópiáról továbbá azt is elmondhatjuk, hogy már 2015 előtt is igyekeztek törvényeket hozni és intézményeket felállítani a kiberbiztonság területén, azonban hiányzik a politikai akarat, hogy azok hatékonyan tudjanak működni. Kína tehát a Digitális Selyemút projekttel ezeket az államokat célozta meg, még több lehetőséget adva ezzel az ICT szektor fejlődésére. Mindkét ország már korábban is kapcsolatban állt Kínával, vagy olyan kínai cégekkel mint a Huawei, vagy a ZTE. A két ország a GCI szerint különböző képességekkel rendelkezik, Tanzánia fejlettebbnek bizonyul a kiberbiztonság terén, azonban a gyakorlatban mégsem látunk nagy különbséget.

A továbbiakban azt vizsgálom, hogy ezekben az instabil rendszerű, nem elég fejlett kiberkultúrával rendelkező államokban milyen hatása volt Kínának, illetve mi történt a szuperhatalom nagyszabású projektjének kezdete óta. Továbbá felteszem azt a kérdést is, hogy vajon a Digitális Selyemút tervének végrehajtása nem hivatalos módon már jóval korábban elkezdődött-e, mint a bejelentés dátuma.

4. KÍNA HATÁSA A KELET-AFRIKAI ORSZÁGOK KIBERBIZTONSÁGÁRA

4.1. Mit tudunk a Digitális Selyemút tervről?

A Digitális Selyemút, mint napjaink egyik legfontosabb kínai külpolitikai kezdeményezése hivatalosan 2015-ben vette kezdetét (Tugendhat & Voo, 2021, p. 5), a Belt and Road Initiative (BRI) program keretében. Hszi Csin-ping elnök 2013-as bejelentése óta azonban nagyrészt homály fedi a projekt részleteit. A kínai elnök kommunikációjából világos, hogy céljuk egy új, modern Selyemút kiépítése, olyan infrastruktúra létrehozása, földön és vízen egyaránt, amely képes összekötni Kínát Európa és Ázsia többi részének legfontosabb országaival, valamint az afrikai kontinenssel is (Shen, 2018, p. 2683). Az első BRI fórumot Pekingben tartották meg 2017-ben, ahol az ENSZ, a Világbank és a Nemzetközi Valutalap legfőbb vezetői is részt vettek. Kína ilyen módon történő terjeszkedése veszélyeztetheti a jelenlegi világrendet, legfőképpen az Egyesült Államok hegemoniáját, ezért jelentős figyelem irányult a BRI-re. Dolgozatomban a program Digitális Selyemút néven elhíresült elemére koncentrálok, amely keretében Kína segítséget nyújt Afrika számára, a kontinens digitális infrastruktúrájának fejlesztése érdekében.

Mivel nincsen egyértelmű, nyilvánosan elérhető dokumentum arról, hogy pontosan mi része a kínai projektnek, ezért csak nagyvonalakban tudhatjuk, mi Kína végső célja és azt milyen eszközökkel óhajtja elérni. Cheney (2019, pp. 4, 9) kutatása szerint a projekt legfontosabb komponensei közt szerepel a digitális infrastruktúrafejlesztésbe való befektetés, ezen belül a telefonhálózatok, optikai kábelek és adatközpontok építése és létrehozása, valamint a digitális diplomácia és kormányzás kínai hatáskör alá vonása. Az afrikai kontinensen ez a két elem jelenik meg legeggyértelműbben, még akkor is, ha hivatalosan nem lehetünk abban biztosak, hogy a Digitális Selyemút programhoz tartoznak az ezeken a területeken történt fejlesztések, befektetések vagy segélynyújtások. Továbbá, a feltételek megteremtése után Kína az olyan modern technológiákat kívánja a projektben résztvevő országok körében meghonosítani, mint például az 5G mobilhálózat, mesterséges intelligencia, valamint a felhő alapú számítástechnika (Triolo et al., 2020, pp. 4-5). Arról sem állnak rendelkezésre hivatalos, kínai forrásból származó információk, hogy egészen pontosan mely országok vesznek részt a programban, azonban ez az óriási kínai befektetésekből és a bárki számára elérhető kínai hitelekéről szóló adatbázisból egyértelművé válhat. Ami azonban még mindig nem egyértelmű, sem a résztvevő országok, sem a világ többi része számára, hogy a Kínától kapott segítség milyen kötelezettségekkel jár. Ez a hiányosság járhat a legsúlyosabb következményekkel, ugyanis, ahogyan azt a későbbiekben is látni fogjuk, például Etiópia esetében valós esélye van annak, hogy nem lesz

képes visszafizetni a kínai kölcsönöket, tehát valamilyen más módon kell kompenzálnia a szuperhatalom számára (Kinyondo, 2019).

4.2. Technológiai fejlődés Kína segítségével

Kína az egész világon rendelkezik befektetésekkel (Cheney, 2019, pp. 4-5). Állami tulajdonú és privát cégek egyaránt adnak kölcsönöket, többek közt afrikai országok számára. Az Egyesült Államok szerint ezek a befektetések súlyos nemzetbiztonsági kockázatot jelentenek, ezért megtiltotta, hogy az amerikai telekommunikációs cégek külföldi felszerelést használjanak, például az 5G hálózat kiépítése során. Afrikában ez a módszer nem vetett fel biztonságpolitikai kérdéseket, Kína ezért képes óriási befolyással lenni a kontinensre (Triolo et al., 2020, p. 7). Az ázsiai ország az Egyesült Államok vezető szerepét veszélyezteti a kulcsfontosságú tenger alatti kábelek építésében és birtoklásában (Hillam, 2021, p. 2). Becslések szerint 2012 és 2015 között a kábelépítési munkálatok 6%-ában, 2016 és 2019 között pedig már azok 20%-ában vettek részt kínai cégek (Cheney, 2019, pp. 4-5). Ezzel felügyelete alá kerül a kibertér fizikai valója, vagyis az a fizikai infrastruktúra, amely lehetővé teszi az adatforgalmat, ilyenek például a tenger alatti száloptikai kábelek, valamint az adatközpontok. Afrika tökéletes célpont, ugyanis népessége a Föld összlakosságának 17%-át teszi ki, az adatközpontjai azonban csak a világon megtalálhatók 1%-át (Hillman, 2021, p. 17). Ez azt jelenti, hogy a kontinens hatalmas növekedési potenciállal rendelkezik, vagyis Kína még számos digitálisan fejletlen térségben tud megjeleni termékeivel. Ez tehát a Digitális Selyemút projekt egyik fő összetevője, amely Kína hatalmát jelentősen megnöveli a kibertérben, hiszen az ő felügyelete alatt épül ki Afrika egyes részeinek digitális infrastruktúrája.

Ahogy már korábban láttuk, Etiópia és Tanzánia a közé a 15 ország közé tartoznak, akik a legmagasabb összegű kínai hitelt kapták az ICT szektor fejlesztésére a XXI. században. Érdekesség, hogy a hitelek mértéke jelentősen csökkent 2015 óta. Ha a Digitális Selyemút tervet úgy vizsgálánk, mint egy szigorúan csak kölcsönökre épülő külpolitikai kezdeményezést, akkor azt állapíthatnánk meg, hogy mire a projektet bejelentették, az már véget is ért (Tugendhat & Voo, 2021, p. 18). Sokkal valószínűbb azonban, hogy Kína már jóval korábban kitűzte céljául befolyásának növelését a fejlődő országok körében, napjainkban pedig nevet adtak ennek a már eddig is látványos eredményeket elért tervnek, hogy így tálalják azt a globális közösség számára. Az alábbi fejezetben bemutatom, hogy Kína a projekt e komponense, vagyis a digitális infrastruktúraépítés keretében hogyan hatott Tanzániára és Etiópiára.

A Pew Global Attitudes 2015-ös felmérésében különböző afrikai országok lakosságának Kínáról alkotott véleményére voltak kíváncsiak (Li, 2016, p. 185). Kiderült, hogy ekkor Etiópiában 75%, Tanzániában pedig 74% szimpatizált a szuperhatalommal. Ezt a pozitív véleményt nagyban befolyásolhatta az az elképesztő mértékű technológiai fejlődés, amely különböző kínai cégek segítségével valósulhatott meg. Etiópia 3,1 milliárd dollárnyi kölcsönöket kapott Kínából, nagyrészt a Huawei és ZTE vállalatok jóvoltából (Tugendhat & Voo, 2021, p. 17). A Huawei, mint vezető vállalat az afrikai ICT szektorban korábban az ebola járvány idején nyújtott segítséget a kontinensen, jó minőségű és megfizethető mobilokkal és internetszolgáltatással (Alkhawajah, 2019, p. 4). Többek között ezzel a lépéssel sikerült elnyerniük az afrikai felhasználók bizalmát. Etiópiában a Huawei az oktatásban is óriási sikereket ért el, a 2015-ben induló Addis-Ababa School Net Project keretében (Li, 2016, p. 190). A kezdeményezés 65 oktatási intézménynek nyújtott segítséget a megfelelő ICT infrastruktúra kiépítésével. Ezzel Kína vélhetőleg lehetőséget teremtett arra is, hogy a jövőben tudatosabb felhasználókat és szakembereket képezhessenek Etiópiában, hiszen egyre több etióp diák tud megismerkedni olyan modern vívmányokkal, mint a személyi számítógép és az internet. Tanzániában szintén nagy népszerűségnek örvend a Kínától kapott technológia. 2008-ban még a tanzániai felhasználók kevesebb, mint 1%-a intézte mobiltelefonján pénzügyeit, 2013-ra pedig ez az arány már 90%-ra nőtt (Li, 2016, p. 189). Ha azonban arra gondolunk, hogy Tanzania és Etiópia milyen szinten áll a kiberbűnözés üldözése és a tudatos internethasználat terén, felmerülhet a kérdés, hogy vajon nem jelent-e kiberbiztonsági kockázatot ez a hirtelen növekedés?

4.2.1. Kockázatok

Afrika összességében egy rendkívül biztonságos helynek bizonyul a kiberbűnözők számára (Eboibi, 2020, p. 31). Hiába vannak érvényben kiberbiztonságra vonatkozó törvények, az implementáció során súlyos problémák lépnek fel. Ahogyan arról korábban is szó esett, nincsenek megfelelő bűnüldözési szervek, hiányoznak a képzett szakemberek és a felhasználók sincsenek tisztában a világháló veszélyeivel. Mindezt alátámasztja, hogy az Africa Cybersecurity Report szerint 2017-ben 3,5 milliárd dollárnyi kárt okozott a kiberbűnözés a kontinensen (Eboibi, 2020, p. 1). Nagy a valószínűsége, hogy a hatalmas digitális növekedés és a fejlődő országok felkészületlenségének találkozása okozta ez a jelenséget. A Symantec (a Norton nevű vírusirtót gyártó vállalat) szerint 2013-ban az egész világon Afrikában nőtt legnagyobb ütemben a kiberbűnözés (Kshetri, 2019).

Egy másik olvasat szerint azonban Kína a digitális fejlődés elősegítésével megalapozza, hogy a jövőben képzett kiberbiztonsági szakemberek javíthassanak országuk helyzetén. A gyakorlat ellenben nem azt mutatja, hogy Kína tevékenysége a megfelelő technológiai tudás átadását segítené elő. Egy Tanzániában végzett felméréséből kiderült, hogy a tanzániaiak nem voltak elégedett a kínaiakkal végzett közös munkával (Kinyondo, 2019, p. 14). Az együttműködésből sokszor kizárták a helyi munkaerőt és inkább a kínai forrásokra támaszkodtak, a munkakörülmények pedig nem voltak kielégítők biztonsági és egészségügyi szempontokból. Ezt alátámasztja egy másik kutatás is, amelyből kiderült, hogy a Huawei Tanzániában nagyrészt valóban helyi dolgozókat alkalmazott (Makundi et al., 2016, p. 137), azonban a nem megfelelő munkakörülmények semmiképpen sem segítették elő a megfelelő szakmai tudás átadását (Nantulya, 2021).

A nyelvi akadályokon túl munkamorálban és módszerekben is különbséget véltek felfedezni a kínaiak és a tanzániaiak közt. Továbbá problémát jelentett, hogy a helyieket nem szívesen alkalmazták magasabb, menedzseri vagy vezetői pozícióban, hiába vettek részt tréningeken (Makundi et al., 2016, p. 139). Ez a diszkrimináció is egy alá-fölé rendeltségi viszonyra enged következtetni, amely a Digitális Selyemút projekt megvalósulása során létrejön Kína és a támogatott afrikai államok között. Ezt az alárendelt szerepet tovább erősíti az a tendencia, hogy az afrikai elit, kihasználva Kína „bőkezűségét”, saját gazdagodására és befolyása növelésére fordítja a kapott forrásokat (Nakulya, 2021). Ez a jelenség mutatkozik meg például a tanzániai kormányzati hivatalok esetében, ahol az informatikai eszközöket megtartották és saját javukra fordították az ICT4RD projekt keretében szerzett támogatásokat (Furuholt & Sæbø, 2018, p. 8).

Összegezve tehát elmondhatjuk, hogy Etiópia és Tanzánia és jelentős fejlődésen ment keresztül az ICT szektorban Kína támogatásával. A Huawei telefonok és az elérhető internetszolgáltatás lehetővé tette sokak számára, hogy kapcsolódjanak a világhálózathoz és élvezhessék a modern vívmányok nyújtotta előnyöket. Ezzel szemben azonban a kínai vállalatok nem fordítottak elég figyelmet az afrikai szakemberek képzésére. A megfelelő tudás hiányában Etiópiának és Tanzániának súlyos kiberbiztonsági következményekkel kell szembenéznük, a kiberbűnözés gyors növekedése miatt. Kína a kialakult helyzetből azonban jelentős előnyt képes kovácsolni, ugyanis a megfelelő tudás hiányában a támogatott afrikai országok továbbá is függenek a kínai szakemberektől és vállalatoktól. A szuperhatalom, mint digitális gyarmatosító számára egyáltalán nem lenne előnyös, ha minden tudást és technológiát átadva a fejlődő országok számára azok az önálló fejlődés útjára léphetnének, hiszen már nem lenne szükségük a támogatásra. Ezzel a módszerrel azonban biztosítják, hogy az olyan országok, mint Tanzánia

és Etiópia a jövőben is Kínához forduljanak segítségért, akár a kiberbűnözés elleni küzdelem során, vagy egyéb kiberbiztonsági kérdés megoldásában.

4.3. Digitális diplomácia – Az internetszuverenitás modellje

A Digitális Selyemút program másik, kutatásom szempontjából kiemelkedően fontos komponense a digitális diplomácia és kormányzás, Kína vezetésével (Cheney, 2019). A kibertér egy olyan határok nélküli terület, amelynek egésze nem áll semelyik állam közvetlen felügyelete alatt, ezáltal nincsenek köbe vésett, általánosan elfogadott normák. Kína ezt a tulajdonságot használja ki saját hatalmának kiterjesztésére, a saját modelljének népszerűsítésével. A korábban már tárgyalt internetszuverenitás modell a fejlődő országok, így Tanzánia és Etiópia számára is vonzó lehet. A harmadik világban, a volt gyarmatok számára a szuverenitás sokáig egy elérhetetlen álom maradt, amely a XXI. században a demokráciaexport, a nyugati normák terjedése, a nemzetközi szervezetek elvárásai okán elveszni látszik. Talán éppen ez Kína sikerének kulcsa az afrikai kontinensen. Ahogyan a hitelek esetében is láthattuk, a keleti kölcsönök jóval kedvezőbben a fejlődő országok számára. Első és legfontosabb tulajdonságuk az olyan nagyhatalmaknak, mint Kína, hogy nem volt gyarmattartók. A második, hogy a Nyugattal szemben a „kemény”, vagyis hagyományos infrastruktúrát részesítik előnyben, ehhez tartozik az internethálózat vagy úthálózatok, vasútvonalak fejlesztése (Kinyondo, 2019, p. 29). A Nyugat azonban a „puha” infrastruktúra fejlesztésére koncentrál, a demokrácia és az emberi jogok helyzetére. Ezeket az ideológiai különbségeket jelképező szakadékokat képes áthidalni Kína, anélkül, hogy feltételeket szabna a segélynyújtáshoz.

A kínai internetmodell, vagyis az internetszuverenitás modellje éppen ezért rendkívül közel áll az olyan országok nézeteihez, mint Tanzánia vagy Etiópia. Ennek a modellnek az átadása alapozza meg minden további együttműködés sikerességét, ugyanis Kína számára közvetett módon megteremti az információáramlás korlátozásának lehetőségét. A továbbiakban bemutatom, hogyan képes erre Kína és milyen módon képes kedvére alakítani a támogatott afrikai országok internethez való viszonyát a kibertéren keresztül.

Ahogyan azt már korábban is láthattuk, az internetszuverenitás egy vitatott fogalom. A kínai elnök szerint azonban a kibertér szuverenitása sérthetetlen, amely azt jelenti, hogy minden országnak joga van korlátozni, hogy a területén élők milyen tartalmakhoz férhetnek hozzá a világhálón keresztül. Kína álláspontja továbbá a 2015-ös International Strategy of Cooperation on Cyberspace szerint, hogy „egy állam sem törhet hegemoniára a kibertérben és nem támogathat olyan tevékenységeket, amelyek már országok kiberbiztonságát aláássák” (Cheney,

2019, p. 10). Kína talán éppen ebből a megfontolásból igyekszik átformálni a jelenlegi nemzetközi rendet a kibertérben, akár egy kiberháborút is megkockáztatva (Arsène, 2016) az Egyesült Államok hegemoniájának megtörése érdekében. Cheney (2019, p. 9) úgy fogalmaz, hogy Kína digitális diplomácián keresztül óhajtja saját nézeteit más térségekben is az általánosan elfogadott normává tenni. Ahhoz, hogy egy új rendszer alakulhasson ki globális szinten az internet szabályozását illetően, Kínának a lehető legtöbb térségben kell elfogadtatnia saját modelljét, hogy erős nemzetközi támogatottságot szerezzen. A digitális neokolonizáció egy hatékony módszernek bizonyul e hosszú távú cél elérésének érdekében.

Ez a folyamat zajlik jelenleg az afrikai kontinensen, ahol azonban az internetszuverenitás modelljével együtt jár az autoriter megfigyelési technológiák, valamint a mesterséges intelligencia és egyéb adathalász technikák exportja (Gravett, 2020, pp. 127-128). Mint tudjuk, a kibertérben zajló megfigyelés és adatgyűjtés rendkívül fontos egy digitális gyarmatosító országnak, ugyanis ezáltal értékes információkhoz jut az adott ország társadalmáról, ráadásul folyamatosan ellenőrizni képes saját befolyását és ez alapján változtathat stratégiáján a siker érdekében. Kína kommunikációja valóban ellentmondásos. A propaganda szerint a szuperhatalom megadja a fejlődő országok számára a rég áhított szuverenitást, azonban ahhoz, hogy ezt valóban megkapják, előtte beleavatkozik a szuverenitásukba azzal, hogy a saját módszerét igyekszik meghonosítani. Mint azt korábban láttuk, Tanzániában és Etiópiában magas a Kína-pártiak aránya, tehát Kína sikeresen elhiteti ezekkel az országokkal, hogy nem avatkozik bele belső ügyeikbe, tiszteletben tartja kultúrájukat és sajátos vonásaikat (Kinyondo, 2019, p. 14). Mindeközben mégis a saját képére formálja a kibertérhez való viszonyukat. Tényleg ez lenne az afrikaiak akarata?

A ZTE, a Huawei után a legbefolyásosabb telekommunikációs vállalat Afrikában az etióp kormány számára biztosította azt a digitális infrastruktúrát és eszközöket, amelyekkel képesek akár az ellenzéket megfigyelni (Gravett, 2020, p. 137). Etiópiában tehát nem érezhetik magukat biztonságban az ellenzéki aktivisták, vagy újságírók, hiszen a Kínától kapott eszközök segítségével a köztük zajló kommunikációt valamilyen módon ellenőrzi a kormány (Horne & Wong, 2014). Etiópia kiemelten fontos Kína számára, hiszen itt épült fel – szintén kínai támogatással – az Afrikai Unió központja. Az itt felépített, megfigyelésre, lehallgatásra alkalmas technológia óriási biztonsági kockázatot jelent, akár az egész Afrikai Unió számára. Az etióp kormány valóban képes arra, hogy a központban elhangzottakat, a tagállamokra tartozó bizalmas információkat valamilyen módon rögzítse és akár továbbítsa Kína számára. 2018 januárjában az Afrikai Unió tisztviselői megvádolták a szuperhatalmat a központ elleni

hackertámadásokkal (Woodhams, 2019). Két évvel később újra felmerült a gyanú, hogy kínai hackercsoportok ismét „bejutottak” az Afrikai Unió központjának épületébe, ezúttal azonban a biztonsági kamerák felvételeihez fértek hozzá (Satter, 2020). Kína ezeket a vádakát egyértelműen tagadja, az Afrikai Unió pedig a történetek ellenére folytatni kívánja az együttműködést a Huawei-el (Triolo et al., 2020, p. 7). Azonban a bizalmas adatok, amik az afrikaiak tudta nélkül egy idegen hatalom kezébe kerültek súlyos nemzetbiztonsági kockázatot jelentenek. Mindezt a Kína által épített etiópiai digitális infrastruktúra teszi lehetővé.

A magas állami intervenció szintje Etiópiában és a kínai modell átvétele további aggodalomra adhat okot. Etiópia 2016 és 2018 között számos alkalommal korlátozta az internethozzáférést az országban, különböző állami érdekek miatt, nemzetbiztonsági okokra hivatkozva (Ayalew, 2019, p. 209). Ezzel az internet leállással szándékoztak megakadályozni a civil felkeléseket, tüntetéseket. Az internet leállás definíciója egyes szerzők szerint az internetes kommunikáció szándékos akadályozása, amikor teljesen elérhetetlenné, vagy használhatatlanul lassúvá teszik az internetkapcsolatot egy bizonyos térségben, ezzel kontrollálva az információáramlást (Ayalew, 2019, p. 210). Ezt természetesen csak azok tehetik meg, akiknek hatalmuk van az internetszolgáltatók és a digitális infrastruktúra működése felett. Etiópia tehát erősen autoriter módszerekhez folyamodik, amikor az aktuális kormány hatalmának megóvása a tét, mindezt pedig a Kínától kapott technológia és eltanult módszerek segítségével teszi.

Az internetes kommunikáció szándékos akadályozása tehát sérti a szólásszabadsághoz való jogot és akadályozza a szabad információáramlást, azonban az erős állami beavatkozás egy sokszor figyelmen kívül hagyott pozitív következménnyel is járhat. A kínai modell nem csak arra alkalmas, hogy izolációban tartsa az állampolgárokat, hanem arra is, hogy fellépjen a valóban káros és illegális tartalmak ellen (Arsène, 2012, p. 13). Ahogyan korábban láttuk, Tanzániában sokan nincsenek tisztában a kiberbűnözés, kiberbűncselekmény fogalmával (Furuholt & Sæbø, 2018; Mambile & Mbogoro, 2020, p. 120). Az egész kontinenst érintő problémák, mint például a kiberbűnözők által okozott hatalmas anyagi károk (Eboibi, 2020, p. 1) orvosolhatóvá válhatnak egy zártabb és kontrollálhatóbb internetmodell alkalmazásával, ugyanis a megfigyelési és adatgyűjtési módszereknek köszönhetően könnyebben felderíthetővé válnak a kibertérben elkövetett bűncselekmények. Éppen ezért a modell átvétele Tanzániában és Etiópiában a kiberbiztonsági fejlődést elősegítő tényezővé is válhat, attól függően, hogy az illetékes szervek hogyan alkalmazzák azt.

Az internetszuverenitás modellje Tanzániában is egyértelműen megjelenik, ahol viszonylag nyíltan elismerik, hogy a kínai modellt követik a kibertérben. A tanzániai kommunikációért

felelős miniszter helyettese elismerően nyilatkozott „kínai barátaikról”, akik „biztonságos” tartalmakat jelenítenek meg az interneten és sikeresen kizárták a nem helyénvalókat (Gravett, 2020, p. 139). Szerinte a kormányoknak biztosítaniuk kell a szólásszabadságot, azonban bárki felelősségre vonható az általa mondottakért. E szerint a kitekért logika szerint a szólásszabadság Tanzániában is megvalósul, ezzel megfelelnek az ENSZ értékeinek. Azonban ha olyan kijelentést tesz egy tanzániai, amely nem megfelelő a vezetőségnek, akkor felelősségre vonják, épp úgy, mint Kínában. A tanzániai kiberbiztonsági oktatás ahelyett, hogy a tudatos és biztonságos internethasználatot helyezné előtérbe, inkább arra fókuszál, hogy a felhasználók hogyan ne kövessenek el bűncselekményeket az online térben (Cross, 2021). Ahogyan azt Gravett (2020) is kiemeli, Tanzánia Etiópiához hasonlóan szigorú kontroll alá vonja a kormány kritikussait. Számos kampány indult annak érdekében, hogy a tanzániai internetfelhasználók gondolják át, milyen tartalmakat osztanak meg a világhálón, nehogy a közösség számára káros információk terjedjenek (Cross, 2021). Ebben a gyakorlatban szintén a kínai modell köszön vissza. A 2015-ben elfogadott Cybercrimes Act-et rengeteg kritika érte, hiszen kísértetiesen hasonlít a kínai szabályozáshoz. A tanzániai törvény tiltja a „valótlan tartalom” megosztását, ez a kínai terminológusban „valótlanosságok állítását” jelenti. Hivatalosan mindkét országban a „dekadens” tartalmak visszaszorításán fáradoznak (Gravett, 2020, p. 139). 2018 áprilisában Tanzánia is nyíltan korlátozta a szabad információáramlást, az úgynevezett blogger-adó bevezetésével, ami egy aránytalanul nagy anyagi terhet rótt a tanzániai bloggerekre és online tartalomgyártókra (Giles, 2018). Ez a nyugati világban teljesen elképzelhetetlen és elfogadhatatlan lépés tökéletesen beleillik az internetszuverenitás modelljébe. Ezzel szemben nem feledkezhetünk meg a zárt modell adta előnyökről sem, ami az alkalmazás módjától és a politikai akarattól függően akár a kiberbűnözéssel szembeni fellépés egyik eszközévé is válhat.

4.3.1. Kockázatok

Az ENSZ szerint a szólásszabadság a demokrácia egyik alapköve, a világháló pedig egy új tér, ahol ezzel a joggal élni lehet (Ayalew, 2019, p. 1). A szabad információáramlás elengedhetetlen egy fejlődő társadalom számára. Tanzánia és Etiópia mindketten tagjai az ENSZ-nek, tehát amennyiben a kínai internetmodellt szándékoznak követni, szembe mennek ezekkel az értékekkel. A szólásszabadság súlyos megsértésén túl további kockázatokat jelent a kibertér sajátos módon való értelmezése. Külső és belső veszélyek egyaránt fenyegetik ezeket az afrikai államokat. Amennyiben egy ország területén az interneten keringő információkat az állam kontroll alatt tartja, képesek lehetnek a felhasználók világképét és véleményét saját akaratuk szerint formálni. Ha a felhasználók nem gyűjthetnek szabadon információt és a kínai modellt

követve bizonyos tartalmak letiltásra kerülnek, amelyek az aktuális kormány érdekeivel ellentétesek, akkor könnyen manipulálhatóvá válhatnak. Mivel az internet fizikai valója, a hálózatot létrehozó infrastruktúra kínai vállalatoknak köszönhetően jött létre, ezért a rajta keresztülmenő adatforgalmat nem csak a tanzániai vagy etióp kormány, hanem maga Kína is felügyelheti. Ez azért jelent jelentős kockázatot, mivel nem egyértelmű, hogy a kínai vállalatok miként dolgozzák fel a begyűjtött adatokat és mire használják azokat a későbbiekben (Triolo et al., 2020, p. 9).

Ezzel nem csak kínai propagandát juttathatnak el Afrikába, tovább növelve az irántuk érzett szimpátiát, hanem könnyedén beleavatkozhatnak a megfigyelt országok belügyeibe. Kína tehát ennek a modellnek az átadásával valójában egy hamis szuverenitásérzetet keltett az olyan országokban, mint Tanzánia vagy Etiópia. Mindez súlyos nemzetbiztonsági kockázatokkal járhat. Nincs rá garancia, hogy miután a támogató ország végez az internethálózat kiépítésével és modern eszközökhöz juttatja az afrikaiakat, végleg távozik, teljes önállóságot engedélyezve számukra a jövőben. Tanzánia és Etiópia könnyedén adósságcsapdába keveredhetnek és amennyiben képtelenek lesznek visszafizetni a kölcsönöket, Kína bármikor ráteheti a kezét mindkét állam digitális infrastruktúrájára. Ez az esemény más régiókban már megtörtént, például Sri Lankán, ahol a kínai hitelekkel épült kikötőben jelent meg saját tengeralattjáróival a szuperhatalom (Kinyondo, 2019, pp. 25-26). Ebből a lépésből arra következtethetünk, hogy Kína bármikor készen áll teljes ellenőrzése alá vonni az afrikai országok „szuverén kiberterét”, kontrollálva ezzel a mobiltelefonokon átmenő adatforgalmat, az interneten megjelenő tartalmakat és bizalmas információkhoz juthat az állami szféra rendszerein keresztül. Amennyiben ez bekövetkezik, Kína teljesíti a digitális gyarmatosítás egyik alapvető feltételét, vagyis képes lesz tömeges adatgyűjtésre az afrikai országokban.

Kína tehát egy olyan modellt honosított meg Tanzániában és Etiópiában, amely az aktuális kormányok számára rendkívül vonzó, hiszen kontrollálhatják a gyors információáramlást és saját érdekeik szerint képesek manipulálni az internethasználókat. Azonban annak érdekében, hogy ezt a hatalmat gyakorolhassák a lakosság felett, saját szuverenitásuk egy részét áldozták fel Kínával szemben. Nehéz megállapítani, hogy ez a folyamat vajon tudatos döntés eredménye, vagy egyszerűen Kína kommunikációja félrevezette ezeket az államokat. Annyit azonban biztosan kijelenthetünk, hogy az internetszuverenitás modelljének átvétele hosszú távon nem Afrika számára lesz az előnyösebb.

4.4. Összefoglalás - A Digitális Selyemút projekt és a digitális gyarmatosítás

Az egyértelmű és nyilvános információk hiánya miatt rendkívül nehéz behatárolni, pontosan mi képezi a Digitális Selyemút projekt részét és mely országok vesznek részt ebben a programban (Cheney, 2019; Tugendhat & Voo, 2021). Valószínű, hogy Kína csupán nevet adott a már évek óta zajló folyamatnak, amelyet digitális gyarmatosításnak is nevezhetünk (Tugendhat & Voo, 2021). A szuperhatalom a XXI. században elképesztően magas összegekkel támogatta az afrikai kontinens ICT szektorát, ezzel hozzásegítve a világ legszegényebb régióját, köztük Tanzániát és Etiópiát is a digitális térhez való csatlakozáshoz. Ezáltal a földrészen jelentősen nőtt az internethasználók száma és Kína új lehetőségeket teremtett saját befolyásának növelésére a kibertéren keresztül.

A digitális neokolonizáció számos állomását láthattuk megjelenni a Digitális Selyemút terv elemzése során. Ahogyan már dolgozatom elején megállapítottam, ahhoz, hogy a digitális gyarmatosító hatalom modern eszközök segítségével növelhesse befolyását egy térségben, ahhoz elsősorban minél szélesebb körű internethozzáférést kell biztosítania. Kína a technológia átadásával, tenger alatti kábelek építésével ezt a feltételt teljesítette, Tanzániában és Etiópiában is jelentősen nőtt az internethasználók száma, a Huawei pedig megfizethető és jó minőségű mobiltelefonokat hozott el az afrikai piacra (Alkhawajah, 2019). Kína a kölcsönökkel kétféleképpen is magához láncolta az olyan országokat, mint Tanzánia és Etiópia. Egyrészt a magas összegű hitelekkel, amelyek visszafizetése nehéz feladatnak bizonyul a két fejlődő ország számára (Kinyondo, 2019, p. 25). Másrészt, mivel ezek az államok még nincsenek felkészülve a kibertér kihívásaira, ezért a jövőben is Kínára fognak támaszkodni a magas szaktudást igénylő ICT szektorhoz kapcsolódó kérdésekben. Kína ezekkel a lépésekkel hű szövetségeseire – vagy gyarmatokra – tett szert. Ezt az állítást bizonyítja az a jelenség, hogy egyértelmű korreláció van a kölcsönök és az ENSZ-béli támogatottság között (Kinyondo, 2019, p. 26). Kína minél nagyobb összegekkel támogatja az afrikai országokat, annál jobban motiválja azokat arra, hogy mellette szavazzanak az ENSZ-ben. Úgy tűnik, Kína sikeresen tudja befolyásolni az általa támogatott államokat, a modern technológiák átadásával, az interneten zajló információáramlás korlátozásával és esetleges megfigyelésével. Példát mutatott Tanzániának és Etiópiának is arra, hogy gyűjthetnek adatokat a felhasználóktól, hogyan figyelhetik meg a kibertéren keresztül a rendszer ellenzőit (Gravett, 2020).

A Nemzetközi Távközlési Unió kutatására reflektálva elmondhatjuk, hogy a Global Cybersecurity Index szerinti várakozásainkkal éppen ellentétes eredményre jutottunk. A rangsor alapján arra számíthattunk, hogy Tanzánia önállóan és hatékonyabban képes kezelni

ezeket a kockázatokat, míg Etiópia nagyobb problémákkal néz majd szembe a kiberbiztonság alacsony fejlettségi szintje miatt. Ennek ellenére kutatásom során nem találtam jelentős különbségeket a Digitális Selyemút projekt hatásának szempontjából a két ország helyzete között. Ebből két lehetséges következtetést vonhatunk le. Egyrészt, egy olyan szuperhatalommal szemben, mint Kína a fejlődő országok védtelenek maradnak a kibertérben. Másrészt elképzelhető, hogy az együttműködés még annyira korai szakaszban van, hogy majd csak évekkel, vagy évtizedekkel később válnak egyértelművé a következmények.

A neokolonizációról szóló szakirodalom egyértelműen negatív jelenséggként mutatja be a múltbéli gyarmatosítást, ugyanis az alá-főlé rendeltségi viszony súlyos egyenlőtlenséget eredményez. A gyarmatok társadalmát kizsákmányolták, hátráltatták, vagy teljesen ellehetetlenítették önálló fejlődésüket és hosszú időre függővé tették azokat a nagyhatalmaktól. A digitális neokolonizáció, ami ma Afrikában zajlik, számos kockázatot jelenthet. Az, hogy Kína hogyan kívánja befolyásolni a tőle függő, fejlődő országokat, az elkövetkezendő évtizedekben világossá válhat a globális közösség számára. Mivel azonban úgy tűnik, Tanzánia és Etiópia örömmel fogadják Kína segítségét (Li, 2016), előfordulhat, hogy számukra még a nyilvánvaló kockázatokkal együtt is kedvezőbb kelet felé fordulni, mint újra nyugati hatalmak árnyékába kerülni. Kutatásom zárásaként az eddigiek alapján kísérletet teszek arra, hogy felsorakoztassam ennek a különös kapcsolatnak az előnyeit és hátrányait a fejlődő országok szempontjából.

5. KÖVETKEZTETÉSEK

5.1. Előnyök és hátrányok mérlegelése

Dolgozatomban részletesen foglalkoztam a Digitális Selyemút projekt megvalósulásával Afrikában. Tanzánia és Etiópia példáján keresztül bemutattam, hogy Kína hogyan indított el a XXI. században egy digitális neokolonizációs folyamatot, amellyel a szuperhatalom az afrikai kontinenst célozta meg. Láthattuk, hogy sem Tanzánia, sem Etiópia nem rendelkezik a megfelelő fejlettségi szinttel ahhoz, felvegyék a harcot a digitális tér veszélyeivel szemben, ellenben Kína hatalmas összegeket fektetett ezeknek az államoknak az ICT szektorába. A tanzániai és etióp esettanulmány alapján ismertettem, hogy Kína ténykedése milyen hatással volt ezeknek az államoknak a fejlődésére a kibertérben. A kínai projekt két komponensét vizsgáltam részletesen, a megfelelő technológia átadását és új normák, egy újfajta internetmodell átadását. Mindezek alapján választ adtam arra a kérdésre, hogy Kína jelenléte milyen kiberbiztonsági, vagy akár nemzetbiztonsági kockázatokkal jár az afrikai országok számára. Kutatásom fő kérdése pedig az volt, hogy melyik fél milyen módon profitál ebből az együttműködésből. Az eredményt egy táblázatban foglalom össze, amelyben a Digitális Selyemút projektben való részvétel előnyeit és hátrányait mutatom be.

Előnyök az afrikai országok szempontjából	Hátrányok az afrikai országok szempontjából	Előnyök Kína szempontjából
infrastruktúra fejlődése – gazdaság alapja	adósságcsapda, Kína kompenzációként felügyelete alá vonhatja	stratégiai pontok megszerzése távoli országokban
modern eszközökhöz való hozzájutás, felzárkózás	a felhasználók még nem állnak készen a digitális világra	afrikaiak kiszolgáltatottakká válnak, kínai szaktudásra szorulnak
szakemberek képzése, iskolai projektek – önállóság lehetősége	csak egy bizonyos réteghez jut el a megfelelő tudás, további függés Kínától	
kontrollálható internet, állampolgárok kommunikációja követhető	Kína is felügyelheti az adatforgalmat, bizalmas információkhoz juthat	adatgyűjtés lehetősége Afrikában, információszerzés
követendő példa	nincs garancia a szuverenitás megtartására	Afrika bizalmának elnyerése, erős befolyás
kölcsönök feltétel nélkül	motiváció hiánya a demokratikus fejlődésre	afrikai országok a keleti hitelek preferálják
erős szövetséges nemzetközi szinten	nyugati világ támogatásának elvesztése	nemzetközi támogatottság, új szövetségesek

3. ábra: A Digitális Selyemút projekt előnyeit és hátrányait összesítő táblázat

5.1.1. Következmények a résztvevők szintjén

Ahogy az a táblázatból is egyértelműen látszik, az afrikai országok szempontjából hátrányként megjelenő elemek mindegyike valamilyen módon megfeleltethető Kína digitális gyarmatosító szándékainak. Ez az eredmény azt a korábbi állítást bizonyítja, miszerint Kína valóban a digitális neokolonizáció elveit követve igyekszik befolyását növelni a fejlődő afrikai országok körében. Ennek a példátlan kolonizációs jelenségnek az egyértelmű győztese Kína. A táblázatban láthatjuk, hogy az afrikai országok hiába kapnak jelentős kölcsönöket a keleti szuperhatalomtól, ha azokat képtelenek lesznek visszafizetni (Kinyondo, 2019). Kína valamilyen módon kompenzációt követel majd. Hiába épül Tanzániában és Etiópiában a digitális infrastruktúra és fejlődik az internethálózat, ha arra Kína akármikor ráteheti a kezét,

ezáltal kiemelkedően fontos stratégiai pontokhoz jutva távoli országokban. Az afrikai országok számára persze a modern technológiához való hozzájutás, az iskolai projektek, tréningek és egyéb informatikai fejlődést elősegítő folyamatok mind pozitív hatással is járhatnak (Li, 2016; Gagliardone & Golooba-Mutebi, 2016). Ugyanis mindezen keresztül az afrikaiak is esélyt kapnak a digitális világgal való szorosabb kapcsolat kialakítására, így több hazai szakemberre tudnak majd támaszkodni a jövőben. Ez a digitális önállóság azonban még sokáig nem fog megvalósulni, amennyiben Kína nem adja át a megfelelő tudást az olyan országokban, mint Tanzánia vagy Etiópia. Márpedig ez a szuperhatalomnak egyáltalán nem áll érdekében, ugyanis a digitális neokolonizáció folyamatának is alapvető eleme a gyarmatosító hatalomtól való függés, ami ilyen módon megvalósul Afrikában. Az egyelőre rendkívül hiányos kiberbiztonsági szabályozás, a szakemberek hiánya és az általános tájékozatlanság a kiberbűnözőknek kedvezett, ezzel óriási anyagi károkat okozva a kontinens országai számára (Eboibi, 2020). A Kínától kapott technológia terjedésének egy további súlyos következménye lehet a fejlettebb városok és a vidéki területek közti digitális szakadék mélyülése.

Az internetszuverenitás modelljének átadása éppen az előbbi folyamatot igyekszik elfedni, egy hamis önállóságérzet megteremtésével. A fejlődő országok számára még sokáig álom maradhat a teljes szuverenitás, amennyiben a tökéletesen kontrollálható és manipulálható internethálózatukat Kína folyamatosan felügyelheti és adatokat gyűjthet a tanzániai és etióp felhasználókról. A támogatott államoknak imponál, hogy egy nagy politikai és gazdasági befolyással rendelkező szuperhatalom példáját követhetik, ebben pedig saját országuk felemelkedésének lehetőségét láthatják. Mivel azonban Kína kommunikációja nem teljesen világos, arra sincsen garancia, hogy tiszteletben tartja az afrikai államok szuverenitását. Ez egy rendkívül érdekes ellentmondás, ugyanis a kínai elnök szerint a kibertér minden ország számára szuverén, sérthetetlen terület, azonban ő mégis megsérti ezt az íratlan szabályt Afrikában. Azt, hogy hol van az a bizonyos határ, ahol Kínának már nagyobb teret kell engednie például az etióp kormányának saját kiberterük felügyeletében és menedzselésében egyelőre homály fedi. Továbbá az sem világos, hogy Kína példamutatásával mit vár el a támogatott országoktól. Csupán a saját internetmodelljük előnyeit mutatták meg számukra, ami a közelmúltban történt események alapján bevált Etiópiában és Tanzániában is, vagy továbbra is jelen kívánnak lenni valamilyen formában a kiberterükben? Erre a kérdésre a jövőbeli kutatásoknak kell válaszokat találniuk, azonban ennek a lehetőségnek a megemlítését fontosnak tartom saját dolgozatom egyik konklúziójaként.

Tanzánia és Etiópia számára az előbbiek alapján tehát rövidtávon előnyösnek bizonyulhat a Digitális Selyemút projektben való részvétel, ugyanakkor hosszútávon Kína az egyértelmű győztes. Rövidtávon a digitális gyarmatosítás folyamata segítheti az elmaradott országok technológiai fejlődését, viszont a távolabbi jövőben az egyének és az államok is egyaránt sínylik meg a következményeket. A kiberbűnözéssel való küzdelem, az egyre növekvő adósság és ezáltal a kiszolgáltatottság Kína felé jelentősen növelik a gyarmati sorba kerülés veszélyét. Ennek további következményei szintén csak az elkövetkezendő években, évtizedekben válnak világossá, hiszen soha korábban nem tapasztalta még meg ezt a jelenséget a Föld egyetlen országa sem.

5.1.2. Következmények globális szinten

Az ENSZ alapvető értékei, köztük a szólásszabadság megsértésével a Kína által támogatott államok politikája nemzetközi szinten is konfliktust szülhet. A fejlett és fejlődő országok közötti aszimmetria következtében egyértelműen az előbbi csoport állítja fel az utóbbi számára a kibertérben alkalmazandó szabályokat (Arsène, 2016). Azonban a fejlett országok körében is folyamatos küzdelem zajlik a hegemoniáért, amit Kína igyekszik megtörni és új normákat elfogadtatni globális szinten (Shen, 2016). Arsène (2016) rámutatott arra, hogy számos kínai szerző szerint elérkezett az a „történelmi pillanat”, amikor Kínának lépéseket kell tennie a kibertérben jelenleg fennálló rend megváltoztatása érdekében. Amennyiben Kína a Digitális Selyemút projekt keretében szövetségesekre talál és sikeresen átadja saját modelljét a támogatott országok számára, a nyugati normák idővel gyengülni fognak. Továbbá, mivel a szuperhatalom a hitelezés során nem szabja ki feltételként az emberi jogok tiszteletben tartását, vagy a demokratikus fejlődést (Kinyondo, 2019, pp. 12-13), ezért nem is motiválja az afrikai országokat arra, hogy - társadalmuk fejlődését ilyen módon is elősegítve - ezeken a területeken eredményeket érjenek el. Ezeket az államokat Kína a digitális gyarmatosítás egyik céljaként igyekszik olyan módon befolyásolni, hogy azok nemzetközi szinten is a szuperhatalom érdekeit támogassák. A nyugati világ sokszor alábecsüli Afrika méretét és hatalmas lakosságát, azonban az olyan nemzetközi szervezetekben, mint az ENSZ, több mint 50 ország szavazata jelentős előnyhöz juttathatja Kínát. Amennyiben számos afrikai ország, köztük Tanzánia és Etiópia digitális gyarmatokká és ezáltal kínai bábokká válnak a nemzetközi színtéren, a világnak fel kell készülnie Kína további térnyerésére. Nem csak az Afrikában egyre nagyobb problémát jelentő kiberbűnözés határokon átívelő problémája juthat el más országokba is, például hackertámadások, újfajta kártevő szoftverek útján, hanem maga Kína is beférkőzhet egy teljes kontinens általa épített digitális infrastruktúrájába. Szabad hozzáférést kap egy olyan

hálózathoz, amelyen keresztül újabb és újabb régiókban érvényesítheti saját akaratát, akár a már látott kölcsönök útján, technológiaátadással, egy újfajta, szuverén internetmodell propagálásával vagy kevésbé nyílt adatgyűjtési módszerekkel.

5.2. Konklúzió - Mire számíthatunk a jövőben?

Dolgozatom készítésekor korlátozott számú források álltak rendelkezésemre, ugyanis a Digitális Selyemút projekt jelenleg is zajlik, valamint nincsenek hivatalos információink arról, hogy mik Kína további tervei a projekt keretein belül. A továbbiakban azonban érdemes lesz a kutatóknak azt vizsgálniuk, hogy a Kína által támogatott afrikai országok mivel kompenzálják a nagy összegű kölcsönöket és az egyéb támogatásokat. Figyelemmel kell kísérnünk, hogy az ázsiai szuperhatalom mely területeken jelenik majd meg Afrikában, hogyan használja ki a kibertér lehetőségeit a további terjeszkedésre. Nem szabad figyelmen kívül hagynunk továbbá az afrikai országok támogatását különböző nemzetközi fórumokon, hiszen ezek tökéletes indikátorai lehetnek a digitális neokolonizáció megvalósulásának. Ahogyan a hagyományos gyarmatosító folyamatok során, úgy a digitális formájában is egyértelművé fog válni, mennyire válnak kiszolgáltatottá a fejlődő országok Kínával szemben. Ez természetesen a nyugati világnak egy újabb megoldandó feladatot jelent, főként az Egyesült Államok számára, amennyiben céljának tekinti a jelenleg fennálló világrend és saját hegemóniája megóvását.

Kutatásom során megállapítottam, hogy az Afrikában zajló neokolonizációs folyamatok abszolút nyertese Kína, mivel a technológia, amivel magához láncolta a fejlődő országokat, a saját tulajdonában áll. Az ország hosszú távon is profitálni tud afrikai kapcsolataiból, óriási nemzetközi támogatottságot szerezve. A világ fejlődő országai, amelyek még megfelelő jogi szabályozás és egyéb hiányosságaik okán nem készültek fel a digitális világ nehézségeire, egyszerre válhatnak a jövőben olyan szuperhatalmak, mint Kína célpontjaivá, és egyszerre jelenthetnek veszélyt a globális közösségre. A XXI. században ugyanis egyre világosabbá válik, hogy aki a kibertérrel uralja, egész országok, régiók működését befolyásolni tudja. Az életünk minden területét összeköti a világháló: folyamatosan digitális eszközökre hagyatkozunk, amelyek egyértelműen hatással vannak arra is, aki használja, és arra is, aki kimarad, hiszen felette azok fognak dönteni, akik rendelkeznek a legmodernebb technológiával.

6. BIBLIOGRÁFIA

Adane, K. (2020). The current status of cyber security in Ethiopia. *IUP Journal of Information Technology*, 16(3), 7-19.

Afrobarometer. (2016/2018). Government should monitor private communication vs right to privacy. Letöltés ideje: 2021. november 7. <https://afrobarometer-online-analysis.com/online.jsp?collection=7&ref=MjAyMDIyNDgzNg>

Alkhawajah, W. (2019). Huawei: An information and communications technology company. *Journal of Information Technology and Economic Development*, 10(1), 1-10.

Anthony, R. (2013. április 3.). *Should China keep its “Africa Dreams” to itself?* The Diplomat. Letöltés ideje: 2021. november 7. <https://thediplomat.com/2013/04/should-china-keep-its-africa-dreams-to-itself/>

Arsène, S. (2012). *The impact of China on global Internet governance in an era of privatized control*. Chinese Internet Research Conference, Los Angeles. Letöltés ideje: 2021. november 8. <https://hal.archives-ouvertes.fr/hal-00704196v2/document>

Arsène, S. (2016). Global Internet governance in Chinese academic literature. Rebalancing a hegemonic world order? *China Perspectives*, 2016(2), 25-35. Letöltés ideje: 2021. november 7. <https://doi.org/10.4000/chinaperspectives.6973>

Ayalew, Y. E. (2019). The Internet shutdown muzzle (s) freedom of expression in Ethiopia: competing narratives. *Information & Communications Technology Law*, 28(2), 208-224.

Cabestan, J. P. (2012). China and Ethiopia: Authoritarian affinities and economic cooperation. *China Perspectives*, 2012(4), 53-62. Letöltés ideje: 2021. november 7. <https://doi.org/10.4000/chinaperspectives.6041>

Césaire, A. (2001). *Discourse on colonialism*. NYU Press.

Cheney, C. (2019). China’s Digital Silk Road: strategic technological competition and exporting political illiberalism. *Pacific Forum, Issues & Insights Working Paper*, 19(WP8). Letöltés ideje: 2021. november 4. <https://tinyurl.hu/kFGj/>

China Africa Research Initiative and Boston University Global Development Policy Center. (2021). Chinese Loans to Africa Database, Version 2.0. Letöltés ideje: 2021. november 7. <https://chinaafricaloandata.bu.edu/>

Coleman, D. (2019). Digital colonialism: The 21st century scramble for Africa through the extraction and control of user data and the limitations of data protection laws. *Michigan Journal of Race and Law*, 24, 417-439.

Craig, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4(10).

Cross, C. (2021). Dissent as cybercrime: social media, security and development in Tanzania. *Journal of Eastern African Studies*, 15(3), 442–463. Letöltés ideje: 2021. november 7. <https://doi.org/10.1080/17531055.2021.1952797>

Douzet, F. (2014). Understanding cyberspace with geopolitics. *Hérodote*, 152-153, 3-21. Letöltés ideje: 2021. november 7. <https://doi.org/10.3917/her.152.0003>

Eboibi, F. E. (2020). Concerns of cyber criminality in South Africa, Ghana, Ethiopia and Nigeria: rethinking cybercrime policy implementation and institutional accountability. *Commonwealth Law Bulletin*, 46(1), 78-109.

Európai Bizottság. (2020). *Statement by President von der Leyen at the roundtable 'Internet, a new human right' after the intervention by Simona Levi*. Letöltés ideje: 2021. november 7. https://ec.europa.eu/commission/presscorner/detail/en/statement_20_2001

Furuholt, B., & Sæbø, Ø. (2018). The role telecentres play in providing e-government services in rural areas: A longitudinal study of Internet access and e-government services in Tanzania. *The Electronic Journal of Information Systems in Developing Countries*, 84(1), 1-14. Letöltés ideje: 2021. november 7. <https://doi.org/10.1002/isd2.12006>

Gagliardone, I., & Golooba-Mutebi, F. (2016). The evolution of the Internet in Ethiopia and Rwanda: Towards a “developmental” model? *Stability: International Journal of Security and Development*, 5(1), 1-24. Letöltés ideje: 2021. november 7. <http://doi.org/10.5334/sta.344>

Giles, C. (2018. május 7.). *Tanzania's bloggers fight back against \$930 fee as court grants injunction*. CNN. Letöltés ideje: 2021. november 4. <https://edition.cnn.com/2018/04/12/africa/tanzania-blogging-internet-freedom-africa/index.html>

Gravett, W. (2020). Digital neo-colonialism: The Chinese model of internet sovereignty in Africa. *African Human Rights Law Journal*, 20(1), 125-146. Letöltés ideje: 2021. november 7. <http://dx.doi.org/10.17159/1996-2096/2020/v20n1a5>

- Hillman, J. E. (2021). *Securing the subsea network: A primer for policymakers*. CSIS Reconnecting Asia Project. Letöltés ideje: 2021. november 4. <https://www.csis.org/analysis/securing-subsea-network-primer-policymakers>
- Horne, F., & Wong, C. (2014. március 25.). “*They know everything we do*” *Telecom and Internet surveillance in Ethiopia*. Human Rights Watch. Letöltés ideje: 2021. november 4. <https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia>
- International Telecommunication Union. (2015). Global Cybersecurity index & Cyberwellness Profiles. Letöltés ideje: 2021. november 5. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf
- International Telecommunication Union. (2019). Individuals using the Internet (% of population). Letöltés ideje: 2021. november 3. <https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=TZ-ET>
- International Telecommunication Union. (2020). Global Cybersecurity Index. Letöltés ideje: 2021. november 4. <https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/>
- Kinyondo, A. (2019). Is China recolonizing Africa? Some views from Tanzania. *World Affairs*, 182(2), 128-164.
- Kohn, M., & Reddy, K. (2017). Colonialism. In Zalta E. N. (szerk.). *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University.
- Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal Of Global Information Technology Management*, 22(2), 77-81.
- Layne, C. (2008). China's challenge to US hegemony. *Current History*, 107(705), 13-18.
- Li, A. (2016). Technology transfer in China–Africa relation: myth or reality. *Transnational Corporations Review*, 8(3), 183-195.
- Loomba, A. (2002). *Colonialism/postcolonialism*. Routledge.
- Makundi, H., Huyse, H., & Develtere, P. (2016). Cooperation between China and Tanzania on ICT: fish, fishing tackle or fishing skills?. *Journal of Chinese Economic and Business Studies*, 14(2), 129-149.

- Mambile, C., & Mbogoro, P. (2020). Cybercrimes awareness, cyber laws and its practice in public sector Tanzania. *International Journal of Advanced Technology and Engineering Exploration*, 7(68), 119-126. Letöltés ideje: 2021. november 7. <http://dx.doi.org/10.19101/IJATEE.2020.762051>
- Mtega, W. P., & Benard, R. (2013). The state of rural information and communication services in Tanzania: A meta-analysis. *International Journal of Information and Communication Technology Research*, 3(2), 64-73.
- Nantulya, P. (2021). *The forum on China-Africa cooperation at 21: Where to next?* Africa Center For Strategic Studies. Letöltés ideje: 2021. november 7. <https://africacenter.org/spotlight/focac-forum-china-africa-cooperation-21-where-to-next/>
- Nkrumah, K. (1965). *Neo-colonialism: The last stage of imperialism*. Thomas Nelson & Sons, Ltd.
- Satter, R. (2020). *Exclusive-Suspected Chinese hackers stole camera footage from African Union – memo*. Reuters. Letöltés ideje: 2021. október 29. <https://www.reuters.com/article/us-ethiopia-african-union-cyber-exclusiv-idINKBN28Q1DB>
- Shen, H. (2016). China and global internet governance: toward an alternative analytical framework. *Chinese Journal of Communication*, 9(3), 304-324.
- Shen, H. (2018). Building a digital silk road? Situating the internet in China's Belt and Road Initiative. *International Journal of Communication*, 12, 2683–2701.
- The Internet in China White Paper. (2010). Letöltés ideje: 2021. november 4. http://www.china.org.cn/government/whitepaper/2010-06/08/content_20207978.htm
- Tiezzi, S. (2015. december 16.). *China vows no compromise on 'cyber sovereignty'*. The Diplomat. Letöltés ideje: 2021. november 3. <https://thediplomat.com/2015/12/china-vows-no-compromise-on-cyber-sovereignty/>
- Triolo, P., Allison, K., Brown, C., & Broderick, K. (2020). *The Digital Silk Road: Expanding China's digital footprint*. Eurasia Group. Letöltés ideje: 2021. november 4. <https://tinyurl.hu/TZ65/>
- Tsagourias, N. (2015). The legal status of cyberspace. In *Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing. Letöltés ideje: 2021. november 7. <https://doi.org/10.4337/9781782547396.00010>

Tugendhat, H., & Voo, J. (2021). China's Digital Silk Road in Africa and the future of Internet governance. Working Paper No. 2021/50. *China Africa Research Initiative*. Letöltés ideje: 2021. november 7. <https://tinyurl.hu/HIUp/>

Világbank. (2020). Population, total. Letöltés ideje: 2021. november 3.
<https://data.worldbank.org/indicator/SP.POP.TOTL?locations=TZ-ET>

Világbank. (2020). Rural population (% of total population). Letöltés ideje: 2021. november 5.
<https://data.worldbank.org/indicator/SP.RUR.TOTL.ZS>

Woodhams, S. (2019. február 23.). *How China exports repression to Africa. China's "techno-dystopian expansionism" is undermining democracy in African countries*. The Diplomat. Letöltés ideje: 2021. október. 28. <https://thediplomat.com/2019/02/how-china-exports-repression-to-africa/>

Zeng, J., Stevens, T., & Chen, Y. (2017). China's solution to global cyber governance: Unpacking the domestic discourse of "Internet sovereignty". *Politics & Policy*, 45(3), 432-464.