DCAF Geneva Centre for Security Sector Governance

გენდერული თანასწორობა, კიბერუსაფრთხოება და უსაფრთხოების სექტორის მმართველობა

გენდერის როლი კიბერუსაფრთხოების მმართველობაში

კატერინ მილარი, ჯეიმს შაიარსი, ტატიანა ტროპინა

DCAF-ის შესახებ

DCAF – უსაფრთხოების სექტორის მართვის ჟენევის ცენტრი ემსახურება სახელმწიფოებისა და მათი ერების უსაფრთხოების გაუმჯობესებას დემოკრატიული მართვის, კანონის უზენაესობის, ადამიანის უფლებების პატივისცემისა და გენდერული თანასწორობის ფარგლებში. 2000 წელს, დაარსების მომენტიდან მოყოლებული DCAF-ს შეაქვს თავისი წვლილი მდგრადი სამყაროსა და განვითარების უზრუნველყოფაში; ეხმარება პარტნიორ სახელმწიფოებს და ამ სახელმწიფოების მხარდამჭერ საერთაშორისო აქტორებს უსაფრთხოების სექტორის მართვის გაუმჯობესებაში ინკლუზიური და მონაწილეობითი რეფორმების მეშვეობით; ქმნის ცოდნის ინოვაციურ პროდუქტებს, ხელს უწყობს ნორმებისა და კარგი პრაქტიკების დანერგვას, უზრუნველყოფს იურიდიულ და პოლიტიკურ კონსულტაციებს და მხარს უჭერს როგორც სახელმწიფო, ისე არასახელმწიფო უსაფრთხოების სექტორის დაინტერესებული მხარეების შესაძლებლობების განვითარებას. DCAF-ის საფონდო საბჭოს წევრები წარმოადგენენ 50-ზე მეტ ქვეყანას და ჟენევის კანტონს. DCAF-ი აქტიურია 70-ზე მეტ ქვეყანაში და საერთაშორისოდ არის აღიარებული, როგორც მოწინავე გამოცდილების მსოფლიოს ერთ-ერთი წამყვანი ცენტრი უსაფრთხოების სექტორის მმართველობისა (SSG) და რეფორმირების სფეროში (SSR). DCAF-ი ხელმძღვანელობს ნეიტრალიტეტის, მიუკერძოებლობის, ადგილობრივი საკუთრების, ინკლუზიური მონაწილეობისა და გენდერული თანასწორობის პრინციპებით. დამატებითი ინფორმაციისთვის ეწვიეთ ვებგვერდს: www.dcaf.ch და თვალყური გვადევნეთ X @DCAF_Geneva-ზე.

ISBN 978-92-9222-749-4

Cover Photo credit: shutterstock_2136788105

ეს პუბლიკაცია შეიქმნა DCAF – უსაფრთხოების სექტორის მართვის ჟენევის ცენტრის პროექტის „დასავლეთ ბალკანეთში კიბერუსაფრთხოების ხარისხიანი მართვის“ ფარგლებში, რომელიც ხორციელდება გაერთიანებული სამეფოს საგარეო საქმეთა, თანამეგობრობისა და განვითარების ოფისის მხარდაჭერით.

DCAF-ის ამ ნაშრომში განხილულია შემდეგი საკითხები:

- რა კავშირია გენდერსა და კიბერუსაფრთხოებას შორის?
- როგორ უწყობს ხელს გენდერული თანასწორობა კიბერუსაფრთხოების კარგ მმართველობას?
- კიბერუსაფრთხოების რა ძირითადი სფეციფიკური გამოწვევები არსებობს უსაფრთხოების სფეროს მმართველობისას, გენდერული თანასწორობის ინტეგრაციის პროცესში?

შესავალი

კიბერუსაფრთხოება – ეს არის უსაფრთხოების იმ საკითხების ფართო სპექტრი, რომლებსაც სახელმწიფოები, კორპორაციები, თემები, სამოქალაქო საზოგადოებები და ცალკეული ინდივიდები აწყდებიან საინფორმაციო და საკომუნიკაციო ტექნოლოგიების გამოყენების შედეგად. კიბერუსაფრთხოება სულ უფრო ფართოდ მოიაზრება ეროვნული და საერთაშორისო უსაფრთხოების მნიშვნელოვან კომპონენტად.[1] ისევე, როგორც უსაფრთხოების მმართველობის სხვა ასპექტები, კიბერუსაფრთხოების კარგი მმართველობა დიდწილად დამოკიდებულია გენდერულ თანასწორობაზე. ამ ნაშრომში ნაჩვენებია კავშირი გენდერულ თანასწორობასა და კიბერუსაფრთხოებას შორის, როგორც უსაფრთხოების სექტორის კარგი მმართველობის მნიშვნელოვანი კომპონენტი; მიმოხილულია არსებული ინსტრუმენტებისა და პრინციპების გამოყენება კიბერუსაფრთხოების კარგ მმართველობაში, განსაკუთრებით გენდერულ უსაფრთხოებასთან დაკავშირებით; ასევე, განხილულია კიბერუსაფრთხოების განსაკუთრებული გამოწვევები, რომლებიც შეიძლება საჭიროებდეს მმართველობის ახალ სტრატეგიებს ან არსებული სტრატეგიების შემოქმედებითად გამოყენებას. ხაზგასმულია, რომ კიბერუსაფრთხოება მოიცავს არა მხოლოდ უსაფრთხოების ტრადიციულ სექტორს (სამხედრო სექტორი, პოლიცია, იუსტიცია, ემიგრაცია და ა.შ.), არამედ, ასევე სხვა საზოგადოებრივ სფეროებსაც (მაგალითად, კერძო სექტორს), რომლებიც ყოველთვის მოიაზრება ეროვნულ და საერთაშორისო უსაფრთხოებასთან კავშირში.

1. რა არის გენდერი და გენდერული თანასწორობა?

გენდერი მიემართება დროის მოცემულ მონაკვეთში კონკრეტული საზოგადოების მიერ მიღებულ მასკულინობასა და ფემინურობასთან დაკავშირებულ სოციო-კულტურულად კონსტრუირებულ როლებს, მოლოდინებს, ატრიბუტებსა და ფასეულობებს. მიუხედავად იმისა, რომ გენდერი ხშირად აღიქმება ქალებისა და კაცებისთვის შედარებით მისაღები ქცევის მოლოდინად, რეალურად არაბინარული და მრავალფეროვანია. მნიშვნელოვანია აღინიშნოს, რომ გენდერი დაკავშირებულია სოციალურ ურთიერთობებთან, რესურსების გადანაწილებასთან და ძალაუფლებისა და შესაძლებლობების ხელმისაწვდომობასთან ქალების, კაცების, არაბინარული და მრავალფეროვანი გენდერული იდენტობისა და გენდერული თვითგამოხატვისთვის.[2]

> გენდერი სულ უფრო ხშირად აღიქმება, როგორც ინტერსექციური: სოციალური ძალაუფლების მრავალ ფორმასთან ერთად არსებული ფენომენი

1. ძირითადი საერთაშორისო ძალისხმევა კიბერუსაფრთხოების სტრუქტურების, ნორმებისა და კანონების შემუშავებისთვის მოიცავს საერთაშორისო უსაფრთხოების კონტექსტში საინფორმაციო და საკომუნიკაციო ტექნოლოგიების საკითხების გაეროს ღია სამუშაო ჯგუფს (OEWG, 2019 წლიდან დღემდე), საერთაშორისო უსაფრთხოების კონტექსტში კიბერსივრცეში პასუხისმგებლობიანი ქცევის ხელშეწყობის ექსპერტთა გლობალურ ჯგუფს (GGE, 2006-2021) და საინფორმაციო და საკომუნიკაციო ტექნოლოგიების კრიმინალური მიზნებისთვის გამოყენების წინააღმდეგ ბრძოლის ყოვლისმომცველი საერთაშორისო კონვენციის შემუშავების დროებით კომიტეტს (AHC, 2022 წლიდან დღემდე). ამ ძალისხმევას თან ახლავს რეგიონალური სტრუქტურები და ინიციატივები, როგორიცაა ევროპის საბჭოს ბუდაპეშტის კონვენცია კიბერდანაშაულის შესახებ, აფრიკის კავშირის კონვენცია კიბერუსაფრთხოებისა და პირადი მონაცემების დაცვის შესახებ და ნატოს მიერ მხარდაჭერილი არასავალდებულო ტალინის სახელმძღვანელო კიბერ ომის მიმართ მოქმედი საერთაშორისო სამართლის შესახებ.

2. გაეროს ქალთა ორგანიზაციის სასწავლო ცენტრის ელექტრონული სწავლების კამპუსი, გენდერული თანასწორობის ლექსიკონი (ნიუ-იორკი: UN Women). https://trainingcentre.unwomen.org/mod/glossary/view.php?id=36&mode=letter&hook=G&sortkey=&sortorder=asc

გენდერი სულ უფრო ხშირად აღიქმება, როგორც ინტერსექციური: სოციალურ კლასთან, რასასთან, კოლონიალიზმთან, ეროვნებასთან, შესაძლებლობებთან, ეთნიკურ კუთვნილებასთან, კასტასთან, სექსუალურ ორიენტაციასთან, ასაკთან და სოციალური ძალაუფლების მრავალ სხვა ფორმასთან ერთად არსებული ფენომენი.[3] ეს ნიშნავს, რომ გენდერული თანასწორობის მისაღწევად საჭიროა ქალების, კაცების და მრავალფეროვანი გენდერული იდენტობისა და გენდერული თვითგამოხატვის მქონე და სხვა ადამიანების გამოცდილების, შესაძლებლობებისა და საჭიროებების გათვალისწინება. ეს უზრუნველყოფს უთანასწორობის ნაკლებად თვალსაჩინო, მაგრამ დაკავშირებული ფორმების, გაუთვიცნობიერებლად გამყარების თავიდან აცილებას. მაგალითად: მიუხედავად იმისა, რომ გენდერი განსხვავდება **სექსუალური ორიენტაციისგან** (ადამიანის ემოციური და/ან რომანტიკული მიზიდულობა სხვა ადამიანებისადმი[4]) – ჰეტეროსექსუალური მიზიდულობა საპირისპირო სქესის ადამიანებისადმი ხშირად არის საზოგადოების გენდერული მოლოდინი ქალებისა და კაცების მიმართ. შედეგად, ყველა გენდერული იდენტობის ბისექსუალი, ლესბოსელი და გეი შეიძლება წააწყდეს სტიგმას, დისკრიმინაციასა და ძალადობას. ამიტომ, გენდერულ თანასწორობაზე მუშაობისას მნიშვნელოვანია სექსუალობისა და ზემოთ აღწერილი რიგი სოციალური ფაქტორების გათვალისწინება.

გენდერული თანასწორობა ნიშნავს „თანაბარ უფლებებს, შესაძლებლობებსა და შედეგებს გოგოებისა და ბიჭების, ქალებისა და კაცების“ და მრავალფეროვანი გენდერული იდენტობისა და გენდერული თვითგამოხატვის მქონე ადამიანებისთვის.[5] გენდერული თანასწორობა გაეროს წესდებითა და ბევრი სხვა საერთაშორისო ვალდებულებით ადამიანის დადგენილი უფლებაა.[6] გენდერული თანასწორობის მხარდაჭერა მოიცავს გენდერული ნიშნით ძალადობასთან ბრძოლის პოლიტიკას; ეს არის ქოლგა-ტერმინი, რომელიც აღნიშნავს ფიზიკური, ემოციური, სექსუალური თუ ფსიქოლოგიური ხასიათის მავნე ქმედებებს, რომლებიც ხორციელდება ადამიანის ნების საწინააღმდეგოდ და ეფუძნება სოციალურ (გენდერულ) განსხვავებას, რომელსაც ქალებსა და კაცებს მიაკუთვნებენ და მომდინარეობს გენდერის ბინარული გაგებიდან.[7]

2. რა კავშირია გენდერსა და უსაფრთხოებას შორის?

გენდერი უსაფრთხოებას ორგვარად უკავშირდება.[8] პირველი: ქალებს, კაცებს, გოგოებს, ბიჭებს და მრავალფეროვანი გენდერული ინტენტობისა და გენდერული თვითგამოხატვის მქონე ადამიანებს აქვთ სხვადასხვა საჭიროება, შესაძლებლობა და მოთხოვნა უსაფრთხოების კუთხით. მაგალითად, მიუხედავად იმისა, რომ ყველა გენდერული იდენტობის ადამიანი კონფლიქტისას თავს დაუცველად გრძნობს, კაცები,

3. კიმბერლი კრენშოუ. „საზღვრების ასახვა: ინტერსექციურობა, იდენტობის პოლიტიკა და ძალადობა ფერადკანიანი ქალების მიმართ“. Stanford Law Review გამოცემა 43, № 6, 1991 წლის ივლისი, გვ. 1241-1299. https://doi.org/10.2307/1229039; და კომბაჰის მდინარის კოლექტივი, „შავკანიანი ფემინისტის განცხადება“, Women’s Studies Quarterly, გამოცემა 42. № ¾, შემოდგომა/ზამთარი 2014, გვ. 271-280. https://www.jstor.org/stable/24365010

4. თავისუფალი და თანასწორი გაერთიანებული ერები, განმარტებები.. https://www.unfe.org/definitions/

5. ანრი მარტინენი, გენდერისა და უსაფრთხოების სახელმძღვანელო მითითებების კრებული 1: უსაფრთხოების სექტორის მმართველობა, უსაფრთხოების სექტორის მმართველობა და გენდერი, გვ. 7. ჟენევის უსაფრთხოების სექტორის მართვის ცენტრი ((DCAF), OSCE/ODIHR და გაეროს ქალთა ორგანიზაცია, 2019. თანასწორობის საკითხების ლექსიკონი. https://www.dcaf.ch/sites/default/files/publications/documents/GSToolkit_Tool-1%20EN%20FINAL_2.pdf. იხ. ასევე გაეროს ქალთა ორგანიზაცია, გენდერული თანასწორობის ლექსიკონი. გაეროს ადამიანის უფლებების უმაღლესი კომისარი, დისკრიმინაციული კანონები და პრაქტიკა და ასევე ძალადობის აქტები სექსუალური ორიენტაციისა და გენდერული იდენტობის ნიშნით, დოკ. გაერო. A/HRC/19/41, 17 ნოემბერი, 2011 წ., პარაგრაფი 20.

6. იხ. DCAF, OSCE/ODIHR და გაეროს ქალთა ორგანიზაცია, გენდერისა და უსაფრთხოების სექტორის რეფორმის სახელმძღვანელო მითითებების კრებული (ჟენევა: DCAF, 2008). https://www.dcaf.ch/gender-and-security-toolkit.

7. რ. ჩარლი კარპენტერი, „კონფლიქტურ სიტუაციებში მოქალაქე კაცებისა და ბიჭების მიმართ გენდერული ნიშნით ძალადობის აღიარება, ომის კრიმინოლოგია“, გვ. 377-397 (Routledge, 2017).

8. გაეროს ადამიანის უფლებათა უმაღლესი კომისრის ოფისი (OHCHR), ქალთა უფლებები და გენდერული პრობლემები კონფლიქტისა და არასტაბილურობის სიტუაციებში. https://www.ohchr.org/en/women/womens-human-rights-and-gender-related-concerns-situations-conflict-and-instability გაეროს ადამიანის უფლებათა საბჭო, აზრისა და გამოხატვის თავისუფლების მ

გენდერით განპირობებული რწმენები და ვარაუდები უსაფრთხოების შესახებ ზეგავლენას ახდენს, თუ რა აღიქმება უსაფრთხოების საფრთხედ, როგორ ხდება პრიორიტეტების განსაზღვრა და უსაფრთხოების რესურსების განაწილება.

ბიჭები და ადამიანები, რომლებიც აღიქმებიან კაცურებად/მასკულინურებად შეიძლება იქცნენ განსაკუთრებულ სამიზნეებად და დაიღუპონ ომში (ან გაიწვიონ ძალდატალებით); ეს განპირობებულია გენდერული ვარაუდით, რომ ყველა კაცი და ბიჭი მეომარი ან პოტენციური მეომარია.[9] ზუსტად ასევე, ქალები, გოგოები და ადამიანები, რომლებიც აღიქმებიან ქალურებად/ფემინურებად, კონფლიქტის პირობებში გენდერული ნიშნით ძალადობის მსხვერპლები ხდებიან. ძალადობის ფორმებს შორის ერთ-ერთია სექსუალური ძალადობა. ქალებს მიაწერენ სტერეოტიპებს, რომელთა მიხედვითაც ისინი ომში ყოველთვის/მხოლოდ მსხვერპლები არიან. ქალების, როგორც მეომრების, მშვიდობისმყოფელების, პოლიტიკოსებისა თუ სამოქალაქო საზოგადოების წარმომადგენლების როლს არასათანადო ყურადღება ექცევა, რაც იწვევს მათ გამორიცხვას მშვიდობიანი მოლაპარაკებების, კონფლიქტების თავიდან აცილების, პოლიტიკისა და აღდგენითი პროგრამების შემუშავების პროცესებიდან. [100]

მეორე: გენდერით განპირობებული რწმენები და ვარაუდები უსაფრთხოების შესახებ ზეგავლენას ახდენს, თუ რა აღიქმება უსაფრთოხების საფრთხედ, როგორ ხდება პრიორიტეტების განსაზღვრა და უსაფრთხოების რესურსების განაწილება. მაგალითად, რადგან სახელმწიფო და სამხედრო უსაფრთხოების უწყებები ხშირად უმეტესად კაცებით არის დაკომპლექტებული და ასოცირდება ისეთ მასკულინურ ატრიბუტებთან, როგორიცაა ძალაუფლება, ავტორიტეტი და საზოგადოებრივი დაცვა, სახელმწიფოს უსაფრთხოება ხშირად ცალკეული პირებისა (განსაკუთრებით ქალების, მრავალფეროვანი გენდერული იდენტობისა და გენდერული თვითგამოხატვის მქონე ადამიანებისა და მარგინალური ჯგუფების წარმომადგენლების) და სამოქალაქო საზოგადოების ორგანიზაციებზე მნიშვნელოვნად მიიჩნევა. სახელმწიფო უსაფრთხოების ისეთი საფრთხეები, როგორიც არის ომი და ტერორიზმი, ასევე, ხშირად უფრო პრიორიტეტულად არის აღქმული, ვიდრე საფრთხეები, რომლების წინაშეც ცალკეული ადამიანები თუ თემები დგანან (მაგალითად: სიღარიბე, იძულებით გადაადგილება, გარემოს დეგრადაცია და გენდერული ნიშნით ძალადობა).

უფრო მოკლედ, ყველა გენდერული იდენტობისა და გენდერული თვითგამოხატვის მქონე ადამიანს აქვს უსაფრთხოების უფლება. შესაბამისად, უსაფრთხოების მმართველობაში გენდერული თანასწორობა მოიცავს იმის გათვალისწინებას, რომ კაცები, ქალები და სხვადასხვა გენდერული იდენტობისა და გენდერული თვითგამოხატვის მქონე ადამიანები განსხვავებულ ზეგავლენას განიცდიან უსაფრთხოების გამოწვევების წინაშე; ასევე, იმაზე დაკვირვებას, თუ რა ზეგავლენა აქვს გენდერულ ნორმებსა და მოლოდინებს ჩვენს წარმოდგენებსა და პრიორიტეტებზე, დაუცველობის ფორმებს შორის. გენდერული თანასწორობა უსაფრთხოების მმართველობაში ასევე მოიცავს ქალების, კაცების და სხვადასხვა გენდერული იდენტობისა და გენდერული თვითგამოხატვის მქონე ადამიანებისთვის ერთნაირი შესაძლებლობის უზრუნველყოფას მონაწილეობა მიიღონ უსაფრთხოების მმართველობაში.

9. გაეროს ადამიანის უფლებათა საბჭო, აზრისა და გამოხატვის თავისუფლების მხარდაჭერისა და დაცვის საკითხებში სპეციალური მომხსენებლის ანგარიში, პარაგრაფი 20-21 (გაეროს გენერალური ასამბლეა, 2011). https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf

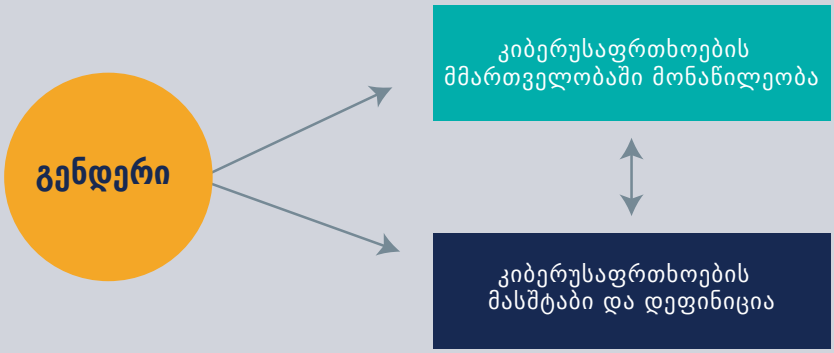
10. გიქვე, პარაგრაფი 53. იხ ასევე: გაეროს ადამიანის უფლებების უმაღლესი კომისარი, გაერთიანებული ერების ორგანიზაციის ადამიანის უფლებების უმაღლესი კომისრის ოფისის ანგარიში: კარგი პრაქტიკები და გამოწვევები, რომლებსაც სახელმწიფოები აწყდებიან საზოგადოებრივ საქმეში მონაწილეობის უფლების ეფექტიანი რეალიზაციის რეკომენდაციების გამოყენებისას, A/HRC/49/42, პარაგრაფი 10. https://www.ohchr.org/en/calls-for-input/2021/report-good-practices-and-challenges-using-guidelines-participation

3. რა კავშირია გენდერსა და კიბერუსაფრთხოებას შორის?

იგივე ფაქტორები – გენდერული დაუცველობის განცდა, გენდერული წარმოდგენები უსაფრთხოებაზე და გენდერული თანასწორობა უსაფრთხოების მმართველობაში მონაწილეობისას – აქტუალურია კიბერუსაფრთხოების კონტექსტშიც. თუმცა ყველაფერს ართულებს ტერმინი „კიბერუსაფრთხოების“ მნიშვნელობის ბუნდოვანება. კიბერუსაფრთხოება თავისი ძირითადი განმარტებით უკავშირდება საინფორმაციო და საკომუნიკაციო ტექნოლოგიების გამოყენების საფრთხეებს, მაგრამ ეს ტექნოლოგიები მსოფლიოში მილიარდობით ადამიანის ყოველდღიურობის უდიდეს ნაწილს იკავებს, რაც ნიშნავს, რომ უსაფრთხოების პრაქტიკულად ყველა პრობლემას აქვს კიბერ კომპონენტი. ამიტომ, მნიშვნელოვანია ყურადღება მიექცეს იმას, თუ როგორ შეიძლება აყალიბებდეს გენდერული მოლოდინები და ღირებულებები კიბერუსაფრთხოების მნიშვნელობას და როგორ მოქმედებს ეს ყველაფერი ქალების, კაცების და მრავალფეროვანი გენდერული იდენტობისა და გენდერული თვითგამოხატვის მქონე ადამიანების უსაფრთხოებაზე. გადაწყვეტილებები იმის შესახებ, თუ რა არის და რა არ არის კიბერუსაფრთხოების პრობლემა, ასახავს და ამყარებს მანამდე არსებულ გენდერულ (ინტერსექციურ) უთანასწორობას, მათ შორის გენდერული ნიშნით ძალადობას და აქვს შესაძლებლობა წარმოშვას საფრთხის ახალი კერებიც.

ეს ურთიერთკავშირი ნაჩვენებია სურათი 1-ში. გენდერი პირდაპირ ზეგავლენას ახდენს კიბერუსაფრთხოების მმართველობის განმარტებაზე, რადგან უსაფრთხოების, მათ შორის, კიბერუსაფრთხოების საკითხები, როგორც უკვე ავღნიშნეთ, თავის არსში მოიცავს გენდერულ ნორმებსა და მოლოდინებს. გენდერი, ასევე, პირდაპირ გავლენას ახდენს კიბერუსაფრთხოების მმართველობაში ჩართულობაზე, რადგან არსებობს გენდერული (და სხვა ინტერსექციური) უთანასწორობა უნარებსა და მახასიათებლებში, რომლებიც აღიქმება სავალდებულოდ კიბერუსაფრთხოების მმართველობისთვის - როგორც ეს დეტალურად არის აღწერილი მომდევნო აბზაცებში. და ბოლოს, გენდერი ირიბად, მაგრამ ორმხრივად ახდენს ზეგავლენას როგორც შესაძლებლობაზე, ასევე მონაწილეობაზე. გენდერული უთანასწორობა დამატებით ამყარებს კიბერუსაფრთხოების შესახებ გენდერულ წარმოდგენებს, ხოლო კიბერუსაფრთხოების ვიწრო გენდერული აღქმა იზიდავს და ფილტრავს მონაწილეებს მსგავსი გენდერული ნიშნით. ამ თავის მომდევნო ნაწილში უფრო დეტალურად არის განხილული ეს სამმაგი კავშირი და საჭიროებისამებრ გამოყენებულია ილუსტრაციები.

სურათი 1: გენდერის ზეგავლენა კიბერუსაფრთხოების მმართველობაზე



გენდერი და კიბერუსაფრთხოებაში მონაწილეობა

ქალებს, მრავალფეროვანი გენდერული იდენტობისა და გენდერული თვითგამოხატვის მქონე ადამიანებსა და კაცებს, ყველას აქვს და უნდა ჰქონდეს უფლება და შესაძლებლობა, მოძებნოს, მიიღოს და გადასცეს ინფორმაცია ინტერნეტის საშუალებით,[11] მონაწილეობა მიიღოს საზოგადოებრივ ცხოვრებაში ონლაინ-ინსტრუმენტების[12] გამოყენებით, მიიღოს განათლება კიბერუსაფრთხოების/საინფორმაციო და საკომუნიკაციო ტექნოლოგიების სფეროში, იმუშაოს ტექნიკურ პოზიციებზე საინფორმაციო და საკომუნიკაციო ტექნოლოგიების/კიბერუსაფრთხოების სფეროში და მონაწილეობა მიიღოს კიბერუსაფრთხოების მმართველობასა და კონტროლში. დღეს ქალები (და, დიდი ალბათობით, მრავალფეროვანი გენდერული იდენტობისა და გენდერული თვითგამოხატვის მქონე ადამიანები, თუმცა მონაცემები ამ საკითხთან დაკავშირებით მწირია) არასათანადოდ არიან წარმოდგენილი კიბერუსაფრთხოებაში მონაწილეობის ყველა ასპექტში.

მაგალითად, ქალების წვდომა ინტერნეტზე გლობალურად შეფასებულია, როგორც კაცების წვდომის 85 პროცენტი; გლობალურ სამხრეთში დაახლოებით 1.7 მილიარდ ქალს შეზღუდული აქვს ინტერნეტზე წვდომა. ეს უთანასწორობა არის სერიოზული გამოწვევა ადამიანის უფლებების თვალსაზრისით. თავის მხრივ ადამიანის უფლებები კი კიბერუსაფრთხოების ყველა ასპექტის საფუძველია, პოტენციური დაუცველობიდან მმართველობაში მონაწილეობამდე. ეს ცნობილია როგორც **ციფრული გენდერული უთანასწორობა**.[13]

მეცნიერების, ტექნოლოგიების, ინჟინერიისა და მათემატიკის დარგის პროფესიები (STEM), რომლებიც (როგორც წესი) კიბერუსაფრთხოების ტექნიკური როლების წინამორბედია (ეროვნული ვარიაციებით), ხასიათდება გენდერული უთანასწორობით ქალებსა და კაცებს შორის (ხანდახან ცნობილი, როგორც „**სხვაობა ციფრულ უნარ-ჩვევებში**“).[14] ეს სხვაობა გამოწვეულია რთული და კონტექსტით განპირობებული მიზეზებით, რომელთა შორისაა: ა) უთანასწორობა ინფრასტუქტურასა (ციფრული გენდერული უთანასწორობა) და განათლებაზე ხელმისაწვდომობაში; ბ) ინდივიდუალური და ოჯახის შეზღუდვები და პრიორიტეტები; და გ) სოციო-კულტურული და ინსტიტუციური გენდერული ნორმები, რომელთა მიხედვითაც STEM სფეროს პროფესიები (და ტექნიკური უნარ-ჩვევები/შესაძლებლობები) უმეტესად კაცურია/კაცებისთვისაა.[15] ეს გენდერული უთანასწორობა განათლებასა და STEM სფეროსთვის მომზადებაში ხანდახან მოიხსენიება მეტაფორად „მილსადენის პრობლემა - **Pipeline Problem**“[16] და თავისი წვლილი შეაქვს გენდერულ უთანასწორობაში ტექნიკური პროფესიებისა და კიბერუსაფრთხოების დარგში, თუმცა ერთადერთი მიზეზი ეს არ არის.

შეფასებების მიხედვით, მთელ მსოფლიოში კიბერუსაფრთხოების სფეროში მომუშავე ადამიანთა დაახლოებით 24 პროცენტია ქალი.[17] და ეს იმის მიუხედავად, რომ ადრე კომპიუტერული მეცნიერებები და პროგრამირება შედარებით უფრო ხელმისაწვდომი იყო ქალებისთვის.[18] დროთა განმავლობაში კომპიუტერული მეცნიერებები სოციო-კულტურულად სულ უფრო მეტად აღიქმებოდა, როგორც კაცური/

11. კეტრინი მილარი, ჯეიმს შაიარსი და ტატიანა ტროპინა, გენდერული მიდგომები კიბერუსაფრთხოებიდასმი: დიზაინი, დაცვა და რეაგირება (UNIDIR, 20-21), სქოლიოს შენიშვნა 86. https://unidir.org/publication/gender-approaches-cybersecurity. იხ. ასევე ვაიკმანი, იანგი და ფიცმორისი (2020), ციტირებული ნაშრომი.

12. იქვე გვ. 33, სქოლიო 87.

13. ა. ვიტორესი და ა. გილ-ხუარესი, „ქალები კომპიუტერულ მეცნიერებებში-სთან დაკავშირებული პრობლემები: კომპიუტერულ მეცნიერებაში გენდერული სხვაობის კვლევის განხორციელების კრიტიკული ანალიზი“, Journal of Gender Studies (2006), 25(6), გვ 666-680.

14. ილარი, შაიარსი, ტროპინა (2021) op. cit., გვ. 31 სქოლიო 80.

15. იხ. მაგ: რენდალ სტროსი, „რამ აიძულა ქალები უარი ეთქვათ კომპიუტერულ მეცნიერებებზე?“, New York Times (2008 წლის 16 ნოემბერი).http://classtap.pbworks.com/f/Women%20Driven%20From%20Computer%20Science%20Field.pdf

16. ჯს. ლაითი, „როცა კომპიუტერები ქალები იყვნენ“, Technology and Culture, 40(3) (1999), გვ. 455-483.

17. მილარი, შაიარსი, ტროპინა (2021), ციტირებული ნაშრომი. გვ. 31 სქოლიო 81.

18. იხ. ლიზა შარლანდი და სხვ. განახლებული სისტემები: ქალების, მშვიდობისა და კიბერუსაფრთხოების დღის წესრიგისკენ (UNINDIR, 2021). გვ 11-15. https://unidir.org/publication/system-update-towards-women-peace-and-cybersecurity-agenda

მხოლოდ კაცებისთვის; ეს ხდებოდა ფორმალური ეკონომიკისთვის, სფეროს მნიშვნელობის ზრდის პარალელურად (და სოციალური ცნობადობისა და პრესტიჟისთვის)[19] ასევე, ქალებს ტექნიკურ პოზიციებზე გამოფიტვის უფრო მაღალი მაჩვენებელი აქვთ, ვიდრე კაცებს; 2016 წელს აშშ-ში ჩატარებული კვლევის მიხედვით, ქალები ორჯერ უფრო ხშირად ტოვებდნენ ტექნოლოგიებთან დაკავშირებულ პოზიციებს.[20] კიბერუსაფრთხოების სფეროში ქალების შესახებ 2017 წლის კვლევამ კი აჩვენა, რომ მათი 87 პროცენტი საუბრობდა ფარულ დისკრიმინაციაზე, ხოლო 19 პროცენტს შეეხო ღია და აშკარა დისკრიმინაცია.[21]1

გენდერული თანასწორობის მნიშვნელობა კიბერუსაფრთხოების მმართველობასა და მოლაპარაკებებში აღიარებულია საერთაშორისო დონეზე. მაგალითად, საერთაშორისო უსაფრთხოების კონტექსტში საინფორმაციო და საკომუნიკაციო ტექნოლოგიების საკითხებზე გაეროს ღია სამუშაო ჯგუფის საბოლოო მოხსენება (OEWG) ადასტურებს ქალების მონაწილეობის მნიშვნელობას კიბერუსაფრთხოების დარგში, საერთაშორისო გადაწყვეტილებების მიღების პროცესში და მოუწოდებს სახელმწიფოებს, იმოქმედონ და განავითარონ პოტენციალი, რათა ქალებისთვის უზრუნველყონ პროცესში მონაწილეობის შესაძლებლობა.[22] სახელმწიფო დელეგაციებმა გაეროს კიბერდანაშაულის სპეციალურ კომიტეტში (AHC) ასევე ხაზი გაუსვეს გენდერული თანასწორობის აუცილებლობას კიბერუსაფრთხოების პრობლემების გადაწყვეტასა და კიბერგამოძიების მმართველობაში. სახელმწიფოებმა აღიარეს კიბერუსაფრთხოების დაკავშირების მნიშვნელობა ქალების, მშვიდობისა და უსაფრთხოების (WPS) დღის წესრიგთან [23] , ომელიც ადგენს ქალთა მონაწილეობას უსაფრთხოების მმართველობაში და გენდერულ თანასწორობასა და ადამიანის უფლებებს საკვანძო კონპონენტად წარმოაჩენს. თუმცა, ამ საერთაშორისო პროცესებისა და ასევე, ეროვნული იურისდიქციების უმეტესობის კუთხით გასაკეთებელი კიდევ ბევრია, მანამ, სანამ კიბერუსაფრთხოების სფეროს მმართველობაში, აღსრულებასა და კონტროლში გენდერული თანასწორობა მიიღწევა.

მთლიანობაში, მიუხედავად იმისა, რომ ქალები წამყვან როლებს ასრულებენ კიბერუსაფრთხოებაში (ტექნიკური ექსპერტებიდან პოლიტიკის შემქმნელებამდე), გენდერული თანასწორობის მიღწევა კიბერუსაფრთხოების ყველა ასპექტში ჯერ მიუღწეველ და მნიშვნელოვან მიზნად რჩება. იმისათვის, რომ უკეთ გავიაზროთ გამოცდილება და მხარი დავუჭიროთ მრავალფეროვანი გენდერული იდენტობის, გენდერული თვითგამოხატვის მქონე და სექსუალური ორიენტაციის ადამიანებს კიბერუსაფრთხოების სფეროში, საჭიროა უფრო დეტალური მონაცემები. კიბერუსაფრთხოების სფეროში გენდერული თანასწორობის ხელშეწყობის საკვანძო, მაგრამ არა განმსაზღვრელი კომპონენტია შემდეგი საკითხების

19. გაეროს გენერალური ასამბლეა, A/AC.290/2021/CRP.3, პარ. 37. https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf. დამატებითი ინფორმაციისთვის კიბერუსაფრთხოებისა და გაეროს ქალების, მშვიდობისა და უსაფრთხოების დღის წესრიგის შესახებ, იხ. შარლანდი და სხვ. (2021), იქვე. გვ. 15-19.

20. ეროვნული სადაზვერვო პრაქტიკასა და მართვაში გენდერული თანასწორობისა და პერსპექტივის მნიშვნელობის შესახებ იხ. ლორენ ჰატონის ნაშრომი DCAF Gender and Security Tool 14: Gender and Intelligence, (DCAF, 2019). https://www.dcaf.ch/sites/default/files/publications/documents/GSToolkit_Tool-14%20EN%20FINAL_0.pdf

21. Mმიმოხილვისთვის იხ. იულია სკუპსკა და ლორა შიპი, „რა უნდა იცოდეთ თვალთვალისა და რეპროდუქციული უფლებების შესახებ როი უეიდის წინააღმდეგ საქმის შემდგომ სამყაროში“, The Conversation (6 ივლისი, 2022). https://theconversation.com/what-you-need-to-know-about-surveillance-and-reproductive-rights-in-a-post-roe-v-wade-world-185933. მსგავსი რისკების ამსახველი ინციდენტების მაგალითებისთვის იხ. Privacy International, „რატომ საჭიროებს რეპროდუქციული ჯანმრთელობა ინდოეთში ჩვენს გადაუდებელ ყურადღებას?“ (24 თებერვალი, 2020). https://privacyinternational.org/long-read/3368/why- does-reproductive-health-surveillance-india-need-our-urgent-attention; ჯესიკა დევისი, „პენსილვანიის ჯანდაცვის სისტემაზე გამოძალვითი თავდასხმის შედეგად გატეხილია 300 000 ჩანაწერი“, Healthcare IT News (26 ივლისი, 2017).https://www.healthcareitnews.com/news/300000-records-breached-ransomware-attack-pennsylvania-health-system; და რ. ერნანდესი, „ჰადადის ადმინისტრაცია ინტერნეტში აქვეყნებს პაციენტების მონაცემებს“, Folha de S.Paulo (6 ივლისი, 2016).). https://www1.folha.uol.com.br/cotidiano/2016/07/1788979-gestao-haddad-expoe-na-internet-dados-de-pacientes-da- rede-publica.shtml

22. იკიბერუსაფრთხოების მსგავსი რისკების ამსახველი მარცხების მაგალითებისთვის იხ. BBC News, „ტრანსგენდერთა საქველმოქმედო ორგანიზაცია Mermaids UK დიდ ბოდიშს იხდის მონაცემთა გაჟონვისთვის“ (16 ივლისი, 2019). https://www.bbc.co.uk/news/uk-48652970; და ფოქსი, კრისი, „გენდერული იდენტობის კლინიკიდან პაციენტების ელექტრონული ფოსტის მისამართებმა გაჟონა“, BBC News (6 სექტემბერი, 2019).https://www.bbc.co.uk/news/technology-49611948

23. დებორა ბრაუნი და ელისონ პიტლაკი, „რატომ არის გენდერი მნიშვნელოვანი საერთაშორისო კიბერუსაფრთხოებისთვის“ (ქალთა საერთაშორისო ლიგა მშვიდობისა და თავისუფლებისთვის და პროგრესული კომუნიკაციების ასოციაცია, 2020), გვ. 10-11. https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf. DDOS თავდასხმების გენდერული ასპექტი ასევე შეიძლება მუშაობდეს საპირისპირო მიმართულებით: მაგალითად, შედარებით დროებითი ან უმნიშვნელო ინციდენტების მიმართულებით, რომლებიც მიმართულია საკვანძო სახელმწიფო ეროვნულ უსაფრთხოებაზე ან ფინანსურ დაწესებულებებზე. ანალოგიური ლოგიკა ასევე შეიმჩნევა „დეფეისმენტის“ ინციდენტებში; მაგალითისთვის იხ. რიკი ბენ-დევიდი, „ისრაელის კიბერ დირექტორატი ავრცელებს ყოველწლიურ გაფრთხილებას ირანის „იერუსალიმის დღის წინ“, The Times of Israel (22 აპრილი, 2022). https://www.timesofisrael.com/israel-cyber-directorate-issues-annual-warning-ahead-of-irans-jerusalem-day/

მოგვარება: ა) გენდერული მიკერძოება და ვარაუდები, რის მიხედვითაც STEM და კომპიუტერული ტექნოლოგიის სფერო არის კაცური/კაცებისთვის; ბ) ამასთან დაკავშირებული გენდერული იერარქია, რომელიც უპირატესობას ანიჭებს უფრო ტექნიკურ STEM ექსპერტიზას და მასკულინობასთან დაკავშირებულ კომპიუტერულ ცოდნას და შედარებით ნაკლებადაა კონცენტრირებული კიბერუსაფრთხოების სფეროს სხვა მნიშვნელოვან მიმართულებებსა და უნარ-ჩვევებზე, მაგალითად, პოლიტიკის შემუშავებაზე, მმართველობაზე, ეთიკასა და ზედამხედველობაზე.

კიბერუსაფრთხოების სფეროსა და მისი საფრთხეების აღქმა გენდერულ ჭრილში

კიბერუსაფრთხოება ხშირად ესმით სახელმწიფო უსაფრთხოების კონტექსტში, რაც დაკავშირებულია ციფრული ქსელების და ეროვნული თავდაცვის მთავარი სისტემების (მათ შორის, „კრიტიკული ინფრასტრუქტურის“) მთლიანობასთან და სახელმწიფო დაზვერვისა და სამხედრო კიბეროპერაციებისთვის ჰაკერული ინსტრუმენტების გამოყენებასთან (ცნობილი, როგორც „შეტევითი კიბერშესაძლებლობები“). ასევე, როგორც ტრადიციული უსაფრთხოების შემთხვევაში, ეს განსაზღვრება პრიორიტეტს ანიჭებს საზოგადოებრივ საქმიანობებს, რომლებიც ხშირად დაკავშირებულია კაცებთან და მასკულინობასთან. კიბერუსაფრთხოების ტრადიციული გაგების კიდევ ერთი მთავარი ასპექტია **კერძო ან კორპორაციული** ერთეულები, რომლებიც ცდილობენ შეინარჩუნონ ქსელების, სისტემების და/ან ორგანიზაციის კონფიდენციალურობა, კეთილსინდისიერება და ხელმისაწვდომობა (CIA ტრიადა).

მოცემულ განმარტებაში არ არის გათვალისწინებული ზეგავლენა, რომელიც ხშირად ეხებათ ცალკეულ პირებს, განსაკუთრებით, ქალებს, გოგოებს, მრავალფეროვანი გენდერული იდენტობის, გენდერული თვითგამოხატვის მქონე და სექსუალური ორიენტაციის ადამიანებს და ასევე, სპეციფიკური საჭიროების მქონე ან უმცირესობების თემების წარმომადგენლებს, მათ შორის როგორც სამოქალაქო საზოგადოების წევრებს. მათი უსაფრთხოების უფლება არ არის გათვალისწინებული. განსაკუთრებით დიდი გამოწვევა არსებობს ქალებისა და გოგოების შემთხვევაში, რაც მოიცავს პირადი ელ. ფოსტის და/ან სოციალური მედიის ანგარიშების გატეხვას, ღილაკების ჩაწერის პროგრამული უზრუნველყოფისა და პროგრამა-ჯაშუშების გამოყენებას ოჯახში ძალადობისა და თვალთვალისთვის. ყველა წარმომადგენელი დგას „გატეხვის“ შედეგად სამედიცინო ინფორმაციის გაჟონვის რისკის ქვეშ. მაგრამ არსებობს დისკრიმინაციის, სტიგმატიზაციისა და გენდერული ნიშნით ძალადობის რისკი იმ პირებისთვის, რომლებსაც დაფეხმძიმება შეუძლიათ, თუ მათი რეპროდუქციული ისტორია და ამასთან დაკავშირებული ინფორმაცია ცნობილი ხდება მონაცემთა გაჟონვის შედეგად.[24] ანალოგიურად, მრავალფეროვანი გენდერული იდენტობის, გენდერული თვითგამოხატვის მქონე და სექსუალური ორიენტაციის ადამიანები შეიძლება იქცნენ სამიზნედ სამედიცინო (და სხვა) მონაცემთა კონფიდენციალურობის დარღვევის შედეგად.[25] სერვისზე წვდომის შეზღუდვის შეტევის (DDOS) ტიპის თავდასხმები, რომლებიც მიმართულია კონკრეტული საინფორმაციო და საკომუნიკაციო ტექნოლოგიების სისტემების, ინფორმაციით გადატვირთვის საშუალებით ქსელების ან მოწყობილობების დაბლოკვაზე, ასევე, შეიძლება აღრმავებდეს გენდერულ უთანასწორობას. მაგალითად, მიუხედავად იმისა, რომ გენდერსა და DDOS-ს შორის კავშირზე დამატებითი კვლევებია საჭირო, პირველადი მონაცემებით ასეთი თავდასხმები შესაძლოა ამძაფრებდეს გენდერული უთანასწორობის არსებულ ფორმებს. მაგალითად – მობილური ელექტრონული კომერციის, მიკროსაბანკო და ფინანსური გადარიცხვების ვებგვერდების მწყობრიდან გამოყვანა, რომლებსაც ბევრი მეწარმე ქალი ეყრდნობა, იწვევს მათ ფინანსურ არასტაბილურობას.[26]

24. კიბერუსაფრთხოების სფეროს ანალიზის უდიდესი ნაწილი კიდევ უფრო დეტალურ განმსახვავებელ ხაზებს ავლებს ამ მაგალითებს შორის: მაგალითად, წვდომის ვექტორებს (მაგ: ფიშინგი), მუდმივი წვდომის აუცილებლობას (რომელიც, როგორც წესი, საჭიროა მონაცემთა გაჟონვისთვის, მაგრამ არა DDoS-ისთვის) და წვდომის მიღების შემდეგ „მიზნის მისაღწევ ქმედებებს“ შორის (გაჟონვა, პიროვნების მოპარვა, ექსფილტრაცია და სხვა).

25. იხ. მილარი, შაიარსი და ტროპინა (2021), ციტირებული ნაშრომი. ადამიანების ან სოციალური ურთიერთობების ნაცვლად ტექნოლოგიურ სისტემებზე ფოკუსირება, სავარაუდოდ, ასევე დეფინიციური მიკერძოებაა, რომელიც ასოცირდება კაცურობის დომინანტურ ფორმებთან.

26. ბრაუნი და პიტლაკი (2020), ციტირებული ნაშრომი, გვ 9-10.

კიბერუსაფრთხოების შეზღუდული სახელმწიფო ან კორპორაციულ-ცენტრისტული განსაზღვრება, ერთი შეხედვით, **გენდერულად ნეიტრალურია** – რადგან, იგულისხმება, რომ საფრთხეები, რომლებსაც ეს დარგი ებრძვის, ერთნაირ ზეგავლენას ახდენს ყველაზე. თუმცა, ამ ვარაუდის დაშვებით, კიბერუსაფრთხოების განსაზღვრება **გენდერულად ბრმად** რჩება, რადგან არ ითვალისწინებს მეთოდებს, რომლებითაც კიბერსაფრთხეები განსხვავებულ ზეგავლენას ახდენს ქალებზე, კაცებსა და მრავალფეროვანი გენდერული იდენტობისა და გენდერული თვითგამოხატვის მქონე ადამიანებზე. გენდერული პერსპექტივა ვარაუდობს, რომ სახელმწიფოზე ან კორპორაციებზე კონცენტრირებული კონცეფციებიდან ჩვენ უნდა გადავიდეთ ინდივიდზე ან ადამიანზე ორიენტირებულ მიდგომებზე, რომლებიც ითვალისწინებს ცალკეული პიროვნებების ზიანს (ასევე, სპეციფიკური საჭიროების მქონე თემებისა და უმცირესობების შემთხვევაში), როგორც კიბერუსაფრთხოების და ეროვნული უსაფრთხოების ან კორპორაციების ეკონომიკური ზარალის საკითხებს.

კიბერუსაფრთხოება, ასევე, შეიძლება განისაზღვროს იმ თვალსაზრისით, თუ როგორ უკავშირდება მავნე ქმედება საინფორმაციო და საკომუნიკაციო ტექნოლოგიების გამოყენებას და არა საფრთხის წინაშე მდგომ აქტორს (მაგალითად, სახელმწიფო პიროვნების წინააღმდეგ). კიბერუსაფრთხოება შეიძლება ვიწროდ გავიგოთ, როგორც კომპიუტერულ სისტემებსა და მოწყობილობებში **მავნე ჩარევის** თავიდან აცილება (მაგალითად, ჰაკინგი, სერვისის დაბლოკვა, „ფიშინგი“ და ა.შ.), ასევე, ინფორმაციაში არასანქცირებული ჩარევა (და/ან შეცვლა), მაგალითად, მონაცემთა გაჟონვა ან პირადი ინფორმაციის მოპარვა. ეს არის განმარტება, რომელსაც ყველაზე ხშირად იყენებენ კიბერუსაფრთხოების ტექნიკური პრაქტიკოსები.[27]

მიუხედავად ამისა, განსაზღვრება შეიძლება იყოს გენდერულად ბრმა, რადგან ვარაუდობს, რომ კიბეროპერაციები ერთი და იგივე მეთოდით ახდენს ზეგავლენას ყველა ადამიანზე ან – რომ მავნე ჩარევის წინაშე დაუცველია სისტემები და არა ადამიანი.[28] ასევე, ეს განმარება არ ითვალისწინებს გენდერულ ზეგავლენას, რომელიც მანიპულაციებით, ექსპლუატაციით, ციფრული ტექნოლოგიების მიზანმიმართული გაუქმებით ან მათზე ხელმისაწვდომობის შეზღუდვით არის გამოწვეული.

სანაცვლოდ, კიბერუსაფრთხოება შეიძლება განიმარტოს უფრო ვრცლად, **როგორც საინფორმაციო და საკომუნიკაციო ტექნოლოგიების გამოყენებასთან დაკავშირებული ინდივიდუალური, ჯგუფური ან საჯარო ზიანისგან დაცვა**. ეს შეიძლება მოიცავდეს ხელოვნურ ინტელექტთან დაკავშირებულ პრობლემებს, ტექნოლოგიების კონსტრუქციების, ალგორითმისა და მონაცემთა უზუსტობებს. კიბერუსაფრთხოების ასეთი ფართო გაგება პოტენციურად შეიძლება აერთიანებდეს ონლაინ-კონტენტისა და სოციალური მედიის ისეთ საკითხებს, როგორიც არის დეზინფორმაცია, ე.წ. დიფფეიკები, სიძულვილის ენა და გამომძალველობა. მიუხედავად იმისა, რომ კონცეფციის გაფართოებას შემოაქვს თანმიმდევრულობისა და გამოყენებადობის საკითხები, მთავარია ის, რომ კიბერუსაფრთხოების მასშტაბი უნდა დადგინდეს იმ ადამიანების მიერ, ვინც საინფორმაციო და საკომუნიკაციო ტექნოლოგიებთან დაკავშირებული საფრთხეებით ყველაზე მეტად ზარალდება.

კიბერუსაფრთხოების ეს უფრო ფართო განმარტება მოიცავს გენდერულად მეტად სპეციფიკურ გამოცდილებებს. ყველაზე ცხად მაგალითს წარმოადგენს: ინტერნეტის ბლოკირებამ, მაშინაც კი, თუ მთავრობის მიერ ხორციელდება ის და არა კიბეროპერაციის შედეგად, შეიძლება ფიზიკური საფრთხის წინაშე დააყენოს გოგოები, ქალები და მრავალფეროვანი გენდერული იდენტობისა და გენდერული თვითგამოხატვის მქონე ადამიანები. ამ დროს მათ არ აქვთ შესაძლებლობა, გამოიყენონ მობილური ტელეფონები და/ან იძულებულები არიან, გადაადგილდნენ საზოგოდოებრივ ადგილებში დღე-ღამის ბნელ მონაკვეთში. კიდევ ერთი მაგალითი: მონაცემთა მოცულობითი ნაკრებების უმეტესობა, რომლებიც

27. ქეროლაინ კრიადო-პერესი, , უხილავი ქალები: მონაცემთა მიკერძოების გამოვლენა კაცებისთვის შექმნილ სამყაროში (ლონდონი: Penguin Vintage, 2019); დ’იგნაზიო, კეტრინი და ლორენ ფ. კლაინი, მონაცემების ფემინიზმი. (ბოსტონი: MIT press, 2020).

28. იხ. ასევე: კეიტლინ ჩინი და მიშაელა რობისონი, „როგორ აძლიერებენ ხელოვნური ინტელექტის ბოტები და ხმოვანი ასისტენტები გენდერულ მიკერძოებებს“, ბრუკინგსის ინსტიტუტი (23 ნოემბერი, 2020). https://www.brookings.edu/research/how-ai-bots-and-voice-assistants-reinforce-gender-bias/; ხმოვანი ასისტენტებისა და რასის შესახებ იხ. ასევე ტ.ს. მორანის ნაშრომი „ტექნოლოგიის რასობრივი მიკერძოება და ხელოვნური ინტერნეტის ხმოვანი ასისტენტების თეთრკანიანი ქალის ხმა“, კომუნიკაცია და კრიტიკული/კულტურული კვლევები, 18(1) (2021), 18(1) (2021), გვ. 19-36. იხ ასევე მარკ ვესტის, რებეკა კრაუტისა და ჩუ ჰან ის კვლევა შემრცხვებოდა, რომ შემეძლოს: ციფრულ უნარ-ჩვევებში გენდერული სხვაობის დახურვა (იუნესკო, 2019). https://en.unesco.org/Id-blush-if-I-could

სულ უფრო ხშირად გამოიყენება ალგორითმების საშუალებით სოციალური სამყაროს შესახებ დასკვნების გამოსატანად და სამთავრობო პოლიტიკის ინფორმირებისთვის, აერთიანებს კაცების შესახებ კვლევების შედეგებს ან ეყრდობა ვარაუდებს კაცის უნივერსალური „ეტალონის“ შესახებ და განაზოგადებს მათ ადამიანზე.[29] ხმოვანი ხელოვნური დამხმარეები პირიქით, ხშირად ქალის ხმითა და სახელით არის წარმოდგენილი, რაც აძლიერებს უთანასწორო გენდერულ ნორმებს.[30] სახის ამომცნობის პროგრამულ უზრუნველყოფებში ხშირად ვხვდებით კარგად დამკვიდრებულ გენდერულ და რასობრივ მიკერძოებას.[31] იგივე ხშირად ვრცელდება ტექნიკის ინტერფეისებსა და პროდუქციაზე. მაგალითად, ჭკვიანი სახლის ტექნოლოგია სახლს ხშირად გულისხმობს უსაფრთხო სივრცედ, რომლის დაცვაც საჭიროა გარეშე პირებისგან. დიზაინში „საფრთხის მოდელირება“ არ ითვალისწინებს, რომ ტექნოლოგიის პოტენციალი, შესაძლოა გამოყენებულ იქნეს თვალთვალის, იძულებითი კონტროლისა და ოჯახში ძალადობისგან თავის დასაცავად.[32]

კიბერუსაფრთხოების ფართო გაგება, ასევე, გულისხმობს ონლაინ ძალადობას ქალებზე, გოგოებსა და მრავალფეროვანი გენდერული იდენტობის, გენდერული თვითგამოხატვის მქონე და სექსუალური ორიენტაციის ადამიანებზე, რაც ცნობილია, როგორც „გოგოებისა და ქალთა მიმართ ონლაინ ძალადობა“ ან უფრო ხშირად და ინკლუზიურად – **„ონლაინ გენდერული ნიშნით ძალადობა“**. მაგალითად, ყველა ადამიანი შეიძლება იქცეს შეუთანხმებლად ინტიმური გამოსახულების გავრცელების მსხვერპლად („პორნოშურისძიება“) – ეს შემდეგ ურთიერთქმედებს პატრიარქალურ და ჰეტერონორმატიულ გენდერულ წარმოდგენებთან, რაც ქალების, გოგოებისა და მრავალფეროვანი გენდერული იდენტობის, გენდერული თვითგამოხატვის მქონე და სექსუალური ორიენტაციის ადამიანების სტიგმატიზაციასა და დისკრიმინაციას იწვევს.[33] ზუსტად ასევე, ყველა გენდერის ადამიანი (ზოგიერთი კვლევის თანახმად, განსაკუთრებით მრავალფეროვანი გენდერული იდენტობის, გენდერული თვითგამოხატვის მქონე და სექსუალური ორიენტაციის ადამიანები) მოწყვლადია უკანონოდ მოპოვებული ინტიმური გამოსახულებით შანტაჟის მიმართ („სექსტორციის“ ფორმა).[34] ინტერნეტი, ასევე, შეიძლება გამოყენებულ იქნეს სექსუალური ძალადობისა და ექსპლუატაციის მიზნით, ადამიანებით ვაჭრობისა და ბავშვებზე სექსუალური ძალადობის მასალის გავრცელებისთვის.[35]6

29. ანასტასია პაუელი და ნიკოლა ჰენრი, ტექნოლოგიის მეშვეობით სექსუალური ძალადობის ვიქტიმიზაცია: ზრდასრული ავსტრალიელების ონლაინ გამოკითხვის შედეგები“, Journal of Interpersonal Violence, 34(17) (2019), გვ. 3637-3665; მანუელ გამეზ-გუადიქსი და დანიელა ინსერა, „ონლაინ ჰომოფობია: სექსუალური ვიქტიმიზაცია და რისკები ინტერნეტში და ფსიქიკური ჯანმრთელობა ბისექსუალ, ჰომოსექსუალურ, პანსექსუალურ, ასექსუალურ და ქვიარ მოზარდებში, კომპიუტერები ადამიანის ქცევაში, 119 (2021), 106728.

30. იხ. შარლანდი და სხვ. (2021), ციტირებული ნაშრომი, გვ. 24.

31. ადრიენ შო, „ინტერნეტი სავსეა არამზადებით, რადგან მსოფლიო სავსეა არამზადებით: რას გვასწავლის ინტერნეტის შესახებ ფემინისტური თეორია“, Communication and Critical/Cultural Studies,11(3) (2014), გვ. 273-277; იხ. ასევე გაეროს ადამიანის უფლებათა საბჭოს ანგარიში, მეცამეტე სესიაზე უმცირესობათა საკითხებზე ფორუმის მიერ გაცემული რეკომენდაციები თემაზე „სიძულვილის ენა, სოციალური მედია და უმცირესობები“: უმცირესობების საკითხებზე სპეციალური მომხსენებლის, ფერნანდ დე ვარენესის ანგარიში, A/HRC/46/58. https://digitallibrary.un.org/record/3901780?ln=en; Plan International, ონლაინ ყოფნის თავისუფლება?, (Plan International, 2020). https://plan-international.org/publications/free-to-be-online/; ქეით მარსტონი, „ლგბტ+ ახალგაზრდობის ინტიმურობისა და სოციალური მედიის კვლევა: მონაწილეთა მიერ მართული ვიზუალური მეთოდების ძლიერი მხარეები და შეზღუდვები“, Qualitative Inquiry 25, გამოცემა 3 (2019), გვ. 278-288; ანასტასია პაუელი, ადრიან ჯ. სკოტი და ნიკოლა ანრი, „ციფრული ძალადობა და შევიწროვება: სექსუალობისა და გენდერული უმცირესობის წარმომადგენელი ახალგაზრდების გამოცდილებები“, European Journal of Criminology, 17(2) (2020), გვ. 199–223.

32. იხ. მაგალითად, შარლანდი და სხვ. (2021), ციტირებული ნაშრომი, გვ. 27-8; რეგიონულად დაშლილი დეტალებისთვის იხილეთ: სერაფინ ავალა, დივინა ფრაუ-აიგსი, ღაიდა ჰასანი, ახალგაზრდობა და ძალადობრივი ექსტრემიზმი სოციალურ მედიაში: კვლევის კარტოგრაფირება (UNESCO Publishing, 2017); ღაიდა ჰასანი და სხვ. „ექსტრემისტული ონლაინ შინაარსის ზემოქმედებამ შეიძლება გამოიწვიოს ძალადობრივი რადიკალიზაცია: ემპირიული მტკიცებულებების სისტემატური მიმოხილვა“, International Journal of Developmental Science, 12(1-2) (2018), გვ. 71-88.

33. გამეზ-გუადიქსი და ინსერა (2021), ციტირებული ნაშრომი; პაუელი და ანრი (2019), ციტირებული ნაშრომი.

34. იხ. ლუსინა დი მეკო და სასკია ბრეხენმახერი, „პოლიტიკოს ქალებზე მიმართული ონლაინ ძალადობისა და დეზინფორმაციის წინააღმდეგ ბრძოლა“, კარნეგის ფონდი საერთაშორისო მშვიდობისთვის (30 ნოემბერი, 2020)“. https://carnegieendowment.org/2020/11/30/tackling-online-abuse-and-disinformation-targeting-women-in-politics-pub-83331; კარნეგის ფონდი საერთაშორისო მშვიდობისთვის (30 ნოემბერი, 2020). https://carnegieendowment.org/2020/11/30/tackling-online-abuse-and-disinformation-targeting-women-in-politics-pub-83331; Amnesty International UK, „შავკანიანი და აზიელი ქალი დეპუტატები უფრო მეტ შეურაცხყოფას იღებენ ონლაინ რეჟიმში“. https://www.amnesty.org.uk/online-violence-women-mps; საპარლამენტთაშორისო კავშირი, „სექსიზმი, შევიწროება და ძალადობა ქალი პარლამენტარების მიმართ“ (IPU, 2016). https://www.ipu.org/resources/publications/issue-briefs/2016-10/sexism-harassment-and-violence-against-women-parliamentarians

35. იხ. DCAF, უსაფრთხოების სექტორის რეფორმის წინამორბედი, კიბერუსაფრთხოების მართვა (მომდევნო).

ინტერნეტი არის ექსტრემისტული, რასისტული, მიზოგინიური, ჰომოფობიური და ტრანსფობიული კონტენტის გავრცელების საშუალება.[36] ეს კონტენტი ხელს უწყობს ქალების, გოგოების, მრავალფეროვანი გენდერული იდენტობის, გენდერული თვითგამოხატვის მქონე და სექსუალური ორიენტაციის ადამიანების და ასევე, სპეციფიკური საჭიროებების მქონე ჯგუფების მიმართ ძალადობას, როგორც ონლაინ, ისე ოფლაინ. ასევე, შეიძლება გამოყენებულ იქნეს ახალგაზრდების გადმოსაბირებლად,[37] რითაც ისინი სხვადასხვა საფრთხის წინაშე დგებიან –სექსუალური ექსპლუატაციიდან ძალადობაში მონაწილეობამდე თუ სისხლის სამართლის სისტემასთან დაკავშირებით.

შედეგად, ქალები, გოგოები და მრავალფეროვანი გენდერული იდენტობის თუ გენდერული თვითგამოხატვის მქონე ადამიანები ხშირად ხდებიან მიზოგინიის, ჰომოფობიისა და ტრანსფობიის (ასევე რასიზმის, ფეტფობიისა და ეიბლიზმის), ზიზღის ენისა და ონლაინ შევიწროების ობიექტები, რაც შესამჩნევად მოქმედებს მათ თანაბარუფლებიან ხელმისაწვდომობაზე ინტერნეტსა და სოციალურ მედიაზე.[38] ვინაიდან ინტერნეტი არის საზოგადოებრივი ცხოვრების საკვანძო ელემენტი ყველა დემოკრატიული ქვეყნისთვის, ეს ფაქტი მნიშვნელოვან საფრთხეს უქმნის ადამიანის უფლებებს. კვლევები ასევე აჩვენებს, რომ ქალი პოლიტიკოსები, განსაკუთრებით უმცირესობათა თემების წარმომადგენლები, ძალიან ხშირად არიან მუქარისა და ონლაინ შევიწროების მსხვერპლი, რაც პოლიტიკაში ქალთა მონაწილეობისთვის შემაფერხებელი ფაქტორია და მნიშვნელოვნად აზიანებს დემოკრატიას.[390]

საერთო ჯამში, კიბერუსაფრთხოების მმართველობაში გენდერული თანასწორობის ინტეგრირება საჭიროებს შემდეგის აღიარებას: ცალკეულ მოქალაქეებს (კერძოდ, მაგრამ არა მხოლოდ, ქალებს, გოგოებს და მრავალფეროვანი გენდერული იდენტობისა და გენდერული თვითგამოხატვის მქონე ადამიანებს), სამოქალაქო საზოგადოებას და ქალებს და მრავალფეროვანი გენდერული იდენტობის, გენდერული თვითგამოხატვის მქონე და სექსუალური ორიენტაციის ადამიანების ინტერესების წარმომადგენელ ჯგუფებს აქვთ კიბერუსაფრთხოების მოთხოვნილება და უფლება. ამის უზრუნველსაყოფად კი სახელმწიფო რესურსებიცაა საჭირო. ასევე, აუცილებელია კიბერუსაფრთხოების მმართველობასა და პრაქტიკის ყველა ფორმაში გენდერული ანალიზის დანერგვა (იმ ნაწილებშიც კი, რომლებიც გენდერთან ან უსაფრთხოების ტრადიციულ გაგებასთან პირდაპირ კავშირში არ აღიქმება). გარდა ამისა, რა თქმა უნდა, საჭიროა გენდერული თანასწორობის მიღწევა კიბერუსაფრთხოების მმართველობის ყველა ასპექტში, იქნება ეს ზედამხედველობა, განხორციელება თუ კონტროლი. კიბერუსაფრთხოების ეს უფრო ფართო სპექტრი, როგორც სახელმწიფო/ინდივიდის, ისე სისტემა/საზოგადოების ჭრილში შეჯამებულია ცხრილში 1.

36. იხ. DCAF, უსაფრთხოების სექტორის მმართველობა: კარგი მმართველობის პრინციპების გამოყენება უსაფრთხოების სექტორში (DCAF, 2015), გვ. 3. (DCAF, 2015). https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_1_Security%20Sector%20Governance_0.pdf

37. იხ. DCAF, OSCE/ODIHR და UN Women, გენდერისა და უსაფრთხოების სექტორის რეფორმის სახელმძღვანელო მითითებების კრებული (ჟენევა, DCAF, 2008). https://www.dcaf.ch/gender-and-security-toolkit

38. კერძო კომპანიებთან დაკავშირებული ეს გამოწვევა შესამჩნევად არ არის წარმოდგენილი გლობალურ არაკომერციულ ორგანიზაციებში, რომლებიც მართავენ უნიკალურ იდენტიფიკატორებს და ავითარებენ ინტერნეტ პროტოკოლებს, რომლებსაც აქვთ ძლიერი პროცესები სხვადასხვა დაინტერესებული მხარის ჩართვისთვის. თუმცა, ასეთი ორგანიზაციები კვლავ აწყდებიან ზემოთ აღნიშნულ მრავალმხრივი მმართველობის უფრო ფართო გამოწვევებს.

39. ავრი დორია, „მრავალმხრივი მმართველობის გამოყენება [და ბოროტად გამოყენება] ინტერნეტში“. სად: რ. რადუ, ჯ.მ. ჩენო და რ. ვებერი (რედაქტორები), გლობალური ინტერნეტის მართვის ევოლუცია (ბერლინი, ჰაიდელბერგი: Springer, 2014), გვ. 116.

ცხრილი 1: გენდერი და კიბერუსაფრთხოების სფერო

	სისტემები და ქსელები	უფრო ფართო ციფრული საზოგადოება
სახელმწიფო/ კორპორაციული	(ჩვეული განმარტება) ❖ პრიორიტეტი ენიჭება სავარაუდოდ მასკულინურ აქტივობებს ❖ არის გენდერულად ბრმა და არა გენდერულად ნეიტრალური ❖ ადამიანები აღიქმებიან უსაფრთხოების საფრთხედ (ადამიანური ფაქტორი, სოციალური ინჟინერია ან „ყველაზე სუსტი რგოლი“) ❖ მიდრეკილება დიქოტომიისკენ: (სახელმწიფო) უსაფრთხოება კონფიდენციალურობის წინააღმდეგ	❖ დეზინფორმაცია, როგორც პოლიტიკური ან საზოგადოებრივი საფრთხე ❖ არჩევნებში ჩარევა, როგორც კიბერუსაფრთხოების პრობლემა ❖ კორპორაციები, რომლებსაც აღელვებთ ონლაინ რეპუტაცია ❖ ინდივიდები, რომლებიც მოიაზრებიან დეზინფორმაციის წყაროებად ან გულუბრყვილო მომხმარებლებად ❖ მიდრეკილება დიქოტომიისკენ: (სახელმწიფო) უსაფრთხოება კონფიდენციალურობის წინააღმდეგ
ინდივიდუალური/ ადამიანზე ორიენტირებული	❖ ადამიანი განიხილება, როგორც კიბეროპერაციების სამიზნე ან მსხვერპლი და არა როგორც რისკფაქტორი ❖ მოიცავს კიბეროპერაციების გენდერულ და ინტერსექციურ გამოცდილებებს ❖ მაგრამ ის მაინც ითვალისწინებს სისტემის გენდერულ პრივილეგიას ადამიანებზე, ხელოვნურად ავიწროებს უსაფრთხოების საფრთხის მნიშვნელობას	**(რეკომენდებული განმარტება)** ❖ ***უსაფრთხოების საფრთხეები საზოგადოების ყველაზე დაუცველი წევრების გამოცდილებაზე დაყრდნობით*** ❖ ***მოიცავს ონლაინ და ციფრულ ტექნოლოგიებთან დაკავშირებული გენდერული ზიანის ფართო სპექტრს*** ❖ ***მოიცავს კონფიდენციალურობას, როგორც ფუნდამენტურ ასპექტს და არა უსაფრთხოების ალტერნატივას***

4. კიბერუსაფრთხოება, გენდერი და უსაფრთხოების სექტორის კარგი მმართველობის პრინციპები

კიბერუსაფრთხოებისადმი მდგრადი მიდგომა ეფუძნება უსაფრთხოების სექტორის კარგი მმართველობის პრინციპებს: უსაფრთხოება უნდა იყოს გამჭვირვალე, ეფექტიანი და პასუხისმგებლობიანი, როგორც საზოგადოებრივი სიკეთე და შესაბამისობაში უნდა იყოს ყველა მოქალაქის უსაფრთხოების საჭიროებებთან. გენდერული თანასწორობა კაცებს, ქალებს და მრავალფეროვანი გენდერული იდენტობისა და გენდერული თვითგამოხატვის მქონე ადამიანებს შორის ღია, უსაფრთხო და მოქმედი კიბერსფეროს, მისი მმართველობისა და ზოგადად, დემოკრატიის განუყოფელი ნაწილია. შესაბამისად, კარგი მმართველობის ყველა პრინციპი მოიცავს გენდერულ თანასწორობას, როგორც განუყოფელ კომპონენტს და მათი განხორციელება ამის გარეშე შეუძლებელია.

ცხრილი 2: უსაფრთხოების სექტორის კარგი მმართველობის [40]

- ეფექტურობა
- ეფექტიანობა
- რეაგირება
- ჩართულობა
- პასუხისმგებლობა
- გამჭვირვალობა
- კანონის უზენაესობა

კიბერუსაფრთხოების მმართველობის ეფექტურობის მიღწევა შეუძლებელია იმის გათვალისწინების გარეშე, რომ კიბერუსაფრთხოების საფრთხეებსა და ასევე, პოლიტიკურ ჩარჩოებს, განსხვავებული ზეგავლენა აქვს სხვადასხვა გენდერის წარმომადგენელზე.

კიბერუსაფრთხოების მმართველობის **ეფექტურობის** მიღწევა შეუძლებელია იმის გათვალისწინების გარეშე, რომ კიბერუსაფრთხოების საფრთხეებსა და ასევე, პოლიტიკურ ჩარჩოებს, განსხვავებული ზეგავლენა აქვს სხვადასხვა გენდერის წარმომადგენელზე. კიბერუსაფრთხოების სფეროს პოლიტიკების ეფექტურობის სტანდარტი უნდა გულისხმობდეს ონლაინ მონაწილეობისა და ციფრული ტექნოლოგიების ნეგატიური შედეგების შერბილებას ყველა გენდერისთვის (რეკომენდებული განმარტება მოყვანილია ცხრილ 1-ში). ამის მიღწევა შესაძლებელია მხოლოდ იმ შემთხვევაში, თუ პოლიტიკური ჩარჩოები და ტექნიკური გადაწყვეტილებები დადგინდება გენდერული ანალიზით, თუ რა შედეგები მოჰყვება კიბერუსაფრთხოების გენდერულ საფრთხეებს ქალების, კაცების და მრავალფეროვანი გენდერული იდენტობისა და გენდერული თვითგამოხატვის მქონე ადამიანებისთვის. ასევე: ეფექტურობის სტანდარტი ეფუძნება კიბერუსაფრთხოების ტრადიციულ, შედარებით ვიწრო გაგებას (ცხრილი 1), ამიტომ მიმზიდველია მოკლე პერიოდისთვის, ხოლო გრძელვადიან პერსპექტივაში ის ანადგურებს დემოკრატიის საკვანძო პრინციპებს, მათ შორის საზოგადოებაში ნდობის შენარჩუნებასა და მოქალაქეთა ფუნდამენტური უფლებების დაცვას.

ციფრულ ტექნოლოგიებს უსაფრთხოების მმართველობის **ეფექტიანობის** გაუმჯობესების დიდი პოტენციალი აქვს. ასევე, ციფრული ტექნოლოგიები შეიძლება გამოყენებულ იქნეს ინსტიტუტების მიერ, რომ მაქსიმალურად ეფექტიანად მართონ საზოგადოებრივი რესურსები თავისი შესაბამისი როლების, პასუხისმგებლობებისა და ამოცანების შესრულებაში. საერთო ჯამში, კიბერუსაფრთხოების კარგი მმართველობა ციფრული ტექნოლოგიების ფართო მასშტაბით გამოყენებასთან დაკავშირებული

40. ასეთი კორპორაციული პასუხისმგებლოები შეიძლება წარმატებით დაეყრდნოს შრომის საერთაშორისო ორგანიზაციის (ILO) 190-ე კონვენციას (რომელიც ძალაში შევიდა 2021), რომელიც „აღიარებს ყველა ადამიანის უფლებას ძალადობისა და შევიწროვებისგან (მათ შორის გენდერული ნიშნით) თავისუფალ შრომის შესაძლებლობაზე“. ILO, Eliminating Violence and Harassment in the World of Work. https://www.ilo.org/global/topics/violence-harassment/lang--en/index.htm

საჭიროებებისა და რისკების შემცირების გზით ხელს უწყობს ამ მიზნის მიღწევას. მაგალითად, სახელმწიფო უსაფრთხოების მრავალი ორგანიზაცია დამოკიდებულია ციფრულ მონაცემთა ბაზების, საკომუნიკაციო საშუალებებისა და ანალიზის ინსტრუმენტების რთულ ფენებზე, რომლებიც მავნე კიბერთავდამსხმელებისთვის „შეტევის ფართო არეალს“ ქმნის. ამ ორგანიზაციების კიბერუსაფრთხოების გაუმჯობესება ხელს შეუწყობს უსაფრთხოების სექტორის უფრო ეფექტიან ფუნქციონირებას და არ შექმნის პოტენციურად კატასტროფულ რისკებს.

თუმცა, კიბერუსაფრთხოების მმართველობისადმი გენდერულად ბრმა მიდგომამ შეიძლება მხოლოდ გააძლიეროს არაეფექტიანობა, რადგან ამ შემთხვევაში ინსტიტუციები ვერ გამოიყენებენ მრავალფეროვან გამოცდილებებს, შესაძლებლობებესა და როლებს. გარდა ამისა, კიბერსაფრთხეების ურთიერთკავშირისა და გადაცემის გათვალისწინებით, გენდერულად ბრმა მმართველობა ბუნდოვანს ხდის ციფრულ ტექნოლოგიებთან პოტენციურად დაკავშირებული ზიანის სრულ სპექტრს. პროგრამული უზრუნველყოფა, რომელიც დღეს გენდერულად ორიენტირებული იძულებითი კონტროლისთვის გამოიყენება, ხვალ შეიძლება სახელმწიფოს ეროვნული უსაფრთხოებისთვის საფრთხედ იქცეს და პირიქით. ამრიგად, მმართველობის გენდერული განზომილებების არ აღიარება და ყველა გენდერის საჭიროებების დაკმაყოფილების უგულებელყოფა იწვევს მნიშვნელოვან არაეფექტიანობას კიბერუსაფრთხოების მმართველობაში და შესაბამისად, უფრო ფართოდ უსაფრთხოების მმართველობაში.

ეფექტიანობის ეს კონცეფცია, ასევე, უშუალო კავშირშია კარგი მმართველობის ფარგლებში **რეაგირების** პრინციპთან. კიბერუსაფრთხოების სფეროს პოლიტიკები და ტექნოლოგიური გადაწყვეტილებები უნდა ეხებოდეს უთანასწორობის პრობლემის არსს და უსაფრთხო ონლაინ გარემოს შექმნით მხარს უჭერდეს ქალებს, კაცებს და მრავალფეროვანი გენდერული იდენტობისა და გენდერული თვითგამოხატვის მქონე ადამიანებს. ეს შეუძლებელი იქნება მანამ, სანამ ყველა თანაბრად არ იქნება **ჩართული** კიბერუსაფრთხოების პოლიტიკების შექმნასა და ტექნიკური სტანდარტების შემუშავებაში. კიბერუსაფრთხოების მმართველობაში გენდერული თანასწორობის პრიორიტეტად დასახვა, თავის მხრივ, ხელს უწყობს ყველა ადამიანის თანაბარ მონაწილეობას პოლიტიკასა და საზოგადოებრივ ცხოვრებაში. შესაბამისად, კიბერუსაფრთხოების გენდერულად თანასწორუფლებიანი მმართველობა აუცილებელია დემოკრატიის მნიშვნელოვანი ფუნქციონირებისთვის.

გენდერული თანასწორობა ასევე საკვანძო ელემენტია კიბერუსაფრთხოების კარგ მმართველობაში **პასუხისმგებლობისა** და **გამჭვირვალობის** პრინციპებისთვის. ჭეშმარიტი პასუხისმგებლობა მიიღწევა მხოლოდ ბარიერების გაუქმებით და ყველას თანაბარუფლებიანი და გააზრებული მონაწილეობით კიბერუსაფრთხოების სფეროში პოლიტიკებისა და სტრუქტურების შექმნასა და დანერგვაში. ტექნოლოგიებში, პრაქტიკებში ან კიბერუსაფრთხოების მმართველობაში გენდერული, სექსუალური და სხვა ინტერსექციური უთანასწორობის გამოვლენის შემდეგ, მათ აღმოსაფხვრელად, საჭიროა ეფექტიანი გადაწყვეტის მექანიზმების დანერგვა. შესაბამისად, კიბერუსაფრთხოების და, ზოგადად, კარგი მმართველობის ერთ-ერთი უმნიშვნელოვანესი ასპექტია სამოქალაქო საზოგადოების ორგანიზაციების, მათ შორის ქალთა ორგანიზაციების, ადამიანის უფლებათა დამცველი ორგანიზაციების, ლგბტქი+ უფლებადამცველების, პირადი ცხოვრების დამცველების, მიგრანტთა უფლებადამცველებისა და კონფიდენციალურობის უფლებადამცველების ჩართულობა. გამჭვირვალობა გენდერული უთანასწორობის გამოვლენისა და დაძლევის გარანტიაა.

და ბოლოს, გენდერული თანასწორობა აუცილებელია **კანონის უზენაესობისთვის.** კანონის უზენაესობის პრინციპი თავისი ბუნებით უზრუნველყოფს ყველა ადამიანის უფლებების თანაბარ დაცვას, მართლმსაჯულებასა და დაცვის სხვა საშუალებებზე თანაბარ ხელმისაწვდომობას. ასევე, ის მნიშვნელოვანი ინსტრუმენტია კიბერსაფრთხეების ან კიბერუსაფრთხოების პოლიტიკის გენდერზე ნეგატიური ზეგავლენის შესამცირებლად. ყველა სხვა პრინციპი უნდა ეფუძნებოდეს კანონის უზენაესობას, როგორც დემოკრატიის ერთ-ერთ ქვაკუთხედს.

5. კიბერუსაფრთხოების გამოწვევები უსაფრთხოების კარგი მმართველობის პრინციპებისთვის

კიბერუსაფრთხოების კარგი მმართველობის ზემოთ მოყვანილ პრინციპებში გენდერული თანასწორობის როლი შეიძლება, ასევე, გავრცელდეს უსაფრთხოების მმართველობის ბევრ სხვა სფეროზე. თუმცა კიბერუსაფრთხოება ავლენს სამ უნიკალურ გამოწვევას ამ პრინციპებისთვის.

ა) კიბერუსაფრთხოების მმართველობა ფუნდამენტურად დგას მრავალ დაინტერესებულ მხარეზე

მრავალმხრივი ან პოლიცენტრული მმართველობა ბევრი სფეროსთვის არის დამახასიათებელი, როგორც უსაფრთხოების, ისე უფრო ფართო კონტექსტში; მაგრამ კიბერუსაფერთხოების მმართველობაში მრავალი დაინტერესებული მხარის ჩართულობა არასტანდარტულ სახეს იძენს. პირველ რიგში, ინტერნეტის მართვა თავისთავად გულისხმობს მრავალმხრივ ჩართულობას, იქნება ეს არასამთავრობო სუბიექტები ტექნიკურ თემებში, სამოქალაქო საზოგადოება თუ კერძო სექტორი, რომლებიც არა მხოლოდ მონაწილეობენ ინტერნეტსფეროს და შესაბამისად, კიბერუსაფრთოხების პოლიტიკის შემუშავებაში, არამედ მართავენ ტექნიკური ინფრასტრუქტურის საკვანძო ნაწილებს, კაბელებიდან სამარშრუტო პროტოკოლებსა და გადაუდებელ რეაგირებამდე. მრავალი დაინტერესებული მხარის არსებობა კიბერუსაფრთხოების მმართველობაში ართულებს **ეფექტიანობის** მიღწევას, რადგან საჭიროა უსაფრთხოების პოლიტიკასა და რეალიზაციის საკითხებზე ბევრი მხარის თანხმობა. ეს ზრდის რისკს, რომ კიბერუსაფრთხოების გენდერულად ბრმა განსაზვრება და მასთან დაკავშირებული პოლიტიკები კონსენსუსურ დეფინიციებად დადგინდეს. მიუხედავად იმისა, რომ ამ ტიპის მმართველობა თავისი არსით მეტად ორიენტირებულია ინკლუზიურ **მონაწილეობაზე**, ვიდრე სხვა ალტერნატივები, კიბერუსაფრთხოებაში მსგავსი სტრუქტურა შეიძლება გამრუდდეს გეოგრაფიული ადგილმდებარეობით, ციფრული ცოდნით და კონკრეტული ტექნიკური უნარებით. სხვა სიტყვებით – ინტერსექციურობის (გენდერი, სექსუალური ორიენტაცია, კლასი, რასა, შეზღუდული შესაძლებლობები, ადგილმდებარეობა და ა.შ) დანერგვა უფრო დიდი გამოწვევაა კიბერუსაფრთხოების მმართველობისა და პოლიტიკის შეფასების პროცესებში.

ბ) კიბერუსაფრთხოების მმართველობა დიდწილად არის დამოკიდებული მსხვილ მრავალეროვნულ კერძო კომპანიებზე

მსხვილ მრავალეროვნულ კერძო კომპანიებს, როგორც უფრო ფართო, მრავალმხრივი მმართველობის სტრუქტურის ნაწილს, აქვთ უდიდესი გავლენა კიბერუსაფრთხოების სფეროზე. ეს მოიცავს სოციალურ მედიაპლატფორმებს, რომლებიც მილიარდობით ადამიანის ონლაინ ურთიერთქმედების საფუძველია, თითქმის ყველა კომპიუტერის მიერ გამოყენებული ოპერაციული სისტემების მწარმოებელ და დამნერგავ მსხვილ კომპანიებს და შერეული ტექნიკის მწარმოებელ კომპანიებს, რომლებიც დაინტერესებულები არიან ინტერნეტ-კაბელების თუ ონლაინ ვაჭრობის სფეროებით, ღრუბლოვანი გამოთვლებით თუ მობილური აპლიკაციებით. მსგავსი დამოკიდებულება გამოწვევებს ქმნის **პასუხისმგებლობის**, ნაწილში, რადგან ამ კერძო კომპანიებს მცირე დემოკრატიული კონტროლი აქვთ ქვეყნებში, სადაც მათი ცენტრალური ოფისი მდებარეობს და ფაქტობრივად ნულოვანი – სხვა ადგილებში. ეს კომპანიები ხშირად არ ისახავენ პრიორიტეტად გენდერულ თანასწორობას და არ უზრუნველყოფენ მას სხვადასხვა გადაწყვეტილების მიმღებ დონეებსა და პოზიციებზე. ეს, ასევე, ქმნის კერძო სექტორში კიბერუსაფრთხოების სფეროს კარგი გენდერული მმართველობის გამოწვევებს. ეს აქტორები თითქმის არ არიან მოტივირებული, **რეაგირება** მოახდინონ კონკრეტულ საკითხებზე, საჭიროებებსა და უფლებებზე, მათ შორის გენდერულ და სექსუალურ თანასწორობაზე, რაც განსაკუთრებით აქტუალურია სპეციფიკური საჭიროებების მქონე თემების, ქალთა და ლგბტქი+ უფლებათა აქტივისტებისა და ადვოკატირების ჯგუფებისთვის. სანაცვლოდ,

კორპორაციები ხშირად ქმნიან გენდერულად ბრმა უსაფრთხოების პოლიტიკას ხარჯებისა და რესურსების დაზოგვის მიზნით, რომლებსაც შეძლებისდაგვარად ფართო გამოყენება აქვს.[41]1

გ) კიბერუსაფრთხოების მმართველობა არის სწრაფად ცვალებადი, არაპროგნოზირებადი და საფუძველშივე საერთაშორისო

ციფრული ტექნოლოგიების ძირითადი სფერო სწრაფად იცვლება, რაც ნიშნავს, იმას რომ კიბერუსაფრთხოების მმართველობა ასევე სწრაფად ცვალებადია. სილიციუმის ველის წარმოებისა და ინოვაციის მთავარი სლოგანი „იმოძრავე სწრაფად და გაარღვიე საზღვრები“ ვრცელდება კიბერუსაფრთხოების სექტორზეც, ეს ძალიან აქტიური ინდუსტრია მუდმივად ვითარდება, რათა დაეწიოს უახლეს ტექნოლოგიურ საფრთხეებს. მიუხედავად იმისა, რომ პრინციპში, ეს სასარგებლოა, როგორც **რეაგირების,** ისე **ეფექტიანობისთვის** პრაქტიკაში ასეთი მუდმივი ოპტიმიზაცია თითქმის ყოველთვის მიმართულია შემოსავლის ზრდაზე ან ბაზარზე ახალი პროდუქტის დანერგვაზე და არა უფლებების, მათ შორის გენდერული თანასწორობის დაცვაზე ან სოციალური თუ დემოკრატიული მიზნების მიღწევაზე (როგორიცაა ყველა ადამიანის თანაბარი და უსაფრთხო მონაწილეობა საზოგადოებრივ ცხოვრებაში). ციფრული ცვლილებების სიჩქარე, ასევე, ართულებს გენდერისა და კიბერუსაფრთხოების სფეროს ინტერსექციური გამოწვევების ეფექტიან გამოვლენას – სიტუაციები, როცა ტექნოლოგიებს ან პოლიტიკებს შეიძლება ხშირად ჰქონდეს უნებლიე სპეციფიკური ზეგავლენა, იზოლაციითა და უფლებების უგულებელყოფით, სხვადასხვა სოციალურ ჯგუფებზე.

სექტორის დინამიკური ბუნება, ასევე, არასტაბილურობას სძენს კიბერუსაფრთხოების მმართველობას, თავისი განმეორებითი გაჟონვებით, სკანდალებითა და მასშტაბური ინციდენტებით. ეს არასტაბილურობა კიბერუსაფრთხოების მმართველობის უსაფრთხოების სხვა სფეროებთან შედარებით **გამჭვირვალეს** ხდის; ყოველ შემთხვევაში, მოვლენების შესახებ ინფორმაციასა და სფეროს გამოწვევებზე საზოგადოების ხელმისაწვდომობის კუთხით. თუმცა, ასეთი ქაოტური გამჭვირვალობა შეზღუდულია და იშვიათად მოიცავს, მაგალითად, ანალიზის, ალგორითმული შეფასების ან ავტომატიზებული გადაწყვეტილების შესაძლებლობას მნიშვნელოვანი ზეგავლენა მოახდინოს კონკრეტულ ადამიანებზე. ზემოთ აღნიშნული გენდერული მიკერძოებების გათვალისწინებით, მონაცემთა დიდ ბაზებში, მოდელებსა და ალგორითმებში, განგრძობითი გენდერული ანალიზის საიმედო პროცედურებისა და სტანდარტების გარეშე, ამას აქვს გენდერული უთანასწორობის გაღვივების შესაძლებლობა. და ბოლოს, კიბერუსაფრთხოებას გლობალურობის კუთხით უსაფრთხოების ცოტა სფერო თუ შეედრება; აქვე იგულისხმება საფრთხეები და ინციდენტები, რომლებიც საზღვრებს პრაქტიკულად მომენტალურად კვეთს. ეს ქმნის გამოწვევებს **კანონის უზენაესობისთვის**, რადგან ნებისმიერ შემთხვევაში კიბერუსაფრთხოებაში ან კიბერდანაშაულში რამდენიმე იურისდიქციაა ჩართული. ამან შეიძლება გაამწვავოს პრობლემები, რომლებსაც ყველა მსხვერპლი, განსაკუთრებით ქალები და მრავალფეროვანი გენდერული იდენტობისა და გენდერული თვითგამოხატვის მქონე ადამიანები აწყდებიან მართლმსაჯულებაზე ხელმისაწვდომობის კუთხით.

41. იხ. მაგ: OHCR, “გენდერული თანასწორობა და გამოხატვის თავისუფლება შორეულ მიზნად რჩება – გაეროს ექსპერტი (OHCR, 18 ოქტომბერი, 2021). https://www.ohchr.org/en/press-releases/2021/10/gender-equality-freedom-expression-remains-distant-goal-un-expert. მაგალითად, კანონმდებლობა, რომელიც თითქოსდა მიზნად ისახავს ქალებისა და გოგოების ონლაინ შევიწროებისგან დაცვას, ზოგიერთ კონტექსტში გამოიყენებოდა ქალი ჟურნალისტებისა და უფლებადამცველების ასევე ფემინიზმის და/ან ლგბტქი+ ადამიანების ხმის ჩახშობას; ამის მაგალითებისთვის იხ. Human Rights Watch, „ქალების ონლაინ შევიწროება პაკისტანში“ (22 ოქტომბერი, 2020).https://www.hrw.org/news/2020/10/22/online-harassment-women-pakistan; „ეგვიპტე: ქალების მორალური დევნის კასკადი“, (17 აგვისტო, 2020). https://www.hrw.org/news/2020/08/17/egypt-spate-morality-prosecutions-women; და „კიბერდანაშაულის ზომების ბოროტად გამოყენება აფერხებს გაეროს მოლაპარაკებებს“ (5 მაისი, 2021).https://www.hrw.org/news/2021/05/05/abuse-cybercrime-measures-taints-un-talks

6. როგორ უზრუნველყოფს გენდერული თანასწორობა კიბერუსაფრთხოების გამოწვევებს უსაფრთხოების სექტორის კარგი მმართველობის ფარგლებში

მოცემულ ნაშრომში, როგორც უკვე დეტალურად არის აღწერილი, გენდერულ თანასწორობაზე აქცენტი გულისხმობს კიბერუსაფრთხოების სფეროს მმართველობის გაფართოებას, რათა მოიცვას შესაბამისი აქტორები და უფლებები (როგორც ზემოთ აღინიშნა მე-3 ნაწილში, თუმცა აღიარებულია, რომ უფრო ფართო განმარტებების პრაქტიკაში დანერგვა და თანმიმდევრულობა უფრო რთულია). კიბერუსაფრთხოების მასშტაბებთან დაკავშირებული აღქმების ამჟამინდელი სივიწროვე და კონსენსუსის არარსებობა (როგორც აღწერილია მე-3 ნაწილში) აფერხებს გენდერულ თანასწორობას; სწორად ამიტომ არის საჭირო დამატებითი სიცხადე. გენდერული თანასწორობა, ასევე, აძლიერებს კიბერუსაფრთხოების მმართველობას და ამყარებს უსაფრთხოების სფეროს კარგი მმართველობის პრინციპებს (როგორც აღწერილია მე-4 ნაწილში). ამგვარად, გენდერული თანასწორობა თავისთავად არის ნორმატიული მიზანი და სწორად ამიტომ გენდერული მეინსტრიმინგი უნდა გავრცელდეს კიბერუსაფრთხოების მმართველობის ყველა ასპექტზე. და ბოლოს, დამატებით – გენდერული თანასწორობა უზრუნველყოფს კიბერუსაფრთხოების მე-5 ნაწილში გამოვლენილი გამოწვევების საჭიროებისამებრ გადაწყვეტას.

ა) გენდერული და ინტერსექციური თანასწორობის ჩართვა მრავალმხრივი მმართველობის მოდელში

მმართველობის მოდელი, რომელშიც მრავალი დაინტერესებული მხარეა ჩართული, თავისი არსით კონსენსუსზე დაფუძნებული პოლიტიკის შემუშავებაზე დგას; ამ პროცესში თანასწორობის პრინციპით ჩართულია რამდენიმე დაინტერესებული ჯგუფი. პრინციპის საფუძველი დაინტერესებული მხარეების ყველა ჯგუფის თანაბარი მონაწილეობის ფორმალური აღიარებაა. ეს ჯგუფები კი სხვადასხვა სექტორში არიან წარმოდგენილნი, იქნება ეს მთავრობა, კერძო სექტორი, ტექნოლოგიური თემები თუ აკადემია. თუმცა, ასეთი მოდელები ვერ ითვალისწინებს კიბერუსაფრთხოების გენდერულ ასპექტებს, რომ არაფერი ვთქვათ ყველა გენდერის ჩართულობის საჭიროებაზე სრულფასოვანი აღიარებისთვის. ამის მიზეზი კი, რა თქმა უნდა ის არის, რომ კიბერუსაფრთხოების მმართველობაში ქალებისა და მრავალფეროვანი გენდერული იდენტობისა და გენდერული თვითგამოხატვის მქონე ადამიანების შედარებით დაბალი წარმომადგენლობაა. აქედან გამომდინარე, სამოქალაქო საზოგადოების ორგანიზაციებს, რომლებიც წარმოადგენენ ქალებისა და მრავალფეროვანი გენდერული იდენტობის, გენდერული თვითგამოხატვის მქონე და სექსუალური ორიენტაციის ადამიანების ინტერესებსა და შესაძლებლობებს, უფლება აქვთ მონაწილეობდნენ კიბერუსაფრთხოების მმართველობაში, მეტიც შეუძლიათ გაზარდონ უსაფრთხოების როლი და ეფექტიანობა ინდივიდუალური უსაფრთხოებისა და დემოკრატიის ხელშეწყობის საქმეში.

გენდერული თანასწორობის საკითხების განხილვა ხელს უწყობს ყურადღების გადატანას იქიდან, რაც დღეს დაინტერესებული ჯგუფების ჩართულობის საფუძველზე განიხილება თანაბარ წვლილად, აქცენტი გადადის იმის აღიარებაზე, რომ თანასწორობის პრინციპის მნიშვნელობის ინტერპრეტაცია საჭიროებს გენდერული თანასწორობისა და ინტერსექციურობის გათვალისწინებას ამ ჯგუფებში. მონაწილეობისა და წარმომადგენლობის უფრო ფართო გაგების ფარგლებში დაინტერესებულმა მხარეებმა უნდა დაადგინონ პრესტიჟისა და პრიორიტეტების გენდერული იერარქია, რომელიც ტექნიკურ ექსპერტიზასა და წვლილს კიბერუსაფრთხოების მმართველობაში მონაწილეობის სხვა ფორმებზე მაღლა აყენებს, პოლიტიკის შემუშავების, ზედამხედველობისა და შეფასებისგან განსხვავებით.

ბ) კარგი კორპორაციული მმართველობის ადვოკატირება

კიბერუსაფრთხოების უზრუნველყოფაში მნიშვნელოვანი როლი აქვს კერძო სექტორს, რომელიც არა მხოლოდ ინფრასტრუქტურისა და ქსელების უსაფრთხოებას უზრუნველყოფს, არამედ შეიმუშავებს ორგანიზაციულ პოლიტიკებსა და ტექნოლოგიებს იმის გათვალისწინებით, რომ კანონიერი ტექნოლოგიები (მათ შორის უსაფრთხოების ფარგლებს გარეთ არსებული) შეიძლება ბოროტად გამოიყენებოდეს გენდერული და სექსუალური უთანასწორობის არსებული ფორმების გასაძლიერებლად და ხელშესაწყობად. ისეთი საკითხები, როგორიც არის გენდერული მიკერძოება ალგორითმებში, კონკრეტული მოწყობილობებისა და ტექნოლოგიების (მაგ: ლოკაციის ან ჯანმრთელობის აპლიკაციების) ბოროტად გამოყენების გენდერული შედეგები, მომხმარებელთა მონაცემებზე წვდომისა და გამოყენების გენდერული (მათ შორის მონაცემთა გადაცემა მესამე მხარისთვის) ზიანი, უნდა განიხილებოდეს როგორც კერძო სექტორის, ისე სამთავრობო ან მთავრობათაშორისი მარეგულირებელი ან სამართლებრივი ჩარჩოების ფარგლებში.

გენდერულ თანასწორობაზე ფოკუსირება უზრუნველყოფს კერძო სექტორის როლისა და პასუხისმგებლობის აღიარებასა და გაძლიერებას კიბერუსაფრთხოების კუთხით ყველა გენდერის საჭიროებებსა და პრიორიტეტებზე რეაგირებაში. ამის მიღწევა შესაძლებელია კორპორაციული სოციალური პასუხისმგებლობის ფარგლებში არსებული პრიორიტეტებისა და ძალისხმევის შედეგად, გენდერული, სექსუალური და რასობრივი თანასწორობისა და ჩართულობის მიმართ ვალდებულებების გაფართოებით, მათ შორის გენდერული ნიშნით ძალადობის წინააღმდეგ ბრძოლის გზით.

გ) კანონის უზენაესობის შენარჩუნებისა და დაცვის ხელშეწყობა

კანონის უზენაესობის გასაძლიერებლად კრიტიკულად მნიშვნელოვანია გენდერული თანასწორობა, რაც თავის მხრივ, კიბერუსაფრთხოების კარგი მმართველობის ერთ-ერთი ძირეული პრინციპია. ეს გაძლიერება სცილდება მართლმსაჯულების თანაბარი ხელმისაწვდომობისა და გამოსწორების მექანიზმების უზრუნველყოფის ფარგლებს. კიბერუსაფრთხოებისა და კიბერდანაშაულის სფეროს ბევრი კანონი დღემდე შედგენილია, როგორც „გენდერულად ნეიტრალური“ და ეყრდნობა მცდარ ვარაუდებს აბსტრაქტული „მოქალაქეების“ თანაბარი დაცვის შესახებ დანაშაულისა და სხვა საფრთხეებისგან, გენდერისგან დამოუკიდებლად. ეს კანონები გენდერულად ბრმაა, რადგან კიბერუსაფრთხოება ვერ იარსებებს ყველა გენდერული იდენტობის მქონე ადამიანის მრავალფეროვანი გამოცდილების, საჭიროებების, შესაძლებლობებისა თუ პრიორიტეტების გათვალისწინების გარეშე. გენდერულ და ინტერსექციურ თანასწორობაზე ყურადღების გამახვილება უზრუნველყოფს გარე ფაქტორების ზეგავლენის თავიდან აცილებას, რომლებიც ხშირად იჩენს თავს სამართლებრივი ჩარჩოების შედეგად, მაგალითად, როცა ონლაინ სივრცეში ქალების დაცვისთვის განკუთვნილი კანონები გამოიყენება ქალების, ჟურნალისტების და ლგბტქი+ პირების შესავიწროვებლად. გენდერული მიდგომა, ასევე, შეიძლება დაეხმაროს კანონმდებლებს უფლებათა ისეთი რთული რიგის დაბალანსებაში, როგორიცაა გენდერული ნიშნით ონლაინ შევიწროებისგან დაცვა და გამოხატვის თავისუფლება. მიუხედავად იმისა, რომ საკითხის უფრო სიღრმისეული შესწავლა სცილდება ამ ნაშრომის ფარგლებს, ის იმსახურებს ცალკე განხილვას უსაფრთხოების სექტორის მმართველობის კონტექსტში.

> კანონის უზენაესობის გასაძლიერებლად კრიტიკულად მნიშვნელოვანია გენდერული თანასწორობა, რაც თავის მხრივ, კიბერუსაფრთხოების სფეროში კარგი მმართველობის ერთ-ერთი ძირიეული პრინციპია.

დასკვნა

დასასრულს, ცხრილი 3 აჯამებს კავშირს შემდეგ საკითხებს შორის: უსაფრთხოების სფეროს კარგი მმართველობის პრინციპები, ამ პრინციპების წინაშე არსებული გამოწვევები კიბერუსაფრთხოების კუთხით, რეკომენდაციები გენდერული პოლიტიკისთვის ამ პრობლემების გადასაჭრელად და კიბერუსაფრთხოების კარგი მმართველობის პრინციპების გასაძლიერებლად. ეს რეკომენდაციები ეფუძნება ამ ნაშრომის ყველა თავში განხილულ ანალიზს.

ცხრილი 3: კარგი მმართველობის, კიბერუსაფრთხოებისა და გენდერის პრინციპები

კარგი მმართველობის პრინციპი	კიბერუსაფრთხოების გამოწვევები	რეკომენდაციები გენდერული პოლიტიკისთვის
ეფექტურობა	მრავალ დაინტერესებულ მხარეს შორის კოორდინაცია ეფუძნება თანაბარუფლებიანობის პრინციპს და არა წარმომადგენლობას.	დაწესებულებებში, რომლებსაც მრავალი დაინტერესებული მხარე მართავს, უზრუნველყავით ადამიანური და სხვა რესურსი, მათ შორის – გენდერის ექსპერტები და უფლებადამცველები, გენდერული თანასწორობის ხელშეწყობისათვის. ჩართეთ პოლიტიკის შემუშავების, დანერგვისა და ზედამხედველობის პროცესში სამოქალაქო საზოგადოების ორგანიზაციები, მათ შორის ქალთა ჯგუფები და ლგბტქი+ ადამიანები.
ეფექტიანობა	კიბერუსაფრთხოების აქტორები ყურადღებას ამახვილებენ ეკონომიკური ან ტექნოლოგიური ოპტიმიზაციის ვიწრო კონცეფციებზე.	დარწმუნდით, რომ კიბერუსაფრთხოების საფრთხეებისა და რისკების ეკონომიკური ანალიზი მოიცავს შრომის, მოგებისა და მთლიანი შიდა პროდუქტის (მშპ) გენდერულად მგრძნობიარე ანგარიშებს და რომ გენდერული უთანასწორობის აღმოფხვრაზე აქტიური მუშაობა მიმდინარეობს. დარწმუნდით, რომ კიბერუსაფრთხოების ეფექტიანობის საკითხები გენდერზე პრიორიტეტული არ არის.

კარგი მმართველობის პრინციპი	კიბერუსაფრთხოების გამოწვევები	რეკომენდაციები გენდერული პოლიტიკისთვის
რეაგირება	კიბერუსაფრთხოების ვიწრო სახელმწიფოცენტრისტულ დეფინიციებში გამოტოვებულია მრავალი გენდერული საფრთხე და ზიანი. კიბერუსაფრთხოებისა და კონტენტის მოდერაციისთვის კერძო სექტორის მიერ მიღებული გლობალური ავტომატიზებული სისტემები ხშირად მოკლებულია საზოგადოებრივ მონაწილეობას ან საზოგადოების საჭიროებებისადმი მგრძნობელობას.	ჩაატარეთ კიბერუსაფრთხოების საკითხის მასშტაბის შესაბამისი საკონსულტაციო შეხვედრები, რათა შექმნათ უსაფრთხოების სექტორისა და კარგი მმართველობის რეფორმის საფუძველი ინტერსექციური გენდერული პერსპექტივის გათვალისწინებით. სქესის ნიშნით სეგრეგირებული მონაცემების შეგროვების საფუძველზე, გააანალიზეთ და გაითვალისწინეთ ტექნოლოგიებისა და პროდუქტების პოტენციურად არასწორად გამოყენების გენდერული ზეგავლენა და ზიანი. დარწმუნდით, რომ მონაცემთა ბაზა ითვალისწინებს გენდერულ მრავალფეროვნებას (არ არის შექმნილი გენდერისადმი ბინარული მიდგომით).
მონაწილეობა	პრესტიჟისა და პრიორიტეტების გენდერული იერარქია ტექნიკურ გამოცდილებასა და წვლილს მონაწილეობის სხვა ფორმებზე მაღლა აყენებს.	განავითარეთ კიბერუსაფრთხოების პოლიტიკაში ყველა გენდერული ინდეტობის მქონე ადამიანის ჩართულობის პოტენციალი. ხელი შეუწყეთ ხელფასისა და კომპენსაციის გათანაბრებას კიბერუსაფრთხოების სფეროს ყველა პოზიციაზე, რათა თავიდან აიცილოთ არატექნიკური ცოდნის გაუფასურება. უზრუნველყავით მენტორინგი, ტექნიკური მომზადება და სამუშაო ადგილები ქალებისა და ლგბტქი+ ადამიანების მხარდასაჭერად, რათა მათ შეძლონ წარმატებას მიაღწიონ კიბერუსაფრთხოების სფეროს ტექნიკურ პოზიციებზე. უზრუნველყავით რესურსები ქალების, ლგბტქი+ ადამიანებისა და სხვა შესაბამისი სამოქალაქო საზოგადოების ორგანიზაციებისთვის.
პასუხისმგებლობა	დიდი ტექნოლოგიური კომპანიების დემოკრატიული ზედამხედველობა რთულია.	შეინარჩუნეთ ღია და თანამონაწილეობრივი დემოკრატიული პროცესი, რომელიც ფოკუსირებული იქნება კორპორაციული მმართველობის გენდერული ასპექტების კონტროლზე. გამოიყენეთ საჯარო-კერძო პარტნიორობები და სახელმწიფო კონტრაქტები კორპორაციების წასახალისებლად, პრიორიტეტად დაისახონ გენდერული თანასწორობა როგორც შრომით რესურსებში, ისე ტექნოლოგიის/პროდუქტის შემუშავებაში.

კარგი მმართველობის პრინციპი	კიბერუსაფრთხოების გამოწვევები	რეკომენდაციები გენდერული პოლიტიკისთვის
გამჭვირვალობა	გამჭვირვალობა დამოკიდებულია ქაოტურ, არაპროგნოზირებად გაჟონვებზე, ხოლო ძირითადი კოდისა და ალგორითმის დეტალური შემოწმება იშვიათად ხდება.	შეინარჩუნეთ საზოგადოების კონტროლი და ისეთი არაკომერციული მხარეების ჩართულობა, როგორიცაა სამოქალაქო საზოგადოება და აკადემია, რათა უზრუნველყოთ სტრუქტურა და გააძლიეროთ კიბერუსაფრთხოების ტექნოლოგიებისა და პოლიტიკების გამჭვირვალობა. უზრუნველყავით ტექნიკური მომზადება ალგორითმებისა და ციფრული მართვის მიმართულებით, მათ შორის ინფორმაცია გენდერული, სექსუალური და რასობრივი მიკერძოებების შესახებ კანონმდებლებისთვის, რომლებიც კიბერუსაფრთხოებას ზედამხედველობენ.
კანონის უზენაესობა	კიბერუსაფრთხოება თავისი ბუნებითვე გულისხმობს საზღვრების გადაკვეთას და მრავალ იურიდსიქციას. და არსებობს გავრცელებული, მაგრამ მცდარი აღქმა, რომ სამართლებრივი ჩარჩოები გენდერულად ნეიტრალურია.	შეეწინააღმდეგეთ მცდარ წარმოდგენებს კიბერუსაფრთხოების სფეროს გენდერულად ნეიტრალური კანონების შესახებ, რომლებიც უნდა ითვალისწინებდნენ გენდერული ზეგავლენის შემცველ შედეგებს. ჩაატარეთ გენდერული აუდიტი ამ თემასთან დაკავშირებით არსებული კანონების გენდერული ზეგავლენის შესაფასებლად. უზრუნველყავით, რომ ორმაგი და მრავალმხრივი შეთანხმება კიბერუსაფრთხოებისა და კიბერდანაშაულის სფეროში თანამშრომლობის შესახებ ნერგავდეს გენდერულ მიდგომას და უზრუნველყოფდეს დაცვას გენდერული და ტრანსსასაზღვრო სექსუალური დისკრიმინაციისგან კიბერუსაფრთხოების სფეროს კონტროლსა და პოლიტიკაში.

DCAF Geneva Centre for Security Sector Governance

DCAF - უსაფრთხოების სექტორის მართვის ჟენევის ცენტრი

Maison de la Paix | Chemin Eugène-Rigot 2E | CH-1202 ჟენევა, შვეიცარია

ტელ: +41 22 730 94 00 | info@dcaf.ch | Twitter @DCAF_Geneva

www.dcaf.ch