ሳይበር ደህንነት በኢትዮጲያ እና ለብሔራዊ ደህንነት ያለው አንድምታ[1]

ይርጋ ባድማ ይታየው[2]

አህጽሮት

ባለፉት አሰርት ዓመታት ሳይበር ጥቃት በኢትዮጲያ ያለማቋረጥ እየጨመረ እንደሆነ ሪፖርቶች ያሳያሉ። ይህም ሳይበር ደህንነትን በሀገር እና በተቋማት ደረጃ ከተወሰዱት የአደረጃጀት፣ የህግ እንዲሁም የአቅም ግንባታ እርምጃዎች በተቃራኒ ነው። የዚህ ጥናት ዓላማ አሁን ያለውን የሀገራችንን የሳይበር ደህንነት ሁኔታ በመዳሰስ እና የሳይበር ደህንነት ምርጥ ተሞክሮዎችን በመዳሰስ የፖሊሲ ግቦች ምክረሀሳብ በማቅረብ ሳይበር ደህንነት በብሔራዊ ደህንነት ላይ የሚኖረውን ተጽዕኖ ለመቀነስ ነው። የጥናቱን ዓላማ ለማሳካት ከ አራት የብሔራዊ ደህንነት ወይም ሳይበር ደህንነት ተልዕኮ ያላቸው መንግስታዊ ተቋማት የተሰበሰቡ የመጠይቅ፣ ቃለ - ምልልስ እና የመዛግብት መረጃዎችን ለመተንተን ቅይጥ የጥናት ዘይዎች ጥቅም ላይ ውለዋል። ዓላማ ተኮር የንሞና ዘዴን በመከተል አስራ ሁለት ቃለ - ምልልሶች የተደረጉ ሲሆን፣ አርባ አራት መጠይቆች መረጃ ለመሰብሰብ ጥቅም ላይ ውለዋል፤ የተሰበሰበውን መረጃ ለመተንተን ደግሞ ዓይነታዊ እና መጠናዊ ዘዴዎችን በአንድ ላይ በማቀናጀት ቅይጥ የጥናት ዘዴ በጥቅም ላይ ውሏል። ከተለያዩ ሀገራት በተለይም የኢስቶኒያን ተቋማት እንዲሁም በዓለማቀፉ ሰርዓት ያላትን ሚና እንደ ምርጥ ተሞክሮ እና የተገኙ ትምህርቶች ሆነው ተወስደዋል። የጥናቱ ውጤቶች እንደሚያሳዩት ጥሩ የሚባል የሳይበር ደህንነት አቋም በመያዝ ሳይበር ስጋቶች ብሔራዊ ደህንነት ላይ የሚያደርሱትን ጉዳት ለመቀነስ በሀገር እና በተቋማት ደረጃ ብዙ መሰራት እንዳለበት ነው። በሀገራዊ እና ተቋማዊ የሳይበር ደህንነት ፖሊሲ እና ስትራቴጂ፣ የህግ ማዕቀፍ፣ የአደረጃጀት፣ የአቅም ግንባታ፣ የቅንጅትና ትብብር ጥረቶች ላይ ውስንነት ታይቷል። በመጨረሻም ሳይበር ደህንነት በኢትዮጲያ ብሔራዊ ደህንነት ላይ የሚኖረውን ተጽዕኖ ለመቀነስ የሚያስችል ፖሊሲ ምክረሀሳቦች ቀርበዋል። ከነዚህም መካከል ኪፖሊቲካ አመራር ጀምሮ በተለያየ ደረጃ ግንዛቤ መፍጠር ሰራዎችን መሰራት፤ ሁሉን አቀፍ የህግ እና ቁጥጥር ማዕቀፍ ማዘጋጀትና መተግበር፤ በተለያየ ተቋማት ያለውን የሳይበር ደህንነት እንቅስቃሴ የሚያጠናክር የጋራ ተቋማዊ አደረጃጀት ማቋቋምና ያሉትን ተቋማት ማጠናከር፤ የሳይበር ደህንነት ፖሊሲና ስትራቴጂ ቀረጻና ውጤታማ ትግበራ እንዲኖር ማስቻል፤ በተቋማት መካከል ግልጽ እና የማያሻማ ድርሻ እና ኃላፊነት መስጠት እና የረጅም ጊዜ አቅም ግንባታ ሰራዎች መሰራት በጣም አስፈላጊ የሆኑት ናቸው።

ቁልፍ ቃላት: *ሳይበር ደህንነት፣ ሳይበር መከላከል፣ ሳይበር ወንጀል፣ ብሔራዊ ደህንነት፣ ፖሊሲና ስትራቴጂ*

1 መግቢያ

ከቅርብ ጊዜያት ወዲህ የሳይበሩ ዓለም ቁሳዊውን ዓለም እየተቆጣጠረ የመጣ ሲሆን በተወሰኑ ዋና ዋና ከተሞች ደግሞ አንድ ሆነው ይገኛሉ። ይህም በተለያዩ ቦታ የሚገኙ እና በየጊዜው ቁጥራቸው እየጨመረ የሚሄዱ አካላት በቅጽበት ጊዜ ግንኙነት እንዲያደርጉ እና የተለያዩ ተግባራትን ለመፈጸም እንዲችሉ አድርጓል። ከጥቂት አሰርት ዓመታት በፊት በወረቀት ላይ የተመሰረቱ የፖለቲካ ዘመቻዎች፣ ፋይናንስ እንቅስቃሴዎች፣ መንግስታዊ መዛግብት፣ የደኅንነት ክትትል፣ የመከላከያ ስትራቴጂዎች ወደ ኮምፒዩተሩ ዓለም መምጣት ተከትሎ የሰው ልጅ እንቅስቃሴ በመጠን ሊገለጽ እና ሊተነተን ወደሚችል አንድ ስርዓት መጥቷል።[3] በሌላ በኩል የሳይበር ምህዳር መምጣት የስጋት ተዋንያን በሰው ልጆች ደኅንነት ላይ ተጽዕኖ ለማድረስ የሚያስችል ሁኔታ ፈጥሯል። እነዚህ ተዋንያን ሀገራት ወይም መንግስታት (በመከላከያ ወይም በደኅንነት ኃይሎቻቸው አማካኝነት) እንዲሁም መንግስታዊ ያልሆኑ ወንጀለኞች፣ የሽብር ቡድኖች፣ ሀክሮች እና አክቲቪስቶች ሲሆኑ የሳይበር ምህዳሩን ለራሳቸው ዓላማ በመጠቀም ዓለማቀፍ የፖለቲካ አለመረጋጋት በመፍጠር የአንድ ሀገር ብሔራዊ ጥቅም ላይ ጉዳት ያደርሳሉ። ከሳይበር አውድ የሚመጡ ስጋቶች ከቁሳዊው ዓለም በተጻራሪ ለመለየት አጠራጣሪና ለመበየን አስቸጋሪ ናቸው።[4] በመሆኑም በማኅበራዊ፣ ፋይናንስ፣ ኢንዱስትሪ እና መከላከያ ዘርፎች ከመቼውም ጊዜ በበለጠ እንዲተሳሰሩና ግንኙነት እንዲያደርጉ ቢያስችልም ተጋላጭነትንም በዚያው ልክ እንዲስፋፋ አድርጓል። በሳይበሩ ዓለም ከፍተኛ ድንበር ተሻጋሪ ግንኙነት ያለ በመሆኑ ሳይበር ደኅንነት በውስጣዊ እና ውጫዊ የብሔራዊ ደህንነት ክፍለ አካላት ውስጥ ይገኛል። የሳይበር ምህዳር

---

[1] ይህ ጽሁፍ በ2013 ዓ.ም ለኢፌዲሪ መከላከያ ዋር ኮሌጅ በስትራቴጂያዊ እና ደህንነት ጥናት ማስተርስ ዲግሪ ማሟያ ከተዘጋጀው ጥናት በመነሳት ለEDJSS እንዲሆን ተደርጎ የተዘጋጀ ነው።

[2] በኢፌድሪ የኢንፎርሜሽን መረብ ደህንነት አስተዳደር (ኢመደአ) የመረጃ ደህንነት ባለሞያ፤ yirgabdm@gmail.com

[3] Henry Kissinger, World Order (Penguin Books, 2014).

[4] Kissinger.

አብዛኛዎቹን ነባር የህግ እና ቁጥጥር ስርዓቶች በመሻገር ከዚህ ሁኔታ ለመውጣት የሚደረገው ጥረት የሚፈጥረው የፖለቲካ ስርዓት አነሳሽ ኃይል እንደሚሆን ፈላስፎች አስቀድመው የገለፁት ነው። በሳይበር አውድ ግልፅ የሆነ ወሰን እንዲሁም በሀገራት መካከል የጋራ ገደብ ሕጎች ስምምነት ባለመኖራቸው ምክንያት ሆን ተብሎም ባይሆን ቀውስ መፈጠሩ እና መሰረታዊ የአለማቀፍ ስርዓት ጽንሰ ሀሳብ መፈተኑ አይቀሬ ነው።[5]

ከቅርብ ጊዜያት ወዲህ የሀገራት ብሔራዊ ደኅንነት ላይ አሉታዊ ተጽዕኖ ያሳረፉ ክስተቶች ከሳይበር የሚመጣ ስጋት በብሔራዊ ደኅንነት ላይ ሊያደርስ የሚችለውን ተጽዕኖ ለማሳየት በአስረጂነት ሊወሰዱ ይችላሉ። በ2007 እ.ኤ.አ በሩስያ እና ኢስቶንያ መካከል የተፈጠረ ዲፕሎማሲያዊ አለመግባባት የኢስቶንያ የፋይናንስ፣ ሚዲያ እና መንግስት ዌብ ሳይቶች አገልግሎት እንዲቋረጥ የሚያደርግ (DDOS) የሳይበር ጥቃቶች ደርሶባቸዋል። በዚህም የኢንተርኔት ባንክ አገልግሎት፣ የመንግስት ሰራተኞች ግንኙነት እንዲሁም የመረጃ ስርጭት እንዲቋረጥ አድርጓል። በ2008 እ.ኤ.አ የደቡብ ኦሴትያ ጦርነት ደግሞ የጆርጅያ ፕሬዚዳንት ዌብሳይት በተመሳሳይ ጥቃት ከጥቅም ውጭ እንዲሆን እንዲሁም የህገራቱን የብሔራዊ ባንክ እና የፖርላማ ዌብሳይቶች በመቆጣጠር (Hacking) የአዶልፍ ሂትለርን ምስል እንዲታይ ለማድረግ ችለዋል።[6] ይህም የመጀመሪያው የሳይበር ጥቃቶች ከጦርነት ጋር የገጠሙበት ክስተት ሆኖ ይታወቃል። ሪፖርቶች እንደሚያሳዩት ጥቃቶቹ ከሩስያ፣ ዩክሬን እና ላቲቪያ የተነሱ ሲሆን የጥቃቱ ፈጻሚዎች ዓላማ ደግሞ በፈቃደኝነት ሩስያን በጦርነቱ ለመደገፍ ነበር። በ2010 እ.ኤ.አ ስተክስኔት (Stuxnet) የተባለ የዓለማችን የመጀመሪያው ዲጂታል የጦር መሳሪያ በኢራን የኑክሌር ፕሮግራም ላይ መጠነሰፊ ጉዳት ማድረሱ ይታወቃል። ሀገራቱ በጋራም ሆነ በተናጠል ኃላፊነት ባይወስዱም የኢራን ኢንዱስትሪ ሲስተም ላይ የኮምፒዩተር ማልዌር (Worm) በመጠቀም ጥቃት ያደረሱት አሜሪካና እስራኤል እንደሆኑ ይታመናል።[7] በ2014 እ.ኤ.አ ሰሜን ኮሪያ "The Interview" የተሰኘው የአሜሪካው ሶኒ ፒክቸርስ (Sony Pictures) ፊልም እንዳይታይ እና እንዳይሰራጭ በዲፕሎማሲያዊ መንገድ ያቀረበችው ጥያቄ ተቀባይነት ባለማግኘቱ በሽብር ጥቃት ማስፈራሪያ ጭምር የሰሜን ኮሪያ የህከር ቡድን የድርጅቱን ምስጢራዊ እና ግላዊ መረጃዎችን ይፋ በማውጣት ትልቅ ኢኮኖሚያዊ እና ስነልቦናዊ ኪሳራ አድርሷል።[8] በ2016 እ.ኤ.አ የአሜሪካ ፕሬዚዳንታዊ ምርጫም መረጃን በማዛባት እና የተሳሳተ መረጃን በዋና ዋና ሚዲያዎች እንዲሁም በማኅበራዊ ሚዲያ በማሰራጨት የሩስያ ጣልቃ ገብነት እንደነበረ የአሜሪካ የስለላ ተቋማት በጋራ ባወጡት ሪፖርት ገልጸዋል።[9] በተጨማሪም ምዕራባውያን ሀገራት ቻይናን በብዙ የስለላ ዘመቻዎች እና ከቻይና የኮምፒዩተር መሰረተ ልማት በሚነሱ ሳይበር ጥቃቶች ይከሳሉ።[10] በሳይበር ምህዳር የአንድን ግለሰብ ትክክለኛ ማንነት ለማወቅ አስቸጋሪ መሆኑ ጥቃቱ መንግስታዊ ድጋፍ ይኑረው አይኑረው ለማወቅ አስቸጋሪ ያደርገዋል። በተመሳሳይ ሁኔታ ቻይና ይህን ክስ የማትቀበለው ሲሆን በተቃራኒው አሜሪካ በቻይና ላይ የሳይበር ጦርነት መክፈቷን ትገልጻለች። ይህንንም ክስ አሜሪካ አትቀበለውም።[11]

በኢትዮጲያም ከሳይበር የሚመጣ ስጋት መጠኑ አነስተኛ ቢመስልም በብሔራዊ ደህንነት ላይ ቀላል የማይባል አደጋ እያደረሰ እንደሆነ የሚያሳዩ ማስረጃዎች አሉ።[12] አነስተኛ እንዲመስል ያደረገው አንድም በ ICT ላይ ያለን ጥገኝነት አነስተኛ በመሆኑ አንድም ጥቃቶቹ ሳይታወቁ መፍትሄም ሳይወሰድባቸው ስለሚቀር ሊሆን ይችላል። ምንም እንኳ እነዚህ ሳይበር ጥቃቶች የሚያደርሱትን ተጽዕኖ ለመቀነስ የሚያስችል ጥረት ቢኖርም ከስጋቱ አንጻር በቂ ወይም ውጤታማ ነው ለማለት አያስደፍርም። በመንግስታዊ እና የግል ተቋማት ሰፊ የቴክኖሎጂ ተጠቃሚነት ፍላጎት እና ጥረት ቢኖርም ያን ተከትሎ ሊመጣ ስለሚችል የሳይበር ተጋላጭነት ያለው ግንዛቤ፣ የህግ ማዕቀፍ፣ የአስተዳደር ስርዓት አነስተኛ መሆኑ ይጠቀሳል። በ2006 እ.ኤ.አ የኢንፎርሜሽን መረብ ደህንነት አስተዳደር (ኢ.መ.ደ.አ) መቋቋም በመንግስት በኩል እንደ አንድ እርምጃ የሚወሰድ

[5] Kissinger.

[6] John Markoff, "Before the Gunfire, Cyberattacks - The New York Times," The New York Times, 2008, https://www.nytimes.com/2008/08/13/technology/13cyber.html.

[7] Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," Wired, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[8] Gabi Siboni and David Siman-Tov, "Cyberspace Extortion: North Korea versus the United States," INSS Insight, no. 646 (2014).

[9] Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," Office of the Director of National Intelligence, no. January (2017): 1–25.

[10] Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," Journal of Strategic Security 4, no. 2 (2011): 1–24, https://doi.org/10.5038/1944-0472.4.2.1.

[11] Dana Rubenstein, "Nation State Cyber Espionage and Its Impacts," 2014, 1–11.

[12] Ethiopian News Agency, "INSA Alarmed by Increase in Cyber Attacks, Calls for Swift Actions | Ethiopian News Agency," Ethiopian News Agency, 2019, https://www.ena.et/en/?p=10542.

ነው። አስተዳደሩ በአሁኑ ወቅት የኢንፎርሜሽን እና ኢንፎርሜሽን መሰረተልማትን ደህንነት ማስጠበቅ፣ ሳይበር ወንጀልን መከላከል፣ ሳይበር-ምህዳርን ደህንነት መጠበቅ እንዲሁም ብሔራዊ የሳይበር ደህንነት ጥረቶችን በማስተባበር የሳይበር ደህንነት ፖሊሲና ስትራቴጂ ቀረጻና ትግበራን እንደ ተልዕኮ ይዞ በመንቀሳቀስ ላይ ይገኛል። ከዚህ በተጨማሪ በቅርቡ የመከላከያ ሠራዊትን አዋጅ ለማሻሻል በወጣው አዋጅ ላይ ሳይበር እንደ መሬት፣ ውሃ፣ አየር እና ስፔስ አውዶች ሁሉ የጦርነት አውድ ሆኖ ተወስዷል።[13] [14] ነገር ግን የ 2002 (እ.ኤ.አ) የውጭ ጉዳይ እና ብሔራዊ ደህንነት ፖሊሲና ስትራቴጂ የሳይበር ጉዳይን ሳያነሳ ያልፈዋል።[15]

የተለያዩ ሀገራት በተለይም ኃያላኑ የሳይበር አቅማቸውን ኦፕሬሽናዊ ከማድረጋቸው ጋር ተያይዞ የሳይበር ክስተቶች መብዛት እና ስጋት የሚፈጥሩ ሁኔታዎች በመኖራቸው ነገ ምን ይፈጠር ይሆን የሚለው አሳሳቢ ጉዳይ ነው። በዓለምአቀፍ ደረጃ ካለው እንቅስቃሴ አንጻር በኢትዮጲያ ያለው ጥረት አነስተኛ እና ሊሻሻል የሚገባው እንደሆነ ማሳያዎች አሉ። ባለፉት ጊዜያት መንግስታዊ ተቋማት በሚገባው መጠን ሳይበር ደህንነትን እንደ አንድ የደህንነት ጉዳይ አድርገው አለማየታቸው ከተልዕኳቸው ጋር በማጣመር የአቅም ግንባታ ስራዎች አለመስራታቸው ሊጠቀስ ይችላል። ለአብነትም አዲሱ የመከላከያ ሠራዊት አዋጅ ሳይበርን እንደ አንድ የጦርነት አውድ የሚወስድ ሲሆን የበለጠ ግልጽነት በመፍጠር ዝርዝር ድርሻና ኃላፊነትን በብሔራዊ እና በተቋማት ደረጃ ማስቀመጥ እንዲሁም ተመጋጋቢ እንዲሆኑ ለማድረግ ግን አልተቻለም።

የዚህ ጥናት ዓላማ የሳይበር ደህንነት በኢትዮጲያ ብሔራዊ ደህንነት ላይ ያለው ሚና የተሰጠውን ትኩረት፣ የተጋላጭነት ደረጃ፣ ብሔራዊ ሀብቶችን ለመከላከል የሚውሉ መንገዶችና ግብዓቶች ላይ ጥናት በማድረግ እና አለማቀፍ ምርጥ ተሞክሮዎችን በመቃኘት የፖሊሲ ምክረ ሀሳቦችን ለማቅረብ ነው። የጥናቱ ወሰን በስትራቴጂያዊ ደረጃ ሲሆን ከተቋማት የሀገር መከላከያ ሰራዊት፣ የኢንፎርሜሽን መረብ ደህንነት አስተዳደር እና የፋይናንስ ደህንነት መረጃ ማዕከልን፣ እንዲሁም የውጭ ጉዳይ ሚኒስቴርን ያካትታል። የጥናቱ ክፍለ-አካላት በባለድርሻ አካላት ውስጥ እና መካከል ያለ የሳይበር ደህንነት የህግ ማዕቀፍ፣ የአመራርና አስተዳደር አቅም ግንባታ፣ ትብብርና ውህደት፣ የመረጃ ልውውጥ ጥረቶችን ያካትታል። ጥናቱ ውሱንነቶች በመለየት በጥናቱ ውጤት ላይ ሊያደርሱ የሚችሉትን አሉታዊ ተጽዕኖ ለመከላከል የሚያስችል ጥረት ተደርጓል። የመጀመሪያው ከጥናቱ ስፋት እና በአንድ አጥኚ የሚደረግ ከመሆኑ ጋር ተያይዞ የሚመጣ ውሱንነት ሲሆን ይህም አጥኚው ራሱን በማብቃት እና በዘርፉ ያሉ የጥናቱ ተሳታፊ ባለሙያዎች ለጥናቱ እንደ አጋዥ ኃይል መጠቀም ተችሏል። ሁለተኛው የስትራቴጂክ አመራር ሰፊ ጊዜ ወስዶ ለማሳተፍ አስቸጋሪ መሆኑን በመረዳት በመረጡት ጊዜ እና ሊሰጡ ከሚችሉት ጊዜ አንጻር ቃለምልልሶቹን በመቃኘት አስፈላጊውን ዳታ ለመሰብሰብ ጥረት ተደርጓል። በተጨማሪም ምስጢራዊነት እና ግላዊነት ለማስጠበቅ የዳታ አሰባሰብ ተሳታፊዎች ሀሳብ ምስጢራዊ በሆነ መልኩ ቀርቧል። በመጨረሻም የኮቪድ-19 ወረርሽኝ የዳታ አሰባሰብ ሂደት ላይ ተጽዕኖ ለመቋቋም በርቀት ዳታ የማሰባሰብ ዘዴን እንዲሁም ወረርሽኙን ለመከላከል የተቀመጡ አሰራሮችን በመከተል ዳታ ለመሰብሰብ ተችሏል። ጥናቱ በአራት ምዕራፎች የተደራጀ ሲሆን የመጀመሪያው ምዕራፍ መግቢያ እና የጥናቱን ዓላማ፣ ወሰን እና ውሱንነቶች ይዟል። ሁለተኛው ምዕራፍ ደግሞ ንድፈ ሀሳባዊ እና ጽንሰ ሀሳባዊ ዳሰሳ አካትቷል። በሶስተኛው ምዕራፍ የጥናቱ ዘዴ እንዲሁም በአራተኛው ምዕራፍ በጥናቱ የተገኙ ውጤቶች የቀረቡ ሲሆን የመጨረሻው ምዕራፍ ድምዳሜዎችን እና ምክረ ሀሳቦችን የያዘ ነው።

2 ጽንሰ ሀሳባዊ እና ንድፈሀሳባዊ መዋቅር

ብሔራዊ ደህንነት የዜጎች፣ የኢኮኖሚ እና የተቋማት በአጠቃላይ የአንድ ሀገር ደህንነት ሲሆን የመንግስት አንዱና ዋነኛ ስራ ተደርጎ ይወሰዳል። በቀድሞ ጊዜ የወታደራዊ ስጋቶች ላይ ያተኮረ ሲሆን በአሁኑ ጊዜ ግን ከወታደራዊና ፖለቲካዊ ጫና ባሻገር ያሉ ጉዳዮችንም ያካትታል።[16] [17] መንግስታት ፖለቲካዊ፣ ኢኮኖሚያዊ፣ ወታደራዊ እና የመረጃ መሳሪያዎችን በመጠቀም የሀገራቸውን ደህንነት ያስጠብቃሉ። ከዚህም በተጨማሪ ድንበር ተሻጋሪ የስጋት ምንጮችን ለመቀነስና ለማስወገድ በጋራ እና

[13] Council of Ministers, “Information Network Security Agency Re-Eslablishment,” Federal Negarit Gazette, 2011.

[14] FDRE House of People Representatives, “Information Network Security Agency Re-Establishment Proclamation,” Federal Negarit Gazette 22, no. 15 (2013): 8686–95; FDRE House of People Representatives, “A Proclamation on the Defense Forces of the Federal Democratic Republic of Ethiopia,” Federal Negarit Gazette 22, no. 15 (2019): 8686–95.

[15] Ministry of Information, “The F.D.R.E Foreign Affairs and National Security Policy and Strategy,” no. November (2002): 1–89.

[16] Joseph J Romm, Defining National Security: The Nonmilitary Aspects (Council on Foreign Relations, 1993).

[17] Prabhakaran. Paleri, National Security: Imperatives and Challenges (New Delhi: Tata McGraw-Hill Pub. Co., 2008).

በተናጠል ይሰራሉ። በሀገራት ሊከሰቱ በሚችሉ ሰፊ አደጋዎች መነጽር የአንድ ሀገር ደህንነት ከብሔራዊ ኃይል ክፍለ አካላት ጋር የሚመሳሰሉ ብዙ ገጽታዎች ይኖሩታል። ይህም የፖለቲካ፣ የኢኮኖሚ፣ የኢነርጂና የተፈጥሮ ሀብት፣ የቁሳዊ፣ የአካባቢያዊ፣ የምግብ፣ የወሰን እና የሳይበር ደህንነት ያካትታል። መንግስታት የደህንነት ፖሊሲዎቻቸውን የብሔራዊ ደህንነት ስትራቴጂ በመቅረጽ ለማሳካት ጥረት ያደርጋሉ፤ ከዚህ በተጨማሪም ለሀገራት መሪዎች በብሔራዊ ደህንነት ጉዳዮች ላይ እገዛ የሚያደርግ የብሔራዊ ደህንነት ምክር ቤት ወይም አማካሪ ይሰይማሉ። በአሁኑ ጊዜ ሀገራት ወታደራዊ ያልሆኑ አማራጮችን (አየር፣ ህዋ፣ ሳይበር፣ እና ስነ-ልቦናዊ) በማስቀደም ብሔራዊ ደህንነታቸውን ለማስጠበቅ ሲሞክሩ ሌሎች ሀገራት አሁንም በመሬት ወይም በውኃ ላይ የተመሰረቱ ወታደራዊ አቅሞቻቸውን ብቻ ይጠቀማሉ።[18] [19]

ሳይበር ደህንነት ማለት የኮምፒዩተር ስርዓቶች እና ዕቃዎች (ስማርት ሞባይል እና ሌሎችንም ጨምሮ) እንዲሁም የግለሰብና የሕዝብ የኮምፒዩተር ኔትወርኮች እና የኢንተርኔት ደህንነት ማለት ነው። በዚህ ስርዓት ውስጥ ሀርድዌር፣ ሶፍትዌር፣ መረጃ፣ ሰው፣ እና ሲስተሞች ማግኘት የሚቻልበት የአሰራር ስርዓቶችን ያካትታል። አብዛኛው ማኅበረሰብ በኮምፒዩተር ስርዓት ላይ ያለው ጥገኝነት እየጨመረ የመጣ በመሆኑ ይህ የደህንነት መስክ የብሔራዊ ደህንነት አንድ አካል እየሆነና የሚሰጠው ጥቅም እየጨመረ መጥቷል።[20] በአሁኑ ወቅት ያልተፈቀደለት አካል የሲቪልና ወታደራዊ መሰረተ ልማቶችን ለማግኘት (ለመቆጣጠር) ከቻለ እንደ ዋነኛ ስጋት የሚቆጠር ሲሆን የሳይበር ምህዳሩም እንደ አንድ የጦርነት አውድ ይወሰዳል።[21] የመሰረተ ልማት ደህንነት ማለት ቁልፍ መሰረተ ልማቶች ለምሳሌ ትራንስፖርት፣ ግንኙነት፣ ኤሌክትሪክ ኃይል፣ የውሃ ስርዓቶች ለህቡዕ አፍራሽ እንቅስቃሴዎች፣ ሽብር እና ብክለት ያላቸውን ተጋላጭነት መቀነስ ሲሆን ከ ICT ጋር ባላቸው ግንኙነት ልክ ሳይበር ደህንነት ያስፈልጋቸዋል።[22]

በ2017 እ.ኤ.አ Galinec, Možnik እና Guberina ሳይበር ደህንነትና ሳይበር መከላከል ላይ በሀገራዊ እና ስትራቴጂያዊ ደረጃ ባደረጉት ጥናት ያዘጋጁት ሞዴል ከዚህ ጥናት ዓላማ አንጻር አነስተኛ ማሻሻያ በማድረግ ቀርቧል።[23] ሳይበር ደህንነት እና የመረጃ ደህንነት ብዙውን ጊዜ በተለዋዋጭነት ጥቅም ላይ የሚውሉ ሲሆን ምንም እንኳ የሚጋሩት ነገር ቢኖርም የተለያየ ትርጉም እና ወሰን ያላቸው የደህንነት ጽንሰ ሀሳቦች ናቸው። ሳይበር ደህንነት ከ ICT ተጋላጭነት ጋር ተያይዞ በሰው፣ በቴክኖሎጂ ወይም በአሰራር ስርዓት ላይ የሚመጣ የደህንነት ክፍተት ሲሆን ማንኛውም በዲጂታል መልኩ ተቀምጦ ያለ የመረጃ ደህንነትን ያካትታል። በሌላ በኩል የመረጃ ደህንነት ማለት በአናሎግም ሆነ በዲጂታል ዓለም የሚገኝ ማንኛውም የመረጃ ደህንነት ማለት ነው። ሳይበር መከላከል ማለት የሀገርን ወይም የአንድን ተቋም የሳይበር ምህዳር ደህንነት ለማስጠበቅ የሚያስችል የተደራጀ የሰዎች፣ የአሰራር ስርዓት እና የቴክኖሎጂ እንቅስቃሴ ነው። የ ICT ደህንነት ደግሞ በሁለቱም ደህንነት ጽንሰ ሀሳቦች ውስጥ የሚገኝ ሲሆን በአብዛኛው ቴክኖሎጂውን ደህንነት ማስጠበቅ ላይ ያተኮረ ነው። የኢንዱስትሪው ዘርፍ ከኮምፒዩተር ስርዓት ጋር እየተገናኘ መምጣቱን ተከትሎ ኦፕሬሽናል ቴክኖሎጂ (OT) በተለይም Cyber Physical System ከመረጃ ደህንነት ባለፈ የኦፕሬሽናል ጉዳዮችን ለማካተት የሳይበር ደህንነት ጉዳዮች እንዲኖሩት አስችሏል። በማጥቃት ላይ የተመሰረተ ደህንነት (Offensive Security) አስቀድሞ ጠላትን በመለየት የኮምፒዩተር እና የግንኙነት ስርዓቶችን እንዲሁም ተያያዥነት ያላቸው ሀብቶችን ለመጠበቅ የሚያስችል የደህንነት ጽንሰሀሳብ ሲሆን ይህም ከተለመደው በመከላከል ላይ ከተመሰረተው እና ክፍተቶችን በመለየት የመዝጋት እና ለክስተቶች ግብረመልስ የመስጠት ጽንሰ ሀሳብ የተለየ ነው።

[18] David Gee, Rethinking Security: A Discussion Paper, 2016.

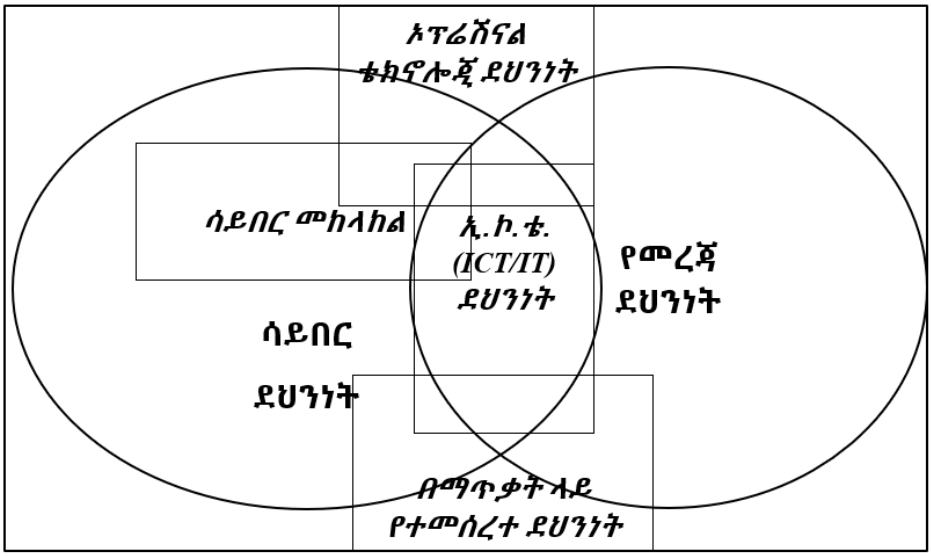
[19] Matt Murphy, "Cyberwar - War in the Fifth Domain | Briefing | The Economist," The Economist, 2010, https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain.

[20] Daniel Schatz, Rabih Bashroush, and Julie Wall, "Towards a More Representative Definition of Cyber Security," Journal of Digital Forensics, Security and Law 12, no. 2 (2017): 53–74.

[21] Murphy, "Cyberwar - War in the Fifth Domain | Briefing | The Economist."

[22] IGI, "What Is Infrastructure Security | IGI Global," IGI Global, 2020, https://www.igi-global.com/dictionary/managing-compliance-with-an-information-security-management-standard/42019.

[23] Darko Galinec, Darko Moznik, and Boris Guberina, "Cybersecurity and Cyber Defence: National Level Strategic Approach," Automatika 58, no. 3 (2017): 273–86, https://doi.org/10.1080/00051144.2017.1407022.



ምስል 1፡ የሳይበር ደህንነት አካላት እና ከሌሎች የደህንነት ጽንሰ ሀሳቦች ጋር ያለው ግንኙነት

ሳይበር ደህንነት እንደ አንድ የደንንነት ዘርፍ ከአለማቀፍ ግንኙነት እንዲሁም ከደህንነት ጥናት የሚመነጭ ሲሆን የብሔራዊ ደህንነት አንድ ከፍለአካል ተደርጎ ይወሰዳል። ለዚህም የአለማቀፍ ግንኙነት ቲዎሪዎች ለሳይበር ደህንነት ያላቸው አግባብነት Howard Kleinberg ለሳይበር ደህንነት ምርጥ ተሞክሮዎች መነሻ እንዲሆኑ አድርጎ ካቀረበው ጥናት መነሻ በማድረግ በአጭሩ ለማቅረብ ተሞክሯል።[24]

ዲሞክራሲያዊ ሰላም ቲዎሪ (Democratic Peace Theory) በስትራቴጂያዊ ደረጃ የሳይበር ስጋቶች ከማን እና ከየት አቅጣጫ ሊመጡ እንደሚችሉ ለመረዳት የሚያስችል ሲሆን ምዕራባውያን የውጭ ግንኙነት ፖሊሲያቸውን መሰረት የሚያደርጉበት ቲዎሪ ነው።[25] በተጨማሪም በዘመናዊነት እንዲሁም በኢኮኖሚ እና ወታደራዊ አቃሞች ውጤታማ መሆን ዲሞክራሲያዊ ካልሆኑ ሀገራት በኩል ጥላቻ፣ ቅናት፣ ተቀናቃኝነት እና ዒላማ መሆንን እንደሚያመጣ ያስረዳል። ስትራቴጂያዊ ባህል ቲዎሪ (Strategic Culture Theory) በተመሳሳይ የጦርነት፣ የጥላቻ እና የጭካኔ ባህል ያላቸው ሀገራት በሳይበር ምህዳርም ያንኑ የማድረግ አዝማሚያ እንዳላቸው ያስረዳል። ስለዚህም ተልዕኳቸውን ለማሳካት፣ ለመበቀል፣ በቁሳዊው ዓለም ለማድረግ የማይችሉትን በሳይበሩ ዓለም ያደርጋሉ። ከለሳዊ ቲዎሪ (Revisionism Theory) ደግሞ ከለሳ የሚያደርጉ ሀገራት የአለማቀፍ ስርዓቱን ለመቀየር እና ልዕለ ሀያል የሆነውን ለማስወገድ ሲሉ በቀጥተኛ እና ቀጥተኛ ባልሆነ መልኩ ሳይበር ምህዳሩን በመጠቀም የሚያደርጓቸው እንቅስቃሴዎች መኖሩን ያስረዳል። ሳይበር የተለያዩ ተዋናዮችን እኩል የሚያደርግ ምህዳር በመሆኑ ይህ ቲዎሪ በሀገራት ብቻ ሳይሆን በተቋማት እና በግለሰቦች ዋቅም ላይ እንዲውል ያደርገዋል።

ቢሮክራሲያዊ ፖለቲካ ቲዎሪ (Bureaucratic Politics Theory) በሳይበር ምህዳሩ ግለሰቦች እና ተቋማት ጠንካራ ተዋንያን እንደሆኑ ያስረዳል። የተቋማት ጥንካሬ በመንግስታዊ አካል ከሚደረግላቸው ድጋፍ እና ማዕቀብ ጋር የሚያያዝ ሲሆን በግለሰቦችና ቡድኖች በኩል ደግሞ ዕውቀቱና ችሎታው ያላቸው ግለሰቦች ከፍተኛ አቅም ካለው ሀብት ጋር ሲጣመሩ የሚገኝ ነው። እነዚህ ተቋማት በተለይም የመከላከያ እና የመረጃና ደህንነት ለመንግስታት ተጠሪና አንዳንዴም በቀጥተኛ መንግስታዊ ትዕዛዝ የሚንቀሳቀሱ በመሆናቸው ተጠያቂነቱ ከዚህ ጋር ይያያዛል።[26] ተቋማዊ ፖለቲካ ቲዎሪ (Organizational Politics Theory) የሳይበር ተዋናዮች በሚሰሩበት ተቋም ተቋማዊ ባህል መንገዶች፣ አቅሞች እና ውሱንነቶች የሚመነጭ ስልጣን እና ገደብ እንደሚኖርባቸው በማስረዳት ስለማንነታቸው፣ ስላላቸው አቅም እና ፍላጎት መረዳት እንድንችል ያስችለናል። ሁሉንም የሚያስማማ ባይሆንም በሳይበር ዓለም ብሎም በቁሳዊው ዓለም

[24] Howard Kleinberg, "Building a Theoretical Basis for Cyber Security Best Practices," Annals of the Master of Science in Computer Science and Information Systems at UNC Wilmington 9, no. 2 (2015).

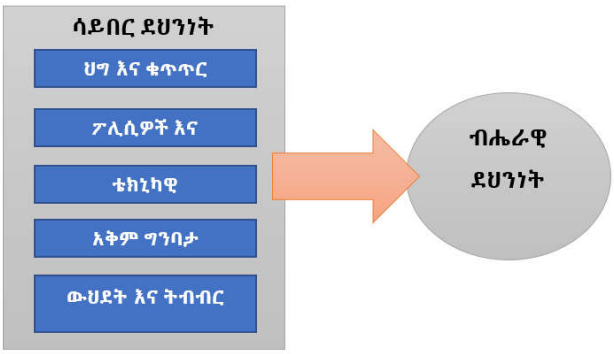
[25] Kleinberg.

[26] Kleinberg.

ከፍተኛ ተጽዕኖ ማድረስ የሚቻለው በዚህ ደረጃ ነው። ስለዚህም የተቋማት ባህል፣ የኦፕሬሽን ባህሪ፣ ፖሊሲ፣ የአሰራር ስርዓት፣ የአመራር እና ሰራተኞች አመለካከት እና ሀብቶች ወደ ሳይበር ደህንነት መፍትሄዎች በማዞር እና ምርጥ ተሞክሮን በመከተል ውጤታማ መሆን ይችላሉ።

በመጨረሻም የግለሰባዊነት ቲዎሪ (Indivisualism Theory) አንድ ግለሰብ ብቻውን ወይም መንግስታዊ ወይም መንግስታዊ ባልሆነ ተቋም በቁሳዊው ዓለም ካለው በላይ የሳይበር ስጋት ሊሆን እንደሚችል ያስረዳል። በሳይበር ምህዳር የሚንቀሳቀስ ግለሰብ ከፍተኛ የመሪነት ኃይል በማግኘት፣ ከምክንያታዊነት በመራቅና ኢ-ተገማች በመሆን የሳይበር ደህንነት ኃይል ወይም የሳይበር ስጋት ኃይል እንዲሆኑ ያስችላል። በዩበልጥም የአንድ ግለሰብ የማሰብ፣ ምክንያታዊነት፣ ብቃት፣ ንቃት እና ዓላማ እና የሚወስዳቸው እንቅስቃሴዎች አስፈላጊ ናቸው። የሳይበር ጦርነት አቅም ያለው ግለሰብ ተመሳሳይ ዓላማና አመለካከት ካላቸው ኃይሎችን በተለይም ለዚህ የተመደበ ሀብት ያላቸው ተቋማትን በመቀላቀል የሳይበር ኦፕሬሽን ቢያካሂድ ትልቅ ተጽዕኖ ማምጣት ይችላል። ስለዚህም በዚህ ደረጃ የሚደረግ ትንተና በሰፊው የሳይበር ደህንነት ቲዎሪን ያብራራል።[27]

ለዚህ ጥናት ማሳያ እንዲሆን ሳይበር ደህንነት በብሔራዊ ደህንነት ላይ ያለው አንድምታ የሚያሳይ ሞዴል በምስል 2 ቀርቧል። ይህ ሞዴል ነጻ ተለዋዋጮች (ማለትም የሳይበር ደህንነት ገጽታዎች) በጥገኛ ተለዋዋጭ (ማለትም በብሔራዊ ደህንነት) ላይ ያላቸውን ተጽዕኖ ያሳያል። እነዚህ የሳይበር ደህንነት ገጽታዎች የሳይበር ደህንነት መገለጫ ሲሆኑ የህግ እና ቁጥጥር፣ ተቋማዊ አደረጃጀት፣ ቴክኒካዊ መቆጣጠሪያዎች፣ አቅም ግንባታ ጥረቶች፣ እንዲሁም ትብብርን ያካትታሉ። ሳይበር ደህንነት ብሔራዊ ደህንነት ላይ ተጽዕኖ ያደርሳል ማለት ደግሞ የሀገራትን ብሔራዊ ደህንነት መሳሪያዎች (ማለትም ዲፕሎማሲያዊ፣ የመረጃ፣ ወታደራዊ እና ኢኮኖሚያዊ) ሚዛንን በማዛባት የአንድን ሀገር ብሔራዊ ጥቅም ይነካል ማለት ነው።



ምስል 2: የጥናቱ ንድፈ ሀሳባዊ ማዕቀፍ

3 የተዛማጅ ጽሁፍ ዳሰሳ

ኢትዮጲያ የረጅም ጊዜ ታሪክ፣ ጥበብ እና ሀገር በቀል ያላት ሀገር ስትሆን በ2020 እ.ኤ.አ መጨረሻ 115 ሚሊዮን የሚሆን ትልቅ እና በማደግ ላይ ያለ ህዝብ ያላት ሀገር ናት (United Nations Statistics Division, 2020 Est.). የኢንተርኔት ተጠቃሚው ቁጥር በ 2000 እ.ኤ.አ ከነበረው 10,000 በ 2019 እ.ኤ.አ 20 ሚሊዮን የደረሰ ሲሆን ይህም ባለፉት ሀያ ዓመታት የኢንተርኔት ዕድገት ፍጥነቱ በመቶኛ ከ200 ሺህ በላይ እንዲሆን አስችሎታል። በ 2020 እ.ኤ.አ ያለው የኢንተርኔት ተጠቃሚ ከአጠቃላይ ህዝቡ 17.8% (23.8 ሚሊዮን) (ወይም እንደ ኢትዮ ቴሌኮም ሪፖርት 20.7%) ሲሆን ይህ ቁጥር በከፍተኛ ፍጥነት በማደግ ላይ ይገኛል። ከማኅበራዊ ሚዲያ አንጻር እስከ 2019 እ.ኤ.አ መጨረሻ የፌስቡክ ተጠቃሚ ኢትዮጲያውያን ቁጥር 6 ሚሊዮን እንደሆነ ይገመታል።[28]

በ 2014 እ.ኤ.አ ከንፈ ሚካኤል የኢትዮጲያን የሳይበር ወንጀል ህግ እና ተፈጻሚነት ዕድገት በዳሰሱበት ጽሁፍ አንድ ወጥ የሳይበር ወንጀል ስርዓትን አስፈላጊነት እንደ ምክረ ሀሳብ አቅርበዋል። በጽሁፉ እያደገ ለመጣው የ ICT አገልግሎት ሽፋን የኢትዮጲያን የአጸፋ የህግ እርምጃዎች የተቃኙ ሲሆን በሌሎች የአፍሪካ ሀገራት አንጻር ተወዳዳሪ የሚባል እንዳልሆነ ተጠቁሟል። ጸሀፊው በመጀመሪያ የዳሰሱት የ 2004 እ.ኤ.አ የወንጀል ህግ ሲሆን በወቅቱ በቂ የማስረጃ አሰባሰብና ህጉን

[27] Kleinberg.

[28] Internet World Stats, “Internet World Stats: Usage and Population Statistics,” Internet World Stats, 2018, https://www.internetworldstats.com/.

ለማስፈጸም የሚያስችል አሰራር ባለመኖሩ የፍርድ ሂደቱን አስቸጋሪ አድርጎታል ሲሉ ይገልጻሉ። በመቀጠልም በወቅቱ ረቂቅ የነበረውንና በአሁኑ ወቅት በስራ ላይ ያለውን የ 2016 እ.ኤ.አ የሳይበር ወንጀል ህግ ከሌሎች ቀጠናዊ እና ሀገራዊ ህጎች አንጻር በመገምገም ዘመናዊ ሊባል የሚችል እና በሳይበር ወንጀል ቤንች ማርክ መሳሪያዎች መረጃ ላይ የተመሰረተ መሆኑን ይገልጻሉ። ነገር ግን ተበታትኖ ያለውን ህግ ወደአንድ ማምጣት አስፈላጊነት የኮፒ ራይት፣ የጸረ ሽብር፣ የማስታወውቂያ እና የቴሌኮም ማጭበርበር እንደ ምሳሌ በማንሳት ያስረዳሉ። በተጨማሪም ያልተዳሰሱ የሳይበር ወንጀሎች እንዳሉ ‘ወሲብን በቪዲዮ በመቅረጽ ለበቀል ዓላማ ማዋል’፣ ከንግድ ህግ እና ሌሎች ግለሰባዊ መረጃን ከመጠበቅ አንጻር ረቂቁ ክፍተቶች እንዳሉበት ያስረዳሉ። በመጨረሻም የምርመራ ሂደቱ የህግ ተርጓሚ እይታ ያለው መሆኑ መልካም ቢሆንም ለብርበራ፣ በቁጥጥር ስር ለማዋል፣ ለክትትል የፍርድ ቤት ማዘዣ አስፈላጊ መሆኑን በተለይም ለኢመደአ የሰጠው ስልጣን አሳሳቢ እንደሆነ ይገልጻሉ።[29]

በ 2015 እ.ኤ.አ ሀለፎም ሳይበር ወንጀልን ለመቀነስ የሚደረገው ጥረት ከፖሊሲ፣ ከተቋማት፣ ከህግ አንጻር በቂ አለመሆኑን ይገልጻሉ። የጥናቱ ተሳታፊዎች ሳይበር ወንጀል መሰረታዊ ችግር መሆኑን እና ዋነኞቹም ማልዌር እና የዌብሳይት ገጽታ ማበላሸት እንደሆነ ያሳያል። ጸሀፊው ከጥቂት ባንኮች በስተቀር አብዛኞቹ ተቋማት ሳይበር ደህንነት ቡድን እንደሌላቸውና የሳይበር ደህንነት አመራር ስርዓት አለመኖሩ የተቋማቱን ዝግጁነት ማነስ ያሳያል በማለት ይገልጻሉ። በጥናቱ ጥቃት እንደተፈጸመ የሚያውቁበት ስርዓት ካለመኖሩ በተጨማሪ የደረሱ ሳይበር ወንጀሎች ለህግ አስከባሪ አካላት ሪፖርት የማይደረጉ ሲሆን 25.7% የሚሆኑት ከባንክ ማጭበርበር ጋር የተገናኙት ብቻ ሪፖርት እንደሚደረጉ ገልጸዋል። ለዚህም አንዱ ምክንያት የህግ አስከባሪ አካላት አቅሙ እንደሌላቸው በማሰብ ሲሆን ሌላኛው ተቋማቱ መልካም ስማቸው እንዳይጠፋ በመፍራት ነው። 22.9% የሚሆኑት ተቋማት በቂ የህግ ማዕቀፍ አለመኖሩን የገለጹ ቢሆንም አብዛኞቹ ተሳታፊዎች የ ICT ፖሊሲ እና የሳይበር ወንጀል ህግ ስለመኖሩ የማያውቁ መሆናቸው ሰፊ የግንዛቤ ክፍተት እንዳለ ያሳያል። ጸሀፊው በኢትዮጲያ ያሉ ለሳይበር ወንጀል ሊውሉ የሚችሉ አሰር ማልዌር የያዙ ዌብሳይቶችን እንደማሳያ አቅርበዋል።[30]

የፖሊሲ ምላሽ የ2009 እ.ኤ.አ የብሔራዊ ICT ፖሊሲና ስትራቴጂ፣ የዕድገትና ትራንስፎርሜሽን ዕቅድ፣ የ2011 እ.ኤ.አ የብሔራዊ ኢንፎርሜሽን ደህንነት ፖሊሲን እንዲሁም 2011 እ.ኤ.አ የወንጀልና ፍትህ ፖሊሲ ያካትታል። የተቋማዊና ቁጥጥር ስርዓቶችን በተመለከተ ኢመደአ ከብሔራዊ የኮምፒዩተር አደጋ ምላሽ ክፍል በተጨማሪ በሌሎች መንግስታዊ ተቋማት ተመሳሳይ አቅም መፍጠር፤ በፖሊስና አቃቤህግ ልዩ የሳይበር ወንጀል ክፍሎችን ማቋቋም እንዲሁም ልዩ የፍርድ ሸንጎ አስፈላጊ መሆናቸውን ጠቁመዋል። በተጨማሪም የ2012 እ.ኤ.አ የቴሌኮም ማጭበርበር ወንጀል አዋጅ ብሔራዊ ቴክኒካዊ ግብረ ሀይል እንደሚቋቋም ነገር ግን እነዚህ ተቋማዊ እርምጃዎች በወቅቱ እንዳልተወሰዱ ይገልጻል።[31]

ከህግ ማዕቀፍ አንጻር የ1961 እ.ኤ.አ የወንጀለኛ መቅጫ ህግ ስርዓት አለመሻሻል፤ ሌሎች የህግ እና የልምድ ውሱንነቶች፤ እንዲሁም በህግ አስፈጻሚ ተቋማት ያለ የህብት እና የዕውቀት ውሱንነት የሳይበር ወንጀልን ምርመራ እና ወንጀለኞችን ተጠያቂ ለማድረግ የማያስችል እንዳደረገው ይገልጻሉ። እንደ አሳሳች የኮምፒዩተር መልዕክቶች እና ማልዌር ፈጽሞ ወደ ፍትህ ስርዓት እንዳልደረሱ ነገር ግን በጣም ጥቂት የባንክ ማጭበርበር ወንጀሎች ወደ ፍርድ ሂደቱ ሌሎች ህጎችን በመጠቀም እንደሆነ (ለምሳሌ “ስልጣንን ያለአግባብ በመጠቀም”) ወይም ማስረጃ በማጣት መዝገቡ እንደሚዘጋ ያስረዳሉ። እንደ ጸሀፊው ገለጻ ምንም እንኳ የሳይበር ወንጀል ህጉ በቂ ነው ባይባልም የህግ አስከባሪ አካላት ያሉትን የሳይበር ወንጀል ህጎች ለማስፈጸም እንዳልቻሉ ያስረዳሉ። የ2016 እ.ኤ.አ የሳይበር ወንጀል ህግ ያለፉትን የሳይበር ወንጀል ህጎች የሚሽር በአንጻራዊነት የተሟላ ሊባል የሚችል እንደሆነ ይገልጻሉ። የዚህ ህግ መሰረታዊ መርህ ከቴክኖሎጂ ጥገኝነት ነጻ መሆን፤ ሆን ተብሎ የሚፈጸም ወንጀልን በመቅጣት እንዲሁም ባለማወቅ እና በየዋህነት የሚፈጸሙ ወንጀሎችን ቅጣት ማቅለል፤ የሦስተኛ ወገን የወንጀል ተጠያቂነት ለመወሰን እንዲሁም አለማቀፋዊነትን ያካተተ በመሆኑ የተሻለ እንደሚያደርገው ይገልጻሉ።[32]

በ2019 እ.ኤ.አ አቤኔዘር በሀገራዊ እና ተቋማዊ ደረጃ የሳይበር ደህንነት ስትራቴጂ ቀረጻ እና ትግበራ አስፈላጊነት በጽሁፉ አስረድቷል። ለዚህም የሀገሪቱ ከፍተኛ አመራር አለማቀፋዊ ማዕቀፎችን እና ወጥ የሆኑ መምሪያዎችን በመጠቀም ለሀገሪቱ እንዲሆን በማድረግ ከሀገሪቱ ራዕይ፣ መመደብ ከምትችለው ሀብት እንዲሁም ቅድሚያ ከምትሰጣቸው ጉዳዮች አንጻር ማጣጣም እንደሚቻል ይገልጻሉ። በጥናቱ ከግል እና ከመንግስት ዘርፎች መረጃን በመሰብሰብ የሀገሪቱን የ ICT ከባቢ በመረዳት፤ እንዲሁም አለማቀፍ ድጋፍ፣ የሌሎች ሀገራት ተሞክሮ እንዲሁም በዘርፉ ካሉ ባለሙያዎች የተገኘ ዕውቀትን በመተንተን ለብሔራዊ ሳይበር ደህንነት ስትራቴጂ መምሪያ የሚሆን ምክረ ሀሳብ አቅርበዋል። በሀገሪቱ ያሉ የሳይበር ደህንነት

[29] Yilma Kinfe Micheal, “ScienceDirect Developments in Cybercrime Law and Practice in Ethiopia,” Computer Law & Security Review 30, no. 6 (2014): 720–35, https://doi.org/10.1016/j.clsr.2014.09.010.

[30] Hailu Halefom, “The State of Cybercrime Governance in Ethiopia,” no. May 2015 (2015): 1–35.

[31] Halefom.

[32] Halefom.

ችግሮችን ለመፍታት በሌሎች ሀገራት እንደሚደረገው ከሀገሪቱ ሁኔታዎች ጋር ሊጣጣም የሚችል እና ከዘርፉ ተለዋዋጭነት ጋር ሊሄድ የሚችል የብሔራዊ ሳይበር ደህንነት ስትራቴጂ በጣም ወሳኝ መሳሪያ እንደሆነ መከራከሪያቸውን ያቀርባሉ።[33]

በ2019 እ.ኤ.አ ባራኪ በኢንተርኔት የሚፈጸም የጥላቻ ንግግሮች ስርጭት በተለያዩ ማኅበረሰቦች መካከል መቻቻልን በማጥፋት፣ አለመተማመንና ልዩነትን በማስፋፋት አፍራሽ እየሆነ መምጣቱን ይገልጻሉ። ከዚህ ጋር በተያያዘ ሁኔታ የሰዎች ህይወት መጥፋት፣ የህዝቦች ከቀያቸው መፈናቀል ወይም ስነ-ልቦናዊ ጫናዎች መድረስ እና በሀገር አቀፍ ፈተናዎች ኩረጃ እንዲስፋፋ ማድረጉን ይገልጻሉ። ጸሀፊው በመንግስት የሚወሰዱ እርምጃዎች ህጋዊ እና ኢኮኖሚያዊ ያልሆኑ ናቸው በማለት የጥላቻ ንግግር ፈጻሚውን አካል ብቻ ለይቶ አሁን ባለው የኢትዮጲያ የህግ ማዕቀፍ ማከናወን እንደሚቻል ያስረዳሉ። ከዚህ በተቃራኒ የሚኒስትሮች ምክር ቤት በ75ኛው መደበኛ ስብሰባው የጥላቻ ንግግር ህግን በማጽደቅ ወደ ህዝብ ተወካዮች ምክርቤት መርቶታል።[34] ባለፉት አምስት ዓመታት የሳይበር ሚዲያ ጥላቻ ንግግር እየጨመረ መሄዱ ብዙኃኑን የሚያስማማ ሲሆን ይህም ፖለቲካዊ እና ማህበረ ስነ-ልቦናዊ ቀውስ በመፍጠር ለመቀልበስ የሚያስቸግር ሁኔታን ይፈጥራል።[35]

ለዚህም መፍትሄው ሁሉን አቀፍ እና አሁን ካለው የህግ ስርዓት ጋር የተዋህደ ከጊዜያዊ ይልቅ ዘላቂነት ያለው የሳይበር ወንጀል የህግ እና ቁጥጥር ማዕቀፍ መቅረጽ እና በቁርጠኝነት ማስፈጸም ይገባል። በህግ እና ቁጥጥር ብቻ ሳይሆን በአሰራር ስርዓቶች፣ በሰው ኃይል እንዲሁም በቴክኖሎጂ አቅም የሚታዩ ክፍተቶችን ለመለየት እና ለመድፈን የሚያስችል ጥረት ማድረግ አስፈላጊ ነው። በተጨማሪም ከሳይበር የሚመጣ ስጋትን ለመከላከል የሚያስችል የትብብርና ቅንጅት ሁኔታ መዳበስ እንዲሁም ማመላከት አስፈላጊ ነው። ይህም ጥናት እነዚህን ክፍተቶች ለመድፈን የሚያስችል ጥረት አንድ አካል ተደርጎ ሊወሰድ ይችላል።

4 የጥናቱ ንድፍ እና ዘዴ

ይህ ጥናት ጥናቱ በሚካሄድበት ወቅት ያለውን የሳይበር ደህንነት ሁኔታ እንዲሁም በብሔራዊ ደህንነት ላይ ሊያሳድር የሚችለውን ተጽዕኖ በመተንተን ለቀጣይ ጊዜያት ጠቃሚ የፖሊሲ አቅጣጫን ማመላከት ነው። የጥናቱ ዘዴ ቅይጥ ሲሆን ይህም ከአይነታዊ እና መጠናዊ ዘዴዎች ሁለት የተለያዩ ዘዴዎችን ለመጠቀም ያስችላል። ይህን ጥናት አይነታዊ እና መጠናዊ ትንተናን በአንድ ውቅር በማድረግ ለማካሄድ ተችሏል። ከመጠይቅ እና ከፊል ቃለምልልስ የተገኙ ዳታዎች ለመጠናዊ ትንተና እንዲሁም ጥናቱ ከሚዳሰሳቸው ተቋማት መካነድር፣ የዜና ምንጮች እንዲሁም ከቃለምልልስ የተገኙትን ዳታዎች ለአይነታዊ ትንተና በመጠቀም ጽንሰሀሳባዊ እና ንድፈሀሳባዊ ዘዴዎች እና መንገዶች በመከተል ለጥናቱ ጥያቄዎች ምላሽ ለማግኘት የሚያስችል መላምት በማቅረብ ትንተና ተደርጓል።

የዳታ ምንጮች

በዚህ ጥናት የሳይበር ደህንነት ወይም ብሔራዊ ደህንነት ተልዕኮ ያላቸው ተቋማት ከፍተኛ አመራር ለቃለምልልስ፣ መካከለኛ አመራር ለቃለምልልስ እና ለመጠይቅ እንዲሁም ዝቅተኛ አመራር እና ባለሙያዎች ለመጠይቅ ዳታ አሰባሰብ ዘዴዎች ተሳታፊ ናቸው። እነዚህም የሀገር መከላከያ ሚኒስቴር፣ የኢንፎርሜሽን መረብ ደህንነት ኤጀንሲ፣ የውጭ ጉዳይ ሚኒስቴር፣ እና የፋይናንስ መረጃ ማዕከል ሲሆኑ ሌሎች ተቋማትን ለማካተት ጥረት የተደረገ ቢሆንም በተለያየ ምክንያት አልተሳካም። በዚህም መሰረት ከአስራ ሁለት ተሳታፊዎች ጋር ቃለምልልስ በማድረግ መረጃ የተሰበሰበ ሲሆን ከአርባ አራት ተሳታፊዎች ደግሞ የመጠይቅ ዳታ ለመሰብሰብ ተችሏል። ይህም ለጥናቱ እንደ መጀመሪያ ደረጃ ዳታ ምንጭ በመሆን ጥቅም ላይ ውሏል። ከኢንተርኔት የተገኙ ሰነዶች፣ ዜናዎች እንዲሁም በተቋማቱ መካነድሮች የሚገኙ መረጃዎች ደግሞ ለጥናቱ እንደ ሁለተኛ ደረጃ የዳታ ምንጭ በመሆን አገልግለዋል።

ናሙና እና የንሞና ዘዴ

ተቋማዊ ሳይበር ደህንነት የሁሉም የተቋሙ ሰራተኞች ጉዳይ ሲሆን ሊረጋገጥ የሚችለው በየደረጃው በሚገኙ የተቋሙ ሰራተኞች ተሳትፎ ነው። ይህ ግንዛቤ ሊኖር የሚገባ ቢሆንም ነገር ግን እያንዳንዱ ሰራተኛ በብሔራዊ ደህንነት ላይ እንዳለው ሀላፊነት ደረጃ እና የስራ ድርሻ መጠን የተለያየ ተጽዕኖ ሊያመጣ ይችላል። እያንዳንዳቸው ጥናቱ የሚዳሰሳቸው ተቋማት በመቶዎች

[33] Weldegiorgis Abenezer Berhanu, “Developing National Cybersecurity Strategy for Ethiopia,” National Security Office (Tallinn University of Technology, 2019).

[34] Zemedkun Baraki Belay, “The Prosecution of Criminal Conducts Committed over Social Media’s in Ethiopia: Acts of ‘Hate Speech’ in Focus” (University of Gondar, 2019).

[35] Ethiopian Press Agency, “Hate Speech and Freedom of Expression in Ethiopia | Ethiopian Press Agency,” Ethiopian Press Agency, 2019, https://www.press.et/english/?p=5520#.

ወይም በሺዎች የሚቆጠሩ ሰራተኞች ቢኖሯቸውም ለዚህ ጥናት አላማ እና ሁሉንም ለማሳተፍ የማይቻል በመሆኑ ወሳኝ የሆኑትን ተሳታፊዎች አላማ ተኮር የንሞና ዘዴ በመጠቀም ተለይተዋል። በዚህም የንሞና ዘዴ ለጥናቱ በአንጻራዊነት አስፈላጊ የሆኑትን የስራ ክፍሎች በመለየት አመራር እና ባለሙያዎች ተሳታፊ እንዲሆኑ ተደርጓል። የመለያ መስፈርቱም ከስትራቴጂያዊ አመራር፣ መካከለኛ አመራር፣ ዝቅተኛ አመራር እና ባለሙያዎች ስብጥር ያለው እና መሰረታዊ የሳይበር ደህንነት ግንዛቤ ያላቸውን እንዲሁም የሳይበር ደህንነት ኃላፊነት ያላቸውን ተሳታፊዎች ያካተተ ነው።

በዚህም 8 ከፍተኛ አመራር፣ 35 መካከለኛ አመራር እንዲሁም 70 ዝቅተኛ አመራር እንዲሁም 19 ባለሙያዎችን ያካተተ ነው። የዒላማ ህዝብ ብዛት 132 ነው። ለቃለምልልስ 4 ከፍተኛ አመራር፣ 8 መካከለኛ አመራር በአጠቃላይ 12 ተሳታፊዎች የተለዩ ሲሆን ለመጠይቅ 4 ከፍተኛ አመራር፣ 15 መካከለኛ አመራር 25 ከዝቅተኛ አመራር እንዲሁም ባለሙያዎችን በአጠቃላይ 44 ተሳታፊዎች ተለይተዋል። የእነዚህ ተሳታፊዎች ሀላፊነት ዋና የኢንፎርሜሽን ኦፊሰር፣ ዋና የኢንፎርሜሽን ደህንነት ኦፊሰር፣ ዋና የቴክኖሎጂ ኦፊሰር፣ ዋና የኢንፎርሜሽን የቴክኖሎጂ ኦፊሰር፣ የምርምርና ልማት ሀላፊ እንዲሁም የተመረጡ የስራ ሂደቶች የኦፕሬሽናል ክፍል ሀላፊዎች እንዲካተቱ ተደርጓል። የሳይበር ደህንነት ባለሙያዎች በሌሎባቸው ተቋማት የኢንፎርሜሽን ቴክኖሎጂ ባለሙያዎች ተሳታፊ ሆነዋል። የጥናቱ ናሙና በጥናቱ ዓላማ እና ከተቋማቱ ተወካዮች በተገኘ ምክረሀሳብ መሰረት በአጥኚው ተለይተዋል። በዚህ አይነት ከየተቋማቱ አስፈላጊ በየደረጃው ያሉ የሳይበር ደህንነት አመራሮች እና ባለሙያዎች ተሳታፊ እንዲሆኑ ተደርጓል።

የዳታ አሰባሰብ ዘዴ

በዚህ ጥናት ቅይጥ የጥናት ዘዴ ጥቅም ላይ የዋለ ሲሆን ለዚህም ከተለዩት የዳታ ምንጮች በቃለ ምልልስ እና በመጠይቅ ዳታ ተሰብስቧል። የቃለምልልሱ ዓላማ አጠቃላይ የሳይበር ደህንነት ሁኔታን ለመረዳት በሚያስችል መልኩ የተዘጋጀ ሲሆን 12 ተሳታፊዎች ለየብቻ ለ ሁለት ሰዓት የሚቆይ ቃለምልልስ አድርገዋል። እንደ ተቋማቱ መዋቅር እና አደረጃጀት ሁኔታ በጥናቱ ከተሳተፉ ተቋማት ከአንድ በላይ መካከለኛና ከፍተኛ አመራሮች የቃለመጠይቁ ተሳታፊ ሆነዋል። የመጠይቁ ዓላማ ደግሞ የህብት አያያዝ አቅም፣ የስጋት ትንተና አቅም እንዲሁም የሳይበር ደህንነት እና የክስተት አስተዳደር ሁኔታዎችን የሚዳስስ ሲሆን በአጠቃላይ 44 ተሳታፊዎችን ያካተተ ነው። መጠይቁን 41 ተሳታፊዎች የመለሱ ሲሆን ይህም 92.3% የምላሽ ምጣኔ ነው። የቃለምልልሱ ጥያቄዎች በአብዛኛው ደረቅ ጥያቄዎች ሲሆኑ የመጠይቁ ጥያቄዎች ደግሞ በአመዛኙ የምርጫ ጥያቄዎች ናቸው። ከዚህ በተጨማሪ ከኢንተርኔት የዳታ ምንጮች የተገኙ ስታቲስቲካል እና መጠናዊ ዳታዎች፣ አዋጆች እና ሌሎች የህግ እና ቁጥጥር ሰነዶች ከማኅበራዊ ሚዲያ እና የዜና ምንጮች የተገኙ መረጃዎች እንደ ደጋፊ የዳታ ምንጭ ተወስደዋል። የዳታ ጥራት ለማረጋገጥ እንዲቻል የመጀመሪያ ደረጃ ዳታ ከሁለተኛ ደረጃ ዳታ እንዲሁም ከሌሎች ተመሳሳይ ጥናቶች ውጤቶች ጋር በማነጻጸር እንዲሁም በተወሰኑት ተቋማት ምልከታን በማድረግ እንዲሁም የቃለምልልስ እና መጠይቅ ምላሾችን በመፈተሽ ጥረት ተደርጓል።

የዳታ ትንተና ዘዴ

ለዚህ ጥናት የተሰበሰበውን ዳታ ለመተንተን አይነታዊና መጠናዊ የትንተና ዘዴዎች በአንድ ላይ በማዋቀር የአንዱን ትንተና ውጤት ከሌላው ጋር በማነጻጸር ቀርቧል። በአይነታዊ ትንተና የይዘት ትንተና እና የተረከ ትንተና በማድረግ ከቃለምልልስ ምላሾች ትርጉም ለመስጠት ተችሏል። ለእያንዳንዱ ተቋም የተሰበሰቡ ቃለምልልሶችን ወደ ጽሁፍ በመቀየር እና ከአንድ በላይ ተሳታፊ ሲኖር በመጀመሪያው ላይ በመጨመር ተቋማዊ ምላሽ ለማግኘት ተችሏል። በመቀጠል በሀገራዊ እና ተቋማዊ ደረጃ ያለውን ተጽዕኖ በመለየት በሁለት ደረጃ ትንተና ለማድረግ ተችሏል። በተጨማሪም ከተለያዩ ምንጮች የተገኙ ሰነዶች በመጠቀም የቃለምልልስ ምላሾችን ትንተና ለማጠናከር ውሏል። መጠናዊ ትንተና የማብራሪት ትንተና በመጠቀም ምላሾችን በየፊርጁ የመሰብሰብ እና ድግግሞሽ እና በመቶኛ በማስላት ጥቅም ላይ ውሏል። ይህም SPSS ሶፍትዌር በመጠቀም የተተገበረ ሲሆን አይነታዊ ዳታ እና የተለያዩ ሰነዶችን በመጠቀም ትንተናውን ውጤት ወደ አንድ ድምዳሜ ለማድረስ ተችሏል።

የተገኙ ውጤቶች እና ውይይት

በዚህ ክፍል በጥናቱ የተገኙ ውጤቶች የሚቀርቡ ሲሆን የጥናቱ ግኝት በሀገራዊ (በፌዴራል መንግስት) ደረጃ እና ተቋማዊ (የብሔራዊ ደህንነት እና ሳይበር ደህንነት ተቋማት) ደረጃ እንዲሁም ለህዝቡ ያለውን አንድምታ ያሳያል። ውይይቶቹ ደግሞ የቃለምልልስ፣ መጠይቅ፣ መዛግብት እና ሌሎችም መረጃዎች ትንተና መሰረት በማድረግ እንዲሁም ምርጥ ተሞክሮዎችን በመውሰድ የተገኙ ውጤቶቹን ተከትለው ይቀርባሉ።

በብሔራዊ ደህንነት ላይ የሳይበር ደህንነት ሚና

በውሳኔ ሰጪ አካላት እንዲሁም በአስተዳደር እና ኤክስፐርቶች ዘንድ ሳይበር ደህንነት በብሔራዊ ደህንነት ውስጥ ያለውን ሚና መረዳት ለኢትዮጲያ ብሔራዊ ደህንነት ትልቅ አስተዋጽዎ አለው። ይህም የሚያስፈልገውን ጥረት ለመለየት፣ ግቦችን ለማስቀመጥ እና ለማሳካት የሚያስችለውን ህብት ለመመደብ የሚረዳ ሲሆን በሀገራዊ፣ በዘርፍ እና በተቋም ደረጃ ቀጣይነት ያለው ጥረት ማድረግን ይጠይቃል። አንድ የጥናቱ ተሳታፊ በሀገራዊ አመራር ዘንድ ጥሩ ግንዛቤ እንዳለ እና ይህ ግንዛቤ ኢመደአን ሙሉ ለሙሉ የሳይበር ደህንነት ተልዕኮን ይዞ ለማቋቋም እንዳስቻለ ይገልጻሉ። ከዚህ ቀደም በነበሩ ጊዜያት

ኢትዮጲያ ሳይበር ደህንነትን በተመለከተ ሁሉን መንግስታዊ ተቋማት ያካተተ አካሄድ ከመከተል ይልቅ ኢመደአን በማቋቋም ኤጀንሲን መሰረት ባደረገ ሁኔታ ስትንቀሳቀስ ቆይታለች። ነገር ግን ከቅርብ ጊዜ ወዲህ ከሳይበር የሚመጣን ስጋት ለመከላከል ይህ ብቻውን በቂ እንዳልሆነ በመረዳት ሁሉን አቀፍ እንቅስቃሴ ማድረግ አስፈላጊ መሆኑ ታምኖበታል።

የ2002ቱ (እ.ኤ.አ) የውጭ ጉዳይ እና የብሔራዊ ደህንነት ፖሊሲና ስትራቴጂ የኢትዮጲያን ብሔራዊ ጥቅሞች እና የብሔራዊ ደህንነት ጉዳዮች እንዲሁም ውስጣዊና ውጫዊ ስጋቶች እና የተጋላጭነት ደረጃ የሚገልጽ ሰነድ ተደርጎ ሊወሰድ ይችላል።[36] የሀገሪቱ ከፍተኛ አመራር ፖለቲካዊ፣ ኢኮኖሚያዊ እና ወታደራዊ እንቅስቃሴዎች የሚደረጉበትን ሳይበር ምህዳርን ደህንነት የመጠበቅን አስፈላጊነት መረዳት እንዲሁም ሳይበር እንደ አምስተኛ አውድ አድርጎ መቀበል በቀጥታ ሳይበር የሀገሪቱ የብሔራዊ ደህንነት እና የጦርነት ጉዳዮች አንድ አካል ተደርጎ ለመታየቱ ማሳያ ነው። የሳይበር ደህንነት አመራሮችም በወረቀት ይሰሩ የነበሩ ስራዎች ወደ ኮምፒዩተር መሄዳቸውን እና መረጃ በሚቀመጥ ወይም በሚጓጓዝ ወቅት ጥቃት ፈጻሚዎች ጉዳት ሊያደርሱበት እንደሚችሉ በመረዳት ሀብቶችን በመለየት ሁልጊዜ አስፈላጊውን ጥበቃ ያደርጋሉ። አንድ ተሳታፊ እንዲህ ሲሉ ይገልጻሉ ፦

> “ሁሉም የመንግስት አገልግሎቶች እና እንቅስቃሴዎች ከኢንተርኔት በተገናኘ ወይም ብቻውን ባለ ኮምፒዩተር የሚፈጸሙ ናቸው። አብዛኛው የመንግስት ሰራተኞች ስማርት ስልክ እና ላፕቶፕ ከእነዚህ ኮምፒዩተር ጋር የመገናኘት ሰፊ ዕድል አላቸው። በተጨማሪም ከኢንተርኔት ጋር ተያያዥነት ያላቸው የግል እና የተቋሙን ስራ ለመፈጸም የሚያስችሉ አገልግሎቶችን ይጠቀማል። ስለዚህም የመንግስት ተቋማት ተልዕኮዎቻቸውን ለመፈጸም የሚጠቀሙባቸው ለምሳሌም ባንኮች እና ቴሌኮም ከፍተኛ የሳይበር ደህንነት ተጋላጭነት አላቸው ተጠቃሚው በቂ የሳይበር ደህንነት ስልጠና አለማግኘቱ ደግሞ ችግሩን የከፋ ያደርገዋል። የዚህ ውጤትም ግለሰቡን፣ ተቋሙን አንዳንዴም ሀገርን እና የሀገርን ጥቅም የሚጎዳ ይሆናል።”

ስለዚህም ሳይበር የስህበት ማዕከል እየሆነ እንደመጣ በመረዳት ከጥቃት ፈጻሚዎች የተሻለ አቅም ለመገንባት ጥረት እየተደረገ ይገኛል። ለምሳሌ በቀድሞ ጊዜ የሰብዓዊ መረጃ አቅምን በመጠቀም የመረጃ የበላይነትን መያዝ የፖለቲካ የበላይነትን ለማግኘት የሚያስችል ነበር። ነገር ግን ዓለም በአሁኑ ወቅት የሳይበር መረጃ ውጤታማ የመረጃ ብሎም የፖለቲካ የበላይነትን እንደሚያስገኝ በመረዳት ተግባራዊ እያደረገው ይገኛል። በኢትዮጲያ ምንም እንኳ በመሬት ላይ የሚደረግ ጦርነት ከሃያ አመታት በላይ ያስቆጠረ ቢሆንም በነዚህ ጊዜያት ብሔራዊ ደህንነትን የሚጎዱ የሳይበር ዘመቻዎች ግን አልተደረገም ለማለት አስቸጋሪ ነው።

በቁልፍ የICT መሰረተ ልማት እንዲሁም ከኮምፒዩተር ኔትወርክ እና ኢንፎርሜሽን ሲስተም ላይ የተመሰረቱ የተለያዩ ከብሔራዊ ደህንነት ጋር ተያያዥነት ያላቸው ተልዕኮዎች እንዲሁም መንግስታዊ እና የልማት ተቋማት አገልግሎቶች መስፋፋት አንጻር ላለፉት 15 ዓመታት ሳይበር ደህንነት አንድ የሀገሪቱ መነጋገሪያ ጉዳይ እየሆነ መጥቷል። ምንም እንኳን ከብሔራዊ ደህንነት አንጻር ቅድሚያ የሚሰጠው አጀንዳ ባይሆንም በቀላሉ ሊተው የሚችል አይደለም። ለምሳሌ በቅርብ ዓመታት የተነሳው የአረብ አብዮት ማኅበራዊ ሚዲያን እንደ ዋና ማቀጣጠያ በመጠቀም የተካሄደና የሀገራቱን ብሔራዊ ደህንነት በብርቱ የፈተነ ሁኔታ ነበር። ስለዚህም ሳይበር ደህንነት ብሔራዊ ጥቅምን ከማስጠበቅ አንጻር ያለው ሚና ቀላል ግምት የሚሰጠው አይደለም። አንድ በሳይበር ምህዳር ውስጥ የሚንቀሳቀስ ተዋናይ አደረጃጀት፣ ቴክኖሎጂ፣ አመራር፣ ባለሙያ አቅሞችን በተገቢው ሁኔታ መጠቀም ከቻለ አሸናፊ መሆን የሚችልበት ይህ ካልሆነ ግን የሚወድቅበት ነው። ስለዚህ የብሔራዊ ደህንነት ተቋማትም ይህን አቅም ማደራጀት እና ተግባራዊ ማድረግ ካልቻሉ ተልዕኳቸውን እና የሀገሪቱ ብሔራዊ ጥቅም የሚጎዳ ሁኔታ ይፈጠራል። አንድ የጥናቱ ተሳታፊ እንዲህ ሲሉ ይገልጻሉ፦

> “እስከ ቅርብ ጊዜ ድረስ ሳይበር ደህንነት በሀገሪቱ የደህንነት ጉዳይ ላይ በአግባቡ አልተካተተም ነበር። ለምሳሌ ፖሊሲዎችና ስትራቴጂዎች፣ ፕሮግራሞች እና ስትራቴጂክ ዕቅዶች ሲዘጋጁ ሳይበር ደህንነትን መውሰድ ባለባቸው ትኩረት ደረጃ አያካትቱም። ስለዚህም በሀገራዊ ደረጃ ኢመደአ ከሚመለከታቸው አካላት ጋር ይሰራል በሚል እሳቤ ወደጎን የማድረግ አዝማሚያዎች ነበሩ። ነገር ግን ከቅርብ ጊዜ ወዲህ መረጃን በአግባቡ ለመጠበቅ ካለመቻል እና በቅርብ ዓመታት ከተመዘገቡ የሳይበር ጥቃቶች መጨመር ጋር ተደምሮ ይህ አመለካከት እንዲቀየር አስችሏል።”

እነዚህ ሁነቶች መነሻነት የሀገሪቱ ከፍተኛ አመራር ኢመደአ ከተመሰረተበት ጀምሮ የተለያዩ ድርሻና ኃላፊነቶችን እያካተተ እንዲሄድ አድርጓል። ከቅርብ ጊዜ ወዲህ ደግሞ የሳይበር ደህንነት ጉዳይ ለኢመደአ ብቻ የሚተው አለመሆኑንና እንደ መንግስት በጋራ እና ሁሉም ከተልዕኮው አንጻር የድርሻውን የሚወጣበት እንደሆነ መረዳቱ አለ። ነገር ግን በግልጽ ሁሉም ከተልዕኮው አንጻር የሚጠበቅበትን የመለየት፣ በየዘርፉ እና በሀገር ደረጃ የትኩረት አቅጣጫዎችን እና የትብብር መስኮችን

[36] Ministry of Information, “The F.D.R.E Foreign Affairs and National Security Policy and Strategy.”

የመለየት እና ተግባራዊ የማድረግ ስራዎች ገና መሆናቸውን የጥናቱ ውጤት ያሳያል። ይህም ሳይበር ደህንነት በብሔራዊ ደህንነት ላይ የሚኖረውን አንድምታ በመረዳት ተጽዕኖውን ለመቀነስ አስቸጋሪ ያደርገዋል።

ተቋማዊ አደረጃጀት እና የህግና ቁጥጥር ገጽታዎች

ሀገራዊ ስትራቴጂያዊ ሰነዶች ብሔራዊ ጥቅሞቻችንን እና ሀገራዊ ግቦችን ለይተው በማስቀመጥ ተቋማት እንዲያስፈጽሙት ያደርጋሉ። የ2002 እ.ኤ.አ የውጭ ጉዳይና ብሔራዊ ደህንነት ፖሊሲና ስትራቴጂ የሳይበር ደህንነት ጉዳይን ከግምት ያላስገባ፣ ከተዘጋጀ ረጅም ጊዜ የሆነው በመሆኑና የውስጥ እና የውጭ ሁኔታዎች በመቀየራቸው ከለሳ የሚያስፈልገው እንደሆነ የዚህን ጥናት ተሳታፊዎች ያስማማል። ካልተረጋገጡ የሁለተኛ ምንጮች አዲስ የብሔራዊ ደህንነት ፖሊሲና ስትራቴጂ እየተዘጋጀ እንደሆነ ለመረዳት የተቻለ ሲሆን ይህን ክፍተት ለመዝጋት እንዲቻል የሳይበር ደህንነት ጉዳይን በተገቢው ሁኔታ ሊያካትት ይገባል። አንድ የጥናቱ ተሳታፊ "ሳይበር ደህንነት ጉዳይን ያካተተ የብሔራዊ ደህንነት ፖሊሲና ስትራቴጂ ከተዘጋጀ በኋላ፣ ራሱን የቻለ የሳይበር ደህንነት ፖሊሲና ስትራቴጂ ሊዘጋጅ ይገባል። ሆኖም እስካሁን ድረስ ብሔራዊ የኢንፎርሜሽን ደህንነት ፖሊሲ ከነውስንነቱ መኖሩ እንደ አንድ ጥሩ ጎን ሊወሰድ ይችላል።" በማለት ይገልጹታል። አብዛኞቹ የብሔራዊ ደህንነት ተቋማት በሀገራዊ ደረጃ የተዘጋጁ ፖሊሲና ስትራቴጂዎችን በመከተል ተቋማዊ የICT እንዲሁም የኢንፎርሜሽን ደህንነት ፖሊሲና ስትራቴጂ አዘጋጅተዋል።

አንድ የጥናቱ ተሳታፊ ምልከታቸውን እንዲህ ሲሉ ይገልጻሉ። "በሀገር ደረጃ ለሳይበር ደህንነት የሚሰጠው ትኩረት ከጊዜ ወደጊዜ እየተሻሻለ መጥቷል። ከቅርብ ጊዜ ወዲህ ሳይበር ደህንነት በብሔራዊ ደህንነት ካውንስሉ አንድ የብሔራዊ ደህንነት አጀንዳ ተደርጎ እየተወሰደ ይገኛል። ቀድሞ ግን ከብሔራዊ ደህንነት አጀንዳ ውጭ ነበር።" ይህም በጠቅላይ ሚኒስትሩ የሚመራው የሀገሪቱ ትልቁ የብሔራዊ ደህንነት አደረጃጀት ለሳይበር ደህንነት የተሰጠውን ቦታ ያሳያል። ይህም የሳይበር ደህንነትን ጉዳይ በብሔራዊ ደህንነት ፖሊሲና ስትራቴጂ እንዲሁም ሀገራዊ ስትራቴጂያዊ ዕቅዶች ላይ ለማካተት ያስችላል። ሌላኛው ተሳታፊ ደግሞ "ተቋማትም የራሳቸውን ፖሊሲና ስትራቴጂ ሲነድፉ የሳይበር ደህንነት ጉዳይን እያካተቱ መሆኑን ለምሳሌም አዲስ እየተዘጋጀ ያለው የውጭ ግንኙነት ፖሊሲ ከሀገራት ጋር በሚኖረው ዲፕሎማሲያዊ ግንኙነት ሳይበርን እንደ አንድ የትብብር መስክ አድርጎ ማካተቱን" ያስረዳሉ።

የሳይበር ደህንነት ፖሊሲና ስትራቴጂ ትግበራን በተመለከተ የ2011 እ.ኤ.አ የኢንፎርሜሽን ደህንነት ፖሊሲና ስትራቴጂ ቢዘገይም በአመዛኙ ጥሩ የሚባል ነው።[37] ከህግና ቁጥጥር አንጻር የሳይበር ወንጀል አዋጅ እና ወሳኝ ኃይል የሳይበር ደህንነት ስታንዳርድ የሚጠቀሱ ሲሆን የህዝቡን ንቃተ ህሊና ለማሳደግ በሚዲያ እየተደረገ ያለ የሳይበር ደህንነት ፕሮግራም እንዲሁም የወሳኝ መሰረተልማት ጥበቃ ይገኙበታል። እንደ አንድ የጥናቱ ተሳታፊ ገለጻ "የሁለተኛ እና ሦስተኛ ዲግሪ ፕሮግራሞች በአዲስ አበባ ዩኒቨርሲቲ እንደሚጀመርና መቀሌ ዩኒቨርሲቲ እና መከላከያ ዩኒቨርሲቲም ለመጀመር ዝግጅት እያደረጉ ነው። " ሲሉ ያስረዳሉ። ምንም እንኳ ፖሊሲው በሁሉም የትምህርት ደረጃ መዳረስ እንዳለበት ቢገልጽም ከተግባራዊነት የራቀ ነው። እንደ ጥናቱ ተሳታፊዎች ግምገማ የፖሊሲው አፈጻጸምም እንደተጠበቀው እንዳልሄደ እና የራሱ ውስንነቶች እንዳሉበት ያስማማሉ። ከዚህም መካከል ፖሊሲውን የሚያስፈጽም ያለበት አካል አለመኖሩና የተጠያቂነት ስርዓት በአግባቡ አለመዘርጋቱ እንዲሁም በተቋማት ደረጃ ያሉ የኢንፎርሜሽን ደህንነት ፖሊሲና ስትራቴጂዎች ቀረጻና ትግበራ እንዲሁም የሀብት አለመመደብ ይጠቀሳሉ። በአሁኑ ጊዜ አዲስ የብሔራዊ ኢንፎርሜሽን ደህንነት ፖሊሲና ስትራቴጂ ረቂቅ መዘጋጀቱን ተሳታፊዎች ለመረዳት ተችሏል።

እንደ ጥናቱ ውጤት ሀገራዊ እና ተቋማዊ ስትራቴጂያዊ ሰነዶች ከላይ ወደ ታች እና ወደጎን ግንኙነት የላቸውም ወይም ያላቸው ግንኙነት የሚጣጣም አይደለም። ከዚህ በተጨማሪ የ ICT እና ኢንፎርሜሽን ደህንነት ፖሊሲዎች ከጊዜው ጋር እየተሻሻሉ አይሄዱም ተግባራዊነታቸውን ለማረጋገጥ የሚያስችል በቂ የግንዛቤ ስራዎች አይሰሩባቸውም።

የሳይበር ደህንነት የህግና ቁጥጥር ማዕቀፍ ከህገመንግስቱ የሚመነጩ ሲሆን አለማቀፍ ግዴታዎችን በማካተት በአዋጆች፣ ደንቦች እና መመሪያዎች ይገለጻል። የህግ አውጪዎቹም የህዝብ ተወካዮች ምክር ቤት፣ የሚንስትሮች ምክር ቤት ወይም ተቋማት ሲሆኑ እንዲተገበሩ የሚያደርጉት ደግሞ የፌዴራል ጠቅላይ አቃቤ ህግ እና ፍርድ ቤቶች፣ ፌዴራል ፖሊስ፣ እንደ ኢመደአ ያሉ ተቆጣጣሪ ተቋማት እንዲሁም ሌሎች የመሰረተ ልማት እና አገልግሎት ሰጪ ተቋማት ናቸው። ህግ የሚወጣበት ወይም ቁጥጥር የሚደረግበት ሳይበር ምህዳር ሲሆን ተጠቃሚዎቹ ደግሞ ህዝብ፣ ተቋማት ብሎም ሀገር ናቸው። በተጨማሪም ሀጉን ተግባራዊ ለማድረግ የሚያስችል የፖለቲካ ቁርጠኝነት እንዲሁም የሚያስፈልጉ ሀብቶችን ያካትታል።

አለማቀፍ ግዴታ የሚባለው ለምሳሌ የተመድ ቻርተር 'threat or use of force' ማለት የሳይበር-ኃይልን የሚያካትት እንደሆነ በመረዳት ግዴታን ማክበር እንዲሁም ብሔራዊ ደህንነትን ማስጠበቅ ይቻላል። ሕገ መንግስቱ በአጠቃላይ ስለ ሀገሪቱ ደህንነትና መከላከያ የሚገልጽ ሲሆን የሳይበር ሕግና ቁጥጥር ስርዓት ለመዘርጋት የሚጋጭ ይዘት እስከሌለው ድረስ በዚህ ደረጃ መገለጹ በቂ ነው ተብሎ ሊወሰድ ይችላል። ሕገ መንግስቱንና አለማቀፍ ግዴታዎችን በመከተል የኢፌዲሪ ሕዝብ

[37] Federal Democratic Republic of Ethiopia, "National Information Security Policy," 2011.

ተወካዮች ምክር ቤት የወጡ አዋጆች ሳይበር አዲስ እና ውስብስብ ምህዳር ከመሆኑ አንጻር ውሱንነት ቢኖርባቸውም የሳይበር ደህንነት ድርሻ፣ ተግባር እና ኃላፊነት ይገልጻሉ። እስካሁን የሳይበር ወንጀልን ለመከላከል የወጣ አዋጅ፣ የቴሌኮም ማጭበርበርን ለመከላከል የወጣ አዋጅ እንዲሁም በኢመደአ የተዘጋጀው ወሳኝ ኃይል የሳይበር ደህንነት ስታንዳርድ የተዘጋጁ ቢሆንም ተፈጻሚነታቸው ዝቅተኛ ነው። በተጨማሪም በአብዛኛው ተቋማት የህግና ቁጥጥር ማዕቀፉን ለመተግበር የሚያስችሉ መመሪያዎች አይገኙም። አንድ ተሳታፊ እንዲህ ሲሉ ያስረዳሉ፦

> "የሳይበር ደህንነት ህግና ቁጥጥር ማዕቀፎች ቀጠናዊ እና አለማቀፋዊ ግንኙነቶችም ጋር ተያያዥ ናቸው። ለምሳሌ የአፍሪካ ነጻ የንግድ ቀጠና መስራች አባል እንደመሆኗ እንዲሁም የዓለም የንግድ ድርጅት አባልነት ሂደት ላይ መሆኗ እነዚህ ማዕቀፎች መኖር እንዲሁም ውጤታማ አተገባበር አስፈላጊ ናቸው። እነዚህን ተግባራዊ ለማድረግ አለመቻል የህግ ተጠያቂነትን በማስከተል የሀገሪቱንና የህዝቦቿን የኢኮኖሚ ጥቅም የሚያሳጣ ሊሆን ይችላል። ስለዚህም የዲጂታል ስርዓቱ እየተስፋፋ በሄደ ቁጥር ስርቆት እና ማጭበርበር እየጨመረ ስለሚሄድ ይህን ለመከላከል የሚያስችል አርምጃ መውሰድ ያስፈልጋል።"

የቁጥጥር ማዕቀፍን በተመለከተ የሳይበር ደህንነት ስታንዳርድ በኢመደአ የተዘጋጀ ሲሆን ለመንግስታዊ ተቋማት የግንዛቤ የተሰጡ ቢሆንም ተፈጻሚነቱ በቂ ሁብት ካለመመደብ እና ቁርጠኝነት ማነስ የተነሳ እምብዛም ነው። የቁጥጥር ስርዓቱ አስገዳጅ አለመሆኑ እንደ አንድ ምክንያት ሊወሰድ ቢችልም በፈቃደኝነት ላይ የተመሰረተ አፈጻጸም መከተልም የራሱ ጥቅም አለው። ከቅርብ ጊዜ ወዲህ በኢመደአ በኩል በየዘርፉ ያሉ ተቋማትን አንድ ላይ በማድረግ እንቅስቃሴ የተጀመረ ሲሆን በአለማቀፍ የኢንፎርሜሽን ደህንነት ቁጥጥር ስርዓቶችም ተመሳሳይ አካሄድ መከተል ውጤት ያመጣ በመሆኑ ጥሩ አቅጣጫ እንደሆነ መረዳት ይቻላል። ለምሳሌ የባንኩ ዘርፍ አንድ ባንክ በአለማቀፍ የክፍያ ካርድ ኢንዱስትሪ የዳታ ደህንነት ቁጥጥር (PCI-DSS) ስርዓትን ማሟላት የሚጠበቅበት ሲሆን በተመሳሳይ ሀገራዊ የሳይበር ደህንነት ቁጥጥር ስርዓትን ለመዘርጋት ያስችላል።

ከቃለምልልስ ውጤቶች መረዳት እንደተቻለው በሀገራዊ እና ተቋማዊ ደረጃ ያሉ የሳይበር ደህንነት ህግ እና ቁጥጥር ማዕቀፍ በቂ አለመሆንናቸውን ያሳያሉ። በቅርቡ የተዘጋጀው የኢትዮጲያ ዲጂታል ስትራቴጂ ከዲጂታል ዝግጁነት ጎን ለጎን የዲጂታል መለያ ለብሔራዊ መታወቂያ መሰረት ሊሆን እንደሚችል እንዲሁም ሳይበር ደህንነት ጉዳዮችን ለምሳሌም የሳይበር ደህንነት ዳሰሳ ማድረግ እና ግንዛቤ መፍጠር አስፈላጊነትን ይገልጻል።[38] ከኢኮኖሚ ዕድገት እና ዘመናዊነት አንጻር የዲጂታል ለውጥ አስፈላጊነት የሚያጠያይቅ ባይሆንም ትይዩ የሆነ የሳይበር ደህንነት ስትራቴጂ አስፈላጊ መሆኑ ለነገ የማይባል ነው። ይህን ማድረግ ካልተቻለ የሳይበር ተጋላጭነትን በመጨመር ለሳይበር ስጋቶች ምቹ ዕድል በመፍጠር ብሔራዊ ደህንነትን ወደሚጎዳ ሁኔታ ሊያመራ ይችላል።

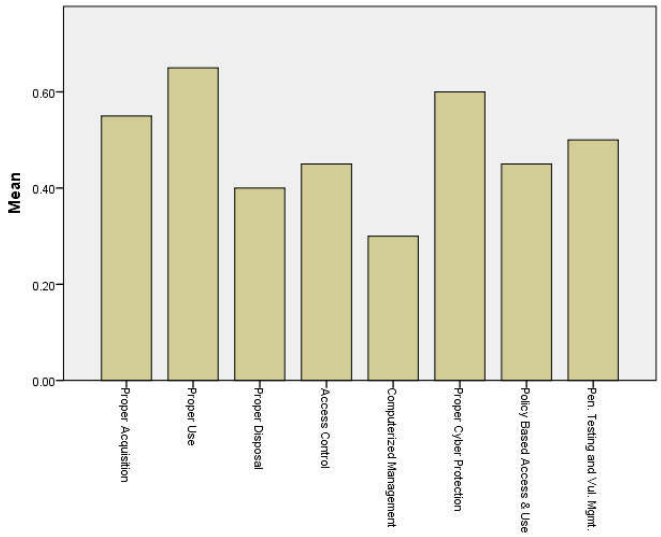
አደረጃጀትን በተመለከተ የብሔራዊ ደህንነት ተቋማት ራሱን የቻለ ወይም በ ICT ስር ያለ የኢንፎርሜሽን ደህንነት ክፍል ያቋቋሙ ሲሆን ይህ ክፍል የተቋማቱ የመረጃ ሀብት እና የ ICT መሰረተልማት ላይ በትኩረት ይሰራል። እነዚህ አደረጃጀቶች እንዳሉ መጠቀም ውጤታማ ስለማያደርግ ሳይበር ደህንነት ከሚፈልገው እይታ እና ክህሎት አንጻር የሰው ኃይል አቅም ግንባታ ስራዎች መስራት አስፈላጊ ነው። ከቅርብ ጊዜ ወዲህ ራሱን የቻለ የኢንፎርሜሽን ደህንነት (የሳይበር ደህንነት) ክፍሎች እየተቋቋሙና በመካከለኛ አመራር የኃላፊነት ደረጃ እያደገ መምጣቱ የተሰጠው ትኩረት መሻሻል እያሳየ እንደሆነ ያሳያል። ይህ ሊበረታታ የሚገባው ሲሆን የብሔራዊ ደህንነት ተቋማት በአለማቀፍ ተልዕኮ እና አደረጃጀት ያላቸው በመሆኑ ይህ አቅም ወደከፍተኛ አመራር ደረጃ እያደገ አፈጻጸሙም እየተሻሻለ የሚሄድበትን ሁኔታ መፍጠር ብሔራዊ ደህንነትን ለማረጋገጥ አስፈላጊ ነው።

የሳይበር ደህንነት አቅም ግንባታ

የሳይበር ደህንነት አቅም ግንባታ ፕሮግራም ሀገራዊ እና ተቋማዊ ደረጃ መኖር ብሔራዊ ደህንነትን ለማረጋገጥ የሚያስችል አስፈላጊ ነው። የብሔራዊ መለያ ስርዓት ተቋማዊ ደህንነት ፖሊሲዎች ጋር በማጣመር በሳይበር ምህዳር ያለ ሀብትን ለማስተዳደር እና ተጠያቂነት ስርዓት ለመዘርጋት መሰረት ነው። ቴክኖሎጂን በመጠቀም የተጠቃሚ አስተዳደር ለመዘርጋት ጥረቶች ቢኖሩም የሳይበር ደህንነትን ከማረጋገጥ አንጻር ብዙ የሚቀራቸው መሆኑ እንዲሁም ብዙ ቦታዎች ደግሞ በሰው ላይ የተመሰረተ ነው። በተጨማሪም ሰፊ የሳይበር ደህንነት የግንዛቤ እጥረት እንዲሁም ያልዳበረ ባህል እንዳለ ለመረዳት ተችሏል። ለምሳሌ ተቋማት ለሠስተኛ ወገን የማይገባውን Access መስጠት እንዲሁም የሳይበር ደህንነት እርምጃዎችን የመንግስት የስለላ መሳሪያ እንደሆኑ አድርጎ የመውሰድ ክፍተቶች ይስተዋላሉ። ከሳይበር ደህንነት ባህል አንጻር አንድ ሰው ማወቅ ያለበትን እንዲያውቅ እና ማግኘት ያለበትን ሁብት እንዲያገኝ ለማድረግ ቢሞክር በሌሎች ዘንድ ለአንዳች ፖለቲካዊ ወይም ኢኮኖሚያዊ ጥቅም እንደሆነ አድርጎ የማሰብ ሁኔታዎች ይስተዋላሉ።

[38] Federal Democratic Republic of Ethiopia, "Ethiopia Digital Strategy 2020," 2020.

ከተቋማዊ የስራ ሂደቶች አንጻር ጥናትና ምርምር፣ ሶፍትዌር ልማት፣ ዲዛይን፣ ግዥ እና ሌሎችም የስራ ሂደቶች ሳይበር ደህንነት የሚሰጠው ቦታ አነስተኛ ነው። ለምሳሌ በተቋማት የዕቃ ግዥ ሂደት ደህንነቱ የተጠበቀ አለመሆን፣ ብሎም በአቅራቢው እምነት በማሳደር የተገዛውን ሲስተም አቅራቢው እንዲያስተዳድረው፣ እንዲቆጣጠረው እና ደህንነቱን እንዲያድስ መፍቀድ ይገኙበታል። በተቋማት የሶፍትዌር ማበልጸግ ሂደት ደግሞ መደበኛ የሶፍትዌር ደህንነት ፍላጎቶች እና መስፈርቶችን አለመተግበር የደህንነት ዲዛይን አለመኖር የስጋት ሞዴል አለማዘጋጀት ይጠቀሳሉ። ስለዚህም እነዚህ የስራ ሂደቶች ያለ ደህንነት ክፍተት በሳይበር ጥቃት አማካኝነት ለብሔራዊ ደህንነት ስጋት የሚሆንበት ዕድል ሰፊ በመሆኑ ትኩረት ሊሰጠው የሚገባ ነው። ከመጠይቅ የተሰበሰበው መረጃ በተቋማቱ ጥሩ የሀብት አያያዝ እና አጠቃቀም ቢኖርም በኮምፒዩተር የታገዘ አለመሆኑን ያሳያል (ምስል 3) ። በተጨማሪም የሀብት አወጋገድ ስርዓት፣ ፖሊሲ ላይ የተመሰረተ አስተዳደር ስርዓት፣ የማሻሻ ቁጥጥር ስርዓት እና ሌሎችም የሳይበር ደህንነት የስራ ሂደቶች መሻሻል እንደሚገባቸው ያሳያል።



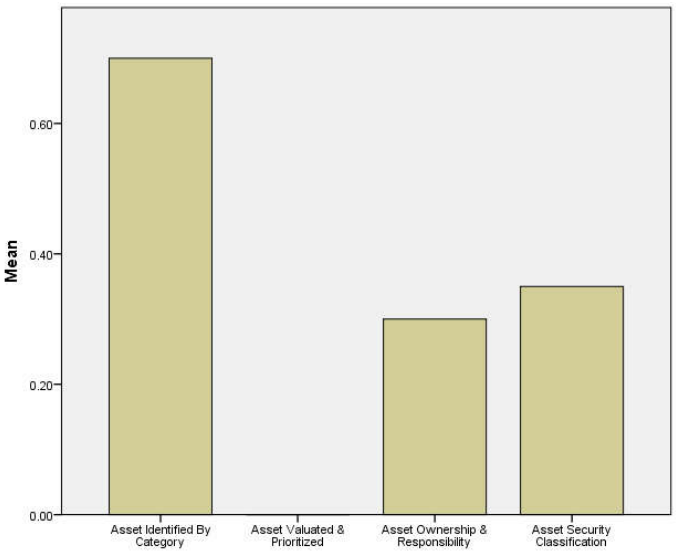
ምስል 3: ተቋማዊ የሀብት አስተዳደር እና የሳይበር ደህንነት የስራ ሂደቶች

የሳይበር ደህንነት አቅም ግንባታ የሰው ኃይል፣ ቴክኖሎጂ እና የአሰራር ስርዓትን የሚያካትት ሲሆን የተቋማትን ተልዕኮ አፈጻጸም ላይ ተጽዕኖ አሳድሯል። በአንድ በኩል ደህንነቱ የተጠበቀ ቴክኖሎጂ እና መደበኛ የትምህርት እና ስልጠና ጥረቶች አነስተኛ በመሆኑ ተቋማቱ ወሳኝ ተልዕኳቸውን ለማሳካት ከቴክኖሎጂ ይልቅ ሰው እና ወረቀት ተኮር እንዲሆኑ አስገድዷቸዋል፤ በዚህ ረገድ እንደ ኢመደአ ካሉ በዘርፉ ከሚሰሩ ተቋማት የሰው ኃይል ዝውውር በማድረግ እንደ አንድ ጥሩ ተሞክሮ ሆኖ ተነስቷል። በሌላ በኩል በቅርብ ጊዜያት የተቋማት አቅም ግንባታ ስራዎች መጀመራቸው የላቀ አቅም ለመገንባት ጥሩ መሰረት ነው፤ ይህም የአመራሩን፣ የአስተዳደሩን እና የባለሙያዎችን እና አጠቃላይ ስታፍ አቅም በምርጥ ተሞክሮዎች አማካኝነት አለማቀፍ ደረጃውን በጠበቀ ሁኔታ ለመገንባት ያስችላል። ነገር ግን የዚህ ጥናት ግኝት የአቅም ግንባታ ስራዎች በአብዛኛው በማዕከል በዋና መስሪያ ቤቶች እንደሆነ ያሳያል፤ ይህም በቅርንጫፍ መ/ቤቶች እና በተቋማት የታችኛው አደረጃጀቶች ድረስ የተዘረጋ ጠንካራ የሳይበር ደህንነት የሰው ኃይል እና አቅም ግንባታ ስራዎች አለመኖር ከተቋማቱ የታችኛውና ከማዕከል ርቀው በሚገኙ ክፍሎች በሚመነጭ ተጋላጭነት ብሔራዊ ጥቅምን የሚሸረሸር ሁኔታ ይፈጥራል።

መደበኛ የሳይበር ደህንነት ኦዲት እና ግምገማ በአለማቀፍ፣ በሀገራዊ ወይም ተቋማዊ ደረጃ የተቀመጡ የኔትወርክ እና ኢንፎርሜሽን ሲስተም ፖሊሲዎች በተግባር መኖራቸውን ለማረጋገጥ ያስችላል። በዚህ ዙሪያ ኢመደአ ከጊዜ ወደጊዜ የራሱን አቅም በመገንባት አጠቃላይ ለሁሉም መንግስታዊ ተቋማት እና በየዘርፉ ያሉ ተቋማትን በመለየት ኦዲት እና ግምገማ እንዲያደርጉ ጥረት እያደረገ ይገኛል። እንደ አንድ የጥናቱ ተሳታፊ ገለጻ "በቅርቡ የዚህ አካል የሆነ በፋይናንስ ዘርፍ አንድ መመሪያ እንዲወጣ የተደረገ ሲሆን አንዳንድ የአፈጻጸም ክፍተቶች ቢኖሩም ይህ መመሪያ በዘርፉ ያሉ ተቋማት አዲስ ሲስተም ጥቅም ላይ ከማዋላቸው በፊት የደህንነት ፍተሻ ማለፍ እንዳለበት ያስገድዳል።" በተጨማሪም ወደ ሀገር ውስጥ በሚገቡ ዕቃዎች ላይ የደህንነት ፍተሻ የሚደረግ ሲሆን ህጋዊ ያልሆኑ ወይም የተቀመጠ መስፈርቶችን ያላሟሉ ዕቃዎች ጥቅም ላይ እንዳይውሉ ለማድረግ ያስችላል። አንድ የጥናቱ ተሳታፊ "ወደ ሀገር ውስጥ የሚገባ ሰው አልባ አውሮፕላን ላይ በቂ የደህንነት ፍተሻ ካልተደረገ የሳይበር ደህንነትን ብሎም ብሔራዊ ደህንነትን ሊጎዳ ይችላል። የደህንነት ፍተሻው መኖሩ ጥሩ ቢሆንም ዕቃዎች ከገቡ በኋላ ስለሚሰጡት አገልግሎት የሚደረገው ቁጥጥር እየተሻሻለ መሄድ ይገባዋል።" በማለት ይገልጻሉ።

የሀብት አስተዳደር እና የክስተት ምላሽ

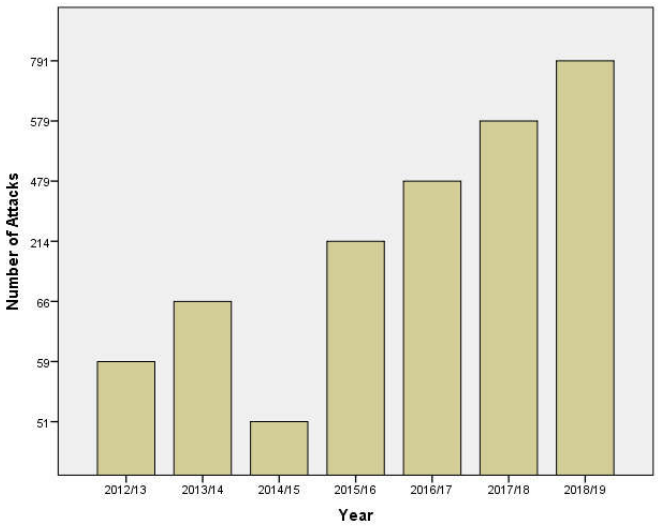
ወሳኝ ሀብቶች ሁልጊዜ በስጋት ኃይሎች ዒላማ የሚደረጉ በመሆኑ ካላቸው ዋጋ ተመጣጣኝ የሆነ የሳይበር ደህንነት ጥበቃ ያስፈልጋቸዋል። በእነዚህ የሀገር ሀብቶች ላይ የሚደርስ የሳይበር ጥቃት የብሔራዊ ደህንነት ስጋት ሊሆን ይችላል። በሀገራዊ ደረጃ ኢመደአ እነዚህን ሀብቶች በመለየት የሚያስከትሉትን አደጋ መሰረት ያደረገ ጥበቃ እንዲሚደረግ ከቃለምልልስ የተገኘው መረጃ ያሳያል። በተቋማት ደረጃ ግን በምስል 4 እንደሚታየው ሀብቶችን ለመለየት ቢቻልም የቅደም ተከተል እና ካላቸው ዋጋ አንጻር ሳይበር ደህንነታቸው የተጠበቀ ነው ለማለት አያስችልም። በተጨማሪም የሀብቶቹን ባለቤት የመለየት እና አግባብነት ያለው የደህንነት ቁጥጥር ስርዓት አልተዘረጋም እንዲሁም ከሳይበር ደህንነት ሪስክ አስተዳደር የስራ ሂደቶች ጋር አልተጣጣመም። ይህም ተቋማዊ የሳይበር ደህንነት ክፍተት በማምጣት አልፎ አልፎም ከሳይበር ስጋት የሚመነጭ የብሔራዊ ደህንነት ክፍተት ያስከትላል።



ምስል 4፡ የተቋማት የሀብት አስተዳደር

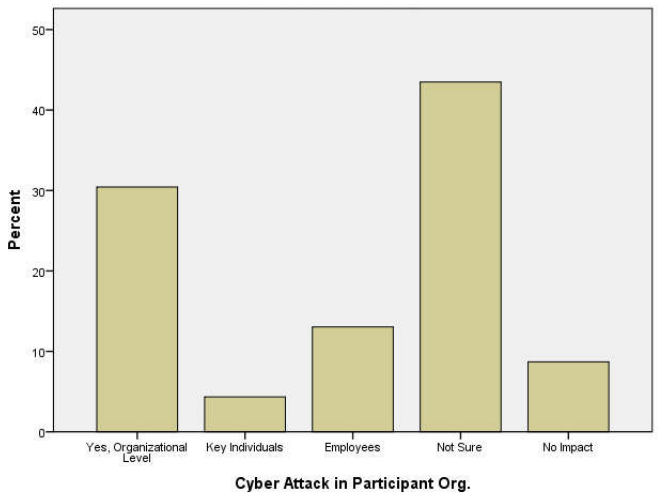
በሀገራዊ ደረጃ ከስጋት ትንተና በመነሳት የሳይበር ስጋቶች ተለይተው ከፖለቲካ አመራሩ በሚመጣ አቅጣጫ መሰረት እየተሰራ ይገኛል። ተጨባጭ ስጋት ሊሆኑ የሚችሉ የሳይበር ተዋንያን ከተለዩ በኋላ ሊያደርሱ የሚችሉትን ጥቃት በመተንተን እና ገዢ ከሆነው ፍልስፍና በመነሳት የስጋት መልከአ ምድር እና አስቻይ ሁኔታዎች በመለየት የሚሰራበት ሲሆን በተቋማዊ ደረጃ ቀጣይነት እንዲኖረው አልተደረገም። ለዚህም እንደ ምክንያት የተጠቀሰው በተቋማት አመራር ዘንድ በቂ ግንዛቤ አለመኖር፤ መደበኛ የግንኙነት መስመር አለመዘርጋቱ፤ እንዲሁም በቂ ሀብት አለመመደብ ይጠቀሳሉ። ተቋማቱ ምንም እንኳ መደበኛ የስጋት ትንተና ቢያደርጉም የሳይበር ደህንነት በኢመደአ እንደሚሰራ በማሰብ እንደሆነ የጥናቱ ተሳታፊዎች ያስረዳሉ። ነገር ግን ተቋማት የስጋት ትንተና ሲያደርጉ የሳይበር ስጋቶችን ጭምር በማካተት ቢሰሩ በሀገራዊ የሳይበር ስጋት ትንተና ላይ በንቃት እንዲሳተፉ ያስችላቸዋል። ተቋማት ዘግይተውም ቢሆን የሳይበር ደህንነት ጉዳዮችን ማካተት መጀመራቸው እንደ መልካም አጋጣሚ ሊወሰድ ይችላል። ነገር ግን በአብዛኞቹ ተቋማት ዘንድ በስጋቶች ላይ ያለ ግንዛቤ የተሟላ አለመሆን እንዲሁም በተቋማት የሳይበር ደህንነት ክፍሎች እና ከፍተኛ አመራር መካከል አንዱ ሌላውን ለመረዳት እንዲችል የሚደረጉ ጥረቶች አነስተኛ በመሆናቸው የተግባቦት ክፍተት እንዳለ የጥናቱ ተሳታፊዎች ያስረዳሉ።

ተቋማት የሳይበር ስጋቶቻቸውን በመለየት በስትራቴጂያዊ እና በቴክኒካዊ ረገድ ሙሉ የሳይበር ደህንነት እይታን (ሰው፣ ቴክኖሎጂ እና የአሰራር ስርዓት) በማካተት ስጋቱን ለመቀነስ የሚያስችል ጥረት ሊያደርጉ ይገባል። አንዱ አቅም የሳይበር ደህንነት ክስተት አስተዳደር ሲሆን የሳይበር ጥቃትን መለየት (እንደተከሰተ ማወቅ) ፣ መተንተን እና ምላሽ መስጠትን ያካትታል። በዚህ ረገድ የተቋማት አቅም እንደ አጠቃላይ ዝቅተኛ ሲሆን አብዛኛው ተቋማት ያላቸው አቅም ሁሉን አቀፍ ከመሆን ይልቅ ወደ ቴክኖሎጂ እይታ ያመዘነ ነው። በዚህም ወሳኝ የሚሏቸውን የመረጃ ሀብቶች፣ የግንኙነት እንዲሁም እንደ ሰርቨር ያሉ ሀብቶቻቸው ጥበቃ ለማድረግ እና ለመከላከል የሚያስችል የክስተት አስተዳደር ስርዓት አላቸው። ጥቂት ተቋማት ደግሞ የኢንፎርሜሽን (ሳይበር) ደህንነት ፕሮግራም በመቅረጽ ከቴክኖሎጂ ባለፈ ከሰው ተጋላጭነት ጭምር የሚመጣን ስጋት ለመከላከል ጥረት የሚያደርጉ ሲሆን ከአሰራር አንጻር ያለ አቅም ግን ዝቅተኛ ነው። በዚህ እና ሌሎች ምክንያቶች ከኢመደአ የተገኘው ሪፖርት በምስል 5 እንደሚታየው ላለፉት አምስት ዓመታት የሳይበር ጥቃት በየዓመቱ ያለማቋረጥ እየጨመረ እንደሆነ ያሳያል።



ምስል 5፡ ሳይበር ጥቃት በኢትዮጲያ [ምንጭ፡ ኢመደአ]

በዚህ ጥናት ተሳታፊዎች በመጠይቅ በተሰብሰበው መረጃ መሰረት 43.5% የሚሆኑት ተሳታፊዎች እስካሁን በተቋማቸው ውስጥ የሳይበር ጥቃት ስለመድረሱ እንደማያውቁ የገለጹ ሲሆን 26.1% እና 34.8% የሆኑት ደግሞ በሌሎች መንግስታዊ ተቋማት እና በግል ተቋማት የሳይበር ጥቃት ስለመድረሱ መረጃ እንደሌላቸው ገልጸዋል። አብዛኞቹ ተሳታፊዎች በተቋማቸው የሳይበር ደህንነት ክስተት መፈጠሩን አለማወቃቸው ከግንዛቤ እጥረት ወይም ደግሞ ምስጢራዊ መረጃ ነው በሚል ከመናገር ለመቆጠብ ሊሆን ይችላል። በአማካኝ 34.8% የሚሆኑት ተሳታፊዎች ሳይበር ጥቃት በኢትዮጲያ ስለመከሰቱ ወይም አያውቁም ወይም መከሰት እና አለመከሰቱን ለመግለጽ የሚያስችል የግንዛቤ እጥረት አለባቸው። ስለዚህም በሀገራዊ እና ተቋማዊ ደረጃ እነዚህንና መሰል የግንዛቤ እጥረቶችን ለመሙላት የሚያስችል እርምጃ መውሰድ ያስፈልጋል። የሳይበር ጥቃት ተጽዕኖን በተመለከተ በምስል 6 እንደሚታየው እንደተከሰተ መረጃው ካላቸው የጥናቱ ተሳታፊዎች መካከል 50.7% ተቋማዊ 13.0% በሰራተኞች ላይ ብቻ 4.3% ደግሞ ቁልፍ ግለሰቦች ላይ ተጽዕኖ እንዳሳረፈ ያሳያል።



ምስል 6፡ በጥናቱ ተሳታፊ ተቋማት የሳይበር ጥቃት ያለው ተጽዕኖ

ከቃለመልልስ በተገኘ ውጤት መሰረት አንድ የሳይበር ደህንነት ክስተት በሚያጋጥማቸው ጊዜ ለኢመደአ የሚያሳውቁ ሲሆን ኢመደአም በተመሳሳይ ለሚመለከታቸው ባለድርሻዎች በማሳወቅ አብሮ ይሰራል። ነገር ግን ከኢመደአ ውጭ በሌሎች ተቋማት ራሱን የቻለ ተቋማዊ የሳይበር ደህንነት ክስተት አስተዳደርና ምላሽ (CIRT) አደረጃጀት አይገኝም። ይህም ተቋማዊ

የቴክኖሎጂ አቅም፣ የሰለጠነ የሰው ኃይል አለመኖር እንዲሁም ይህን ለማድረግ የሚያስችሉ አሰራሮች በሀገራችን ያልተለመዱ ከመሆናቸው ጋር ይገናኛል። በማዕከል የሚታወቁ ከዚህ በፊት ከተከሰቱ የሳይበር ጥቃቶች ተመዝግበው የሚገኙ ሲሆን ምስጢራዊነቱን በጠበቀ ሁኔታ ዝርዝር መረጃዎችን ግልጽ ከማድረግ እንዲሁም በቴክኖሎጂ በተደገፈ መልኩ ከማስቀመጥና ለተለያየ ጥቅም እንዲውሉ ከማድረግ አንጻር ውስንነቶች አሉበት። ለምሳሌ አንድ ተቋም የተከሰተ ሳይበር ጥቃት የተወሰደ ትምህርት ለሌሎች ተቋማት በሚገባ ማድረስ ስለማይቻል ተመሳሳይ ጥቃት እንዲደገም ዕድል ይፈጥራል። የጥናቱ ተሳታፊዎች የተቋማቸውን የዝግጁነት ደረጃ 47.8% መካከለኛ፣ 34.8% ዝቅተኛ እና 17.4% ከፍተኛ እንደሆነ ገልጸዋል።

ባለፉት ጊዜያት በኢትዮጲያ ብዙ መንግስታዊ ተቋማት ዌብ ሳይቶቻቸው የፖለቲካ ዓላማ ባላቸው ጠላፊዎች ያልተፈለገ መልዕክት ለማስተላለፍ ውለዋል፤ የማልዌር ጥቃቶች ራንሰምዌርን ጨምሮ ተከስተዋል፤ የቴሌኮም እና ፋይናንስ ማጭበርበሮች ተፈጽመዋል፤ በሳይበር ምህዳር ላይ ያሉ አገልግሎት እንዲቆም የሚያደርግ ጥቃት (DDoS) እንዲሁም ሌሎች ሳይበር ጥቃቶች እና ሳይበር ወንጀሎች ታይተዋል። እነዚህን ጥቃቶች እየጨመሩ የሚሄዱ በመሆኑ በአግባቡ ለመመከት ከሀገራዊ አመራር እና ከተቋማት ከፍተኛ ጥረት ይጠይቃል።

የሳይበር ደህንነት ጥረቶች ውህደት እና ትብብር

የሳይበር ደህንነት አቅሞች ተደማሪነት እና የትብብር ገጽታዎች በተቋማት ውስጥ እንዲሁም በተቋማት መካከል የሚደረጉ እንቅስቃሴዎችን የሚያካትቱ ሲሆን በሀገር ውስጥ ወይም በሀገራት መካከል ባሉ ግንኙነቶች የሚፈጸም ሊሆን ይችላል። እነዚህ ግንኙነቶች በስትራቴጂያዊ፣ በኦፕሬሽናዊ፣ ወይም በታክቲካዊ ደረጃ ሊደረጉ የሚችሉ ሲሆን የሚይዙት ዓላማ ደግሞ የሳይበር ደህንነት አቅም ግንባታ፣ የሳይበር ደህንነት ፖሊሲና ስትራቴጂ እንዲሁም ፕሮጀክትና ፕሮግራም ቀረጻና ትግበራ፣ የሳይበር ደህንነት ምርምርና ልማት፣ የሳይበር ኦፕሬሽናዊ ተግባራት፣ የሳይበር ደህንነት ቴክኖሎጂ ሽግግር፣ እንዲሁም የሳይበር ደህንነት መረጃ ልውውጥን ያካትታሉ። በሀገራዊ ደረጃ መንግስታዊ ተቋማትን በየዘርፉ ትብብር እንዲኖራቸው በኢመደአ በኩል የሚደረጉ ጥረቶች የሚገኙ ሲሆን መደበኛ፣ ሁሉን አካታች እንዲሁም በስትራቴጂያዊ በኦፕሬሽናዊ እና ታክቲካዊ ደረጃ አለመሆኑ እንደ ክፍተት ይጠቀሳል። በተጨማሪም ዘርፍ ተሻጋሪ የሆኑ የሳይበር ደህንነት ትብብር እና ውህደት ጉዳዮች ተጨማሪ ስራ ይጠይቃሉ። አሁን ያለ የተቋማት የሁለትዮሽ ግንኙነቶች በአብዛኛው በደብዳቤ፣ በስልክ እና በኢ-ሜይል እንዲሁም ደህንነቱ የተጠበቀ የዳታ ግንኙነቶች ላይ የተመሰረተ ነው። ነገር ግን ከአጠቃቀም ጋር ተያይዘ በአንዳንድ ተቋማት ጥብቅ የደህንነት ፖሊሲ ቀረጻ እና ትግበራ አለመኖር ለመረጃ ደህንነት ክፍተት የዳረጋቸው መሆኑን ለመረዳት የተቻለ ሲሆን ያለባቸው ስጋት በአግባቡ ባለመፈታቱ ለወደፊትም ተመሳሳይ አደጋ ሊያጋጥም ይችላል።

እንደ ኢመደአ እና መከላከያ ሰራዊት ባሉ ተቋማት መካከል ያሉ የትብብር ጥረቶች ከኢመደአ መቋቋም ጀምሮ የነበሩ ሲሆን ውጤታማነቱ ለብቻው ሌላ ጥናት ሊሆን የሚችል ቢሆንም ከግንኙነቱ ጥሩ እና መጥፎ ውጤቶች ተገኝተዋል። ቀድሞ የነበረው አካሄድ በአብዛኛው ኢመደአ እንደ አቅራቢ መከላከያ ደግሞ እንደ ተጠቃሚ የነበሩ ሲሆን ከቅርብ ጊዜ ወደህ ግን ኢመደአ በዘርፉ የተሻለ ልምድና አቅም ያለው በመሆኑ፣ መከላከያም የሳይበር ደህንነትን እንደ አንድ ወሳኝ አቅም በተልዕኮው ውስጥ በማካተቱ እና ከተጠቃሚነት ይልቅ በባለቤትነት እየተንቀሳቀሰ በመሆኑ የረጅም ጊዜ የጋራ ተጠቃሚነት መርህ አቅምን ለመገንባት የሚያስችሉ የትብብር ጅምሮች አሉ። የሚደረጉት ትብብር ጥረቶች የተግባቦት ለምሳሌ የመረጃ ልውውጥ፤ ስትራቴጂያዊ እና ቴክኒካዊ አቅም ግንባታ ለምሳሌ የሰው ኃይል ዝውውር እንዲሁም ትምህርት እና ስልጠና፤ እንዲሁም የፕሮጀክት ቀረጻና ትግበራ ድጋፍን ያካትታሉ። ነገር ግን እነዚህ የግንኙነት ጥረቶች መደበኛ ያለመሆን፣ ሁሉን አካታችነት እና ውህደት እንዲሁም በቴክኖሎጂ የተደገፉ ያለመሆን ውስንነቶች አሉባቸው።

በጥናቱ የተካተቱ ተቋማት የሳይበር ደህንነት አደረጃጀት በማዕከል ወይም በየደረጃው በሁሉም ክፍሎች ያላቸው ሲሆን በአደረጃጀቶቹ መካከል የንዑሶሽ ወይም ከላይ ወደታች ግንኙነት እና የጥረቶች ውህደት የሳሳ መሆን ወይም አለመኖር እንደ ክፍተት ታይቷል። ይህም ወደ ርቀት ቦታ የሚገኙ ወይም ዝቅተኛ ደረጃ ያሉ አደረጃጀቶች በሀብት የተጠናከሩ ካለመሆናቸው እንዲሁም ከተቋማዊ የሳይበር ደህንነት የአመራር እና አስተዳደር ክፍተት ጋር ይያያዛል። ከማዕከል እስከ ታችኛው መዋቅር ድረስ ተቋማዊ የሳይበር ደህንነት የመረጃ ልውውጥ መኖር የሳይበር ጥቃትን ለመከላከል፣ ለፖሊሲና ስትራቴጂ ትግበራ እንዲሁም፣ ግንዛቤን ለማሳደግ ይረዳል። ጥቂት ተቋማት በመደበኛነት በአነስተኛ ቴክኖሎጂ በመታገዝ ይህንን ስርዓት ተግባራዊ የሚያደርጉ ሲሆን ሌሎች ደግሞ ከቴክኖሎጂ እና ስርዓት ይልቅ በሰዎች ላይ የተመሰረተ ነው። በሀገር ወይም በተቋም ደረጃ ተጽዕኖ ያለው የሳይበር ደህንነት ክስተት በሚፈጠር ጊዜ ኢመደአ ከባለድርሻ አካላት ጋር አግባብነት ያለው ምላሽ እንዲያገኝ እና እንደ አስፈላጊነቱ በመገናኛ ብዙኃን ለህብረተሰቡ የመግለጽ እና ግንዛቤ የመፍጠር ስራዎች ይሰራሉ።

ማጠቃለያ

በዚህ ጥናት ሳይበር ደህንነት በኢትዮጲያ ያለበትን ሁኔታ በመዳሰስ ለብሔራዊ ደህንነት ያለው አንድምታ ለማቅረብ ተሞክሯል። ጥናቱ የሳይበር ደህንነት የህግ ማዕቀፍ፣ የተቋማዊ አደረጃጀት እርምጃዎችን፣ የአቅም ግንባታ እንዲሁም የውህደት እና ትብብር ጥረቶችን ያካተተ ሲሆን ምንም እንኳ መሰረታዊ የሳይበር ደህንነት አቅሞች እና ጅምሮች ያሉ ቢሆንም ከሂደቶቹ እና ከውጤታማነት አንጻር በብሔራዊ ደህንነት ላይ ከሳይበር የሚመጣን ስጋት ለመከላከል በቂ እንዳልሆኑ ለመረዳት ተችሏል።

በመጀመሪያ በስትራቴጂያዊ ደረጃ ሳይበር ምህዳሩ የሚመራበት መርህ፣ ስትራቴጂያዊ ግቦች እንዲሁም ግቦችን ለመምታት የሚያስችሉ የትግበራ መስመሮች ካለው ውስጣዊ እና ውጫዊ ሁኔታ በመነሳት እና የምህዳሩን ሁኔታ ትንተና በማድረግ አቅጣጫን ለመለየት የሚደረግ እንቅስቃሴ በቂ አለመሆኑን እና ይህም ትልቅ ተጽዕኖ ያለው መሆኑን ያሳያል።

በመቀጠል የህግ እና ቁጥጥር ማዕቀፍ ሳይበር ደህንነትን ለማረጋገጥ የሚያስችል አንድ መሳሪያ በመሆኑ በሀገሪቱ የሳይበር ምህዳር ላይ የሚንቀሳቀሱ ተዋንያንን ድርሻና ሀላፊነት እንዲሁም እንዲያደርግ የተፈቀደለትን እና ገደብ የተጣለበትን ነገሮች ግልጽ ማድረግ አስፈላጊ ነው። አሁን ያለው የህግ እና ቁጥጥር ማዕቀፍ ያለበት ክፍተቶች በሀገራዊ እና ተቋማዊ ደረጃ ሳይበር ደህንነትን ለማረጋገጥ የሚያስችሉ በመሆናቸው በማጠናከር እንዲሁም የህግ አስፈጻሚ እና ተቆጣጣሪ አካላትን አቅም በማሳደግ ውጤታማነቱን ማረጋገጥ ያስፈልጋል። ወንጀለኞች በአንጻራዊነት ከተጠያቂነት በቀላሉ ለማምለጥ የሚያስችላቸውን እንዲሁም ቀላል ወጪ ያለውን የሳይበር ምህዳር በመምረጥ አላማቸውን ለማሳካት ጥረት የሚያደርጉ ሲሆን ይህን መግታት የሚቻለው ሁሉን አካታች እና ተግባራዊ ሊደረግ የሚችል የሳይበር ህግ እና ቁጥጥር ስርዓትን በማሻሻል እንዲሁም አስፈላጊውን ሀብት በመመደብ ተግባራዊ በማድረግ ብቻ ነው።

የሳይበር ደህንነት ተቋማዊ አደረጃጀትን በተመለከተ ኢትዮጲያ እስካሁን ባለው ኤጀንሲ ላይ የተመሰረተ አካሄድ ስትከተል የቆየች መሆኑ የኢመደአ ጉዳይ ብቻ ተደርጎ እንዲታይ እና በወሳኝ የመከላከያ እና ደህንነት ተቋማት ከተልዕኳቸው አንጻር ይህ አቅም ሳይገነባ ቀርቷል። ስለዚህም በአብዛኞቹ ተቋማት ያሉ በአብዛኛው ቴክኒካዊ የ ICT እና ኢንፎርሜሽን ደህንነት አቅሞች ናቸው። በሀገር ደረጃ የተቋማት አደረጃጀት፣ የሚሰጡት ጥቅም፣ የኢንፎርሜሽን ሲስተም እና ኔትወርክ ፖሊሲ እና ስታንዳርድ በግልጽ የሚያሳይ የሳይበር ደህንነት አርክቴክቸር እስካሁን ባለመኖሩ የሚደረጉ ጥረቶች ውጤታማነት እንዲቀንስ አድርጓል። ይህንንም በበቂ ደረጃ ለማሳካት የሚያስችል ብሔራዊ የመረጃ ደህንነት (ሳይበር ደህንነት) ፖሊሲና ስትራቴጂ አለመኖር አንዱና ዋነኛው ችግር ነው። ያሉትንም ተያያዥ ፖሊሲ እና ስትራቴጂዎች ለመተግበር ውጤታማነቱንም ለመገምገም አስቸጋሪ መሆኑን ለመረዳት ተችሏል።

ሌላኛው የሳይበር ደህንነት በረስክ ላይ የተመሰረተ አለመሆኑ ጉዳቱን መጠን ለመግለጽ ባይቻልም የሳይበር ጥቃት በቁጥር እንዲሁም በመጠን እንዲጨምር አድርጎታል። ስለዚህም በተለይም ተቋማት በረስክ ላይ የተመሰረተ የሳይበር ደህንነት ጥበቃ ማድረግ እንደሚያስፈልጋቸው እንዲሁም በየዘርፉ የሳይበር ደህንነት ምርጥ ተሞክሮዎችን በመለየት እና ተግባራዊ በማድረግ በብሔራዊ ደህንነት ላይ የሚኖረውን ተጽዕኖ መቀነስ አስፈላጊ ነው። ጥቂት በማይባሉ ተቋማት አሁን ያለው የ ICT ዘርፍ ባህል የተሰረቁ፣ ርካሽ ወይም ነጻ ሶፍትዌር እና ሀርድዌር መጠቀም በብዛት የሚታይ በመሆኑ የዚህ አይነት የ ICT እና ሳይበር ደህንነት ውጤቶች ደግሞ የብሔራዊ ደህንነት ተልዕኮ እና ጥብቅ የመረጃ ደህንነት ፍላጎት ላላቸው ተቋማት አግባብ ባለመሆናቸው እንዲህ አይነት ልምዶችን ለማስተካከል ፈጣን እርምጃ ይፈልጋል።

ከፋይናንስ ደህንነት ጋር ተያይዞ በሀገራችን ሽብርተኝነትን በገንዘብ ከመደገፍ እና በወንጀል የተገኘ ገንዘብን ህጋዊ የማድረግ እንቅስቃሴዎችን ለመከላከል እየተደረጉ ያሉ ጥረቶች ቢኖሩም ውጤታማነታቸው ዝቅተኛ ነው። ለዚህም የ ICT ዘርፉ በፍጥነት እያደገ በመሆኑ ይህን ለመቆጣጠር የሚያስችል በዘመናዊ ቴክኖሎጂ የተደገፈ ሲስተም ባለመኖሩ እንዲሁም ብሔራዊ መታወቂያ ስርዓት ትግበራ መዘግየት ጋር ይገናኛል። ለእያንዳንዱ ዜጋ ፎርጅድ ለማድረግ የማይቻል ብሔራዊ መለያ መኖር እንደ ምርጥ ተሞክሮ በተወሰዱ ሀገራት መሰረት ነው። ብሔራዊ መለያ ስርዓት ዲጂታል የህዝብ ቁልፍ መሰረተ ልማት (Public Key Infrastructure) እንዲሁም ሚጎኛውም ኔትወርክ እና ኢንፎርሜሽን ሲስተም የሚመሰረትበት ስርዓት በመሆኑ አሁን ላይ የሚስተዋሉ የማጭበርበር፣ ስርጎ መግባት ለመግታት እንዲሁም ህግን ለማስከበር እና ተጠያቂነትን ለማረጋገጥ የሚያስችል ማስረጃ አለመኖር ከዚህ ጋር ተያያዥ ናቸው። ለዚህም አሁን ካለው አዋጆች የሚያጠናክር የህግ እና ቁጥጥር ማዕቀፎችን መዘርጋት እና ተግባራዊ እንዲሆኑ ማስቻል እንዲሁም የህዝብ ቁልፍ መሰረተልማትን ተግባራዊ ማድረግ ያስፈልጋል።

ምክረ ሀሳቦች

በዚህ በመጨረሻው ክፍል ሳይበር ደህንነት በኢትዮጲያ ብሔራዊ ደህንነት ላይ የሚኖረውን አሉታዊ ተጽዕኖ ለመቀነስ የሚረዱ የፖሊሲ አቅጣጫዎችና ግቦች እንዲሁም ምርጥ ተሞክሮዎችን የያዙ ምክረ ሀሳቦች ቀርበዋል። በሀገራዊ ደረጃ የብሔራዊ ሳይበር ደህንነት ፖሊሲና ስትራቴጂ እንዲሁም የብሔራዊ መረጃ ደህንነት ፖሊሲና ስትራቴጂ ክለሳ በሚመለከታቸው ባለድርሻ አካላት ተሳትፎ እንዲሁም በክፍተኛ አመራር ያልተቋረጠ ድጋፍና ክትትል ሊዘጋጅ እና በትጋት ሊተገበር ይገባል። ለዚህም ስትራቴጂያዊ የሁኔታ ትንተና ከአምስት እስከ አስር ዓመት ጊዜ በሚዘጋጅ የስጋት ትንተና እንዲሁም የሪስክ ትንተናን መነሻ ማድረግ አስፈላጊ ነው። ይህም በሀገራዊ እና ተቋማዊ ደረጃ ለሚደረግ የሀብት ምደባ መሰረት ይሆናል።

ተቋማትም በዚህ መነሻነት የራሳቸውን ፖሊሲና ስትራቴጂ በመቅረጽ ሀገራዊ ጥረቶችን አሟጦ በመጠቀም፣ ከሌሎች ተቋማት ጋር በመተባበር የጋራ የሳይበር ደህንነት ጉዳዮች ላይ በጋራ በመስራት እንዲሁም ከራሳቸው ተልዕኮ አንጻር በመቃኘት

ለተግባራዊነቱ ሊሰሩ ይገባል። ከዚህ በተጨማሪ ከአመራር ጀምሮ በየደረጃው ያሉ ግለሰቦችንና ቡድኖችን እና አጠቃላይ ዜጎችን አቅም በመገንባት እና ግንዛቤ በመፍጠር እና እነዚህ አቅሞች አስተባብሮ ጥቅም ላይ እንዲውሉ በማድረግ ውጤት ማምጣት ይቻላል። ለዚህም አመራሩ በባለቤትነት መንፈስ እንዲሳተፍ ማድረግ እና ጉዳዩን ትኩረት እንዲያገኝ በማድረግ በሀገራዊ እና ተቋማዊ ደረጃዎች የብዙኃን መነጋገሪያ እንዲሆን ማድረግ አስፈላጊ ነው። ሳይበር ደህንነት በብሔራዊ ደህንነት ምክርቤት እየተሰጠው ካለው ትኩረት በተጨማሪ በህዝብ ተወካዮች ምክር ቤት እንዲሁም በሚኒስትሮች ምክርቤት አጀንዳዎችን ለይቶ በማቅረብ ውይይት ቢደረግበት ይህንን አቅም ለማሻሻል የሚያስችል አቅጣጫዎችን ለመለየት ያስችላል። በተለይም የህዝብ ተወካዮች ምክርቤት በመከላከያ፣ ደህንነት እና የውጭ ጉዳይ ቋሚ ኮሚቴው በኩል በሚደረግ ክትትል እና ቁጥጥር መነሻነት በሳይበር ደህንነት ጉዳይ እየተነጋገረ አቅጣጫዎችን መስጠት ወሳኝ ነው።

ከፖሊሲና ስትራቴጂ ቀረጻና ትግበራ አንጻር በመጀመሪያ ስትራቴጂያዊ አመራሩ ሊደረስባቸው እና ሊለኩ የሚችሉ የሳይበር ደህንነት ስትራቴጂያዊ ግቦችን ለይቶ በማስቀመጥ ሁሉም የሳይበር ደህንነት አካል የሚኖረውን ድርሻና ኃላፊነት ለይቶ በማስቀመጥ ግቦቹን ለማሳካት የሚጠይቀውን ሀብትን መመደብ እና ለታለመለት ዓላማ ጥቅም ላይ መዋሉን ማረጋገጥ ያስፈልጋል። ስለዚህም እያንዳንዱ ባለድርሻ አካል ሊያሳካ የሚፈለገውን ግብ፣ የሚኖረውን ተግባርና ኃላፊነት ለይቶ የሚያውቅ በመሆኑ የሀብት ብክነትን ለመቀነስ እና የሚደረጉ ጥረቶችን በማዋሀድ ስትራቴጂያዊ ግቦችን ለማሳካት ያስችላል። አደረጃጀትን በተመለከተ በአንዳንድ ሀገራት እንደሚደረገው ብሔራዊ የሳይበር ደህንነት ጉዳዮች ላይ ብቻ አተኩሮ የሚሰራ ከሳይበር ደህንነት ተቋማት የተውጣጣ የብሔራዊ ሳይበር ደህንነት ምክርቤት ማቋቋም አስፈላጊ ነው። ይህ ተቋም ለብሔራዊ ደህንነት ምክርቤት ተጠሪ ሊደረግ የሚችል ሲሆን የራሱ ዕቅድ አውጥቶ በመንቀሳቀስ በሀገራዊና ተቋማዊ ደረጃ አሁን ያለውን እንቅስቃሴ ውጤታማነት ከፍ ለማድረግ ያስችላል። ከዚህም መካከል ብሔራዊ የሳይበር ደህንነት አርክቴክቸር ማዘጋጀት፤ የሳይበር ደህንነት አቅም ግንባታ ስራዎች እንዲሁም ሀገራዊ እና ዘርፋዊ ትብብር እንቅስቃሴዎችን ማጠናከር፤ የሳይበር ደህንነት ፖሊሲና ስትራቴጂ ቀረጻና ትግበራ ውጤታማነት ከፍ ለማድረግ፤ እንደ ሀገር የምንከተለው ፍልስፍና እና አቅጣጫ፤ የሳይበር ደህንነት ቋንቋ አጠቃቀም እንዲሁም ስታንዳርድ ዝግጅት፤ የፕሮግራምና ፕሮጀክት ቀረጻና ትግበራ እንዲሁም ጥናትና ምርምር ስራዎችን ውጤታማ ለማድረግ ይረዳል።

በመቀጠል የተቋማትን የሰው፣ የቴክኖሎጂያዊ እና የአሰራር አቅም በሚፈለገው ደረጃ መገንባት እና ጥሩ የሚባል የሳይበር ደህንነት ባህል መገንባት ያስፈልጋል። ትምህርትና ስልጠና በጣም ጠቃሚ ቢሆኑም ለሁሉም ሰራተኛ ይህን ማድረግ ስለማይቻል በንባብ፣ ግንዛቤን መፍጠሪያ መድረኮች እንዲሁም ሌሎች መደበኛና መደበኛ ያልሆኑ አማራጮችን መጠቀም ያስፈልጋል። ለምሳሌ ሰዎች የሻይ ዕረፍት ሰዓታቸውን ወደካፌ በመሄድ፣ በማኅበራዊ ሚዲያ ወይም ከባልደረቦቻቸው ጋር በማውራት ሊያሳልፉ ይችላሉ፤ እንደዚህ አይነት አጋጣሚዎችን በመጠቀም ሰዎችን እያዝናኑ የሳይበር ደህንነት ዕውቀትና ግንዛቤ እንዲሁም አመለካከት ለመቀየር የሚያስችሉ ስራዎችን መስራት ይቻላል፤ ፖምፍሌቶችን፣ አዝናኝ እና ቀልብ ሳቢ ቪዲዮዎችን ወይም ጨዋታዎችን እና ውድድሮችን በማዘጋጀት በጊዜ ሂደት ተቋማዊ የባህል ለውጥ ማምጣት ይቻላል። ስለዚህም የሚመለከታቸው ባለድርሻ አካላት በጋራ በመገናኘት በጥናት ላይ ተመስርተው የተቋማትን ባህል መቀየር የሚቻልበትን ሁኔታ መፍጠር ይችላሉ። ለምሳሌ አሁን ባለው የመከላከያ ሰራዊት ተቋማዊ አደረጃጀት ጥናትና ምርምር ማዕከል እንዲሁም ከሙኒኬሽን፣ ኤሌክትሮኒክስ እና ሳይበር ዋና መምሪያ በተቋሙ እንዲህ አይነት ስራዎችን መምራት የሚችሉ ክፍሎች ናቸው።

ብሔራዊ ደህንነትን ሊጎዱ የሚችሉ ሳይበር ጥቃቶችን ከመከላከል አንጻር በሀገራዊ ደረጃ ያሉንን ሀብቶች በመለየት፣ ያሉባቸውን ስጋቶች እና ተጋላጭነት በየጊዜው በመፈተሽ ሪስክ ላይ የተመሰረተ ጥበቃ ማድረግ ያስፈልጋል። ሀብቶችን ከተለዩና ቅደምተከተል ከወጣላቸው በኋላ ሊከሰቱ የሚችሉ ጥቃቶችን አስቀድሞ ለመከላከል እና በጥቃቱ የሚደርሱ ጉዳቶችን ለመቀነስ ያስችላል። በየጊዜው የሚደርሱ የሳይበር ጥቃቶችን በመመዝገብ እና በባለድርሻ አካላት መካከል የመረጃ ልውውጥን በማበረታታት ግንዛቤን ለመፍጠርና በአንድ ተቋም ላይ የደረሰ ጥቃት በሌሎች እንዳይደርስ ለመከላከል ያስችላል። ይህም በሰው ኃይል ብቻ ሊሆን ስለማይችል በጥናትና ምርምር እንዲሁም ልማት ላይ በመመስረት የሳይበር ጥቃትን ለመመከት የሚያስችል የተቀናጀ ኃይል መገንባት ያስፈልጋል። ሳይበር ጥቃትን ለመከላከል ይህ ነው የሚባል አንድ መፍትሄ ባይኖርም ተገቢውን አሰራር፣ ቴክኖሎጂ እና ዕውቀት በማጣመር ሪስክ በከፍተኛ ደረጃ ለመቀነስ ያስችላል።[39] አሰራር ማለት ፖሊሲና ስትራቴጂ፣ ማስፈጸሚያ ዕቅዶችእንዲሁም ክትትልና ግምገማ አንድ ርዕሣዊ ጀነራል "ሰላምን ከፈለግክ ለጦርነት ተዘጋጅ" ሲሉ እንደገለጹት ሁልጊዜ የመከላከል አቅም ግንባታ ላይ ማተኮር ይገባል። ከቴክኖሎጂ አንጻር በየጊዜው የሚዘምኑ ጸረ ቫይረስ፣ ፋየር ዎልን ያካተተ የመሳሪያዎች ደህንነት ሲሆን በየጊዜው በእነዚህ የደህንነት ሶፍትዌሮች እየተፈተሸ ተልዕኳችንን ለማሳካት እንቅፋት የማይፈጥሩ መሆን አለባቸው። እያንዳንዱ የ ICT መሳሪያ ተያያዥ ሪስክ ያለው ሲሆን ምን ያክል ሪስክ እንዳለው መለካትና ያን ሪስክ ማካካስ የምንችልበት ዘዴ ማበጀት፤ ሁልጊዜ የደህንነት ፍተሻ ማድረግ፤ እንዲሁም በረጅም ጊዜ ከሶስተኛ ወገን ይልቅ የራሳችንን አቅም በመገንባት ጥገኝነታችን በራሳችን ላይ ማድረግ አለብን። ሳይበር ጥቃትን ለመከላከል የሚያስችል

[39] Strategy, "Types of Cyber Attacks Every Business Should Avoid," Strategy LLC, 2020, https://strategynewmedia.com/types-of-cyber-attacks/.

ዕውቀትን በተመለከተ ለሰራተኞች ከተሰጣቸው ኃላፊነት አንጻር የተቃኘ በየጊዜው አዳዲስ ግንዛቤዎችን ማስጨበጥ አስፈላጊ ነው። ለምሳሌ፦ ከኢንተርኔት ዳውንሎድ ስለሚያደርጓቸው ፋይሎች፣ ደህንነቱ የተጠበቀ የኢ-ሜይል እና ማኅበራዊ ሚዲያ አጠቃቀም፣ ስለ ይለፍ ቃል ጥንካሬ እንዲሁም በአሁኑ ጊዜ እየተከሰቱ ስላሉ አዳዲስ ጥቃቶች እና ማድረግ ስላለባቸው ጥንቃቄዎች ሊያውቁ ይገባል።

በተቋማት ሊዘወተሩ የሚገባ የሳይበር ደህንነት ልምምዶች መካከል በየዓመቱ ወይም በሁለት ዓመት አንድ ጊዜ ስትራቴጂያዊ የሳይበር ደህንነት ዳሰሳ እንዲሁም ቴክኒካዊ የሳይበር ደህንነት ግምገማ ማድረግ ወይም ህግ በሚፈቅደው እና የተቋሙን ወይም ብሔራዊ ጥቅምን በማይጎዳ መልኩ በሦስተኛ ወገን ማስደረግ አለባቸው። ይህም እንደ ሰርቨር ያሉ የተቋማት ወሳኝ ሀብቶች ጉዳት እንዳይደርስባቸው ለማድረግ፤ የተቋማት ኮምፒዩተሮች እና ኔትወርኮች እኩይ አላማ ባላቸው አካላት ሌሎችን ለማጥቃት እንዳይውሉ ለማድረግ፤ የምናደርጋቸው ግንኙነቶች እንዳይጠለፉ ለማድረግ ያስችላል። ልክ እንደ ጦርነት ሁሉ አንድ ተቋም ምንም ያክል ቢዘጋጅ ሳይበር ጥቃትን ሙሉ ለሙሉ ማስቀረት የማይችል በመሆኑ ለማይቀረው መዘጋጀት ይኖርበታል። ከሳይበር የሚመጣ ብዙ ኪሳራ የሚያደርስ ቀውስ ማስቀረት የሚቻለው ጥቃቱ ከመከሰቱ በፊት፣ በተከሰተ ጊዜ እንዲሁም ከተከሰተ በኋላ በሚሰሩ ስራዎች ነው። ስለዚህም ተቋማት ከኢመደአ የብሔራዊ የሳይበር ኢመርጀንሲ ሪስፖንስ (ETHIO-CERT) በመተባበር የሚሰራ የራሳቸውን የሳይበር ጥቃት መከላከል ቡድን ሊያቋቁሙ ይገባል። የ 24/7 ክትትል እና የመረጃ ልውውጥ በማድረግ ማስጠንቀቂያ ማግኘት ይችላሉ፤ በቅጽበት የሳይበር ጥቃት ሲከሰት ደግሞ እነዚህ ቡድኖች ተቀናጅተው የመከላከል ዕቅድ በማውጣት ቶሎ ለመመለስ እና ጥፋቱን ለመቀነስ ይችላሉ። ከዚህም በመነሳት ለወደፊቱ ትምህርት መውሰድ የሚቻልበትን ሁኔታ መፍጠር እና መሻሻል የሚገባቸውን አቅሞቻችንን ለማሻሻል ያስችላል።

በተጨማሪም በቅርቡ የተጀመረው የብሔራዊ መታወቂያ ፕሮግራም ትግበራ ተጠናክሮ መቀጠል ሳይበር ደህንነትን ለማረጋገጥ ትልቅ ሚና አለው።[40] ይህም ለዲጂታል ትራንስፎርሜሽን መሳካት እንዲሁም ለሳይበር ደህንነት ተግባራት አስቻይ ሁኔታን ከመፍጠር ባሻገር የሳይበር ወንጀልን ለመከላከል ያስችላል። በተጨማሪም የሳይበር ደህንነትን ፈተናዎችን ለመቋቋም የሚቻልባቸውን ስርዓቶች በሀገራዊና ተቋማዊ ደረጃ ለመተግበር ያስችላል።

በመጨረሻም በዚህ ጥናት የቀረቡት የፖሊሲ ምክረ ሀሳቦች መተግበር ከሳይበር የሚመጣው ስጋት ብሔራዊ ደህንነት ላይ አሉታዊ ተጽዕኖ እንዳይኖረው በማድረግ ተልዕኮን ለማሳካት የሚያግዙ ሲሆን ይህን ለማስፈጸም ሀገራዊ እና ተቋማዊ አመራር የግንዛቤ ለውጥ በማምጣት ያለውን የአመራር ጥበብ በመጠቀም የመሪነት ድርሻውን መወጣት አለበት። ይህም ግልጽ ግቦችን በማስቀመጥና አቅጣጫዎችን በማሳየት፤ ለተቋማት ግልጽ ድርሻና ኃላፊነትን በመስጠት እና የሚያደርጉትን ጥረት በማስተባበር፤ እንዲሁም በየደረጃው የአቅም ግንባታ ስራዎችን በመስራት እና የህብት ምደባ በማድረግ ይገለጻል። ይህም በአንድ ጊዜ የሚሳካ ስለማይሆን በየጊዜው ዳሰሳ በማድረግ የእርምት እርምጃ መውሰድ ይጠበቃል። ለዚህም የመንግስት ሀብት የሚመደብ በመሆኑ የሳይበር ደህንነት ግልጽነት (የመረጃ ነጻነት) ማረጋገጥ እንዲሁም የህዝብን ሀሳብ እና ጥቅም ማስጠበቅ የሚቻልበትን ስርዓት መዘርጋት ያስፈልጋል። ይህም በዘርፉ ከጥርጣሬ ይልቅ የህዝብን እምነትና ድጋፍ ለማግኘት ይረዳል።

ዋቢ መጽሐፍት

Abenezer Berhanu, Weldegiorgis. “Developing National Cybersecurity Strategy for Ethiopia.” *National Security Office*. Tallinn University of Technology, 2019.

Baraki Belay, Zemedkun. “The Prosecution of Criminal Conducts Committed over Social Media’s in Ethiopia: Acts of ‘Hate Speech’ in Focus.” University of Gondar, 2019.

Council of Ministers. “Information Network Security Agency Re-Eslablishment.” *Federal Negarit Gazette*, 2011.

[40] ENA, “Ministry Launches National ID Pilot Project | Ethiopian News Agency,” Ethiopian News Agency, 2020, https://www.ena.et/en/?p=15393.

ENA. "Ministry Launches National ID Pilot Project | Ethiopian News Agency." Ethiopian News Agency, 2020. https://www.ena.et/en/?p=15393.

Ethiopian News Agency. "INSA Alarmed by Increase in Cyber Attacks, Calls for Swift Actions | Ethiopian News Agency." Ethiopian News Agency, 2019. https://www.ena.et/en/?p=10542.

Ethiopian Press Agency. "Hate Speech and Freedom of Expression in Ethiopia | Ethiopian Press Agency." Ethiopian Press Agency, 2019. https://www.press.et/english/?p=5520#.

FDRE House of People Representatives. "A Proclamation on the Defense Forces of the Federal Democratic Republic of Ethiopia." *Federal Negarit Gazette* 22, no. 15 (2019): 8686–95.

———. "Information Network Security Agency Re-Establishment Proclamation." *Federal Negarit Gazette* 22, no. 15 (2013): 8686–95.

Federal Democratic Republic of Ethiopia. "Ethiopia Digital Strategy 2020," 2020.

———. "National Information Security Policy," 2011.

Galinec, Darko, Darko Moznik, and Boris Guberina. "Cybersecurity and Cyber Defence: National Level Strategic Approach." *Automatika* 58, no. 3 (2017): 273–86. https://doi.org/10.1080/00051144.2017.1407022.

Gee, David. *Rethinking Security: A Discussion Paper*, 2016.

Halefom, Hailu. "The State of Cybercrime Governance in Ethiopia," no. May 2015 (2015): 1–35.

Hjortdal, Magnus. "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." *Journal of Strategic Security* 4, no. 2 (2011): 1–24. https://doi.org/10.5038/1944-0472.4.2.1.

IGI. "What Is Infrastructure Security | IGI Global." IGI Global, 2020. https://www.igi-global.com/dictionary/managing-compliance-with-an-information-security-management-standard/42019.

Internet World Stats. "Internet World Stats: Usage and Population Statistics." Internet World Stats, 2018. https://www.internetworldstats.com/.

Kinfe Micheal, Yilma. "ScienceDirect Developments in Cybercrime Law and Practice in Ethiopia." *Computer Law*

& Security Review 30, no. 6 (2014): 720–35. https://doi.org/10.1016/j.clsr.2014.09.010.

Kissinger, Henry. *World Order*. Penguin Books, 2014.

Kleinberg, Howard. "Building a Theoretical Basis for Cyber Security Best Practices." *Annals of the Master of Science in Computer Science and Information Systems at UNC Wilmington* 9, no. 2 (2015).

Markoff, John. "Before the Gunfire, Cyberattacks - The New York Times." The New York Times, 2008. https://www.nytimes.com/2008/08/13/technology/13cyber.html.

Ministry of Information. "The F.D.R.E Foreign Affairs and National Security Policy and Strategy," no. November (2002): 1–89.

Murphy, Matt. "Cyberwar - War in the Fifth Domain | Briefing | The Economist." The Economist, 2010. https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain.

Office of the Director of National Intelligence. "Assessing Russian Activities and Intentions in Recent US Elections." *Office of the Director of National Intelligence*, no. January (2017): 1–25.

Paleri, Prabhakaran. *National Security: Imperatives and Challenges*. New Delhi: Tata McGraw-Hill Pub. Co., 2008.

Romm, Joseph J. *Defining National Security: The Nonmilitary Aspects*. Council on Foreign Relations, 1993.

Rubenstein, Dana. "Nation State Cyber Espionage and Its Impacts," 2014, 1–11.

Schatz, Daniel, Rabih Bashroush, and Julie Wall. "Towards a More Representative Definition of Cyber Security." *Journal of Digital Forensics, Security and Law* 12, no. 2 (2017): 53–74.

Siboni, Gabi, and David Siman-Tov. "Cyberspace Extortion: North Korea versus the United States." *INSS Insight*, no. 646 (2014).

Strategy. "Types of Cyber Attacks Every Business Should Avoid." Strategy LLC, 2020. https://strategynewmedia.com/types-of-cyber-attacks/.

Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." Wired, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.