ICT მიწოდების ჯაჭვის უსაფრთხოება

საქართველოს ეროვნული კრიტიკული ინფორმაციული ინფრასტრუქტურის კონტექსტში

დოკუმენტი მომზადდა საქართველოს ინფორმაციის და ტექნოლოგიების ანალიზის ცენტრის (GITAC) მიერ, ევროკავშირის მიერ დაფინანსებული პროექტის **„უსაფრთხოების სექტორის ანგარიშვალდებულების გაძლიერება სამოქალაქო საზოგადოების ეფექტური ზედამხედველობით“** ფარგლებში, რომელსაც IRC ახორციელებს. ნაშრომი მიზნად ისახავს საქართველოს წინაშე არსებული გამოწვევების იდენტიფიცირებასა და ევროკავშირის დირექტივებთან შესაბამისობის მისაღწევად შესაბამისი რეკომენდაციების შემუშავებას.

დოკუმენტში გამოთქმული მოსაზრებები შეიძლება არ ასახავდეს ევროკავშირის წარმომადგენლობის და ინოვაციების და რეფორმების ცენტრის (IRC) მოსაზრებებს.

კვლევაზე იმუშავა

- **დავით შავგულიძე** - კვლევის ხელმძღვანელი.
- **გიორგი გურგენიძე** - კიბერუსაფრთხოების ექსპერტი.
- **მარიამ მაღრაძე** - ანალიტიკოსი.

თარიღი

ივნისი, 2024 წ.

სარჩევი

შემაჯამებელი მიმოხილვა 5

ძირითადი მიგნებები და რეკომენდაციები 7

მმართველობისა და პოლიტიკის დონე 7

სახელმწიფო შესყიდვების ღია მონაცემების ანალიზი 14

მიწოდების ჯაჭვის სასიცოცხლო ციკლთან დაკავშირებული კიბერშეტევების ტექნიკური ანალიზი 17

1. თავი 1: ICT მიწოდების ჯაჭვის უსაფრთხოების რეგულაციების ანალიზი დასავლეთის ქვეყნებში 18

1.1. აშშ-ს მარეგულირებელი ჩარჩოს ანალიზი 19

1.1.1. ძირითადი რეგულაციები და აქტები 19

1.2. ევროკავშირის მარეგულირებელი ჩარჩოს ანალიზი 40

1.2.1. ძირითადი რეგულაციები და აქტები 40

2. თავი 2: სპეციფიკური ICT მიწოდების ჯაჭვის შეტევების ანალიზი და მათი ტექნიკური ასპექტები 45

2.1. დიზაინი და შემუშავება 46

2.1.1. საფრთხეები 46

2.1.2. რეალური კიბერინციდენტები 46

2.1.3. საუკეთესო პრაქტიკა და რეკომენდაციები 47

2.2. წარმოება 48

2.2.1. საფრთხეები 48

2.2.2. რეალური კიბერინციდენტები 48

2.2.3. საუკეთესო პრაქტიკა და რეკომენდაციები 49

2.3. შესყიდვა და მიწოდება 50

2.3.1. საფრთხეები 50

2.3.2. რეალური კიბერინციდენტები 51

2.3.3. საუკეთესო პრაქტიკა და რეკომენდაციები 51

2.4. დანერგვა 52

2.4.1. საფრთხეები 53

2.4.2. რეალური კიბერინციდენტები 53

2.4.3. საუკეთესო პრაქტიკა და რეკომენდაციები 54

2.5. ოპერირება და მართვა 54

2.5.1. საფრთხეები 55
2.5.2. რეალური კიბერინციდენტები 55
2.5.3. საუკეთესო პრაქტიკა და რეკომენდაციები 55
2.6. მხარდაჭერა 56
2.6.1. საფრთხეები 57
2.6.2. რეალური კიბერინციდენტები 57
2.6.3. საუკეთესო პრაქტიკა და რეკომენდაციები 58
2.7. ჩამოწერა 59
2.7.1. საფრთხეები 59
2.7.2. რეალური კიბერინციდენტები 60
2.7.3. საუკეთესო პრაქტიკა და რეკომენდაციები 60
შეჯამება 61
3. თავი 3: ICT მიწოდების ჯაჭვის უსაფრთხოების ღია მონაცემთა ანალიზი საქართველოში 62
3.1. მართვის ელექტრონული სისტემების შემუშავება და შესყიდვა 62
3.1.1. ERP სისტემები 63
3.1.2. სხვადასხვა სისტემები 65
3.1.3. სამართალდამცავი პროგრამული უზრუნველყოფა (LES) 66
3.1.4. გლობალური ნავიგაციის სატელიტური სისტემები (GNSS) 69
3.2. აპარატურული უზრუნველყოფის შესყიდვები 70
3.2.1. კომპიუტერული მოწყობილობების შესყიდვა 70
3.2.2. ვიდეო სათვალთვალო კამერების შესყიდვა 72
3.2.3. აშშ-ს მიერ სანქცირებული მწარმოებლებისა და პროდუქტების შესყიდვები 72
3.2.4. ქსელური მოწყობილობები 75
3.2.5. სატელეკომუნიკაციო მოწყობილობები და აქსესუარები 77
3.3. სერვისების შესყიდვა 79
3.3.1. ინტერნეტ სერვის პროვაიდერები 82
3.3.2. ტელეკომუნიკაციები 83
4. **თავი 4: საქართველოს კონტექსტი და რეკომენდაციები** 85
4.1. საქართველოს კონტექსტი 85
4.1.1. ძირითადი რეგულაციები და აქტები 85
4.1.2. სამთავრობო უწყებების როლი 85
4.1.3. გამოწვევები და სისუსტეები 86

4.2. ხედვა და რეკომენდაციები 87
4.2.1. კრიტიკული ინფრასტრუქტურისა და კრიტიკული სისტემების განსაზღვრა 87
4.2.2. როლების გადანაწილება და კოორდინაცია 89
5. დანართები 99
დანართი #1: ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების ორგანოები 99
6. ბიბლიოგრაფია 101
რეგულაციები 101
სახელმძღვანელოები და სამუშაო ჯგუფები 103

შემაჯამებელი მიმოხილვა

ევროკავშირის კიბერუსაფრთხოების სააგენტოს (ENISA) 2023 წლის ევროკავშირის კიბერსაფრთხეების ლანდშაფტის (ETL) კვლევის მიხედვით, მიწოდების ჯაჭვის შეტევები ზრდადი ტენდენციით ხასიათდება და მნიშვნელოვან გამოწვევას წარმოადგენ. გასული წლების მანძილზე, მნიშვნელოვნად გაიზარდა მიწოდების ჯაჭვის შეტევები და ამასთან, უფრო და უფრო მეტად რთულდება შეტევის მეთოდები, ტექნიკები და პროცედურები (TTP).

მიწოდების ჯაჭვის შეტევა არის **მინიმუმ ორი შეტევის კომბინაცია. პირველი თავდასხმა ხდება მიმწოდებელზე, რომელიც შემდეგ გამოიყენება სამიზნეზე თავდასხმისთვის მის აქტივებზე წვდომის მისაღებად.** სამიზნე შეიძლება იყოს საბოლოო მომხმარებელი ან სხვა მიმწოდებელი. ამიტომ, იმისთვის, რომ თავდასხმა კლასიფიცირდეს როგორც მიწოდების ჯაჭვის შეტევა, ორივე **- მიმწოდებელი და მომხმარებელი უნდ ა იყოს სამიზნე.**

მნიშვნელოვან ტექნოლოგიურ გამოწვევას წარმოადგენს მიწოდების ჯაჭვის შეტევების ან/და კომპრომიტირებული სისტემების გამოვლენა. შესაბამისად, წინამდებარე ნაშრომში მოცემული მსჯელობა და რისკების ანალიზი ეფუძნება შემდეგს:

- **საქართველოს 20% ოკუპირებულია რუსეთის ფედერაციის მიერ.** ამასთან გასული 15 წლის მანძილზე, საქართველოს კრიტიკულ ინფორმაციულ ინფრასტრუქტურაზე, **მიკუთვნების მაღალი ალბათობით,** რუსეთის ფედერაციასთან დაკავშირებულმა აქტორებმა მიიტანეს არაერთი მსხვილი კიბერშეტევა. შესაბამისად, რუსული წარმომავლობის ICT და სერვისები განხილულია, როგორც საფრთხის შემცველი საქართველოს კრიტიკული ინფორმაციული ინფრასტრუქტურისთვის.
- საქართველოს კონსტიტუციის შესაბამისად, **ქართველი ხალხის არჩევანია ევროკავშირისა და ევროატლანტიკურ უწყებებში გაერთიანება**. შესაბამისად, ნაშრომში წარმოდგენილი რეკომენდაციები მიზნად ისახავს **ევროინტეგრაციის კონტექსტის გათვალისწინებას და ხელშეწყობას.** კერძოდ, შემოთავაზებული **რეკომენდაციები შედგენილია ევროკავშირის ქსელისა და ინფორმაციული უსაფრთხოების დირექტივისა (NIS2) და ციფრული საოპერაციო მედეგობის აქტის (DORA) შესაბამისობის უზრუნველსაყოფად**.
- ICT და სერვისების მიწოდების ჯაჭვის კიბერსაფრთხეების ანალიზი კომპლექსური საკითხია და საჭიროებს მაღალი დონის ექსპერტიზას. **ხშირ შემთხვევაში, ღია წყაროებით არ არის ხელმისაწვდომი ნაშრომში განხილული ICT პროდუქტთან თუ სერვისთან დაკავშირებული კიბერსაფრთხეები**. შესაბამისად, კრიტიკული ინფრასტრუქტურის მიერ რუსული, ჩინური ან/და სანქცირებული პროდუქტების გამოყენების რისკების ანალიზში **ნაშრომი ეყრდნობა აღქმული კიბერსაფრთხეების (perceived cyber threats)** კონცეფციას.

ანალიტიკური ნაშრომი მომზადდა ააიპ „საქართველოს ინფორმაციის და ტექნოლოგიების ანალიზის ცენტრის“ (შემდგომში „GITAC“) მიერ, ევროკავშირის პროგრამის, EU4 Security, Accountability and Fight against Crime in Georgia, საგრანტო პროექტის ფარგლებში. **GITAC-ის ანალიტიკური საქმიანობის (line of effort) ძირითად მიმართულებას წარმოადგენს ევროკავშირის კიბერ და ციფრულ რეგულაციებთან ჰარმონიზაცია**, რაც სხვა დანარჩენთან ერთად გულისხმობს, საქართველოს ციფრული მმართველობისა და კრიტიკული

ინფორმაციული ინფრასტრუქტურის მიმართულებით ქართული გამოცდილების დაგროვების უზრუნველყოფასა და ქართული ანალიტიკური ორგანიზაციის (ე.წ. „Think Tank") ჩამოყალიბებას.

წინამდებარე კვლევაში წარმოდგენილია შემდეგი ძირითადი საკითხები:

- **თავი 1:** ICT მიწოდების ჯაჭვის უსაფრთხოების რეგულაციების ანალიზი დასავლეთის ქვეყნებში;
- **თავი 2:** სპეციფიკური ICT მიწოდების ჯაჭვის შეტევების ანალიზი და მათი ტექნიკური ასპექტები;
- **თავი 3:** ICT მიწოდების ჯაჭვის უსაფრთხოების ღია მონაცემთა ანალიზი საქართველოში;
- **თავი 4:** საქართველოს კონტექსტი და რეკომენდაციები.

შემაჯამებელ მიმოხილვაში წარმოდგენილია იდენტიფიცირებული გამოწვევები და ჩვენი ხედვა/რეკომენდაციები საქართველოს ICT მიწოდების ჯაჭვის უსაფრთხოების უზრუნველყოფისათვის.

ძირითადი მიგნებები და რეკომენდაციები

მმართველობისა და პოლიტიკის დონე

კრიტიკული ინფრასტრუქტურა არ არის განსაზღვრული

არ არსებობს ეროვნულ დონეზე შეფასებული და განსაზღვრული კრიტიკული ინფრასტრუქტურა. ამასთან, განსაზღვრულია **კრიტიკული <u>ინფორმაციული</u> ინფრასტრუქტურის 3 სექტორი / კატეგორია, რაც არასაკმარისია.** გამოწვევას წარმოადგენს მეთოდოლოგიის შემუშავება და პრაქტიკაში იმპლემენტაცია.

<u>რეკომენდაცია:</u>

- ყველა დაინტერესებული მხარის ჩართულობით, დამტკიცდეს საქართველოს კრიტიკული ინფრასტრუქტურის პირველადი სექტორული სია.
- საწყის ეტაპზე, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტებს გამოეყოს ყველა ის სექტორი, რომელიც სიმწიფის მაღალ დონეზეა და რომელსაც უკვე ყავს **<u>ინსტიტუციურად ძლიერი სექტორული მარეგულირებელი. საწყის ეტაპზე, ასეთი სექტორებია საფინანსო და ენერგო სექტორები.</u>**

ეროვნული კიბერუსაფრთხოების არქიტექტურა საჭიროებს ოპტიმიზაციას

კრიტიკულად მნიშვნელოვანია, რომ **<u>პირველ რიგში, უზრუნველყოფილი იქნეს კიბერუსაფრთხოების ეკოსისტემის ქმედითი, დაბალანსებული, ანგარიშვალდებული და ეფექტიანი არქიტექტურა, ადეკვატურად იქნეს გადანაწილებული როლები და პასუხისმგებლობები.</u>**

<u>რეკომენდაცია:</u>

- **<u>როლი:</u> კიბერუსაფრთხოების მთავარი მარეგულირებელი უწყება** - შეიმუშავებს ეროვნულ მიდგომას, პოლიტიკებსა და რეგულაციებს და უზრუნველყოფს კოორდინაციას ეროვნული კიბერკრიზისების დროს.
- **<u>როლი:</u> სექტორული მარეგულირებელი უწყება** - შეიმუშავებს სექტორისთვის მორგებულ პოლიტიკებსა და რეგულაციებს, რომელიც თანხვედრაშია მთავარი მარეგულირებლის მიერ შემუშავებულ რეგულაციებთან. ასევე, უზრუნველყოფს სექტორული რეგულაციების აღსრულების ზედამხედველობას.
- **<u>როლი:</u> კრიტიკული სუბიექტი / კრიტიკული სისტემა** - უზრუნველყოფს რეგულაციების შესრულებას.

ეროვნული კიბერუსაფრთხოების ცენტრის ჩამოყალიბების საჭიროება

NIS2 დირექტივის შესაბამისად, აუცილებელია არსებობდეს ცენტრალური მაკოორდინირებელი უწყება და კომპიუტერულ ინციდენტებზე რეაგირების ეროვნული ჯგუფი (CSIRT). აღნიშნულის მიზანია, ეროვნული დონის კიბერშეტევებისას ან კრიზისებისას, უწყებამ **უზრუნველყოს უწყებათაშორისი კოორდინაცია და ასევე, საჭიროების შემთხვევაში ევროკავშირის კიბერუსაფრთხოების სააგენტოს (ENISA) კიბერკრიზისების ქსელთან (CyCLONe) ინფორმაციის გაზიარება.**

ინფორმაციული უსაფრთხოების შესახებ საქართველოს კანონის თანახმად, სსიპ **ოპერატიულ-ტექნიკური სააგენტო** წარმოადგენს პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების ზედამხედველ ორგანოს. ამასთან, ეროვნული კიბერკრიზისის დროს, **სააგენტო უფლებამოსილი ხდება უხელმძღვანელოს უწყებათაშორის კოორდინაციას.**

სახელმწიფო ინფორმაციული და კიბერუსაფრთხოების ცენტრი წარმოადგენს ოპერატიულ-ტექნიკური სააგენტოს უწყებრივ ერთეულს (დეპარტამენტს), რომელიც პასუხისმგებელია კრიტიკული ინფორმაციული ინფრასტრუქტურის ზედამხედველობასა და დაცვაზე.

თუმცა, სსიპ ოპერატიულ-ტექნიკური სააგენტოს ძირითადი მანდატი და საქმიანობა გავლენას ახდენს **ეროვნული კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის მხრივ გატარებული ღონისძიებების სანდოობასა და პოლიტიკურ დამოუკიდებლობაზე.**

<u>რეკომენდაცია</u>

1. საშუალო ვადიან პერსპექტივაში, უზრუნველყოფილი უნდა იქნეს კიბერუსაფრთხოების მთავარი მარეგულირებელი ორგანოს დეპოლიტიზირება, დამოუკიდებლობისა და ანგარიშვალდებულების გაზრდა. აღნიშნულისათვის, შესაძლებელია სსიპ „ოპერატიულ-ტექნიკური სააგენტოს“ სახელმწიფო ინფორმაციული და კიბერუსაფრთხოების ცენტრის გაძლიერება და ცალკეულ უწყებად, „**ეროვნული კიბერუსაფრთხოების ცენტრი“, ჩამოყალიბება**. შედეგად, მოხდება საკითხის მნიშვნელობის ხაზგასმა, ადექვატური რესურსების მობილიზება და საზოგადოებაში ნდობის ამაღლება, რაც ხელს შეუწყობს ეროვნული კრიტიკული ინფრასტრუქტურის დაცვას.
2. მოკლე ვადიან პერსპექტივაში, სსიპ **ოპერატიულ-ტექნიკური სააგენტოს ცერტს მიენიჭოს ეროვნული ცერტის სტატუსი და გამოირიცხოს გადაფარული** პასუხისმგებლობები.
3. მოკლე ვადიან პერსპექტივაში, სსიპ ოპერატიულ-ტექნიკურმა **სააგენტომ შეიმუშაოს და დაამტკიცოს ICT მიწოდების ჯაჭვის უსაფრთხოების პოლიტიკა,** რომელიც იქნება ძირითადი მარეგულირებელი დოკუმენტი საქართველოს კრიტიკული ინფრასტრუქტურისთვის.

საფინანსო სექტორის კიბერზედამხედველობის მექანიზმების ოპტიმიზაცია

ციფრული საოპერაციო მედეგობის აქტის (DORA) შესაბამისად, ევროკავშირის საფინანსო ინსტიტუციებს უჩნდებათ ვალდებულება, სხვა მოთხოვნებთან ერთად, **დაიცვან ICT მიწოდების ჯაჭვის უსაფრთხოების მოთხოვნები.** ამასთან, ინსტიტუციებისთვის ჩნდება ვალდებულება სხვა უწყებებთან ერთად, ცენტრალურ ბანკს გაუზიარონ ინციდენტების შესახებ ინფორმაცია.

ინფორმაციული უსაფრთხოების შესახებ საქართველოს კანონისა საფუძველზე, **მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტებად განისაზღვრა კომერციული ბანკების (საფინანსო ინსტიტუტების) ნაწილი.** შესაბამისად, სსიპ **ციფრული მმართველობის სააგენტოს მანდატი გავრცელდა** ამ ორგანიზაციებზე. თუმცა, მეორეს მხრივ, **საქართველოს ეროვნული ბანკი წარმოადგენს მთავარ მარეგულირებელ (კომპეტენტურ) ორგანოს** საფინანსო ინსტიტუტების ზედამხედველობისთვის.

აღსანიშნავია, **<u>რომ ეროვნულ ბანკს, განსხვავებით ციფრული მმართველობის სააგენტოსი,</u>** გააჩნია სფეროს რეგულირების უფრო ხანგრძლივი ინსტიტუციური გამოცდილება და ქმედითი მექანიზმები. **<u>არსებობს და პრაქტიკაში ქმედითია ეროვნული ბანკის რეგულაციები საოპერაციო რისკების მართვის, კიბერუსაფრთხოების ჩარჩოს, SWIFT სისტემასთან თავსებადობისა და შეღწევადობის ტესტირების მიმართულებით.</u>** ამასთან, **ეროვნული ბანკის ICT ინფრასტრუქტურა, საკუთარი უსაფრთხოების შესაძლებლობები (ერთ-ერთი საჯარო დაწესებულებაა რომელიც აკმაყოფილებს ISO/IEC 27001) და პროცესების სიმწიფე უფრო განვითარებულია.**

ფიგურა 1: სექტორული გადაფარვის მაგალითი

<u>რეკომენდაცია</u>

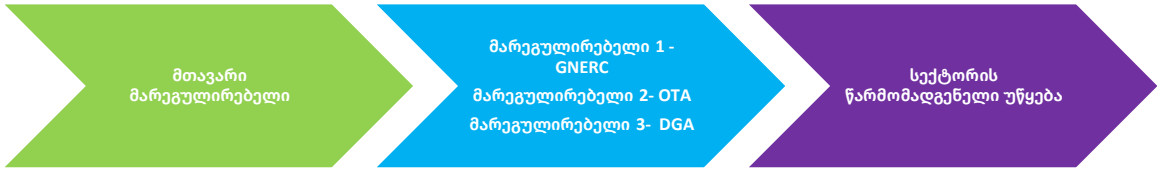
1. ევროკავშირის დირექტივებთან შესაბამისობისა და სექტორის საჭიროებების უზრუნველყოფისათვის, მნიშვნელოვანია, **<u>საფინანსო სექტორი გამოიყოს როგორც დამოუკიდებელი კრიტიკული სექტორი</u>**.
2. სექტორის რეგულირების ეფექტიანობის გაზრდისათვის, მიზანშეწონილია საფინანსო სექტორს **<u>ყავდეს კომპეტენტური მარეგულირებელი</u>**, რომელიც უზრუნველყოფს **სექტორზე მორგებული რეგულაციების შემუშავებას.** კერძოდ, გადაფარვების თავიდან აცილებისათვის, მიზანშეწონილია **<u>საფინანსო სექტორის კიბერრეგულაციებზე პასუხისმგებელი იყოს მხოლოდ საქართველოს ეროვნული ბანკი</u>**.
3. საფინანსო სექტორის ICT მიწოდების ჯაჭვის უსაფრთხოების უზრუნველყოფისათვის და ამასთან, ევროკავშირის დირექტივებთან ჰარმონიზაციის მიზნით, **ეროვნულმა ბანკმა მიიღოს DORA-სთან თავსებადი ICT მიწოდების ჯაჭვის უსაფრთხოების რეგულაციები.**

ენერგო და წყალმომარაგების სექტორის კიბერზედახმედველობის ოპტიმიზაცია

ევროკავშირისა და აშშ კრიტიკული ინფრასტრუქტურის მიმოხილვა აჩვენებს, რომ ენერგეტიკისა და წყალმომარაგების სექტორები წარმოადგენს ერთ-ერთ პრიორიტეტულ და დამოუკიდებელ სექტორს. მსგავსად საფინანსო სექტორისა, **ენერგეტიკისა და წყალმომარაგების სექტორს გააჩნია სექტორისთვის დამახასიათებელი საოპერაციო და კიბერუსაფრთხოების საჭიროებები. მაგალითისთვის, ფინანსური სექტორისგან განსხვავებით, ენერგო სექტორი**

აქტიურად იყენებს ინდუსტრიული კონტროლის სისტემებს (ICS) და შესაბამისად, შესაძლოა მეტი აქცენტი გააკეთოს საოპერაციო ტექნოლოგიების (OT) უსაფრთხოებაზე, ვიდრე ინფორმაციული ტექნოლოგიების (IT) დაცვაზე. მნიშვნელოვანია, სექტორის მიმართ გამოყენებული იყოს ერთგვაროვანი მიდგომა და შემუშავებული იყოს სექტორზე მორგებული რეგულაციები.

კვლევის მიმდინარეობისას, საქართველოს კრიტიკული ინფორმაციული **ინფრასტრუქტურა არ ცნობდა ცალკეულად გამოყოფილ ენერგეტიკისა და წყალმომარაგების სექტორს. მიმდინარე მდგომარეობით, სახელმწიფოს კუთვნილებაში / კონტროლის ქვეშ მყოფი ენერგო კომპანიების ნაწილი განსაზღვრულია, როგორც პირველი კატეგორიის სუბიექტები, ხოლო კერძო სექტორის მფლობელობაში არსებული ენერგო ორგანიზაციები მიეკუთვნება მესამე კატეგორიას.** ამასთან, არ არსებობს ენერგო სექტორის საჭიროებებზე მორგებული ICT მიწოდების ჯაჭვთან დაკავშირებული მოთხოვნები.



ფიგურა 2: სექტორული გადაფარვის მაგალითი

<u>რეკომენდაცია</u>

1. ენერგეტიკისა და წყალმომარაგების სექტორის კიბერუსაფრთხოების საჭიროებებისა და სფეროს მნიშვნელობის გათვალისწინებით, კრიტიკული ინფორმაციული სისტემის სუბიექტებში **ცალკეულ კატეგორიად გამოიყოს ენერგო და წყალმომარაგების სექტორი.**
2. სექტორის რეგულირების ეფექტიანობის გაზრდისათვის, მიზანშეწონილია ენერგეტიკისა და წყალმომარაგების სექტორს **<u>ყავდეს კომპეტენტური მარეგულირებელი</u>**, რომელიც უზრუნველყოფს **სექტორზე მორგებული რეგულაციების შემუშავებას.** კერძოდ, გადაფარვების თავიდან აცილებისათვის, მიზანშეწონილია **<u>ენერგეტიკისა და წყალმომარაგების სექტორის კიბერრეგულაციებზე პასუხისმგებელი იყოს მხოლოდ საქართველოს ენერგეტიკისა და წყალმომარაგების ეროვნული კომისია.</u>**

ICT მიწოდების ჯაჭვის მოთხოვნების ინტეგრაცია საჯარო ფინანსების მართვის სისტემაში

აშშ გამოცდილება ცხადყოფს, რომ ფედერალური შესყიდვების უსაფრთხოების საბჭო (FASC) და კომერციის დეპარტამენტი ფლობს შესაბამის მანდატსა და ინსტრუმენტებს დროულად

უზრუნველყოს **რისკის შემცველი შესყიდვის იდენტიფიცირება და საჭიროების შემთხვევაში მიმდინარე ტრანზაქციის შეჩერება.**

კვლევის მიმდინარეობისას, არ არსებობდა ICT მიწოდების ჯაჭვთან დაკავშირებული კონტროლები, რომელიც ინტეგრირებული იქნებოდა სახელმწიფო შესყიდვებისა და სახელმწიფო ხაზინის (აგრეგირებულად საჯარო ფინანსების მართვის - PFM სისტემაში) სისტემებში.

რეკომენდაცია

1. სახელმწიფო შესყიდვების სააგენტომ უზრუნველყოს ICT მიწოდების ჯაჭვის უსაფრთხოებასთან დაკავშირებული მიღებული პოლიტიკებისა და სტრატეგიების აღსრულების მონიტორინგი **საკუთარი კომპეტენციის ფარგლებში.** კერძოდ, **უზრუნველყოს აკრძალული ICT და სერვისების შესყიდვების მცდელობის იდენტიფიკაცია და პრევენცია** სახელმწიფო შესყიდვების ერთიანი ელექტრონული სისტემის საშუალებით.
2. სახელმწიფო შესყიდვების სააგენტომ **უზრუნველყოს ICT შესყიდვების შემთხვევაში სტანდარტული კონტრაქტუალური მოთხოვნების შემუშავება და იმპლემენტაციის მონიტორინგი**.
3. საქართველოს ფინანსთა სამინისტრომ, **სახელმწიფო ხაზინასთან** ერთად, უზრუნველყოს იმ **ტრანზაქციების იდენტიფიცირება და პრევენცია,** რომელიც დაკავშირებულია ICT და სერვისის მიწოდების ჯაჭვის რეგულაციებით.

გლობალური ღირებულებების ჯაჭვები და საქართველოს პოზიციონირება

დამოუკიდებლობის მოპოვების შემდგომ, წლების მანძილზე, ICT და სერვისების მიწოდების ჯაჭვის ერთ-ერთ მნიშვნელოვან გამოწვევას **წარმოადგენს რუსეთის ფედერაციის ICT ბაზარზე დამოკიდებულება**. კერძოდ, ICT და სერვისის მიმწოდებელი კომპანიების უმრავლესობა, საქართველოში პროდუქტებს ყიდდა რუსეთის (დსთ) ოფისის გავლით. ანალოგიურად, ICT პროდუქტების **შესყიდვა, დანერგვა და მხარდაჭერა ძირითადად ხორციელდებოდა რუსეთის** წარმომადგენლობის გავლით.

კვლევის მიმდინარეობისას, საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტროსა და საგარეო საქმეთა სამინისტროს არ გააჩნია გამოკვეთილი როლი ICT მიწოდების ჯაჭვის უსაფრთხოების უზრუნველყოფაში.

რეკომენდაცია

1. ICT და სერვისების მიწოდების ჯაჭვის უსაფრთხოების უზრუნველსაყოფად, **საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრომ, საქართველოს საგარეო სამინისტროს დახმარებით, უზრუნველყოფს მოლაპარაკება** დასავლურ კომპანიებთან უსაფრთხო ღირებულებათა და მიწოდების ჯაჭვების უზრუნველსაყოფად.

საპარლამენტო ზედამხედველობისა დ ანგარიშვალდებულების მექანიზმების განვითარება

აშშ გამოცდილება ცხადყოფს, რომ **აშშ მთავრობის ანგარიშვალდებულების ოფისი (US Government Accountability Office) აქტიურად მონაწილეობს ICT მიწოდების ჯაჭვის უსაფრთხოების უზრუნველყოფაში.** მაგალითად, თავდაცვის ავტორიზაციის აქტში (NDAA), ისევე, როგორც სხვა აქტებში, მითითებულია, რომ აქტის მიღებიდან 150 დღის შემდეგ US GAO ჩაატარებს აუდიტს იმის დასადგენად თუ რამდენად ეფექტიანად შეასრულა თავდაცვის დეპარტამენტმა აქტით დაკისრებული ვალდებულება.

ევროკავშირის შემთხვევაში, **NIS2 დირექტივა განსაზღვრავს ევროპის აუდიტორთა სასამართლოს (European Court of Auditors - ECA) უფლება-მოვალეობებს.** ECA წარმოადგენს ევროკომისიისა და ევროპარლამენტის საზედამხედველო ინსტრუმენტს, რომელიც ამ ორგანოებს წარუდგენს დამოუკიდებელი, მიუკერძოებელ და პროფესიულ მოსაზრებებს.

მნიშვნელოვანია, საქართველოს კონტექსტში გაძლიერდეს სახელმწიფოს უმაღლესი მაკონტროლებელი კონსტიტუციური ორგანოს, სახელმწიფო აუდიტის სამსახურის, როლი, რაც ასევე, ხელს შეუწყობს **საპარლამენტო ზედამხედველობის განხორციელებას.**

<u>რეკომენდაცია</u>

1. სახელმწიფო აუდიტის სამსახურმა უზრუნველყოს საქართველოს კონსტიტუციით დაკისრებული მოვალეობა, რაც სხვა დანარჩენთან ერთად, გულისხმობს **სახელმწიფო კრიტიკული ინფორმაციული ინფრასტრუქტურისა და სახელმწიფო მარეგულირებლების საქმიანობის შეფასებას.**
2. უზრუნველყოს **სახელმწიფო შესყიდვების რისკების რეესტრში ICT** და სერვისების მიწოდების რისკების გათვალისწინება და ყოველწლიური აუდირება.

საჯარო-კერძო თანამშრომლობის მექანიზმებისა და Think Tank-ების გაძლიერება

ევროკავშირისა და აშშ გამოცდილება ცხადყოფს, რომ **კერძო სექტორი წარმოადგენს ყველა მნიშვნელოვანი რეფორმის, სტრატეგიისა და პოლიტიკის განუყოფელ ნაწილს.** ამასთან, NIS2 და DORA მნიშვნელოვან ყურადღებას უთმობს საჯარო-კერძო თანამშრომლობის მექანიზმების შექმნასა და განვითარებას, რაც მოიცავს როგორც გამოცდილების გაზიარებას, ასევე, მნიშვნელოვანი ინციდენტების შესახებ ინფორმაციის გაზიარებასაც (cyber threat intelligence).

კიბერუსაფრთხოების საჯარო-კერძო თანამშრომლობის მექანიზმები განვითარების საწყის ეტაპზეა. მეორეს მხრივ, მნიშვნელოვანია, რომ ბაზარზე არ ხდება კიბერუსაფრთხოების Think Tank-ების ჩამოყალიბება და განვითარება.

<u>რეკომენდაცია</u>

1. კიბერუსაფრთხოების კვლევითი ორგანიზაციების განვითარებისა და ხელშეწყობის სტრატეგია. ქმედითი მექანიზმების დანერგვა, როგორიცაა საგრანტო ფონდები, კვლევითი პროექტებისა და მნიშვნელოვან პროექტებში ჩართულობის წახალისება, რაც უზრუნველყოფს საქართველოში შესაბამისი ექსპერტიზის შექმნასა და დაგროვებას.

2. ICT და სერვისების მიწოდების ჯაჭვის რეგულაციების შექმნაში აქტიურად ჩაერთოს ინდუსტრიის წარმომადგენელი ორგანიზაციები, მათ შორის, IT და კიბერ კომპანიები, კვლევითი ინსტიტუტები და არასამთავრობო ორგანიზაციები.

სახელმწიფო შესყიდვების ღია მონაცემების ანალიზი

საფრთხის შემცველი ICT და სერვისის მიწოდების შესყიდვის ანალიზისათვის, კვლევის ფარგლებში დამუშავდა **საქართველოს სახელმწიფო შესყიდვების სააგენტოს პორტალსა (spa.gov.ge)** და **Tendersmonitor.ge**-ზე არსებული ღია მონაცემები. კვლევისას ფოკუსი გაკეთდა **ინფორმაციული და საკომუნიკაციო ტექნოლოგიების (ICT) პროდუქტების შესყიდვაზე** ეროვნული კრიტიკული ინფორმაციული ინფრასტრუქტურის (CII) სუბიექტებში (შემდგომში „სუბიექტებში“).

კვლევის ფარგლებში ყურადღება გამახვილდა რამდენიმე მნიშვნელოვანი შესყიდვების კატეგორიის მიხედვით, როგორიც არის:

- **30200000** -კომპიუტერული მოწყობილობები და აქსესუარები
- **32300000** - ტელე და რადიოსიგნალის მიმღებები და აუდიო ან ვიდეოგამოსახულების ჩამწერი ან აღწარმოების აპარატურა
- **32400000** - ქსელური მოწყობილობები და სერვისი
- **48200000** - ქსელის, ინტერნეტისა და ინტრანეტის პროგრამული პაკეტები
- **72200000** - პროგრამული უზრუნველყოფის შესყიდვა და შემუშავება

წინამდებარე კვლევის ფარგლებში დეტალურად გაანალიზდა კრიტიკული ინფორმაციული სისტემის სუბიექტების (საჯარო უწყებების) მიერ ტენდერისა და პირდაპირი შესყიდვის გზით **2021-2023 წლებში განხორციელებული შესყიდვები.**

შესყიდვის ტიპი	რაოდენობა
ტენდერი	**93 116**
გამარტივებული შესყიდვები	**317 318**
კონსოლიდირებული შესყიდვები	**46 309**

თუმცა, შესყიდვის და ICT სფეროს სპეციფიკიდან გამომდინარე სრული სურათისათვის, რიგ შემთხვევებში გამოყენებულ იქნა წინა პერიოდის მონაცემებიც.

საფრთხის შემცველი შესყიდვები - პროგრამული უზრუნველყოფა

ERP სისტემები

პირველი კატეგორიის კრიტიკული ინფორმაციული ინფრასტრუქტურის უსაფრთხოებისთვის, მნიშვნელოვანია, სუბიექტების მიერ შესყიდული და გამოყენებული **ERP პროგრამული პროდუქტები** და **ფინანსური აღრიცხვის სისტემები იყოს უსაფრთხო.**

საქართველოს ბაზარზე, ერთ-ერთი ყველაზე გავრცელებული **ERP სისტემაა რუსული წარმომავლობის - „1C“ და „FMG Soft“,** თავისი დაბალი ფასისა და შედარებით მარტივი დანერგვის პროცესის გათვალისწინებით.

- „1C“ წარმოადგენს რუსული წარმომავლობის ERP პროგრამულ უზრუნველყოფას, რომლის **პროგრამული მხარდაჭერა და განახლებები იმართება რუსული კომპანიის** მიერ. კვლევაში წარმოდგენილია პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტებში აღნიშნული პროდუქტის მოხმარება.
- FMG Soft არის რუსული წარმომავლობის ბუღალტრულ/ERP სისტემა, რომელსაც საქართველოში წარმოადგენს კომპანია „ეფემჯი სოფტი“. აღნიშნული კომპანია იყენებს რუსული მწარმოებლის „ნოვა სოფტის“ მიერ წარმოებულ „ინფო საწარმოს“. წლების მანძილზე კრიტიკული ინფორმაციული სისტემის სუბიექტები აქტიურად იყენებენ „ეფემჯი სოფტთან“ დაკავშირებულ პროდუქტებს.

<u>შენიშვნა:</u> შესყიდვების ანალიზის დეტალური შედეგები წარმოდგენილია მესამე თავში: „ICT მიწოდების ჯაჭვის უსაფრთხოების ღია მონაცემთა ანალიზი საქართველოში“.

სამართალდამცავი პროგრამული უზრუნველყოფის სისტემები (LES)

კვლევის ფარგლებში შესწავლილი იქნა **სამართალდამცავი პროგრამული უზრუნველყოფის (Law Enforcement Software – LES) შესყიდვები** და ICT უსაფრთხოების ჯაჭვის რისკები.

- **ჰაბიტოსკოპიური სისტემის შესყიდვა** - პირველი კატეგორიის კრიტიკულ ინფორმაციულ სისტემაში გამოიყენება **რუსული წარმომავლობის ჰაბიტოსკოპიურ საექსპერტო-კრიმინალისტური სისტემა „PolyFace”**, რომელიც უზრუნველყოფს სახის ამოცნობას.
- **<u>ფონოსკოპიური სისტემის შესყიდვა</u>** - პირველი კატეგორიის კრიტიკულ ინფორმაციულ სისტემაში გამოიყენება რუსული წარმომავლობის **ფონოსკოპიური ექსპერტიზის სისტემა „IKAR Lab 3“**, რომელიც **უზრუნველყოფს ხმის და მეტყველების ფონოგრამების კრიმინალისტიკურ გამოკვლევას**.
- **<u>დაქტილოსკოპიური სისტემის შესყიდვა</u>** - პირველი კატეგორიის კრიტიკულ ინფორმაციულ სისტემაში **გამოიყენება რუსული წარმომავლობის დაქტილოსკოპიური სისტემა „DACTO 2000“,** რომელიც უზრუნველყოფს თითებისა და ხელის გულის ანაბეჭდის ანალიზს.
- **<u>ბალისტიკური სისტემის შესყიდვა</u>** - პირველი კატეგორიის კრიტიკულ ინფორმაციულ სისტემაში **გამოიყენება რუსული წარმომავლობის ბალისტიკური ავტომატური საძიებო საიდენტიფიკაციო სისტემა - „არსენალი“.**

<u>შენიშვნა:</u> შესყიდვების ანალიზის დეტალური შედეგები წარმოდგენილია მესამე თავში: „ICT მიწოდების ჯაჭვის უსაფრთხოების ღია მონაცემთა ანალიზი საქართველოში“.

გლობალური ნავიგაციის სატელიტური სისტემები (GNSS)

კვლევის ფარგლებში შესწავლილი იქნა გლობალური ნავიგაციის სატელიტური სისტემების (GNSS) შესყიდვები. **პირველი კატეგორიის კრიტიკულ ინფორმაციულ სისტემაში დაფიქსირდა რუსული გლობალური პოზიციონირების სისტემის GLONASS ლიცენზიების შესყიდვები.**

საფრთხის შემცველი შესყიდვები - აპარატურული უზრუნველყოფა

კვლევისას გამოვლენილი იქნა **სანქცირებული მწარმოებელი კომპანიებისა და რუსული წარმომადგენლობისგან შეძენილი სხვადასხვა კატეგორიის მოწყობილობები:**

- **<u>კომპიუტერული მოწყობილობები -</u>** აღნიშნული მიმართულებით *2021-2023 წლებში განხორციელებული შესყიდვების ფარგლებში* ***ჩინეთში წარმოებული და ჩინური პროდუქციის წილმა 69% შეადგინა.***
- **<u>ვიდეო სათვალთვალო კამერები</u>** - 2021-2023 წლების მანძილზე შესყიდული **<u>კამერების უმრავლესობის წილი მოდის ამერიკის მიერ სანქცირებულ კომპანიებზე, კერძოდ Hangzhou Hikvision Digital Technology Co. Ltd და Zhejiang Dahua Vision Technology.</u>**
- **<u>სანქცირებული პროდუქტები</u>** - 2021-2023 წლებში კრიტიკული ინფორმაციული სისტემის სუბიექტების მიერ შეძენილია პროდუქტები ჩინეთის სანქცირებული მომწოდებლებისგან.
- **<u>სატელეკომუნიკაციო მოწყობილობები</u>** - კრიტიკული ინფორმაციული სისტემის სუბიექტების მიერ 2021-2023 წლებში **შესყიდული IP ტელეფონების 50% ჩინური წარმოების მოწყობილობებია.**
- **<u>სატელეკომუნიკაციო მოწყობილობები</u>** - სატელეკომუნიკაციო მოწყობილობების შესყიდვის ფარგლებში განხილული იყო VoIP ტელეფონების, შესაბამისი საკომუნიკაციო მოწყობილობების და აქსესუარების შესყიდვა. აღნიშნული მიმართულებით **<u>2021-2023 წლებში განხორციელებული შესყიდვების ფარგლებში ჩინეთში წარმოებული და ჩინური პროდუქციის წილმა 78% შეადგინა.</u>**

<u>შენიშვნა:</u> შესყიდვების ანალიზის დეტალური შედეგები წარმოდგენილია მესამე თავში: „ICT მიწოდების ჯაჭვის უსაფრთხოების ღია მონაცემთა ანალიზი საქართველოში“.

ინტერნეტ სერვის პროვაიდერები

კვლევის ფარგლებში იდენტიფიცირდა ინტერნეტ სერვის პროვაიდერი და მასთან დაკავშირებული შესყიდვები, რომელიც **კრიტიკული ინფორმაციული სისტემის სუბიექტის გლობალურ ქსელზე დაერთებისათვის იყენებს რუსულ ინტერნეტ პროვაიდერებს.**

მიწოდების ჯაჭვის სასიცოცხლო ციკლთან დაკავშირებული კიბერშეტევების ტექნიკური ანალიზი

ორგანიზაცია „Identify Theft Resource Center-ის 2023 წლის კვლევის[1] მიხედვით, მიწოდების ჯაჭვზე განხორციელებული შეტევების შედეგად დაზარალდა 1,743 ორგანიზაცია და 10 მილიონამდე ადამიანი.

იმისათვის, რომ დავინახოთ საფრთხეების სრული ლანდშაფტი, კვლევაში **წარმოდგენილია ICT მიწოდების ჯაჭვის სრული სასიცოცხლო ციკლი და თითოეულ ეტაპთან დაკავშირებული კიბერშეტევის პრაქტიკული მაგალითები.**

ზემოთ ჩამოთვლილი ეტაპებისთვის განხილულია 3-3 მიმართულება:

- **საფრთხეები** - რისკები და საფრთხეები;
- **რეალური კიბერინციდენტის მაგალითი** - რეალურად მომხდარი ქეისები, ერთის მხრივ გლობალური პერსპექტივიდან (US, UK, EU), ხოლო მეორეს მხრივ, საქართველოს რეალობის გათვალისწინებით.
- **საუკეთესო პრაქტიკა და რეკომენდაცია** - რა მიდგომამ იმუშავა აღნიშული ინციდენტების შემთხვევაში და რა პრაქტიკა შეიძლება გაითვალისწინოს საქართველომ, პოტენციური **კიბერრისკების უკეთ სამართავად** და **საფრთხეების მინიმიზაციისათვის.**

ICT მიწოდების ჯაჭვი იმდენად დაცულია, რამდენადაც მისი შემადგენელი ყველაზე სუსტი კომპონენტი. შესაბამისად, **კვლევის ფარგლებში შემუშავდა ტექნიკური ხასიათის რეკომენდაციები, რომელიც აუცილებელი იქნება საქართველოს კრიტიკული ინფორმაციული ინფრასტრუქტურის ICT და სერვისების მიწოდების ჯაჭვის უსაფრთხოებისთვის.**

[1] https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf

1. თავი 1: ICT მიწოდების ჯაჭვის უსაფრთხოების რეგულაციების ანალიზი დასავლეთის ქვეყნებში

ევროკავშირის კიბერუსაფრთხოების სააგენტოს (ENISA) მიხედვით, მიწოდების ჯაჭვი მოიცავს პროცესების, ადამიანების, ორგანიზაციებისა და დისტრიბუტორების ეკოსისტემას, რომლებიც მონაწილეობენ საბოლოო გადაწყვეტის ან პროდუქტის შექმნასა და მიწოდებაში. კიბერუსაფრთხოებაში, მიწოდების ჯაჭვი მოიცავს რესურსების ფართო სპექტრს (აპარატურული და პროგრამული უზრუნველყოფა), საცავი (ღრუბელი ან ლოკალური), განაწილების მექანიზმები (ვებ აპლიკაციები, ონლაინ მაღაზიები) და მართვის პროგრამული უზრუნველყოფა.

მიწოდების ჯაჭვი მოიცავს ოთხ ძირითად ელემენტს:

- **მიმწოდებელი:** არის ერთეული, რომელიც აწვდის პროდუქტს ან მომსახურებას სხვა სუბიექტს.
- **მიმწოდებლის აქტივები:** არის ღირებული ელემენტები, რომლებსაც მიმწოდებელი იყენებს პროდუქტის ან მომსახურების წარმოებისთვის.
- **მომხმარებელი:** არის სუბიექტი, რომელიც მოიხმარს მიმწოდებლის მიერ წარმოებულ პროდუქტს ან მომსახურებას.
- **მომხმარებელთა აქტივები:** არის ღირებული ელემენტები, რომლებსაც ეკუთვნის სამიზნე.

ერთეული შეიძლება იყოს ინდივიდები, ინდივიდთა ჯგუფები ან ორგანიზაციები. აქტივები შეიძლება იყოს ადამიანები, პროგრამული უზრუნველყოფა, დოკუმენტები, ფინანსები, აპარატურა ან სხვა.

მიწოდების ჯაჭვის შეტევა არის **მინიმუმ ორი შეტევის კომბინაცია. პირველი თავდასხმა ხდება მიმწოდებელზე, რომელიც შემდეგ გამოიყენება სამიზნეზე თავდასხმისთვის მის აქტივებზე წვდომის მისაღებად.** სამიზნე შეიძლება იყოს საბოლოო მომხმარებელი ან სხვა მიმწოდებელი. ამიტომ, იმისთვის, რომ თავდასხმა კლასიფიცირდეს როგორც მიწოდების ჯაჭვის შეტევა, ორივე მიმწოდებელი და მომხმარებელი უნდა იყოს სამიზნე.

წინამდებარე თავში განხილული იქნება აშშ-ს და ევროკავშირის ეკოსისტემების ძირითადი პარამეტრები, რაც უზრუნველყოფს სახელმწიფო კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვას.

გამომდინარე იქედან, რომ ზემოხსენებული **რეგულაციები ძალიან კომპლექსურია** და აერთიანებს მრავალ დაინტერესებულ მხარეს, **ამიტომ, კვლევის მიზნებიდან გამომდინარე და ნაშრომის აღქმადობის გაუმჯობესებისთვის,** წინამდებარე თავებში წარმოდგენილი იქნება შემდეგი სტრუქტურა:

- ***ძირითადი რეგულაციები და აქტები;***
- ***სახელმწიფო უწყებების როლი;***

1.1. აშშ-ს მარეგულირებელი ჩარჩოს ანალიზი

წინამდებარე თავში მოცემულია აშშ-ს ძირითადი რეგულაციების, კანონმდებლობისა და სახელმწიფო უწყებების ანალიზი, რომლებიც მონაწილეობენ ICT მიწოდების ჯაჭვის უსაფრთხოებაში. კვლევისას დამატებით განხილული იქნება იმპლემენტაციისა და აღსრულების მექანიზმები.

1.1.1. ძირითადი რეგულაციები და აქტები

აშშ-ს რეგულაციების ანალიზისას, მნიშვნელოვანია, გათვალისწინებული იქნეს **სახელმწიფო მოწყობის მოდელი, ინსტიტუციური განვითარების სიმწიფე და ქვეყნის მასშტაბი.** ყოველივე აღნიშნულის გათვალისწინებით, სახეზეა კომპლექსური, მრავალშრიანი დაცვის სისტემა, რომელიც შემუშავდა წლების მანძილზე. წინამდებარე ცხრილში **მოცემულია კვლევის ფარგლებში შესწავლილი რეგულაციების ჩამონათვალი და შესაბამისი მნიშვნელოვანი თარიღები, რომლებიც დალაგებულია ქრონოლოგიურად. ამასთან საყურადღებოა, რომ აშშ ეკოსისტემის კომპლექსურობის გათვალისწინებით, კვლევაში შეიძლება არ მოხვდა ან სიღრმისეულად არ იყო წარმოდგენილი ზოგიერთი რეგულაცია, აქტი თუ სახელმძღვანელო.**

ICT მიწოდების ჯაჭვის უსაფრთხოება

2002 - Federal Information Security Management Act (FISMA)	• FISMA აყალიბებს სამთავრობო ინფორმაციის, ოპერაციების და აქტივების დაცვის კონტროლებს ბუნებრივი ან ადამიანის მიერ შექმნილი საფრთხეებისგან.
2013 - Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012	• თავდაცვის კონტრაქტორები ვალდებული არიან უზრუნველყონ თავდაცვის ინფორმაციის დაცვა.
2014 - Cybersecurity Enhancement Act	• საჯარო-კერძო თანამშრომლობის ხელშეწყობის მექანიზმების განვითარება კრიტიკული ინფრასტრუქტურის დაცვის საუკეთესო პრაქტიკის შექმნისათვის.
2014 - Federal Information Security Modernization Act (FISMA) Update	• FISMA-ს განახლება, რომელიც ხაზს უსვამს კიბერუსაფრთხოების რისკების მართვისა და რეალურ დროში შეფასების კონტროლებს.
2015 - Cybersecurity Information Sharing Act (CISA)	• კიბერ საფრთხეების ინფორმაციის გაზიარების მექანიზმების შექმნა ფედერალურ მთავრობასა და კერძო სექტორის კომპანიებს შორის.
2015 - NIST Special Publication 800-161 (Supply Chain Risk Management Practices for Federal Information Systems and Organizations)	• სახელმძღვანელო მითითებები ფედერალური საინფორმაციო სისტემების ICT მიწოდების ჯაჭვის რისკების იდენტიფიცირების, შეფასებისა და შემცირების უზრუნველსაყოფად.
2017 - Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"	• ფედერალურ სააგენტოებს დაევალათ დაიცვან NIST კიბერუსაფრთხოების ჩარჩო და მართონ კიბერუსაფრთხოების რისკები ქვეყნის კრიტიკულ ინფრასტრუქტურაში.
2018 - SECURE Technology Act	• ამ აქტით შეიმნა ფედერალური შესყიდვების უსაფრთხოების საბჭო (FASC), რათა შეიმუშაოს პოლიტიკა და პროცედურები ფედერალური შესყიდვების მიწოდების ჯაჭვის რისკების შესამცირებლად.
2018 - Federal Acquisition Supply Chain Security Act (as part of the SECURE Technology Act)	• აქტის საფუძველზე შეიქმნა FASC და მიენიჭა მას უფლებამოსილება, მართოს მიწოდების ჯაჭვის რისკები ფედერალურ შესყიდვებში.
2019 - Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain"	• ICT მიწოდების ჯაჭვის რისკების შემცირებისათვის, სხვა ღონისძიებებთან ერთად, კომერციის მდივანს(secretary of commece) მიენიჭა უფლებამოსილება აკრძალოს ტრანზაქციები სარისკო ICT პროდუქტებთან ან სერვისებთან დაკავშირებით.
2020 - Cybersecurity Maturity Model Certification (CMMC)	• თავდაცვის სამინისტროს ინიციატივა ავალდებულებს თავდაცვის კონტრაქტორებს გაიარონ მესამე მხარის შეფასებები და მიაღწიონ სერტიფიცირების დონეს სენსიტიური ინფორმაციის დასაცავად.
2021 - Executive Order 14017, "America's Supply Chains"	• მიწოდების კრიტიკული ჯაჭვების, მათ შორის ICT, ყოვლისმომცველი მიმოხილვა მოწყვლადობის იდენტიფიცირებისთვის და მიწოდების ჯაჭვის მდგრადობის გაძლიერების სტრატეგიების შემუშავება.
2021 - Executive Order 14028, "Improving the Nation's Cybersecurity"	• კიბერუსაფრთხოების გაძლიერება ფედერალურ სააგენტოებში, რაც ასევე მოიცავს ICT მიწოდების ჯაჭვის უსაფრთხოებაზე გაუმჯობესებული სტანდარტების, გაიდლაინების და ინციდენტებზე რეაგირების მექანიზმების შემუშავებას.
2021 - Federal Acquisition Regulation (FAR) Case 2018-017, "Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment"	• 2019 წლის NDAA-ს 889-ე პუნქტის საფუძველზე აეკრძალათ ფედერალურ სააგენტოებს კონტრაქტის დადება იმ სუბიექტებთან, რომლებიც იყენებენ სატელეკომუნიკაციო აღჭურვილობას ან გარკვეული ჩინური კომპანიების მიერ წარმოებულ სერვისებს.
2019 - National Defense Authorization Act (NDAA) Section 889	• ფედერალურ სააგენტოებს აეკრძალათ აღჭურვილობის ან სერვისების შესყიდვას კონკრეტული ჩინური კომპანიებისგან უსაფრთხოების მიზნებიდან გამომდინარე.
2020 - DoD Instruction 5000.90 "Cybersecurity for Acquisition Decision Authorities"	• ეს ინსტრუქცია ასახავს პასუხისმგებლობებსა და პროცედურებს შესყიდვის პროცესში კიბერუსაფრთოების ინტეგრირებისთვის.
DoD Defense Industrial Base (DIB) Cybersecurity Program	• ეს პროგრამა აძლიერებს თავდაცვის სამინისტროს არასაიდუმლო ინფორმაციის უსაფრთხოებას თავდაცვის ინდუსტრიულ ბაზაში, ხელს უწყობს კიბერ საფრთხეების ინფორმაციის გაზიარებასა და თავდაცვის კონტრაქტორებთან თანამშრომლობას.
2020 - Defense Acquisition Regulation Supplement (DFARS) Case 2019-D041, "Assessing Contractor Implementation of Cybersecurity Requirements"	• თავდაცვის კონტრაქტორებს მოეთხოვებათ წარმოადგინონ საკუთარი კიბერუსაფრთხოების პრაქტიკის თვითშეფასება NIST SP 800-171-სთან და დაექვემდებარონ DoD აუდიტს.
2021 - DoD Cybersecurity Maturity Model Certification (CMMC) 2.0	• განახლებული ვერსია აუმჯობესებს თავდაპირველ CMMC ჩარჩოს, უზრუნველყოფს გამარტივებულ მოდელს კონტრაქტორის კიბერუსაფრთხოების პრაქტიკის შესაფასებლად და DoD მოთხოვნების შესაბამისობის უზრუნველსაყოფად.

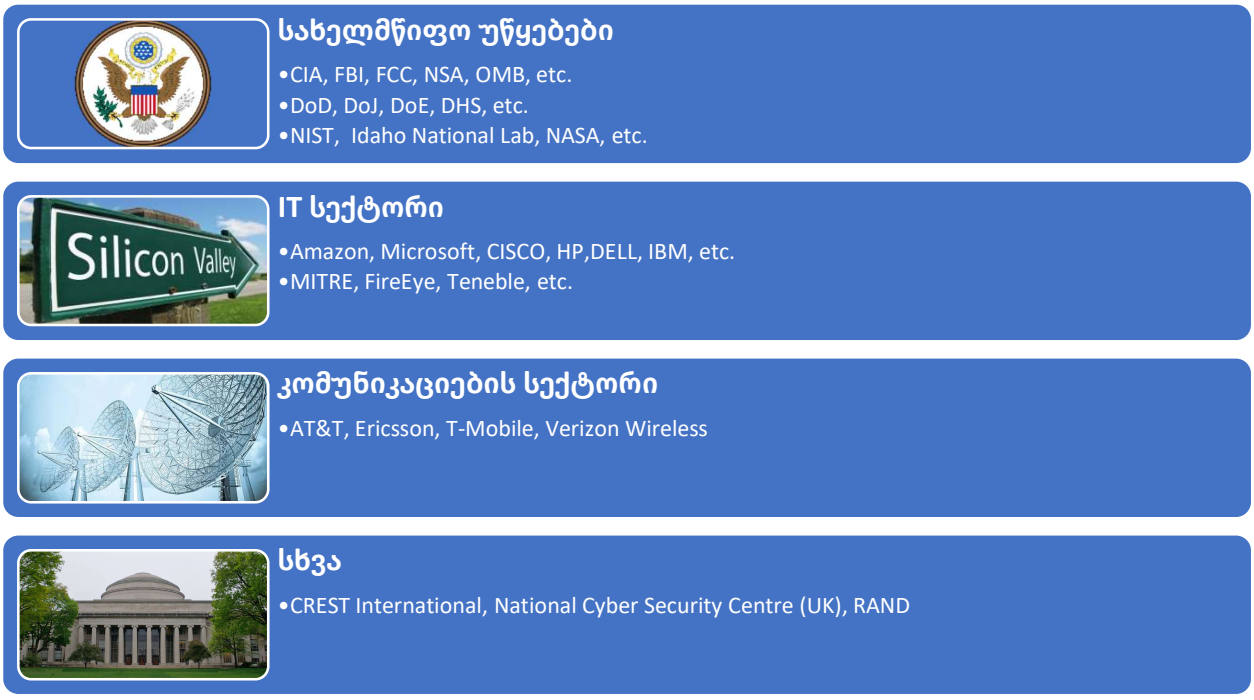
1.1.1.1. CISA-ს საინფორმაციო და საკომუნიკაციო ტექნოლოგიების მიწოდების ჯაჭვის რისკის მართვის[2] (ICT SCRM) პროგრამა

2018 წელს დაფუძნდა აშშ კიბერუსაფრთხოებისა და ინფრასტრუქტურის უსაფრთხოების სააგენტოს (CISA) ICT მიწოდების ჯაჭვის რისკის მართვის (SCRM) პროგრამა. აღნიშნული უზრუნველყოფს **ჰოლისტიკურ მიდგომას ICT მიწოდების ჯაჭვთან დაკავშირებული რისკების მართვისთვის.** ეს პროგრამა ფოკუსირებულია რისკების იდენტიფიცირებაზე, შეფასებასა და შემცირებაზე ქვეყნის კრიტიკული ინფრასტრუქტურის მდგრადობის უზრუნველსაყოფად.

ზემოხსენებული მიზნის მისაღწევად, და იმის გათვალისწინებით, რომ **ICT მიწოდების ჯაჭვის რისკები ცვალებადია და საჭიროებს მაღალი დონის ექსპერტიზას,** ინიციატივა აერთიანებს როგორც სახელმწიფო, ასევე, კერძო სექტორის წარმომადგენლებს.

CISA ICT SCRM სამუშაო ჯგუფის ძირითადი მიმართულებებია:

1. ***<u>საჯარო-კერძო თანამშრომლობა:</u>*** სამუშაო ჯგუფი ხელს უწყობს თანამშრომლობით გარემოს, სადაც საჯარო და კერძო სექტორის ერთეულებს შეუძლიათ ერთად იმუშაონ ICT მიწოდების ჯაჭვში რისკების იდენტიფიცირებისთვის და შესამცირებლად. ეს თანამშრომლობა აძლიერებს საფრთხის დაზვერვის, საუკეთესო პრაქტიკისა და მიღებული გაკვეთილების გაზიარებას, რაც საშუალებას იძლევა ერთიანი მიდგომა კიბერუსაფრთხოების გამოწვევებთან მიმართებაში.



2. ***<u>რისკების იდენტიფიკაცია და მართვა:</u>*** CISA ICT SCRM სამუშაო ჯგუფის **ერთ-ერთი უმთავრესი მიზანია** შეიმუშაოს ICT მიწოდების ჯაჭვთან დაკავშირებული **რისკების იდენტიფიცირებისა და მართვის მეთოდოლოგიები.**

[2] https://www.cisa.gov/resources-tools/groups/ict-supply-chain-risk-management-task-force

3. ***<u>ინფორმაციის გაზიარება:</u>*** სამუშაო ჯგუფის ერთ-ერთ პრიორიტეტს წარმოადგენს დაინტერესებულ მხარეებს შორის **ინფორმაციის დროული და უსაფრთხო გაზიარების** ხელშეწყობა. **კიბერსაფრთხეების შესახებ (cyber threat intelligence) ინფორმაციის** გაცვლით, სამუშაო ჯგუფი ეხმარება ორგანიზაციებს დროულად მიიღონ ინფორმაცია მოწყვლადი პროდუქტებისა თუ მიმდინარე კიბერშეტევების შესახებ.
4. ***<u>მიწოდების ჯაჭვის მთლიანობა (integrity):</u>*** მოიცავს მომწოდებლებისა და კომპონენტების ანალიზს, რათა თავიდან იქნას აცილებული მავნე პროგრამული უზრუნველყოფისა და აპარატურის დანერგვა კრიტიკულ ინფრასტრუქტურაში.
5. ***<u>საუკეთესო პრაქტიკისა და გაიდლაინების შემუშავება:</u>*** სამუშაო ჯგუფი მუშაობს ICT მიწოდების ჯაჭვის უსაფრთხოების საუკეთესო პრაქტიკისა და გაიდლაინების შემუშავებასა და გავრცელებაზე.
6. ***<u>ინციდენტზე რეაგირება და აღდგენა:</u>*** სამუშაო ჯგუფი შეიმუშავებს მითითებებს ინციდენტებზე რეაგირების გეგმების შედგენისათვის.
7. ***<u>მხარდაჭერა მცირე და საშუალო ბიზნესისათვის:</u>*** კიბერუსაფრთხოების რესურსებზე წვდომას, ტრენინგსა და ინსტრუმენტებს, რომლებიც ეხმარება მცირე და საშუალო ბიზნესს გააძლიეროს მიწოდების ჯაჭვის უსაფრთხოების ზომები და დაიცვან ფედერალური სტანდარტები.

2019 წლის 15 მაისს, ძალაში შევიდა **<u>თეთრი სახლის აღმასრულებელი ბრძანება საინფორმაციო და საკომუნიკაციო ტექნოლოგიებისა და სერვისების მიწოდების ჯაჭვის უსაფრთხოების შესახებ</u>**[3] (Executive Order 13873). აღნიშნულის საფუძველზე, CISA-ს დაევალა, იმ აპარატურის, პროგრამული უზრუნველყოფისა და სერვისების შეფასება და აღმოჩენა, რომლებიც ამერიკის შეერთებულ შტატებს უქმნის საფრთხეს. ამის საპასუხოდ, ICT მიწოდების ჯაჭვის რისკის მართვის (SCRM) სამუშაო ჯგუფმა, კერძო სექტორისა და სამთავრობო პარტნიორების ჩართულობით:

- **შეიმუშავა ICT ელემენტების სტანდარტიზებული ტაქსონომია** (მაგ., აპარატურა, პროგრამული უზრუნველყოფა და სერვისები);
- მოამზადა ზემოხსენებული **ICT ელემენტების კრიტიკულობის გავლენის** მეთოდოლოგია.
- მოამზადა და შეაფასა **ეროვნული უსაფრთხოების რისკები,** რომლებიც დაკავშრებულია **ICT აპარატურასთან, პროგრამულ უზრუნველყოფასთან და სერვისებთან.**

ამასთან, სამუშაო ჯგუფის **<u>მიერ შემუშავდა და გამოიცა შემდეგი სახელმძღვანელო დოკუმენტები:</u>**

- Hardware Bill of Materials (HBOM)[4] Framework for Supply Chain Risk Management;
- Software Bill of Materials (SBOM)[5] Framework for Supply Chain Risk Management;

[3] Executive Order on Securing the Information and Communications Technology and Services Supply Chain - https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/

[4] https://www.cisa.gov/sites/default/files/2023-09/A%20Hardware%20Bill%20of%20Materials%20Framework%20for%20Supply%20Chain%20Risk%20Management%20%28508%29.pdf

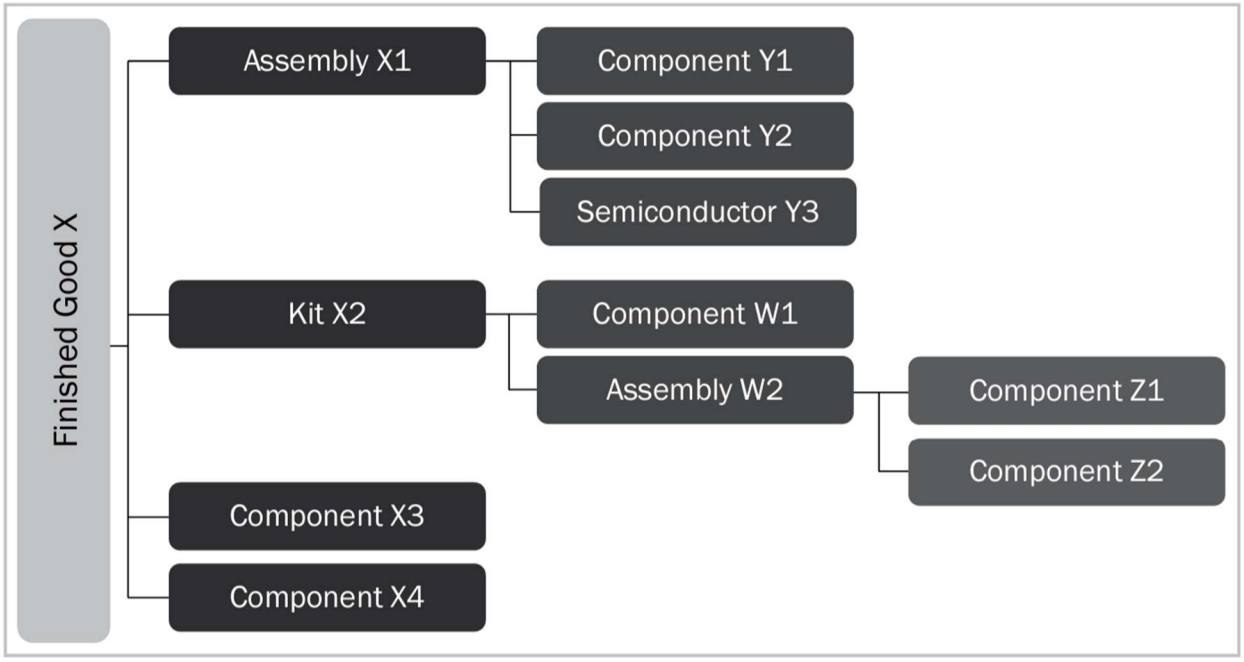
[5] https://www.cisa.gov/sbom

- **Securing the Software Supply Chain**: Recommended Practices for Developers;
- **Securing the Software Supply Chain**: Recommended Practices Guide for Suppliers and accompanying Fact Sheet;
- **Securing the Software Supply Chain:** Recommended Practices Guide for Customers and accompanying Fact Sheet.

თითოეული სახელმძღვანელო და პუბლიკაცია საკმაოდ კომპლექსურია და საჭიროებს შესაბამისს ექსპერტიზას დანერგვისა და აღსრულების ეტაპებზე. კვლევის მიზნებიდან გამომდინარე, **ნაშრომში წარმოდგენილი იქნება მთავარი აქცენტები,** რომელიც აუცილებელია გვესმოდეს ICT მიწოდების ჯაჭვის უსაფრთხოებისთვის.

Hardware Bill of Materials (HBOM)

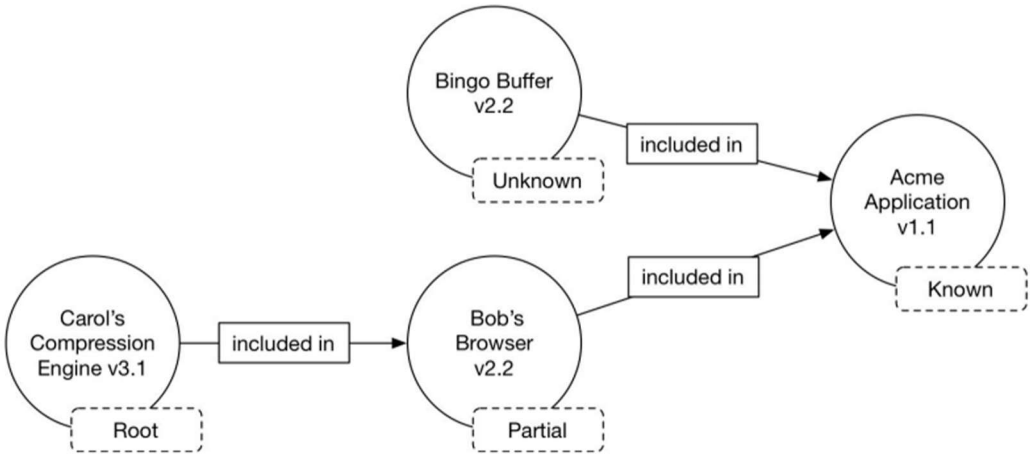
ყოველდღიურად რთულდება კრიტიკულ ინფრასტრუქტურაში გამოყენებული აპარატურის კომპლექსურობა და სახეობა. ამასთან, რთულდება აპარატურაში გამოყენებული კომპონენტების მიკვლევადობის დადგენა. **ICT SCRM ჯგუფის მიერ შემუშავებული HBOM** გვთავაზობს მეთოდოლოგიას იმის დასადგენად, თუ **რა კომპონენტებისგან შედგება შესასყიდი** აპარატურა. ამასთან, წარმოდგენილი მეთოდოლოგია არის მანქანისთვის წაკითხვადი, რაც ამარტივებს ინფორმაციის დამუშავებასა და გაცვლას.



ფიგურა 3: Hardware Bill of Materials

Software Bill of Materials (SBOM)

მსგავსად აპარატურული კომპონენტების წარმომავლობის დადგენისა, დღითიდღე რთულდება პროგრამული უზრუნველყოფისა და მისი კომპონენტების წარმომავლობის დადგენა. ICT SCRM ჯგუფის მიერ შემუშავებული **SBOM ეხმარება ორგანიზაციებს, მწარმოებლებს, მომხმარებლებსა და უსაფრთხოების რგოლებს გაზარდონ პროგრამული უზრუნველყოფის კომპონენტების ხილვადობა და დროულად უზრუნველყონ აღმოჩენილ სისუსტეზე** რეაგირება.

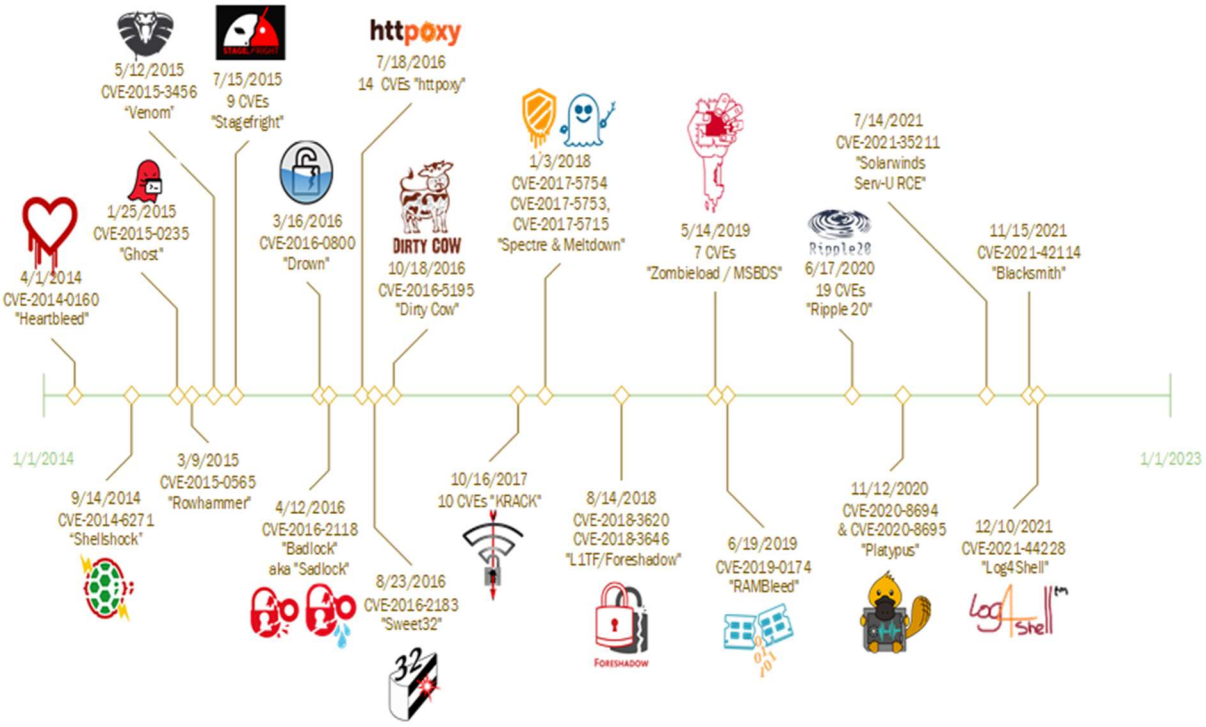


ფიგურა 4: Software Bill of Materials

Vulnerability Exploitability eXchange (VEX)[6]

„Vulnerability Exploitability eXchange-ის (VEX) მიზანია პროგრამული უზრუნველყოფის მიმწოდებელს ან სხვა მხარეებს მისცეს საშუალება, **გადაამოწმონ კონკრეტული დაუცველობის სტატუსი კონკრეტულ პროდუქტში ან პროდუქტებში.** VEX ინფორმაციის გაცემა საშუალებას აძლევს დეველოპერებს, მომწოდებლებსა და სხვებს, **გაცვალონ ინფორმაცია ადამიანისთვის წასაკითხ და მანქანით აღსაქმელ ფორმატში**.

[6] https://www.cisa.gov/sites/default/files/2023-11/When-to-Issue-a-VEX-508c.pdf



ფიგურა 5: მოწყვლადობების აღმოჩენისა და გამჟღავნების მაგალითები

ახალი **მოწყვლადობის აღმოჩენისა და გამჟღავნების** დროს, აუცილებელია პროგრამული უზრუნველყოფის კომპონენტების მომხმარებლებისთვის სტატუსის განახლება. VEX ინფორმაციის გაცემა მომხმარებლებსა და საზოგადოებას საშუალებას აძლევს დაინახონ **აღმოჩენილი სისუსტე და უნდა შეამცირონ მისი გავლენა სხვა კომპონენტებზე.** მოწყვლადობის მენეჯმენტის ან უსაფრთხოების მონიტორინგის აქტივობების დროს, მიმწოდებელი იღებს ინფორმაციას **ახლად აღმოჩენილ დაუცველობის შესახებ, რომელიც გავლენას ახდენს პროგრამული უზრუნველყოფის სხვა კომპონენტზე, რომელსაც შეიძლება იყენებდეს ერთი ან მეტი მიმწოდებლის პროდუქტი.**

1.1.1.2. აღმასრულებელი ბრძანება საინფორმაციო და საკომუნიკაციო ტექნოლოგიების მიწოდების ჯაჭვის უსაფრთხოების[7] შესახებ (EO 13873)

2019 წლის 15 მაისს, პრეზიდენტმა დონალდ ჯ. ტრამპმა დაამტკიცა აღმასრულებელი ბრძანება (EO) 13873, სახელწოდებით **„ინფორმაციული და საკომუნიკაციო ტექნოლოგიებისა და სერვისების მიწოდების ჯაჭვის უსაფრთხოება“.** კვლევის მიზნებიდან გამომდინარე, წინამდებარე თავში წარმოდგენილია აღმასრულებელი ბრძანების ის კომპონენტები, რომელიც რელევანტურია კვლევის მიზნებიდან გამომდინარე. **ბრძანება ითვალისწინებს:**

<u>საგანგებო მდგომარეობის გამოცხადება</u>

ბრძანებით ცხადდება **ეროვნული საგანგებო მდგომარეობა (national emergency declaration) ICT და სერვისების მიწოდების ჯაჭვის საფრთხეებთან დაკავშირებით.** აღნიშნული გამოწვეულია ეროვნული კრიტიკული ინფრასტრუქტურის მავნე აქტორებისგან დაცვის გადაუდებელი აუცილებლობით. კერძოდ, მავნე აქტორებში მოიაზრება უცხო ქვეყნის ძალები (foreign adversaries).

<u>ტრანზაქციების აკრძალვის უფლებამოსილება</u>

აღმასრულებელი ბრძანების საფუძველზე, აშშ კომერციის მდივანს (Secretary of Commerce) მიენიჭა უფლებამოსილება **აკრძალოს / შეაჩეროს ნებისმიერი ტრანზაქცია ICT პროდუქტებთან ან სერვისებთან დაკავშირებით, რომლებიც შეიძლება აზიანებდეს ეროვნულ უსაფრთხოებას.** აღნიშნული უფლებამოსილება მდივანს საშუალებას აძლევს პროაქტიულად გამოავლინოს და შეამციროს ICT მიწოდების ჯაჭვის რისკები.

<u>რისკების განსაზღვრის კრიტერიუმები</u>

აღმასრულებელ ბრძანებაში მოცემულია კონკრეტული კრიტერიუმები, რომლის საფუძველზეც შესაძლებელია შეფასდეს შეიცავს თუ არა ICT ტრანზაქცია რისკს. ეს კრიტერიუმებია:

- *გამოყენებული ტექნოლოგიის **დიზაინში, განვითარებაში ან მიწოდებაში** ჩართულია მოწინააღმდეგე უცხო ქვეყნის (foreign adversaries) წარმომადგენლები.*
- *პოტენციური **ზემოქმედება / გავლენა** აშშ-ს ციფრულ **ეკონომიკასა და კრიტიკულ ინფრასტრუქტურაზე.***
- *მონაცემებისა და სისტემების **კონფიდენციალურობის, მთლიანობისა** და **ხელმისაწვდომობის** დარღვევის ალბათობა.*

<u>უწყებათაშორის თანამშრომლობის პროცესი</u>

აღმასრულებელი ბრძანება ადგენს უწყებათაშორის პროცესს, რომელიც მიმართულია რეგულაციების შემუშავებისაკენ და საეჭვო ტრანზაქციების აკრძალვისაკენ. პროცესი მოიცავს კონსულტაციებს ძირითად დაინტერესებულ მხარეებთან, მათ შორის სამშობლოს უსაფრთხოების, თავდაცვისა და იუსტიციის დეპარტამენტებთან.

[7] https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/

1.1.1.3. აღმასრულებელი ბრძანება ამერიკის მიწოდების ჯაჭვებზე[8] (EO 14017)

2021 წლის 24 თებერვალს, პრეზიდენტმა ბაიდენმა ხელი მოაწერა **„ამერიკის მიწოდების ჯაჭვების**“ შესახებ აღმასრულებელ ბრძანებას (# 14017), რომელიც მიზნად ისახავდა აშშ-ს კრიტიკულად მნიშვნელოვანი მიწოდების ჯაჭვების გაძლიერებას. აღნიშნული ბრძანება, სხვა დანარჩენ მნიშვნელოვან თემებთან ერთად, ფოკუსირებულია საინფორმაციო და საკომუნიკაციო ტექნოლოგიების (ICT) მიწოდების ჯაჭვებზეც. წინამდებარე **თავში წარმოდგენილია ძირითადი აქცენტები, რომელიც რელევანტურია** კვლევის მიზნებისთვის:

<u>რისკის ყოვლისმომცველი შეფასება</u>

ბრძანების საფუძველზე, შესაბამისს უწყებებს მიეცათ 1 წლიანი ვადა კრიტიკული **მიწოდების ჯაჭვებისთვის ჩაეტარებინათ სექტორული (მათ შორის ICT) რისკების საფუძვლიანი შეფასება**. პროცესი მოიაზრებს **ნებისმიერი მოწყვლადობის, პოტენციური შეფერხებებისა და დამოკიდებულების იდენტიფიცირებას აშშ კრიტიკულ მიწოდების ჯაჭვში.**

<u>დივერსიფიკაცია და მეღეგობა</u>

ბრძანება მიზნად ისახავს დაიგეგმოს და მოხდეს კრიტიკული **მიწოდების ჯაჭვების დივერსიფიკაცია და გამოირიცხოს ცალკეულ წერტილზე დამოკიდებულება.** აღნიშნული განსაკუთრებით მნიშვნელოვანია ისეთ შემთხვევებში, როდესაც **მიწოდების ჯაჭვში მონაწილეობს ქვეყანა,** რომელიც პოტენციურად, უქმნის საფრთხეს აშშ-ს.

<u>შიდა წარმოების გაძლიერება</u>

ბრძანება მიზნად ისახავს ხელი შეუწყოს შიდა წარმოების შესაძლებლობების გაძლიერებას, მათ შორის ICT კრიტიკული კომპონენტებისთვის. აღნიშნული მოიცავს **ინვესტიციებს წარმოებაში, კვლევაში, განვითარებასა და სამუშაო ძალის მომზადებაში. <u>შიდა წარმოების გაძლიერება ხელს უწყობს უცხოელ მომწოდებლებზე დამოკიდებულების შემცირებას და აძლიერებს მიწოდების ჯაჭვის უსაფრთხოებასა და საიმედოობას.</u>**

<u>მოკავშირეებთან და პარტნიორებთან თანამშრომლობა</u>

ბრძანება მიზნად ისახავს მოკავშირე ქვეყნებთან და მთავარ პარტნიორებთან **თანამშრომლობის მექანიზმების გაძლიერებას** გლობალური მიწოდების ჯაჭვების უზრუნველსაყოფად. აღნიშნული მოიაზრებს ერთობლივ პროექტებს **<u>საერთო სტანდარტებზე, საუკეთესო პრაქტიკასა და მიწოდების ჯაჭვის საფრთხეებზე კოორდინირებულ პასუხებზე.</u>** საერთაშორისო თანამშრომლობა სასიცოცხლოდ მნიშვნელოვანია გლობალური რისკების მოსაგვარებლად და ICT მიწოდების ჯაჭვის მთლიანობის უზრუნველსაყოფად.

[8] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/

აღმასრულებელი ბრძანების შესაბამისად, აშშ კომერციის დეპარტამენტსა (Department of Commerce) და სამშობლოს (შიდა) უსაფრთხოების დეპარტამენტს (Department of Homeland Security) დაევალა ICT მიწოდების ჯაჭვების უსაფრთოხების საკითხების შესწავლა და შესაბამისი რეკომენდაციების მომზადება. **ბრძანების შესრულების ნლიურ ანგარიშში** წარმოდგენილია რეკომენდაციები, რომელიც გაიცა მედეგი ICT სამრეწველო ბაზის შესაქმნელად,[9]:

ფიგურა 6: აღმასრულებელი ბრძანება ამერიკის მიწოდების ჯაჭვებზე (EO 14017)

[9] https://www.whitehouse.gov/wp-content/uploads/2022/02/Capstone-Report-Biden.pdf

1.1.1.4. ფედერალური შესყიდვების მიწოდების ჯაჭვის უსაფრთხოების (FASC)[10] აქტი (2020)

2020 წელს ამოქმედდა **ფედერალური შესყიდვების მიწოდების ჯაჭვის უსაფრთხოების აქტი**, რომელიც გამომდინარეობს 2018 წლის SECURE Technology Act[11]-იდან. აღნიშნული აქტი ადგენს **მიწოდების ჯაჭვის რისკების მართვის ჩარჩოს ფედერალური შესყიდვებისთვის.** რეგულაციის ძირითადი ფოკუსია საინფორმაციო და საკომუნიკაციო ტექნოლოგიების (ICT) უსაფრთხოება.

ICT მიწოდების ჯაჭვის უსაფრთხოების უზრუნველსაყოფად, აქტი ითვალისწინებს შემდეგს:

<u>ფედერალური შესყიდვების უსაფრთხოების საბჭო (FASC)</u>

აქტით განისაზღვრება ფედერალური შესყიდვების უსაფრთხოების საბჭოს მიზნები, მათ შორის **პოლიტიკისა და პროცედურების შემუშავების ვალდებულება ICT მიწოდების ჯაჭვის რისკების შესამცირებლად.** საბჭო წარმოადგენს **ცენტრალურ უწყებას ფედერალურ სააგენტოებს შორის,** რომელიც უზრუნველყოფს ერთიანი მიდგომის ჩამოყალიბებას მიწოდების ჯაჭვის უსაფრთხოებასთან დაკავშირებით.

FASC წარმოადგენს აღმასრულებელი შტოს უწყებათაშორის საბჭოს, რომელიც დაკომპლექტებულია:

- **საბჭოს თავმჯდომარე** - მენეჯმენტისა და ბიუჯეტის ოფისის (OMB) უმაღლესი დონის თანამდებობის პირი.
- ზოგადი სერვისების ადმინისტრაცი (GSA);
- სამშობლოს უსაფრთხოების დეპარტამენტი (DHS);
- ეროვნული დაზვერვის დირექტორის აპარატი (DNI);
- თავდაცვის დეპარტამენტი (DoD);
- იუსტიციის დეპარტამენტი (DOJ);
- კომერციის დეპარტამენტი (DoC).

<u>რისკის შეფასება და შერბილება</u>

აქტის საფუძველზე, საბჭო ვალდებულია შეაფასოს ICT მიწოდების ჯაჭვთან დაკავშირებული რისკები. საბჭოს მიზანია, თავიდან იქნეს აცილებული მავნე აქტორების მონაწილეობა ფედერალური ICT სისტემების შესყიდვებში.

<u>აკრძალვისა და გამონაკლისის დადგენის უფლებამოსილება</u>

აქტის თანახმად, FASC-ს აქვს უფლებამოსილება **გამოსცეს აკრძალვისა და გამონაკლისის დადგენის ბრძანებები ICT პროდუქტებისა და სერვისებისთვის,** რომლებიც შეიცავს ეროვნული უსაფრთხოების რისკებს. აღნიშნული ბრძანებების მიზანია, არ დაუშვას პოტენციურად საფრთხის შემცველი ICT კომპონენტების შესყიდვა ფედერალურ უწყებებში.

[10] https://www.federalregister.gov/documents/2020/09/01/2020-18939/federal-acquisition-supply-chain-security-act

[11] Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act - https://www.congress.gov/bill/115th-congress/house-bill/7327/text

<u>ინფორმაციის გაზიარება</u>

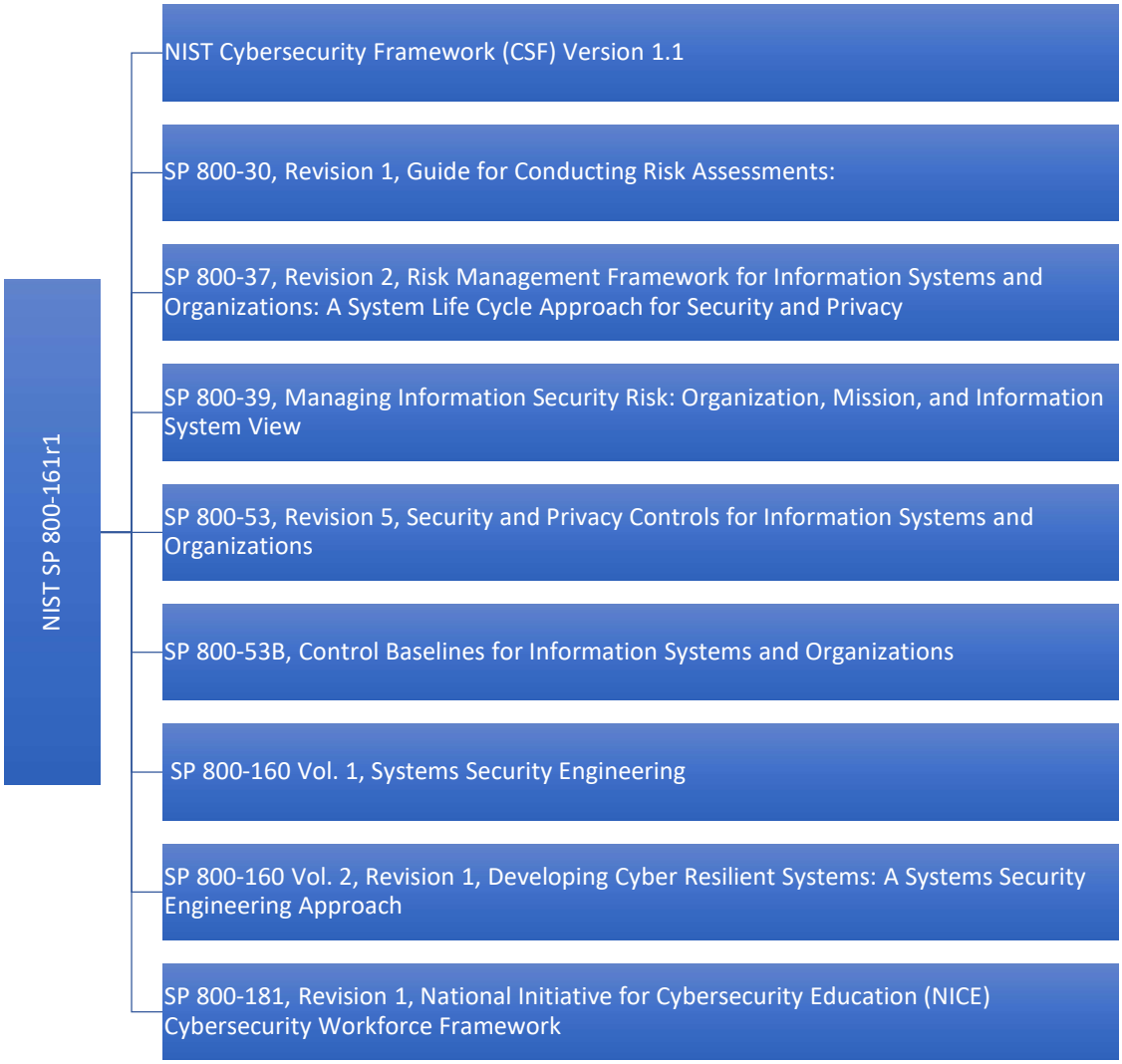
აქტის საფუძველზე, საბჭოს დაეკისრა ფედერალურ უწყებებსა და კერძო ორგანიზაციებს შორის **ინფორმაციის გაზიარების მექანიზმების ხელშეწყობა.** საფრთხეების დაზვერვისა (cyber threat intelligence) და საუკეთესო პრაქტიკის გაცვლის ხელშეწყობით, აქტი აძლიერებს მიწოდების ჯაჭვის რისკების გამოვლენის, რეაგირების და შერბილების კოლექტიურ უნარს.

<u>სტანდარტები და სახელმძღვანელოები</u>

საბჭო პასუხისმგებელია **მიწოდების ჯაჭვის რისკის მართვის სტანდარტებისა და სახელმძღვანელოების შემუშავებასა და გავრცელებაზე.** აღნიშნული სტანდარტები ეხმარება ფედერალურ სააგენტოებს მიწოდების ჯაჭვის რისკების შეფასებასა და მართვაში.

1.1.1.5. NIST SP 800-161[12] (Supply Chain Risk Management Practices)

მიწოდების ჯაჭვის კიბერუსაფრთხოების რისკების მართვა (C-SCRM) არის სისტემური პროცესი, რომლის მიზანია მიწოდების ჯაჭვის სრულ სასიცოცხლო ციკლში იდენტიფიცირებული და მართული იყო კიბერრისკები. **NIST SP 800-161 მიზანია,** ორგანიზაციას მიაწოდოს **სახელმძღვანელო მითითებები იმის თაობაზე, თუ როგორ შეიძლება მოხდეს რისკების იდენტიფიცირება და შეფასება, რის საფუძველზეც ორგანიზაცია შეძლებს რისკის მართვის პროცესების დანერგვასა და კონტროლის მექანიზმების დანერგვას.** სახელმძღვანელოში წარმოდგენილ მითითებების შესრულებაზე პასუხისმგებელი შეიძლება იყოს ორგანიზაციის სხვადასხვა ერთეული (არამხოლოდ IT ან/და უსაფრთხოება) სხვადასხვა SCRM პერსპექტივით, უფლებამოსილებითა და სამართლებრივი მექანიზმებით.

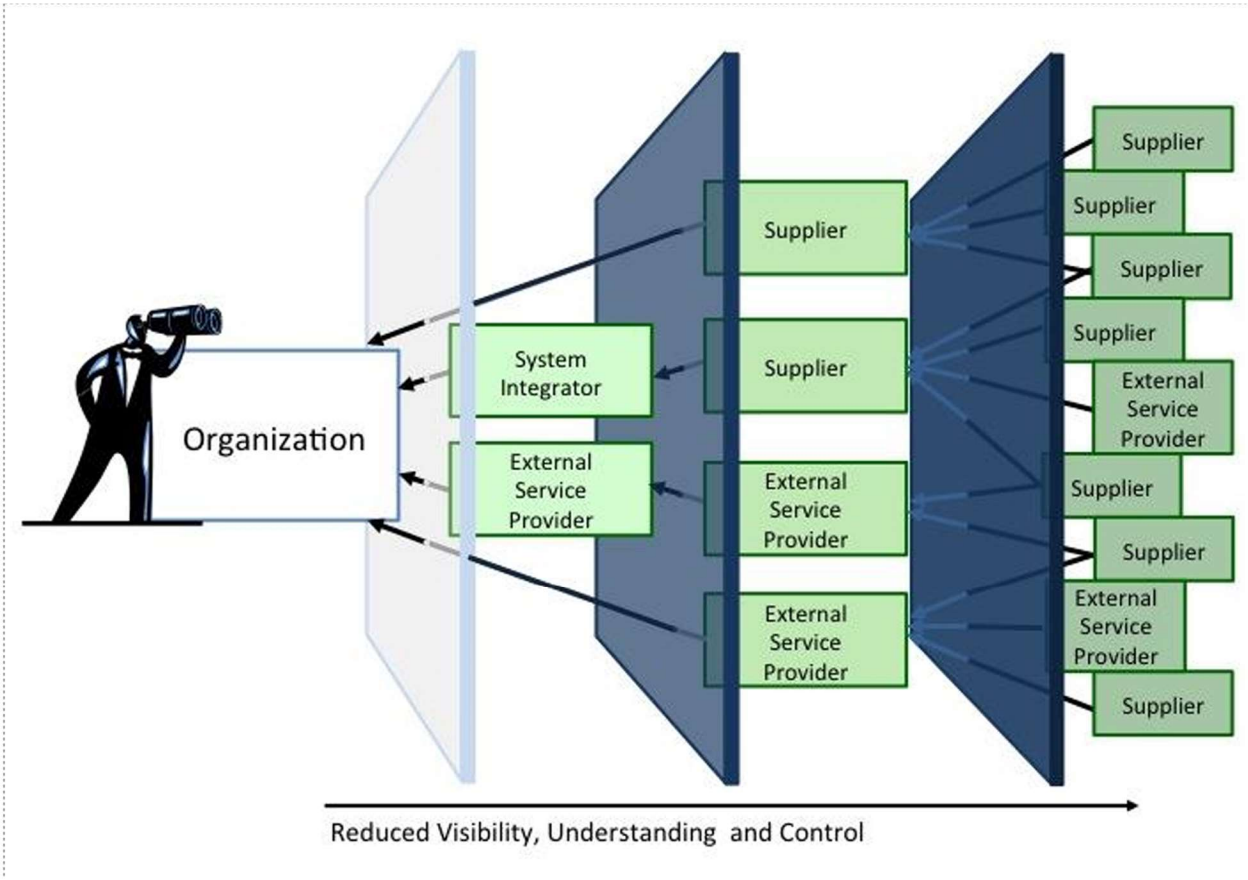


ფიგურა 7: NIST პუბლიკაციები და მიწოდების ჯაჭვის უსაფრთხოების კონტროლები

[12] https://csrc.nist.gov/pubs/sp/800/161/r1/final

NIST SP 800-16 1 Rev. 1 სპეციალური პუბლიკაცია **მჭიდრო კავშირშია უკვე არსებულ, NIST პუბლიკაციებთან** ინფორმაციული და კიბერ უსაფრთხოების მიმართულებით. შესაბამისად, ორგანიზაციას, რომელიც უკვე იყენებს რომელიმე ზემოხსენებულ პუბლიკაციას / სახელმძღვანელოს შეუძლია მარტივად დააინტეგრიროს მიწოდების ჯაჭვის უსაფრთხოების მოთხოვნები საკუთარ რისკების მართვისა და შიდა კონტროლის სისტემებში.

NIST SP 800-161 Rev. 1-ის მთავარი მიზანია, შემსყიდველ ორგანიზაციებს დაეხმაროს შესასყიდ ICT პროდუქტებთან დაკავშირებული გამოწვევების დაძლევაში. ერთ-ერთი ასეთი მნიშვნელოვანი **გამოწვევაა ICT და სერვისების მიწოდების ჯაჭვის ხილვადობა (visibility).** რაც უფრო მეტად **იზრდება ICT და სერვისის კომპონენტების კომპლექსურობა, მით მეტად უმცირდება ორგანიზაციას მიწოდების ჯაჭვის სრული ხილვადობა.**



ფიგურა 8: მიწოდების ჯაჭვის ხილვადობის კონცეფცია

კვლევის მიზნებიდან გამომდინარე, წინამდებარე თავში განხილულია რამდენიმე მნიშვნელოვანი დომენი, რომელსაც ფარავს NIST SP 800-161.

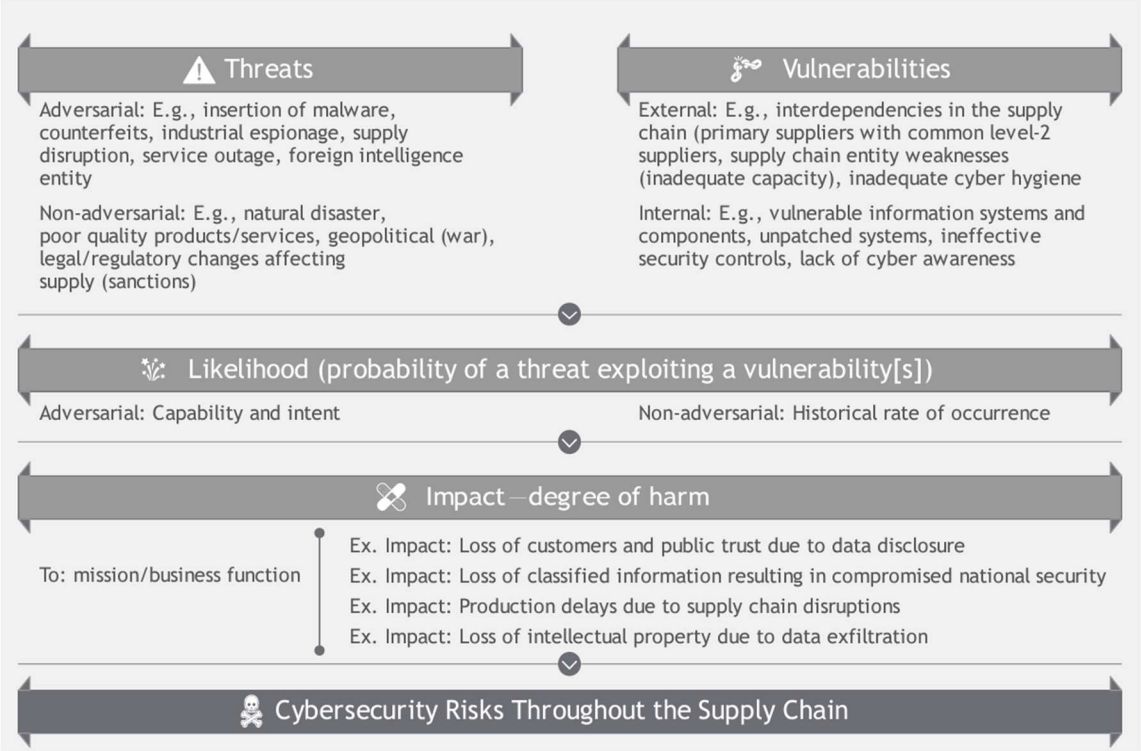
C-SCRM ინტეგრაცია ორგანიზაციულ რისკების მართვის ჩარჩოში:

NIST SP 800-161 პუბლიკაციაში წარმოდგენილია მიწოდების ჯაჭვის კიბერრისკების მართვის (C-SCRM) მეთოდოლოგია, რომელიც უნდა **დაინტეგრირდეს ორგანიზაციის ერთიან რისკების მართვის მიდგომაში.** პროცესი მოიცავს:

- **Frame Risk** - აყალიბებს ორგანიზაციის ICT რისკების კონტექსტს, რომელშიც უნდა დაინტეგრირდეს მიწოდების ჯაჭვის რისკები.
- **Assess Risk** - კრიტიკულობის, საფრთხის, მოწყვლადობის, ალბათობის, ზემოქმედებისა და სხვა დაკავშირებული ინფორმაციის მიმოხილვა და ინტერპრეტაცია.
- **Respond to Risk** - რისკების შეფასების საფუძველზე კონტროლების შერჩევა, მორგება და განხორციელება.
- **Monitor Risk** - რისკის გავლენის მუდმივი მონიტორინგი და რისკის შემცირების კონტროლების ეფექტურობის ზედამხედველობა.

<u>კიბერუსაფრთხოების ინტეგრირება მიწოდების ჯაჭვის პროცესებში:</u>

პუბლიკაციაში წარმოდგენილი კონტროლები და კიბერრისკები ადაპტირებულია მიწოდების ჯაჭვის პროცესებზე. მიწოდების ჯაჭვის სხვადასხვა ეტაპზე განხორციელებული პრაქტიკული შეტევის სცენარები განხილულია კვლევის მესამე თავში.



ფიგურა 9: მიწოდების ჯაჭვის კიბერრისკები

<u>C-SCRM-ის ინტეგრაცია შესყიდვების პროცესში</u>

პუბლიკაციაში წარმოდგენილია მიწოდების ჯაჭვის **კიბერუსაფრთხოების კონტროლების ინტეგრაციის სქემა ორგანიზაციის შესყიდვების პროცესში.** კერძოდ,

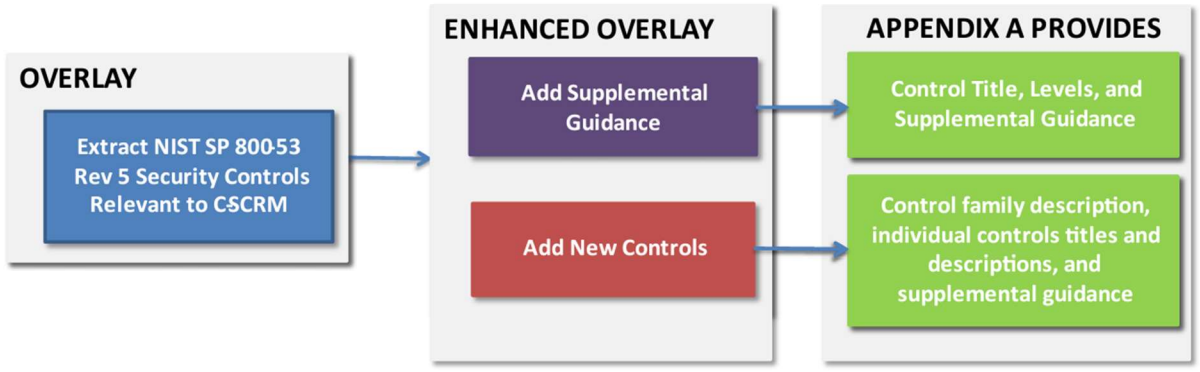
შესყიდვების სასიცოცხლო ციკლის მანძილზე გასათვალისწინებელი და დასანერგი კონტროლების სქემა წარმოდგენილია წინამდებარე ცხრილში.

ცხრილი 1: მიწოდების ჯაჭვის უსაფრთხოების მოთხოვნები შესყიდვების სასიცოცხლო ციკლში

შესყიდვების პროცესი	**რისკის შეფასება სერვისისთვის**	**რისკის შეფასება მიმწოდებლისთვის**	**რისკის შეფასება პროდუქტისთვის**
შესყიდვის დაგეგმვა	შესასყიდი სერვისის კრიტიკულობის განსაზღვრა	რამდენად შესაბამისია მოთხოვნებთან	შესასყიდი პროდუქტის კრიტიკულობის განსაზღვრა
მოთხოვნების განსაზღვრა ან შემუშავება	C-SCRM კონტროლების შერჩევა / იდენტიფიცირება	C-SCRM კონტროლების შერჩევა / იდენტიფიცირება	C-SCRM კონტროლების შერჩევა / იდენტიფიცირება
ბაზრის კვლევა	რისკების საწყისი შეფასება (due diligence კითხვარები)	რისკების საწყისი შეფასება (due diligence კითხვარები)	პროდუქტის ალტერნატივების მოკვლევა და თანდაყოლილი რისკების გამოვლენა
წინადადებების გადარჩევა / შესყიდვის დასრულება	C-SCRM მოთხოვნებთან შესაბამისობის დადგენა რისკების შეფასება	C-SCRM მოთხოვნებთან შესაბამისობის დადგენა რისკების შეფასება	Pre-deployment რისკების შეფასება
ოპერირება და მხარდაჭერა	რისკების უწყვეტი მონიტორინგი	რისკების უწყვეტი მონიტორინგი	რისკების უწყვეტი მონიტორინგი

<u>დანართი A: უსაფრთხოების კონტროლები</u>

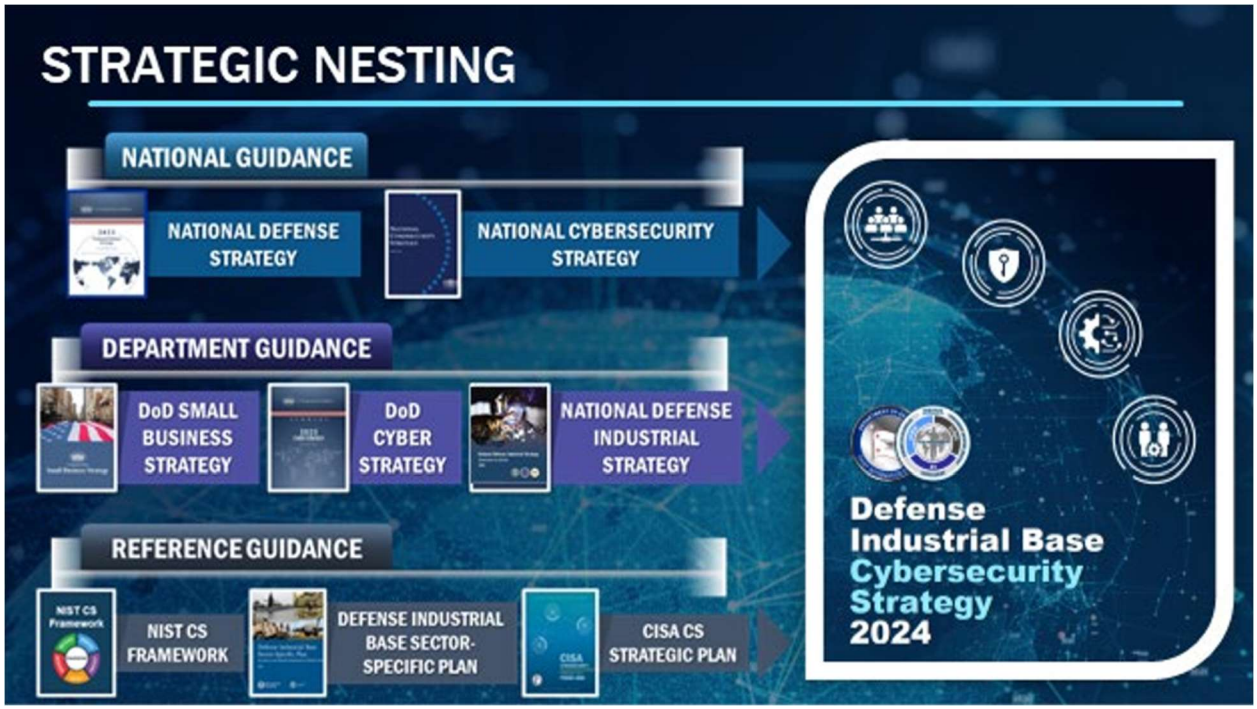
პუბლიკაციის დანართი A მოიცავს მიწოდების ჯაჭვის კიბერუსაფრთხოების კონტროლებს, რომელიც ძირითადად, ეფუძნება NIST SP 800-53 R5 პუბლიკაციას. ამასთან, დანართში წარმოდგენილია დამატებითი კონტროლები, რომელიც სპეციფიურია ICT და სერვისების მიწოდების ჯაჭვებისათვის.



ფიგურა 10: მიწოდების ჯაჭვის უსაფრთხოების კონტროლები

1.1.1.6. ეროვნული თავდაცვის ავტორიზაციის აქტი (NDAA) 2024[13] და თავდაცვის ინდუსტრიული ბაზის (DIB) კიბერუსაფრთხოების სტრატეგია 2024[14]

თავდაცვის ეროვნული ავტორიზაციის აქტი (NDAA) და თავდაცვის ინდუსტრიული ბაზის (DIB) კიბერუსაფრთხოების სტრატეგია 2024 ადგენს ძირითად ვალდებულებებს აშშ თავდაცვის **დეპარტამენტისა (DoD) და მისი ქვეკონტრაქტორების მიმართ.** კერძოდ, რეგულაციისა და სტრატეგიის უმთავრესი მიზანია, უზრუნველყოფილი იქნეს აშშ **თავდაცვის ძალების ხელთ არსებული ICT და სერვისების შემადგენელი კომპონენტების საიმედოობა და უსაფრთხოება.** განსაკუთრებით, აღსანიშნავია, რომ **კონტრაქტორების სიმრავლე, შესყიდული ტექნოლოგიებისა და კომპონენტების წარმომავლობა და ხშირ შემთხვევაში დამოკიდებულება უცხო ქვეყნებზე** ზრდის მიწოდების ჯაჭვის რისკებს.

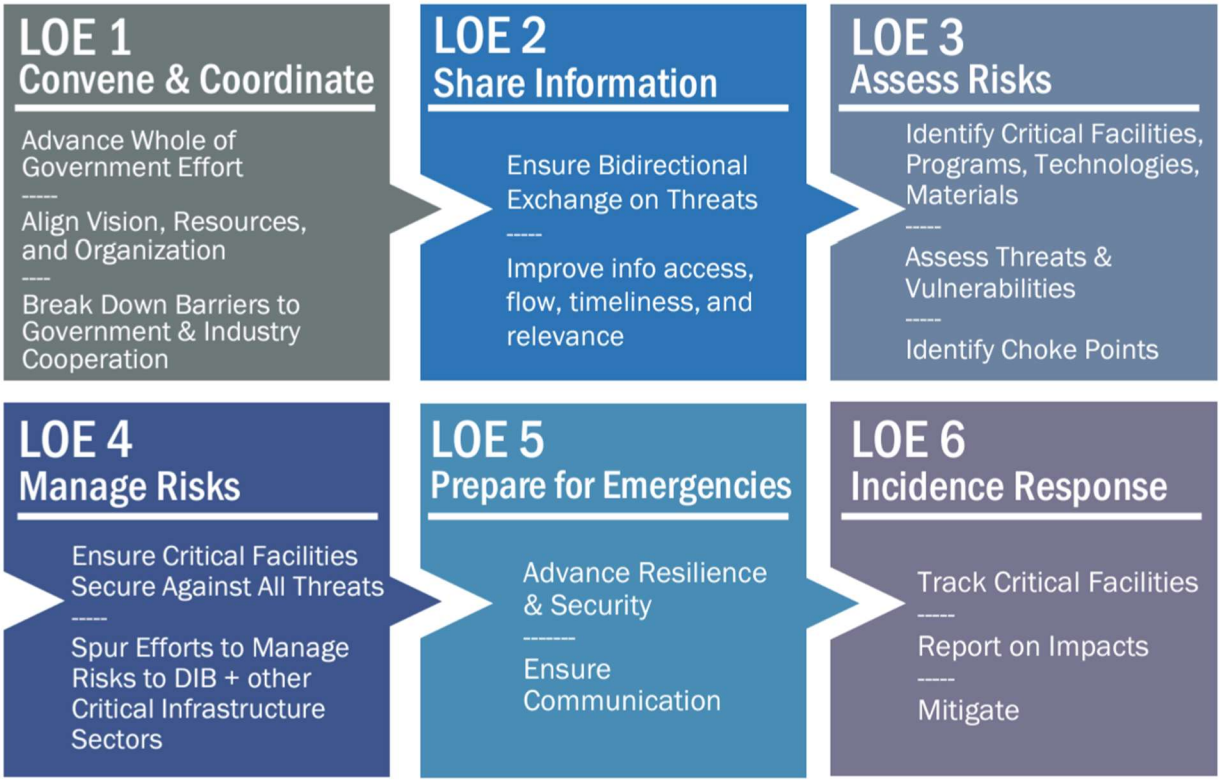


ფიგურა 11: თავდაცვის ინდუსტრიული ბაზის კიბერუსაფრთხოების სტრატეგია 2024

წინამდებარე თავში წარმოდგენილია ის ძირითადი მიმართულებები, რომელიც **რელევანტურია** კვლევის მიზნებიდან გამომდინარე:

13 https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/FY24%20NDAA%20CHM%20Mark%20Package.pdf

14 https://media.defense.gov/2024/Mar/28/2003424523/-1/-1/1/DOD_DOB_CS_STRATEGY_DSD_SIGNED_20240325.PDF



ფიგურა 12: სტრატეგიის ძირითადი მიზნები

<u>რისკის შეფასებისა და მართვის გაძლიერება</u>

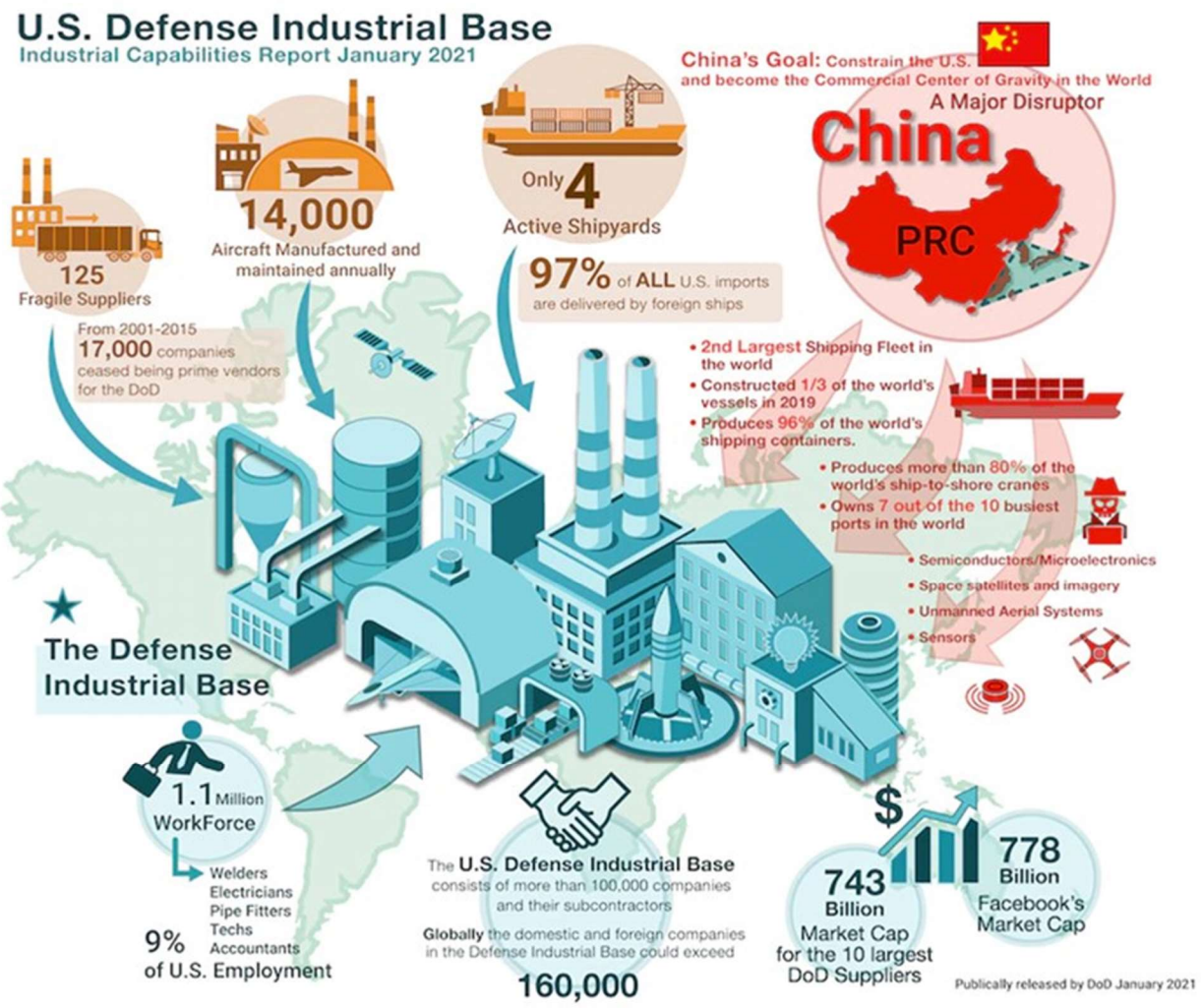
აქტები ავალდებულებს თავდაცვის დეპარტამენტს (DoD) ჩაატაროს ყოვლისმომცველი რისკების შეფასება ICT მიწოდების ჯაჭვებისათვის. ტრადიციულ რისკფაქტორებთან ერთად, აღნიშნული ასევე მოიცავს **უცხოური საკუთრების, კონტროლის ან ზეგავლენის რისკების იდენტიფიცირებას** და **შემცირებას** ICT მიწოდების ჯაჭვის კრიტიკულ კომპონენტებზე. მიზანია, უზრუნველყოფილი იქნეს თავდაცვის კრიტიკული სისტემების მთლიანობა, უსაფრთხოება და მედეგობა.

<u>კიბერუსაფრთხოების პრაქტიკის გაძლიერება და სტანდარტებთან შესაბამისობა</u>

აქტები ავალდებულებს თავდაცვის **დეპარტამენტის კონტრაქტორებს შესაბამისობაში იყვნენ კიბერუსაფრთხოების განახლებულ სტანდარტებთან,** მათ შორის NIST გაიდლაინებსა და კიბერუსაფრთხოების სიმწიფის მოდელის სერტიფიკაციასთან ((CMMC) 2.0).

<u>მომარაგების ჯაჭვის დივერსიფიკაცია :</u>

უცხოელ მომწოდებლებზე, განსაკუთრებით **<u>მოწინააღმდეგე ქვეყნების მომწოდებლებზე დამოკიდებულების შესამცირებლად,</u>** NDAA 2024 ხელს უწყობს ICT მიწოდების ჯაჭვის დივერსიფიკაციას. ის ხელს უწყობს **პარტნიორობას სანდო შიდა და მოკავშირე ქვეყნების მომწოდებლებთან**, ხელს უწყობს ინოვაციას და უზრუნველყოფს ალტერნატიულ წყაროებს კრიტიკული ტექნოლოგიებისა და კომპონენტებისთვის.



ფიგურა 13: აშშ თავდაცვის ინდუსტრიული ბაზა

<u>გაძლიერებული ინფორმაციის გაზიარება და თანამშრომლობა:</u>

განსაკუთრებული აქცენტი კეთდება **საჯარო-კერძო თანამშრომლობის მექანიზმების განვითარებასა** და ამავდროულად, **კიბერსაფრთხეების შესახებ ინფორმაციის გაზიარების მნიშვნელობაზე.** თავდაცვის დეპარტამენტი ვალდებულია შექმნას და უზრუნველყოს უსაფრთხო საკომუნიკაციო არხების მიწოდების ჯაჭვის მოწყვლადობის გაზიარებისა და აღმოფხვრის მიზნით. წახალისებულია ერთობლივი ძალისხმევა საუკეთესო პრაქტიკის შემუშავებისა და წარმოშობილ საფრთხეებზე რეაგირების სტრატეგიების შესამუშავებლადაც.

<u>გარე გავლენისა და ჯაშუშობის წინააღმდეგ ბრძოლა:</u>

აქტები მიზნად **ისახავს უცხოური აქტორების მიერ ჯაშუშობისა და ზემოქმედების ოპერაციების წინააღმდეგ ბრძოლას.** კერძოდ, განსაზღვრულია საფრთხის შემცველი ICT პროდუქტებისა და სერვისების იდენტიფიცირებისა და შეზღუდვის მექანიზმები,

რომლებიც წარმოადგენენ უსაფრთხოების მნიშვნელოვან რისკებს უცხოური გავლენის გამო.

<u>მხარდაჭერა მცირე და საშუალო საწარმოებისთვის:</u>

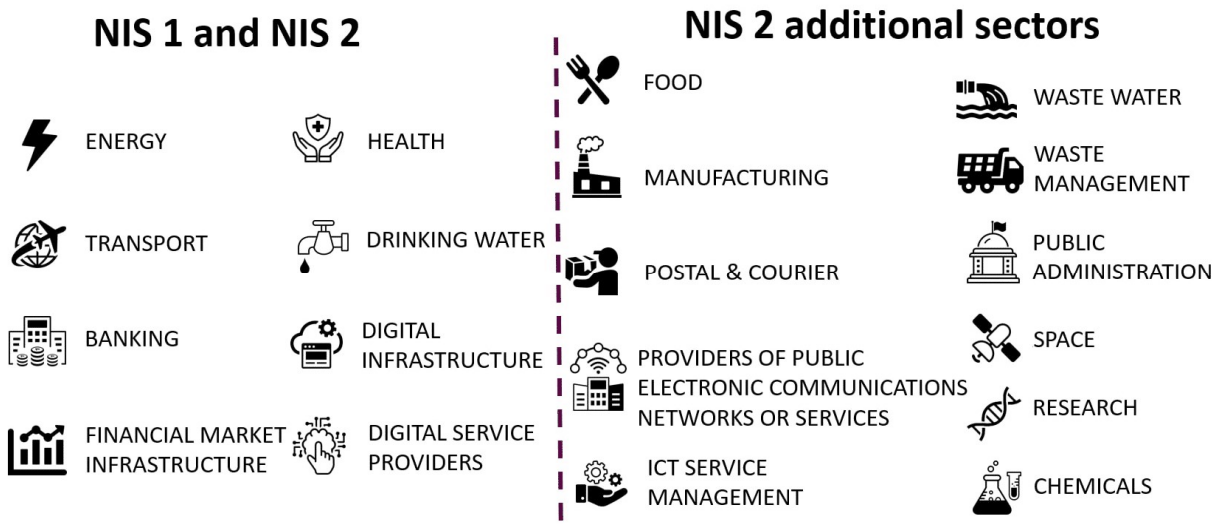
მცირე და საშუალო ბიზნესი სასიცოცხლო როლს თამაშობს თავდაცვის მიწოდების ჯაჭვში, შესაბამისად, თავდაცვის დეპარტამენტი უზრუნველყოფს **<u>მიზნობრივ მხარდაჭერას ამ ბიზნესებისთვის.</u>** აღნიშნული გულისხმობს კიბერუსაფრთხოების რესურსებზე ხელმისაწვდომობას, ტრენინგებსა და ფინანსურ დახმარებას, რათა მცირე და საშუალო ბიზნესმა შეძლოს კიბერუსაფრთხოების მკაცრი მოთხოვნების დაკმაყოფილება.

1.2. ევროკავშირის მარეგულირებელი ჩარჩოს ანალიზი

1.2.1. ძირითადი რეგულაციები და აქტები

ქსელისა და საინფორმაციო სისტემების დირექტივა[15] (NIS 2 Directive)

2022 წლის 14 დეკემბერს დამტკიცდა და 2023 წლიდან ძალაში შევიდა **ევროკავშირის ქსელისა და ინფორმაციის უსაფრთხოების დირექტივა 2** (Network and Informatino Security Directive 2) წარმოადგენს პირველი **NIS დირექტივის განახლებას,** რომელიც მიზნად ისახავს გააძლიეროს კიბერუსაფრთხოება და კრიტიკული ინფრასტრუქტურის მედეგობა ევროკავშირში. განახლებული რეგულაცია ითვალისწინებს პირველ დირექტივაში გამოვლენილ ხარვეზებსა და გამოწვევებს და აწესებს უფრო მკაცრ უსაფრთხოების მოთხოვნებს.



ფიგურა 14: NIS1 და NIS2 დირექტივების შედარება

NIS2 დირექტივა **მოქმედებს ევროკავშირის წევრ ქვეყნებში და ითვალისწინებს სხვადასხვა სექტორის მიმართ დაწესებულ კიბერუსაფრთხოების მოთხოვნებს.** კერძოდ, დირექტივა ვრცელდება ისეთ კრიტიკულ სექტორებზე, როგორიცაა **ენერგეტიკა, ტრანსპორტი, საბანკო სფერო, ჯანდაცვა და ციფრული ინფრასტრუქტურა**.

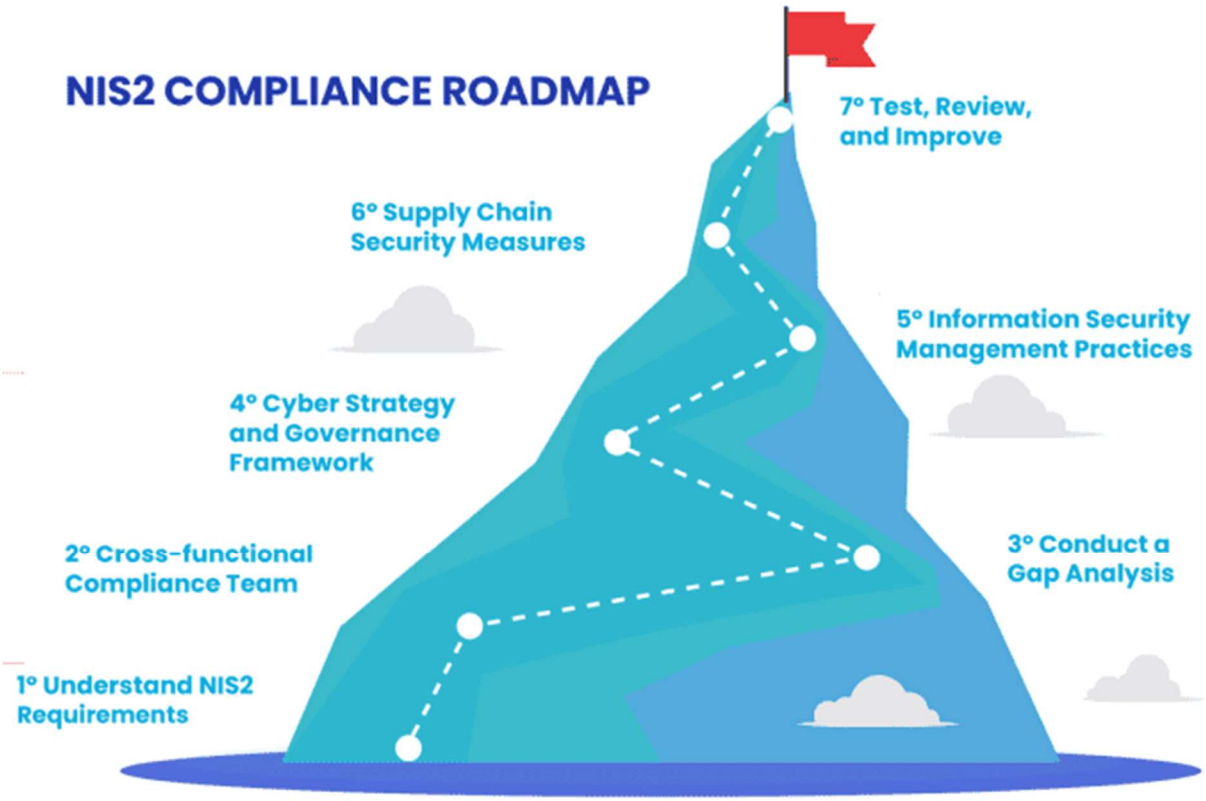
NIS 2 დირექტივა ადგენს 10 მნიშვნელოვან მოთხოვნას:

1. ინფორმაციული სისტემების **რისკების შეფასება** და უსაფრთხოების პოლიტიკა.
2. უსაფრთხოების **კონტროლების ეფექტურობის შეფასების** პოლიტიკა და პროცედურები.
3. **კრიპტოგრაფიის გამოყენების პოლიტიკა** და პროცედურები და, საჭიროების შემთხვევაში, დაშიფვრა.
4. უსაფრთხოების **ინციდენტების მართვის გეგმა.**

[15] https://eur-lex.europa.eu/eli/dir/2022/2555

5. **სისტემების შესყიდვის, სისტემების განვითარებისა და ექსპლუატაციის უსაფრთხოების უზრუნველყოფა.** აღნიშნული ასევე ნიშნავს მოწყვლადობის მართვისა და რეპორტინგის პოლიტიკას.
6. **კიბერუსაფრთხოების ტრენინგები და კომპიუტერული ჰიგიენის** პრაქტიკაში დანერგვა.
7. უსაფრთხოების პროცედურები და **მონაცემებზე წვდომის წესები** თანამშრომლებისთვის, რომლებსაც აქვთ წვდომა სენსიტიურ ან მნიშვნელოვან მონაცემებზე. რეგულაციის გავლენის სფეროში შემავალ ორგანიზაციებს ასევე უნდა ჰქონდეთ ჩატარებული აქტივის ანალიზი და უზრუნველყონ მათი სწორად გამოყენება და მოპყრობა.
8. **ბიზნეს ოპერაციების მართვის გეგმა უსაფრთხოების ინციდენტის დროს** და მის შემდეგ. ეს ნიშნავს, რომ სარეზერვო ასლები უნდა იყოს განახლებული / მიმდინარე. ასევე, უნდა არსებობდეს გეგმა IT სისტემებზე და მათ საოპერაციო ფუნქციებზე წვდომის უზრუნველსაყოფად უსაფრთხოების ინციდენტის დროს და მის შემდეგ.
9. **მრავალფაქტორიანი ავთენტიფიკაციის,** უწყვეტი ავთენტიფიკაციის გადაწყვეტილებების, ხმის, ვიდეოს და ტექსტის დაშიფვრის და დაშიფრული შიდა გადაუდებელი კომუნიკაციის გამოყენება, საჭიროების შემთხვევაში.
10. **მიწოდების ჯაჭვების და მომწოდებელ კომპანიასთან ურთიერთობის უსაფრთხოება.** კომპანიებმა უნდა აირჩიონ უსაფრთხოების ზომები, რომლებიც შეესაბამება თითოეული პირდაპირი მიმწოდებლის მოწყვლადობას. შემდეგ კომპანიებმა უნდა შეაფასონ უსაფრთხოების საერთო დონე ყველა მომწოდებლისთვის.

კვლევის მიზნებიდან გამომდინარე, წინამდებარე თავში წარმოდგენილია NIS 2 დირექტივის მოთხოვნები ICT მიწოდების ჯაჭვის უსაფრთხოების.



ფიგურა 15: NIS2 დირექტივის შესაბამისობის სამოქმედო გეგმა

დირექტივა ვრცელდება ევროკავშირის წევრი ქვეყნების იმ ორგანიზაციებზე, რომელიც ვარდება „ძირითადი“ და „მნიშვნელოვანი“ ორგანიზაციის კლასიფიკაციაში. შესაბამისად, მიწოდების ჯაჭვის კონტექსტში, ორგანიზაციას ევალდებულება:

მიიღოს ICT მიწოდების ჯაჭვის უსაფრთხოების ზომები - რაც გულისხმობს, მიმწოდებლის რისკების შეფასებას. აღნიშნულის ფარგლებში, შემსყიდველს შეუძლია შეაფასოს მომწოდებელი კომპანიის კიბერუსაფრთხოების სიმწიფე, პრაქტიკა, წარსული ინციდენტების ისტორია და სხვა. ყოველივე ზემოხსენებული ეხმარება შემსყიდველ ორგანიზაციას დროულად განსაზღვროს შესყიდულ ICT და სერვისებთან დაკავშირებული მოწყვლადობები და რისკები.

უსაფრთხოების ინციდენტების რეპორტინგი და საფრთხეების შესახებ ინფორმაციის გაზიარება - სუბიექტებს ვალდებულება აქვთ უზრუნველყონ უსაფრთხოების ინციდენტების შესახებ მარეგულირებელ ორგანოებში რეპორტინგი. ასევე, დროულად გააზიარონ ინციდენტის შესახებ არსებული ინფორმაცია, რომლებიც გავლენას ახდენენ მათ ოპერაციებზზე ან მათ მიწოდების ჯაჭვზე.

უწყვეტი მონიტორინგი და გაუმჯობესება - სუბიექტებს მოეთხოვებათ მუდმივად აკონტროლონ თავიანთი ICT მიწოდების ჯაჭვები გაჩენილი საფრთხეებისა და მოწყვლადობების

მიმართ. ეს მოიცავს უსაფრთხოების რეგულარულ აუდიტს, შეღწევადობის შეფასებას და მაღალი დონის მონიტორინგის ინსტრუმენტების დანერგვას.

სერტიფიკაცია და სტანდარტიზაცია - NIS2 ხელს უწყობს კიბერუსაფრთხოების სერტიფიცირების სქემების გამოყენებას, რათა გამოყენებული პროდუქტები, სერვისები და პროცესები უზრუნველყოფდეს უსაფრთხოების სტანდარტებს.

Digital Operational Resilience Act[16] (DORA)

2023 წლის 16 იანვარს, ძალაში შევიდა ციფრული საოპერაციო მდგრადობის აქტი (DORA), რომელიც წარმოადგენს ევროკავშირის მთავარ საკანონმდებლო რეგულაციას ფინანსური **სექტორის ციფრული ინფრასტრუქტურის კიბერუსაფრთხოებისა და საოპერაციო მდგრადობის გასაძლიერებლად.** რეგულაციის აღსრულება და ზედამხედველობა დაიწყება 2025 წლის 17 იანვარს, ხოლო მანამდე, რეგულაციის ქვეშ მოქცეულ საფინანსო დაწესებულებებს ევალდებულებათ უზრუნველყონ შემდეგი:

კვლევის მიზნებიდან გამომდინარე, წინამდებარე თავში ძირითადი აქცენტი კეთდება ICT მიწოდების ჯაჭვის უსაფრთხოების კონტროლებთან დაკავშირებულ მოთხოვნებზე.

საფინანსო უწყებებმა უნდა მართონ **ICT მიწოდების ჯაჭვის რისკები, როგორც ICT რისკის განუყოფელი კომპონენტი შემდეგი პრინციპების** შესაბამისად:

[16] https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

- საფინანსო უწყება, რომლებსაც შეიყიდის ICT სერვისებს, **სრულად პასუხისმგებელია ამ რეგულაციისა** და ფინანსური მომსახურების შესახებ მოქმედი კანონმდებლობით გათვალისწინებული ყველა ვალდებულების შესრულებაზე.
- საფინანსო უწყების **მიერ ICT მიწოდების ჯაჭვის რისკის მართვა განხორციელდება პროპორციულობის პრინციპის** გათვალისწინებით.

ICT სერვისების გამოყენების შესახებ სახელშეკრულებო შეთანხმების დადებამდე საფინანსო უწყებამ უნდა:

- შეაფასოს, მოიცავს თუ არა **სახელშეკრულებო შეთანხმება ICT სერვისების გამოყენებას,** რომლებიც ატარებს კრიტიკულ ან მნიშვნელოვან ფუნქციას;
- შეაფასოს, დაცულია თუ არა ხელშეკრულების გაფორმების **საზედამხედველო პირობები;**
- დაადგინოს და შეაფასოს ყველა **შესაბამისი რისკი სახელშეკრულებო პირობებთან დაკავშირებით**, მათ შორის შესაძლებლობა, რომ ასეთმა საკონტრაქტო პირობებმა ხელი **შეუწყოს ICT რისკების გაძლიერებას.**
- განახორციელოს ყველა **სათანადო Due Dilligence პროცედურა** ICT მიმწოდებლებთან დაკავშირებით და უზრუნველყოს შერჩევისა და შეფასების პროცესის განმავლობაში.
- **დაადგინოს და შეაფასოს ინტერესთა კონფლიქტი,** რომელიც შეიძლება გამოიწვიოს სახელშეკრულებო შეთანხმებამ.

2. თავი 2: სპეციფიკური ICT მიწოდების ჯაჭვის შეტევების ანალიზი და მათი ტექნიკური ასპექტები

ბოლო ათწლეულის განმავლობაში განსაკუთრებით მოიმატა ე.წ. „Software Supply Chain“ კიბერშეტევებმა. ორგანიზაცია „Identify Theft Resource Center-ის 2023 წლის კვლევის[17] მიხედვით, მიწოდების ჯაჭვზე განხორციელებული შეტევების შედეგად დაზარალდა 1,743 ორგანიზაცია და 10 მილიონამდე ადამიანი.

იმისათვის რომ დავინახოთ საფრთხეების სრული ლანდშაფტი, საჭიროა განვიხილოთ რა ეტაპებისგან შედგება ICT მიწოდების ჯაჭვი როგორც მწარმოებლისა და ორგანიზაციული პერსპექტივიდან.

ფიგურა 16: მიწოდების ჯაჭვის სასიცოცხლო ციკლი

ICT მიწოდების ჯაჭვის თითოეულ ეტაპს გააჩნია სისუსტეები და არსებობს მათი შესაბამისი საფრთხეები.

წინამდებარე კვლევაში, წარმოდგენილია ზემოთ ჩამოთვლილი ეტაპებისთვის განხილული 3-3 მიმართულება:

- **საფრთხეები** - რისკები და საფრთხეები;
- **რეალური კიბერინციდენტის მაგალითი** - რეალურად მომხდარი ქეისები, ერთის მხრივ გლობალური პერსპექტივიდან (US, UK, EU), ხოლო მეორეს მხრივ, საქართველოს რეალობის გათვალისწინებით.
- **საუკეთესო პრაქტიკა და რეკომენდაცია** - რა მიდგომამ იმუშავა აღნიშული ინციდენტების შემთხვევაში და რა პრაქტიკა შეიძლება გაითვალისწინოს საქართველომ, პოტენციური **კიბერრისკების უკეთ სამართავად** და **საფრთხეების მინიმიზაციისათვის.**

[17] https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf

2.1. დიზაინი და შემუშავება

აღნიშნულ ეტაპზე ხდება პროდუქტის (აპარატურა, პროგრამული უზრუნველყოფა, სერვისი) დიზაინის შექმნა და მისი შემუშავება. პროცესი როგორც წესი მოიცავს ერთი ან რამდენიმე მხარის / ორგანიზაციის ჩართულობას. მნიშვნელოვანია, აღნიშნული გარემოება, რადგან რაც უფრო მეტია პროცესში ჩართული გარე მხარეებისა და ორგანიზაციების რაოდენობა, მით უფრო იზრდება საფრთხეების ლანდშაფტი და რთულდება კიბერუსაფრთხოების რისკების მართვა.

მაგალითისათვის, ქსელური აპარატურის მწარმოებელმა კომპანიამ, ***შესაძლებელია პროდუქტის დიზაინი შეიმუშავოს საკუთარი გუნდის მეშვეობით, ხოლო მისი პრაქტიკაში განხორციელება დაუკვეთოს მესამე მხარეს, სხვა ორგანიზაციას, რომელიც სხვა ქვეყნის, იურისდიქციისა და მარეგულირებელი გარემოს შემადგენლობაშია.***

2.1.1. საფრთხეები

ამ ეტაპზე შესაძლებელია დიზაინისა და შემუშავების პროცესში ე.წ. მავნე კოდის (malicious code) განზრახ ჩასმა, ასევე, **კოდის შემუშავების დროს დაშვებული შეცდომების გამო პროგრამულ-აპარატურული სისუსტეების (vulnerabilities) წარმოშობა, არა-შესაბამისი და არასაკმარისი უსაფრთხოების მოთხოვნების გათვალისწინება, უსაფრთხოების ტესტირების არ ჩატარება ან არასათანადოდ განხორციელება.**

მავნე კოდის ჩასმა და სისუსტეების წარმოშობა შეუძლია როგორც თავად **ორგანიზაციას,** ასევე **ინსაიდერებს** (insider), **მესამე მხარეების** (third-party) **დეველოპერებსა** და **კიბერშემტევებს.**

შედეგად მივიღებთ პროდუქტს, რომელიც საწყის ფაზაზევე შეიცავს განზრახ ჩაშენებულ ან ბუნებრივად გაჩენილ სისუსტეებს.

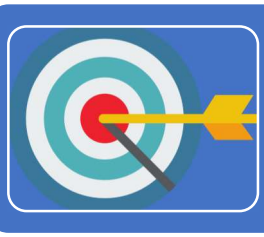
2.1.2. რეალური კიბერინციდენტები

ბოლო ათწლეულის ერთ-ერთი ყველაზე მეტად გახმაურებული შემთხვევა მოხდა 2020 წლის დეკემბერში. კომპანია SolarWinds პროდუქტზე, კერძოდ Orion platform-ის network management system-ზე, განხორციელდა კიბერშეტევა. მიკუთვნების მაღალი სანდოობით (attribution confidence - high) რუსულ სპეცსამსახურთან (SVR) აფილირებულმა APT29[18] (Advanced Persistent Group) ჯგუფმა არასანქცირებული წვდომა მოიპოვა კომპანიის დეველოპმენტის გარემოზე და ზემოხსენებული პროდუქტის ერთ-ერთ განახლებაში (Update) ჩააშენა მავნე კოდი (malicious code). შეტევის შესახებ დეტალური ინფორმაცია:

[18] https://attack.mitre.org/groups/G0016/

შემტევი მხარე (Threat Actor)

- რუსულ სპეცსამსახურ SVR-თან აფილირებული APT29 (Advanced Persistent Group) ჯგუფი - **მაღალი ალბათობით.**



სამიზნე ორგანიზაცია

- Solarwinds Corporation

სამიზნე პროდუქტი

- Orion platform-ის network management system

გამოყენებული მეთოდი

- შემტევმა მოიპოვა არასანქცირებული წვდომა კომპანიის Development გარემოზე და პროდუქტის განახლებაში (Update) მავნე კოდი ჩააშენა.

გამოწვეული ზიანი

- **გავრცელდა** - მრავალი ქვეყნის სხვადასხვა ინდუსტრიისა და სექტორის წარმომადგენელ ორგანიზაციაში, მათ შორის ეროვნული კრიტიკული ინფრასტრუქტურის სუბიექტებში.
- **ზიანი** - სენსიტიური ინფორმაციის გაჟონვა, კრიტიკულ ქსელში შეღწევა და დამატებითი მავნე აქტივობები (რეპუტაციულ, ფინანსური ზიანი).

2.1.3. საუკეთესო პრაქტიკა და რეკომენდაციები

მსგავსი ტიპის კიბერრისკების სამართავად საჭიროა კომპლექსური მიდგომა. კერძოდ, მნიშვნელოვანია, რომ ორგანიზაციას წინასწარ ჰქონდეს შემუშავებული აღნიშნული სახის კიბერინციდენტების მართვის მიდგომები: **პრევენციის, დეტექციისა და რეაგირების** გზები.

ასევე, ინციდენტის დადგომამდე, საჭიროა ორგანიზაციის მიერ გამოყენებული კრიტიკული **ბიზნეს-აპლიკაციების გარემოს მონიტორინგი** - შესაბამისად, მათი მეშვეობით (კომპრომეტირებით) განხორციელებული **არასანქცირებული წვდომის იდენტიფიცირება**

უფრო ეფექტური ხდება. **განახლებების** და **ახალი ფუნქციონალის** ტესტირება, მის **ძირითად სამუშაო გარემოში გაშვებამდე.**

ორგანიზაციული პერსპექტივიდან მნიშვნელოვანია, ასევე, **მომწოდებელი კომპანიის უსაფრთხოების გუნდთან** მუდმივი კონტაქტი და **ორმხრივი აქტიური თანამშრომლობა.** ამ შემთხვევაში გაცილებით სწრაფად და ეფექტურად იქნება შესაძლებელი მსგავსი ინციდენტების სრული სასიცოცხლო ციკლის მართვა.

ყველაზე მნიშვნელოვანი ასპექტია, მწარმოებელი კომპანიის მიერ საბოლოო მომხმარებლისთვის **მარწმუნებელი (assurance), ობიექტური შეფასების შედეგების (მაგალითად, აუდიტი) ჩვენება,** თუ როგორ უზრუნველყოფს კიბერუსაფრთხოებას მისი პროდუქტი დიზაინისა და შემუშავების ფაზებში. აღნიშნული მეტი დეტალიზაციით დაფარულია წინამდებარე კვლევის - „შესყიდვის ფაზის“ ანალიზში.

2.2. წარმოება

ფიგურა 17: მიწოდების ჯაჭვის სასიცოცხლო ციკლი

პროდუქტის წარმოების პროცესი შედგება მრავალი კომპონენტისაგან და ხშირ შემთხვევაში გადანაწილებულია რამდენიმე ორგანიზაციაზე. მაგალითისთვის, ცნობილი ქსელური მოწყობილობები, აპარატული მხარდაჭერის საშუალებები, მობილური მოწყობილობები, ინდუსტრიული კონტროლის SCADA სისტემები და ა.შ. შედგება მრავალი ურთიერთდაკავშირებული კომპონენტისაგან, რომლებიც იწარმოება სხვადასხვა ორგანიზაციისა და ჯგუფის მიერ. კერძოდ, რადიო კომპონენტები, მეხსიერების მოდულები, მიკროსქემები, დამაკავშირებელი მიკროჩიპები, ა.შ.

2.2.1. საფრთხეები

ICT მიწოდების ჯაჭვის ამ ეტაპის შესაბამისი საფრთხეებია: **აპარატული (Hardware) კომპონენტების ცვლილება/დაზიანება, აპარატურული მართვის პროგრამის (Firmware) ცვლილება სისუსტის ან ე.წ. backdoor-ის ჩაშენებით,** წარმოების **პროცესში ჩარევა**, **ყალბი და მავნე კომპონენტების გამოყენება (ჩანაცვლება)**. შესაბამისად, ირღვევა საბოლოო პროდუქტის მთლიანობა და მისი უსაფრთხოება.

2.2.2. რეალური კიბერინციდენტები

განვიხილოთ 2 მაგალითი:

- *Android სმარტფონების firmware-ში ჩინური კომპანიის მიერ ჩაშენებული ჯაშუშური პროგრამა და*
- *მაღალი ალბათობით ჩინური სპეცსამსახურების მიერ ამერიკული კომპანია Microsemi Corp-ის მოწყობილობებში ჩამატებული ფიზიკური ჩიპი მავნე მაკომპრომეტირებელი ფუნქციით.*

კიბერინციდენტი #1

2016 წლის ნოემბერში, ამერიკული კიბერუსაფრთხოების კომპანია Kryptowir[19]e-ის მკვლევარებმა აღმოაჩინეს, დაბალბიუჯეტურ ანდროიდის სმარტფონებში ჩაშენებული მწარმოებლის აპლიკაცია „Adups.FOTA“. აპლიკაცია აგროვებდა SMS მესიჯებს, ზარების ისტორიას, ტელეფონის მნიშვნელოვან პარამეტრებს და გზავნიდა ჩინეთში არსებულ სერვერებზე.

აღმოჩნდა რომ აღნიშული ანდროიდის სმარტფონების წარმოების პროცესში ჩართული იყო ჩინური კომპანია „Shanghai Adups Technology Co. Ltd.“, რომელმაც განზრახ ჩააშენა მავნე აპლიკაცია მილიონობით სმარტფონში. 2016 წლის მონაცემებით, კომპანიას ყავდა 700 მილიონი აქტიური მომხმარებელი და წარმოდგენილი იყო 150 ქვეყანაში. ოფიციალური ინფორმაციით Adups აწარმოებდა ე.წ. აპარატურული მართვის პროგრამულ კოდს (Firmware) 400-მდე წამყვანი მობილური ოპერატორისთვის, ნახევარგამტარების ვენდორებისთვისა და ისეთი მოწყობილობების მწარმოებლებისთვის როგორებიცაა მანქანები, ტელევიზორები, ჭკვიანი მოწყობილობები, ე.წ. „wearable“-ს და ა.შ.

კიბერინციდენტი #2

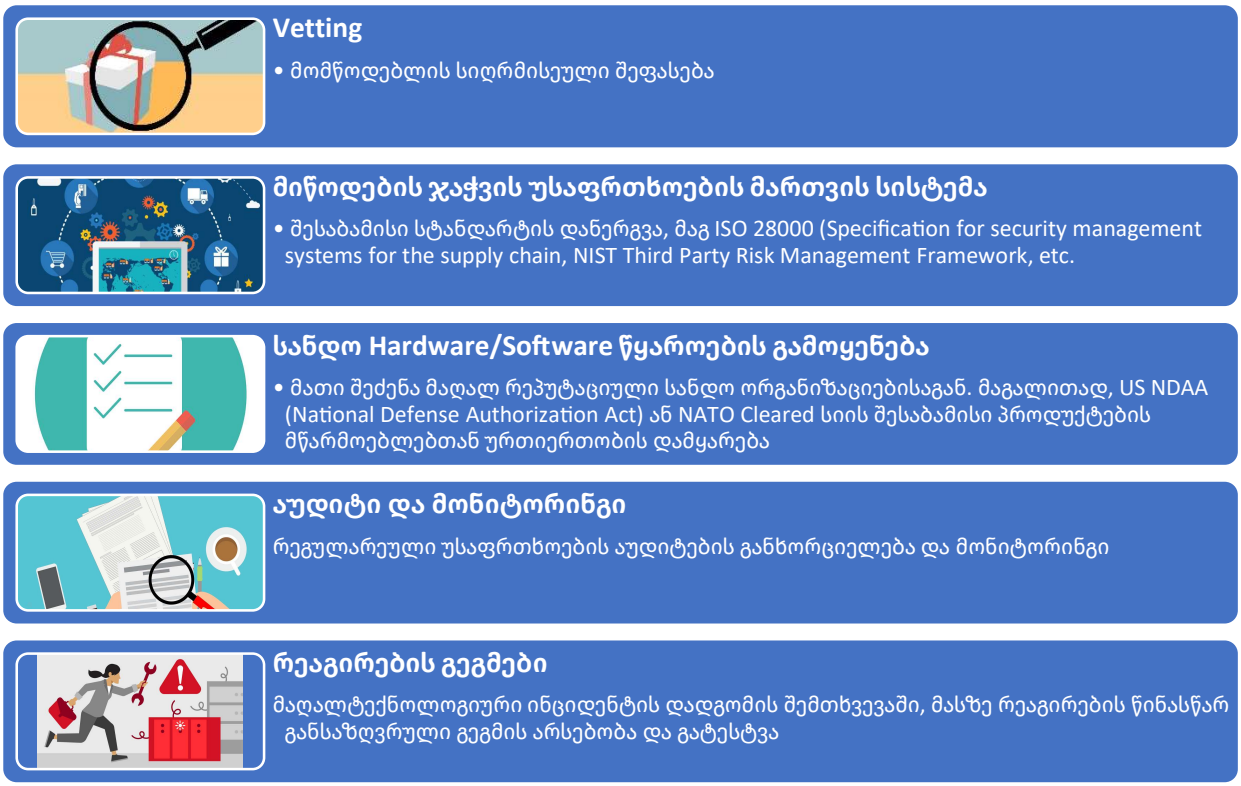
2012 წელს კემბრიჯის უნივერსიტეტის ორმა მკვლევარმა, ამერიკული კომპანია Microsemi Copr-ის მიერ წარმოებულ ე.წ. „Miltary-Grade silicon device“-ში, აღმოაჩინა მიკროჩიპი, რომელშიც განზრახ იყო ჩაშენებული არასანქცირებული წვდომის შესაძლებლობა. აღმოჩნდა, რომ ჩიპი დამზადდა ტაივანში TSMC-ის მიერ და მისი შემდგომი წარმოება-შეფუთვა მოხდა ჩინეთში. შესაბამისად, მკვლევარებს გაუჩნდათ ეჭვი, რომ აღნიშული ჩიპის მოდიფიცირება მოხდა ჩინეთის შესაბამისი სპეცსამსახურების მიერ.

ორივე ინციდენტის შემთხვევაში საკითხზე ოფიციალური მოკვლევა დაიწყო ამერიკულმა სპეციალურმა სამსახურებმა. ანდროიდის სმარტფონების შემთხვევაში **აშშ სამშობლოს უსაფრთხოების დეპარტამენტის (Department of Homeland Security - DHS) მითითებით,** მწარმოებელმა **გაიწვია და გაყიდვიდან ამოიღო საეჭვო** და სახიფათო მოწყობილობები. რაც შეეხება Micorsemi-ს ინციდენტს, მის შესახებ გამოძიება ჩაატარა **აშშ ფედერალური გამოძიების ბიურომ (Federal Bureau of Investigation - FBI)**, თუმცა საკითხის სენსიტიურობიდან გამომდინარე, მისი შედეგები არ გასაჯაროებულა.

2.2.3. საუკეთესო პრაქტიკა და რეკომენდაციები

აღნიშნული ტიპის საფრთხეებისგან თავდასაცავად საჭიროა კომპლექსური მიდგომა, რომელიც შედგება დამოუკიდებელი და ურთიერთდაკავშირებული აქტივობებისაგან, კერძოდ:

[19] https://www.blackhat.com/us-17/briefings.html#all-your-sms-and-contacts-belong-to-adups-and-others



2.3. შესყიდვა და მიწოდება

ფიგურა 18: მიწოდების ჯაჭვის სასიცოცხლო ციკლი

როგორც საყოველთაოდ მიღებულია, დაინტერესებული მხარის მიერ აპარატურის შესყიდვა **ხდება ავტორიზებული გადამყიდველი (authorized reseller) ორგანიზაციის** გავლით. მაგალითისთვის, **ამერიკული კომპანია CISCO-ს** ქსელის მართვისა და უსაფრთხოების აპარატურის შეძენისას ბაზარზე არსებობს მრავალი მიმწოდებელი, რომელსაც აქვს **უფლებამოსილება გაყიდოს ზემოხსენებული აპარატურა.** აღსანიშნავია, რომ რეგიონისა და ქვეყნების მიხედვით განსხვავდება მომსახურების პირობები და შესაბამისი ფასები.

2.3.1. საფრთხეები

პირველ რიგში გასათვალისწინებელია ის გარემოება, რომ შესყიდვის პროცესი იყოს **მრავალ-კრიტერიუმიანი და არ გაიმარჯვოს იმ ვენდორმა, რომელსაც მხოლოდ უკეთესი ფასი აქვს.** შესაძლებელია დაბალი საბაზრო ფასი მიღებული იყოს, მათ შორის, უსაფრთხოების მოთხოვნებზე რესურსების დაზოგვის ხარჯზე.

აღსანიშნავია, **ლოგისტიკური და ტრანსპორტირების უსაფრთხოების კომპონენტი**. ამ შემთხვევაში შესაძლებელია შუალედურმა რგოლმა მოახდინოს საბოლოო მისაწოდებელ პროდუქტში **ცვლილებების შეტანა, დაზიანება, გაზრახ აპარატულ-პროგრამული ე.წ. Backdoor-ებისა და ჩიპების ჩაშენება.**

2.3.2. რეალური კიბერინციდენტები

2024 წლის 2 მაისს აშშ იუსტიციის დეპარტამენტმა (US Department of Justice[20]) დააკავა აშშ და თურქეთის ორმაგი მოქალაქე Onur Aksoy. მან აღიარა ბრალი, რაც გულისხმობს შემდეგ აქტივობებს: მრავალი წლის განმავლობაში, ის ყიდდა **ჩინეთიდან და ჰონკონგიდან, დაბალი ხარისხის, მოდიფიცირებული და გაყალბებული CISCO-ს ქსელური მოწყობილობებს აშშ ბაზარზე,** რომლის მოცულობაც შეადგენდა ასეულ მილიონ აშშ დოლარს. გამოძიების დეტალების მიხედვით მის მიერ **გაყიდული ქსელური მართვისა და უსაფრთხოების მოწყობილობები შეძენილია ამერიკული ჰოსპიტალების, სკოლების, მაღალი სენსიტიურობის სამხედრო ობიექტების, სახელმწიფო სტრუქტურებისა და სხვა კრიტიკული ინფრასტრუქტურის მიერ.**

აღნიშნულმა ქმედებამ განსაკუთრებული რისკის წინაშე დააყენა აშშ კრიტიკული ინფრასტრუქტურის უსაფრთხოება, მედეგობა და ოპერაციული საიმედოობა.

ზემოხსენებული მოდიფიცირებული და ყალბი მოწყობილობები დადასტურებულად აღმოჩნდა საბრძოლო და არასაბრძოლო სამხედრო ოპერაციებისას გამოყენებულ პლატფორმებში, რომლებიც მხარს უჭერს და ისეთ საფრენ აპარატებს, როგორებიცაა „F-15, F-18, and F-22 fighter jets, AH-64 Apache attack helicopter, P-8 maritime patrol aircraft, and B-52 Stratofortress bomber aircraft."

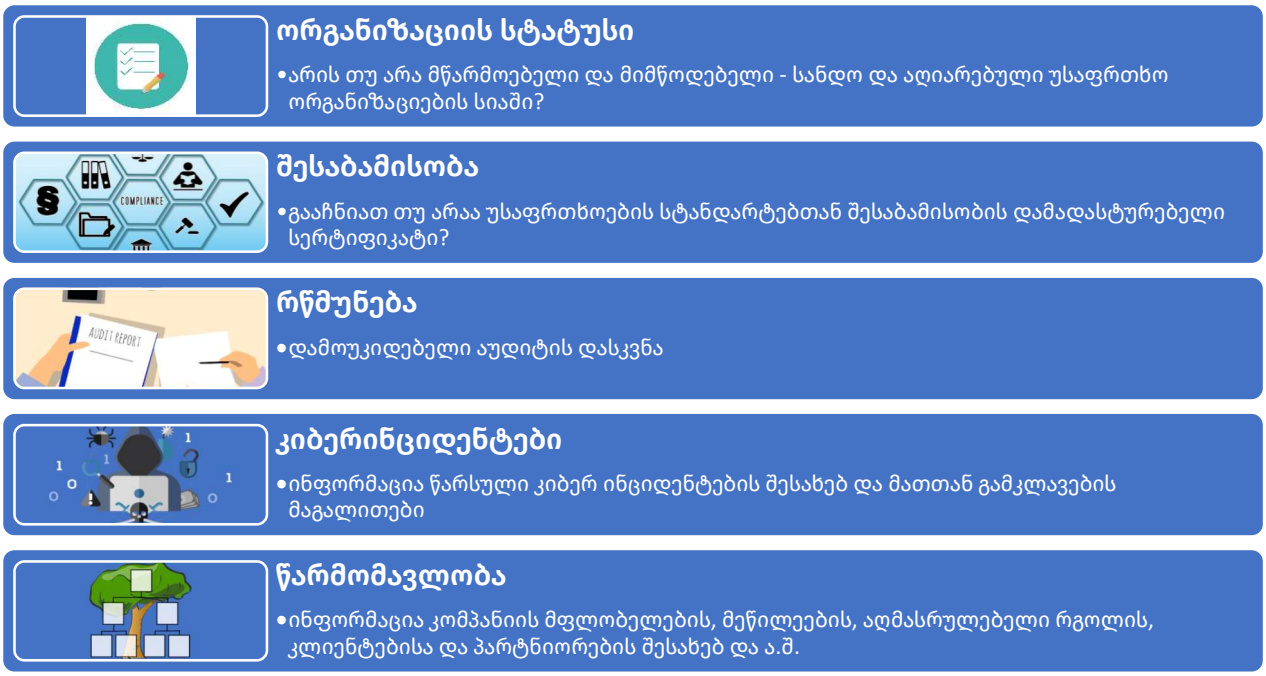
როგორც გამოძიებით დგინდება, აღნიშნული პიროვნება ფლობდა აშშ რეგისტრირებულ 19 კომპანიას, 15 Amazon და 10 eBay storefront-ს.

შესყიდვისა და მიწოდების ჯაჭვის კომპრომიტირებას ხშირად იყენებენ სხვადასხვა ქვეყნის სპეცსამსახურები, რის თაობაზეც არსებობს სხვადასხვა სახელმწიფო, ჟურნალისტური და არასამთავრობო ორგანიზაციების (Think Tank) მიერ შემუშავებული კვლევა. კერძოდ, საბოლოო მომხმარებლამდე მიწოდების პროცესში, **კრიტიკული ქსელური და აპარატული მოწყობილობები** ხვდება **„შუალედურ რგოლში**", სადაც ხორციელდება მათი მოდიფიცირება და **ე.წ. Hardware/Software Backdoor-ების ჩაშენება.** ამის შემდეგ **პროდუქტი უბრუნდება პირვანდელ სახეს, იფუთება და მიეწოდება შესაბამის საბოლოო მომხმარებელს, დათქმულ ვადებში და პირვანდელი იერსახით.**

2.3.3. საუკეთესო პრაქტიკა და რეკომენდაციები

მნიშვნელოვანია არა მხოლოდ მწარმოებელი არამედ მიმწოდებელი კომპანიის უსაფრთხოების სტატუსის შესახებ აქტუალური ინფორმაციის ფლობა:

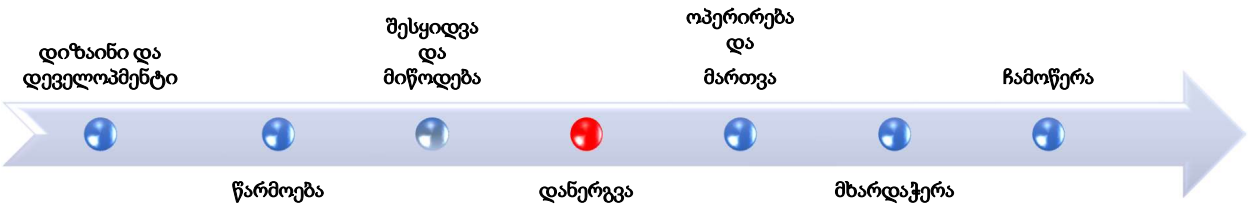
[20] https://www.justice.gov/opa/pr/leader-massive-scheme-traffic-fraudulent-and-counterfeit-cisco-networking-equipment



თუ მიუხედავად ზემოთჩამოთვლილი კონტროლებისა, მსგავსი ტიპის მოწყობილობა მაინც მოხვდება ორგანიზაციაში, საჭიროა არსებობდეს **მუდმივი მონიტორინგისა და აპარატურულ-პროგრამული უსაფრთხოების ანალიზის შესაძლებლობა.**

ეროვნული კრიტიკული ინფრასტრუქტურის განსაკუთრებით სენსიტიურ მიმართულებებში ამა თუ იმ მოწყობილობის ჩართვამდე, აუცილებელია, **მისი Hardware/Software კომპონენტების უსაფრთხოების სტატუსის შემოწმება.** ტესტირების პროცესში დაკვირვება ქმედებებზე. ასევე, **საოპერაციო მდგომარეობაში გადასვლისთანავე მისი ქცევის მონიტორინგი და საეჭვო ქსელური-აპარატურული აქტივობების იდენტიფიცირება.**

2.4. დანერგვა



ფიგურა 19: მიწოდების ჯაჭვის სასიცოცხლო ციკლი

დანერგვის ეტაპზე ორგანიზაციაში ხდება შესყიდული **ICT პროდუქტის იმპლემენტაცია და ინტეგრაცია არსებულ ტექნოლოგიურ გარემოში**. ამ შემთხვევაშიც, არსებობს სხვადასხვა მიდგომა: შესაძლებელია **პროდუქტი დანერგოს მწარმოებელმა, მიმწოდებელმა, ტექნოლოგიურმა კომპანიამ, დროებით დაქირავებულმა გარე ანდ შიდა თანამშრომლების**

გუნდმა. პროდუქტს დამოუკიდებლად ნერგავს ისეთი ორგანიზაცია ან ერთეული, ვისაც აქვს შესაბამისი ცოდნა და გამოცდილება აღნიშნულ პროდუქტთან დაკავშირებით.

როგორც წესი, მწარმოებელი კომპანიები გასცემენ პარტნიორობისა და ცოდნის დამადასტურებელ დოკუმენტაციას იმ მესამე მხარეებისთვის, ვისაც შეუძლია მათი პროდუქტის დანერგვა სხვადასხვა ორგანიზაციაში.

დანერგვის პროცესი მოიცავს, შესყიდული პროდუქტის შესახებ **სრული და ამომწურავი ინფორმაციის მიღებას, შემსყიდველი ორგანიზაციის ტექნოლოგიური გარემოს შესწავლას და ინფორმაციის შეგროვებას, აქტიურ კომუნიკაციას მის თანამშრომლებთან, სხვადასხვა სტრუქტურულ ერთეულებთან, არსებული აპარატურულ-პროგრამული ტექნოლოგიების შესახებ ინფორმაციის მიღებას და ანალიზს.**

როგორც აღწერიდან ჩანს, ამ ეტაპზე პროცესში ჩართულ მხარეებს მიეწოდებათ მნიშვნელოვანი ინფორმაცია როგორც შესყიდული პროდუქტის, ასევე, მომხმარებელი ორგანიზაციის საჭიროებების, ტექნოლოგიური მოწყობისა და ბიზნეს პროცესების შესახებ. შესაბამისად, განსაკუთრებით საყურადღებოა დანერგვის პროცესის უსაფრთხოების სწორად დაგეგმვა და მართვა.

2.4.1. საფრთხეები

დანერგვის პროცესის საფრთხეები გამომდინარეობს მასში ჩართული და მონაწილე ორგანიზაციებისგან, პირებისგან. პირველ რიგში, საყურადღებოა, თუ **ვინ ახორციელებს პროდუქტის იმპლემენტაციას**, აქვს თუ არა გავლილი შესაბამისი უსაფრთხოების შემოწმება, **ხომ არ არის კავშირში ორგანიზაცია ან კონკრეტული თანამშრომლები წარსულ კიბერინციდენტებთან ან კიბერკრიმინალურ დაჯგუფებებთან.**

ამ პროცესში, **<u>დამნერგავი ორგანიზაცია იღებს მნიშვნელოვან, კრიტიკულ ინფორმაციას, როგორც დასანერგი პროდუქტის რაობის, მისი კონფიგურაციისა და უსაფრთხოების სტატუსის, ასევე, ზოგადად მთლიანი ორგანიზაციის ტექნოლოგიური გარემოს შესახებ.</u>** შედეგად, დამნერგავი ორგანიზაცია კარგი სამიზნე ხდება კიბერშემტევებისათვის, საბოლოო მომხმარებლის შესახებ დამატებითი სენსიტიური ინფორმაციის მოსაპოვებლად.

მეორეს მხრივ, ორგანიზაციული პერსპექტივიდან, შესაძლებელია კონკრეტული პროდუქტის **ინსტალაციის პროცესში განზრახ ან უნებლიედ არ გაითვალისწინონ საუკეთესო პრაქტიკა და უსაფრთხოების მოთხოვნები, რითაც პოტენციურად სამომავლოდ მოწყვლადი ხდება აღნიშნული ახალ დანერგილი რესურსი და შედეგად მთელი ორგანიზაცია.**

დანერგვის პროცესი მოიცავს, ასევე, დ**ისტანციურ წვდომას გარე დამნერგავი ორგანიზაციის მიერ, საბოლოო მომხმარებლის ICT ინფრასტრუქტურაზე**, რაც შეიძლება გამოყენებული იქნას განზრახ ან უნებლიედ, კიბერშეტევისათვის.

2.4.2. რეალური კიბერინციდენტები

2017 წლის ინციდენტი ტექსასის შტატის ქალაქ დალასში. კერძოდ, უსაფრთხოების ინციდენტის გამო, ქალაქში **შუაღამით ერთდროულად ჩაირთო 156 საგანგებო გაფრთხილების სირენა**, დაახლოებთ 90 წამის განმავლობაში. ამან გამოიწვია, ერთის მხრივ, პანიკა მოსახლეობაში, მეორეს მხრივ, კი **<u>რამდენიმე საათით გადაუდებელი დახმარების</u>**

<u>სატელეფონო ქსელის გადატვირთვა.</u> აღნიშნული სირენა ირთვება ბუნებრივი კატასტროფების და შესაბამისი კრიტიკული სიტუაციების დროს.

როგორც აღმოჩნდა, აღნიშნული **სირენების დანერგვის პროცესში დაშვებული იყო შეცდომები** და შესაბამისად საერთო რეაგირების ქსელი შეიცავდა სისუტეებს, რისი გამოყენებაც შეძლეს კიბერშემტევებმა. **კონკრეტულ რადიო სიხშირეებზე დაკავშირება შესაძლებელი იყო დაშიფრული კავშირის გარეშეც**, ასევე, არ იყო გამართული და კონფიგურირებული სათანადო ავთენტიფიკაციის მექანიზმები. დამატებით, **არ მოხდა უსაფრთხოების იმ განახლებების დროული და ადექვატური იმპლემენტაცია, რაც უზრუნველყოფდა მსგავსი ინციდენტის პრევენციას.**

შედეგად, **<u>საჭირო გახდა დროებით აღნიშული ქსელის სრულად გათიშვა,</u>** ინციდენტის მოკვლევა მიზეზის დასადგენად, საჭირო უსაფრთხოების განახლებების ინიცირება და შემდეგ საოპერაციო რეჟიმში დაბრუნება.

2.4.3. საუკეთესო პრაქტიკა და რეკომენდაციები

როგორც ზემოთ აღვნიშნეთ, განსაკუთრებით მნიშვნელოვანია დამნერგავი კომპანიის შემოწმება უსაფრთხოების თვალსაზრისით, რათა დავაზღვიოთ მათ მიერ განზრახ დაშვებული უსაფრთხოების ნაკლოვანებები.

მეორეს მხრივ, **<u>საჭიროა მიმწოდებლებმა წარმოადგინონ საკუთარი ორგანიზაციის შიგნით გამოყენებული უსაფრთხოების პრაქტიკებისა და სერტიფიცირების ამსახველი დამოუკიდებელი აუდიტის ან სერტიფიცირების დამადასტურებელი დოკუმენტები.</u>**

მიუხედავად ზემოთ ჩამოთვლილ კომპონენტებთან შესაბამისობისა, საჭიროა დანერგვის სრული პროცესის განმავლობაში უსაფრთხოების მართვა და მონიტორინგი. ორგანიზაციის **თანამშრომლებზე გადაცემული პრივილეგიებისა და წვდომების ადექვატური მართვა,** საეჭვო ქმედებების აღრიცხვა და პოტენციურ ინციდენტებზე რეაგირებისთვის მზადყოფნა.

ასევე, ორგანიზაციის პოლიტიკის გაცნობა, თუ როგორ რეაგირებენ კიბერუსაფრთხოების ინციდენტებზე და რა კონტროლის მექანიზმებს გვთავაზობენ დანერგვის პროცესის უსაფრთხოების უზრუნველსაყოფად.

2.5. ოპერირება და მართვა

ფიგურა 20: მიწოდების ჯაჭვის სასიცოცხლო ციკლი

ამ ეტაპზე ხდება პროდუქტის გამართულად და უსაფრთხოდ მუშაობის უზრუნველყოფა. პროცესი განგრძობით ხასიათს ატარებს და მოიცავს მუდმივ მონიტორინგს, ცვლილებებსა და

მართვას. როგორც წესი, **წინა ეტაპებზე დაშვებული შეცდომები და გაუთვალისწინებელი აქტივობები, თავს იჩენს ოპერირებისა და მართვის დროს როგორც ტექნიკური გაუმართაობა ან უარეს შემთხვევაში - კიბერინციდენტი.** განვიხილოთ ამ ეტაპის შესაბამისი საფრთხეები.

2.5.1. საფრთხეები

ოპერირებისა და მართვის პროცესთან მიმართებაში არსებობს შემდეგი ტიპის საფრთხეები:

- **Zero Days** - არსებული ან ახლად აღმოჩენილი (უცნობი - Zero Day) სისუსტეების გამოყენება.
- **ინსაიდერული საფრთხე** - ლეგალური პრივილეგიის მქონე თანამშრომლის ან კონტრაქტორის მხრიდან.
- **არაადექვატური მონიტორინგისა და აღმოჩენის** შესაძლებლობების შედეგად განხორციელებული შეტევები და ინციდენტები.
- **მხარდაჭერა-დაკარგული** და **მოძველებული** სისტემები, პროდუქტები.
- **საფრთხის შემცველი და სუსტი კონფიგურაციის** გამოყენება.
- **ფიზიკური შეღწევის** საშუალებით პროდუქტზე წვდომის მოპოვება და დაზიანება.
- **ადამიანური შეცდომები** და სხვ.

2.5.2. რეალური კიბერინციდენტები

2015 წელს მომხდარი კიბერინციდენტი, რომელიც შეეხო აშშ პერსონალის მართვის (United States Office of Personnel Management) სამსახურს. აღნიშნული წარმოადგენს ერთ-ერთ ყველაზე მასშტაბურ მონაცემების გაჟონვის ინციდენტს აშშ ისტორიაში. შემტევ მხარედ, **მიკუთვნების მაღალი სანდოობით,** დადგენილია **ჩინეთის პროვინციის სახელმწიფო უსაფრთხოების სამსახური** - Jiangsu State Security Department.

შეტევის შედეგად, დაახლოებით **22.1 მილიონი ჩანაწერის კომპრომეტირება მოხდა,** რომელიც მოიცავდა **პერსონალურ და სენსიტიურ მონაცემებს, ამერიკულ სახელმწიფო სტრუქტურებში მომუშავე თანამშრომლების შესახებ.** ასევე ინფორმაცია მოიცავდა მათ ე.წ. Background Check-ებს, **პერსონალურ მონაცემებს მათი ოჯახის წევრების შესახებ.**

როგორც მოგვიანებით ჩატარებული კვლევისა და ანალიზის შედეგად დადგინდა, განსაკუთრებით მაღალი პრივილეგიების მქონე (“with root access to every row in every database”) ერთ-ერთი **თანამშრომელი ფიზიკურად იმყოფებოდა ჩინეთის ტერიტორიაზე და იქიდან მუშაობდა**, ასევე, ერთ-ერთი კონტრაქტორი კომპანიის ორ თანამშრომელს ჰქონდათ ჩინური პასპორტები.

დამატებით, მნიშვნელოვანი და კრიტიკული 4**7 სისტემიდან 11 სისტემა ვერ პასუხობდა შესაბამის უსაფრთხოების სერტიფიცირების მოთხოვნებს**. გარკვეული სისტემების ნაწილი განთავსებული იყო **საჯარო ე.წ. Cloud-ზე,** უსაფრთხოების ნაკლოვანებებით.

2.5.3. საუკეთესო პრაქტიკა და რეკომენდაციები

პირველ რიგში, გასათვალისწინებელია, რომ კრიტიკული სისტემებისა და პროდუქტებისათვის შემუშავებულია საერთაშორისო სტანდარტები, სახელმძღვანელოები და რეკომენდაციები,

რომლებშიც ზედმიწევნით ჩაშლილია ის უსაფრთხოების მოთხოვნები რაც გასათვალისწინებელია ოპერირებისა და მართვის დროს.

ორგანიზაციისთვის პრიორიტეტული უნდა იყოს მსგავსი მოწყობილობების მართვის პროცესში მაღალ **პროფესიული ადამიანური რესურსის, პროფესიონალი კადრების არსებობა,** რომელთაც აქვთ შესაბამისი ცოდნა და კომპეტენცია არა მხოლოდ ICT ტექნოლოგიის, არამედ მათი უსაფრთხოების მხარდაჭერის კუთხით.

გამართული უნდა იყოს **შეღწევადობის ტესტირების, უსაფრთხოების აუდიტისა და სისუსტეების მართვის პროცესი**, რასაც შეუძლია აღმოაჩინოს უსაფრთხოების ნაკლოვანებები შესაბამის ეტაპებზე და მოახდინოს პოტენციური ინციდენტების პრევენცია.

კონკრეტული ტიპის ინციდენტებზე რეაგირების გეგმების არსებობა და მათი ტესტირება. ბიზნეს უწყვეტობისა და კატასტროფიდან აღდგენის გეგმები, რომლებიც მოიცავს აღნიშნულ კრიტიკულ პროდუქტებს.

2.6. მხარდაჭერა

ფიგურა 21: მიწოდების ჯაჭვის სასიცოცხლო ციკლი

ICT პროდუქტების სრული სასიცოცხლო ციკლის შემადგენელი და განუყოფელი ნაწილია მხარდაჭერის პროცესი. პროდუქტების უმრავლესობა მუდმივად საჭიროებს განახლებებს, ახალი ფუნქციების დამატებას, ცვლილებების შეტანას, პრობლემების მოგვარებასა და სხვა საჭირო აქტივობებს. შესაბამისად, ორგანიზაციებმა **პროდუქტის მხარდაჭერის მომსახურება შეიძლება შეიძინონ როგორც მწარმოებლისგან, ასევე მიმწოდებელი ან დამნერგავი კომპანიებისგან.**

ხშირ შემთხვევაში, კონკრეტულ რეგიონებსა და ქვეყნებს მხარდაჭერას უწევენ ამ არეალზე მიმაგრებული შესაბამისი სპეციალისტები. ბუნებრივია, განსხვავებულია ამ სპეციალისტების **კვალიფიკაცია, გამოცდილება და უსაფრთხოების მოთხოვნებში გათვიცნობიერებულობის** დონე. შესაბამისად, დიდი **მნიშვნელობა უნდა მიენიჭოს ორგანიზაციული გადმოსახედიდან არა მხოლოდ კონკრეტულ პროდუქტზე სწრაფ და ლოკალურ რეაგირებას, არამედ ამ რეაგირება მხარდაჭერის ფარგლებში უსაფრთხოების კომპონენტს.**

მნიშვნელოვანი წინასწარ ზედმიწევნით მოხდეს შეფასება, მხარდაჭერის პროცესში ჩართული კომპანიისა და მისი თანამშრომლების უსაფრთხოების პროფილები.

ასევე შეთანხმდეს მხარდაჭერის პროცესის უსაფრთხოების უზრუნველყოფის გზები.

2.6.1. საფრთხეები

გამომდინარე იქედან, რომ პროდუქტის მხარდაჭერის პროცესი მოიაზრებს გარკვეული სახის წვდომას ორგანიზაციის აქტივებზე (ქსელური დაშორებული წვდომა, ფიზიკური შეხვედრა, ელ. კომუნიკაცია, ვიდეო ზარი, ინფორმაციის გაცვლა, ორგანიზაციის შიდა რესურსებზე დამატებითი წვდომები, ა.შ.) - კიბერშემტევები **<u>განსაკუთრებულ მნიშვნელობას ანიჭებენ მხარდაჭერის პროცესის კომპრომეტირებას</u>**. კერძოდ, შესაძლებელია მხარდამჭერი კომპანიის თანამშრომლების იმიტაციის გზით სამიზნე კომპანიაზე წვდომის მოპოვება.

ასევე, მხარდამჭერი კომპანიის თანამშრომლების ე.წ. credential-ების (სახელი, პაროლი, ლეგიტიმური წვდომა) მითვისების გზით, უკვე არსებული კომუნიკაციის არხების გამოყენება და ორგანიზაციაში შეღწევა.

გასათვალისწინებელია **ფიზიკური შეღწევის კომპონენტიც,** შესაბამისად აუცილებელია წინასწარ განსაზღვრული მხარდაჭერის სპეციალისტების იდენტიფიცირება, მათი background check-ის განხორციელება და აქტივობების მონიტორინგი.

2.6.2. რეალური კიბერინციდენტები

2013 წელს ამერიკული კომპანია Target-ის მიმართ განხორციელებული კიბერშეტევის გამომწვევი მიზეზი (ე.წ. root-cause) აღმოჩნდა მათ მიერ არასათანადოდ შერჩეული და შემოწმებული სერვისის მხარდაჭერის კომპანია. კერძოდ, **HVAC სისტემების სამართავად** Target-მა დაიქირავა კომპანია, ისე, რომ არ მოსთხოვა და **არ გაითვალისწინა ინფორმაციული და კიბერუსაფრთხოების შესაბამისი მზაობა და სიმწიფის დონე.** შედეგად, აღნიშნული HVAC მხარდაჭერის კომპანიის ქსელში შეღწევით, კიბერშემტევმა, ამ ორგანიზაციის გავლით წვდომა **მოიპოვა Target-ის ქსელზეც, განახორციელა გადახდის ტერმინალების ინფიცირება და მილიონობით მომხმარებლის საბარათე მონაცემების მითვისება.**

შემტევი

- კიბერ-კრიმინალები, პოტენციური კავშირით რუსული დაჯგუფებების მიერ გამოყენებულ ტექნიკურ ინფრასტრუქტურასთან.

მსხვერპლი

- კორპორაცია Target, უდიდესი retail კომპანია, 107 მილიარდ დოლარიანი შემოსავლით, აშშ ტერიტორიაზე.

სამიზნე სისტემა

- HVAC სისტემების მხარდამჭერი კომპანია და მისთვის განკუთვნილი ქსელური ინფრასტრუქტურა Target-ის შიგნით. მეორე ნაბიჯად POS point-of-sale (POS) გადახდის ტერმინალის სისტემები.

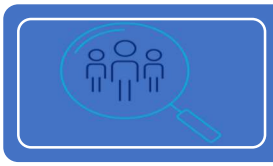
შეტევის ტიპი და მეთოდი

- მიმწოდებელი კომპანიის კუთვნილი ე.წ. network credential ხელში ჩაგდების გზით, კომპანია Target-ის ქსელში არასანქცირებული შეღწევა, POS გადახდის სისტემების დაინფიცირება და მათზე გატარებული მილიონობით საბანკო ბარათების შესახებ ინფორმაციის მოპარვა.

ზიანი

- დაახლოებით 40 მილიონამდე საკრედიტო და სადებეტო ბარათების ინფორმაცია და 70 მილიონი კლიენტის პერსონალური მონაცემების გაჟონვა. პირდაპირი ფინანსური და რეპუტაციული ზიანი, ასევე ინციდენტის მოგვარების, სასამართლო გარიგებების, ჯარიმებისა და შესაბამისობის ხარჯები - მილიონობით დოლარი და აქციების ფასის ვარდნა, საბაზრო კაპიტალიზაციის შემცირება.

2.6.3. საუკეთესო პრაქტიკა და რეკომენდაციები



Vetting & Due Dilligence

- მხარდაჭერის განმახორციელებელი კომპანიის Vetting და Due Diligence. მათი უსაფრთხოების პრაქტიკის შემოწმება ან დამადასტურებელი დოკუმენტაციის წარდგენა.

უსაფრთხო კომუნიკაციის არხი

- წინასწარ განსაზღვრული უსაფრთხოების მოთხოვნები, შედეგად მხოლოდ შეთანხმებული უსაფრთხო გზებით მხარდაჭერის განხორციელების შესაძლებლობა.
- უსაფრთხო კომუნიკაციის არხები მხარდაჭერის განსახორციელებლად.

ინციდენტებზე რეაგირების სცენარები

- სერვისის მიმწოდებლისგან გამოწვეულ კიბერინციდენტებზე რეაგირების წინასწარ განსაზღვრული სცენარები.

მიმწოდებლის მუდმივი მონიტორინგი

- ინფორმაცია მათზე განხორციელებული შეტევების და ინციდენტების შესახებ, რაც ირიბად შეიძლება უკავშირდებოდეს სერვისის შემსყიდველ ორგანიზაციას.

განსაკუთრებით მნიშვნელოვანია **მხარდამჭერი კომპანიის მდებარეობის, რეგისტრაციის და თანამშრომლების უსაფრთხოების გათვალისწინება**. **ზოგიერთი ქვეყნის მარეგულირებელი ორგანოები აღჭურვილი არიან უფლებით, ნებისმიერ დროს მოსთხოვონ შესაბამის მხარდამჭერ კომპანიებს, გარკვეული სენსიტიური ინფორმაციის გამჟღავნება, რაც შეიძლება მოიცავდეს კონფიდენციალურ და სენსიტიურ მონაცემებს მათი კლიენტების შესახებ.**

ასევე, ამ ორგანიზაციებში, მხარდაჭერის რგოლში მომუშავე თანამშრომლები განსაკუთრებული სამიზნეები ხდებიან მაღალი დონის კიბერშემტევებისათვის, ვინაიდან, **პოტენციურად 1 თანამშრომელი შეიძლება ემსახურებოდეს და წვდომას ფლობდეს ათობით პარტნიორი კომპანიის ICT ინფრასტრუქტურაზე.**

შესაბამისად მნიშვნელოვანი ხდება მხარდაჭერის პროცესის სრული მონიტორინგი და მის დროს განხორციელებული აქტივობების დეტალური ანალიზი.

2.7. ჩამოწერა

ფიგურა 22: მიწოდების ჯაჭვის სასიცოცხლო ციკლი

დანერგილი პროდუქტის გამოყენების შეჩერება, ანუ ჩამოწერა, ICT მიწოდების ჯაჭვის სასიცოცხლო ციკლის საბოლოო ფაზაა. ამ პროცესში მოიაზრება ისეთი შემთხვევები როდესაც ხდება **პროდუქტის ჩანაცვლება ახალი ვერსიით, სხვა მწარმოებლის პროდუქტით ან სხვა ფუნქციონალის მქონე პროდუქტით**. ნებისმიერ შემთხვევაში აუცილებელია გამოყენებული პროდუქტის ჩამოწერა უსაფრთხო გზით.

ასევე, მწარმოებელ, **მომწოდებელ და მხარდამჭერ კომპანიასთან ურთიერთობის გაწყვეტის პროცესში,** შესაბამისი უსაფრთხოების რისკების გათვალისწინება.

2.7.1. საფრთხეები

პროდუქტის ჩამოწერისას ერთ-ერთი გავრცელებული საფრთხეა მისი არაადექვატური და არაუსაფრთხო „განადგურება“. იგულისხმება მასში **არსებული ინფორმაციის, კონფიგურაციის, ძველი ჩანაწერების ან სრულად პროდუქტის ფიზიკური განადგურება.**

ვინაიდან, არსებობს **საექსპერტო კრიმინალისტიკური მიდგომა წაშლილი ფაილებისა და სისტემური ინფორმაციის აღსადგენად,** მნიშვნელოვანია გამოყენებული პროდუქტების ჩამოწერისას, **შესაბამისი უსაფრთხოების პროტოკოლების და წესის გათვალისწინებით,** მოხდეს მათში არსებული **ინფორმაციის განადგურება**, რათა **ვერ მოხდეს ან გართულდეს სხვადასხვა გზით ძველი სენსიტიური ინფორმაციის ამოღება.**

ჩამოწერილი მოწყობილობები ზოგ შემთხვევაში გადაეცემა სხვა დეპარტამენტებს, თანამშრომლებს, შვილობილ კომპანიებს, იყიდება ან ხდება მათი გადაგდება ან გადაცემა გადამამუშავებელი კომპანიებისათვის. **ნებისმიერ ზემოხსენებულს პოტენციურად შეუძლია არასათანადოდ და არა-უსაფრთხოდ განადგურებული მოწყობილობიდან ძველი, სენსიტიური ინფორმაციის აღდგენა.**

ამ შემთხვევაში ხდება არამარტო სენსიტიური ინფორმაციის გაჟონვა **(პერსონალური მონაცემები, ინტელექტუალური საკუთრება, კონფიდენციალური ფაილები, ა.შ.)** არამედ, შესაბამისობის დარღვევა დარგობრივ რეგულაციებთან და საკანონმდებლო მოთხოვნებთან.

2.7.2. რეალური კიბერინციდენტები

2022 წელს გერმანელმა უსაფრთხოების მკვლევარებმა ონლაინ გაყიდვების პლატფორმა ebay-ზე შეიძინეს და გააანალიზეს **აშშ სამხედრო ძალების მიერ გამოყენებული უსაფრთხოების მოწყობილობები.** კერძოდ, კვლევისას გაანალიზეს ბიომეტრიული სკანირების ხელსაწყოები. აღმოჩნდა, რომ მათში **ჯერ კიდევ ჩარჩენილი იყო ბიომეტრიული მონაცემები** (თითის **ანაბეჭდი, თვალის ბადურის გარსის ანარეკლი,** ა.შ.) იმ ინდივიდებისა, რომლებმაც გაიარეს და შემოწმდნენ გამშვებ პუნქტებზე ავღანეთსა და ერაყში.

ასევე, კერძო სექტორი პერსპექტივიდან, 2016 წელს ერთერთმა უდიდესმა ბანკმა Morgan Stanley-მ დახურა მისი კუთვნილი ორი დატა ცენტრი, მაგრამ არასათანადოდ გაანადგურა მასში არსებული აპარატურა (hardware). შედეგად, აღნიშნულ პროდუქტებში აღმოჩნდა კლიენტების შესახებ არსებული სენსიტიური ჩანაწერები. შედეგად, კომპანია დაჯარიმდა რამდენიმე მილიონი აშშ დოლარით და დაირღვა კლიენტების პრივატულობა.

2.7.3. საუკეთესო პრაქტიკა და რეკომენდაციები

ICT პროდუქტების ჩამოწერისას, საჭიროა ორგანიზაციამ გაითვალისწინოს უსაფრთხო განადგურების შესაბამისი სახელმძღვანელოები და წესები. ერთ-ერთი ასეთია: ინდუსტრიული სტანდარტი „NIST SP 800-88 Rev. 1 Guidelines for Media Sanitization[21]“.

ასევე, პროფესიული სერვისების გამოყენება, რომლებიც სთავაზობენ მომხმარებლებს, **ხელსაწყოების უსაფრთხო და კვალიფიციურ განადგურების სერვისებს.** თუმცა, ეს შემთხვევაც განსაკუთრებით საყურადღებოა, თანმდევი პოტენციური რისკები გამო.

აქტივების მართვა და მისი სისრულის უზრუნველყოფა. ორგანიზაციამ ზედმიწევნით ზუსტად უნდა იცოდეს, დროის კონკრეტულ მომენტში **რა რაოდენობის კრიტიკული აქტივი აქვს, სად ინახება, ვინ იყენებს მას და რა სენსიტიური მონაცემები მუშავდება** მასში. განადგურების და ჩამოწერის შესახებ ცნობები უნდა აისახოს მომენტალურად. მოხდეს ამ ბაზის მართვა და ხშირი აუდირება, შეცდომების გამოსარიცხად.

[21] https://csrc.nist.gov/pubs/sp/800/88/r1/final

შეჯამება

ICT მიწოდების ჯაჭვის თითოეული ეტაპი მოიცავს შესაბამის რისკებს, არსებობს მისკენ მიმართული საფრთხეები და რეალურად მომხდარი რელევანტური კიბერინციდენტები. აქედან გამომდინარე საჭიროა კომპლექსური მიდგომა და აღნიშული ჯაჭვის თითოეული კომპონენტის ჭრილში უსაფრთხოების კომპონენტის გათვალისწინება.

ICT მიწოდების ჯაჭვი იმდენად დაცულია, რამდენადაც მისი შემადგენელი ყველაზე სუსტი კომპონენტი.

რეკომენდაციების შეჯამების შედეგად შეგვიძლია მოვიყვანოთ რამდენიმე ძირითადი საკითხი:

1. მიწოდების ჯაჭვის სრული ციკლის ფარგლებში, გარე მხარეებთან ურთიერთობის დახმარებამდე, შემოწმდეს **მათი მიკუთვნება აღიარებულ, სანდო და უსაფრთხო მწარმოებლების სიასთან. მსგავს სიებს აწარმოებს US, UK, EU, NATO და ა.შ.**
2. ურთიერთობის დაწყებამდე უნდა შეფასდეს პარტნიორი ორგანიზაციის **უსაფრთხოების არსებული სტატუსი, გამოითხოვოს მათი უსაფრთხოების შესაბამისობის დამადასტურებელი დოკუმენტაცია.**
3. განხორციელდეს არსებული **ინფორმაციის ანალიზი, პარტნიორი ორგანიზაციის მიმართ განხორციელებული კიბერ შეტევების და მათ მიერ რეაგირების შესახებ.**
4. გაანალიზდეს **ორგანიზაციის მფლობელები, თანამშრომლები და პარტნიორები.**
5. რომელ **ქვეყანასა და იურისდიქციაში ოპერირებს პარტნიორი ორგანიზაცია** (პრივატულობისა და უსაფრთხოების შემაფერხებელი დარგობრივი რეგულაციების გასათვალისწინებლად).
6. დანერგვის პროცესის განხორციელება წინასწარ შეთანხმებული უსაფრთხო გზით.
7. ოპერირებისა და მართვის პროცესში, საუკეთესო პრაქტიკების გათვალისწინება მესამე მხარეების რისკების სამართავად.
8. მხარდაჭერის პროცესის მონიტორინგი, ანომალიური ქმედებების აღმოსაჩენად.
9. პროდუქტის გაუქმება, ჩამოწერის პროცესში უსაფრთხოების მოთხოვნების გათვალისწინება - უსაფრთხო განადგურების გზების გამოყენებით.
10. საფრთხეების შესახებ ინფორმაციის შეგროვება და გაზიარება პარტნიორებთან.

3. თავი 3: ICT მიწოდების ჯაჭვის უსაფრთხოების ღია მონაცემთა ანალიზი საქართველოში

წინამდებარე თავში წარმოდგენილია **საქართველოს სახელმწიფო შესყიდვების სააგენტოს პორტალისა (spa.gov.ge)** და **Tendersmonitor.ge**-დან მიღებული ღია მონაცემების ანალიზი. კვლევისას ფოკუსი გაკეთდა **ინფორმაციული და საკომუნიკაციო ტექნოლოგიების (ICT) პროდუქტების შესყიდვაზე** ეროვნული კრიტიკული ინფორმაციული ინფრასტრუქტურის (CII) სუბიექტებში (შემდგომში „სუბიექტებში“). კერძოდ, **კვლევისას გაანალიზდა რამდენად იყენებენ სუბიექტები სანქცირებულ ICT პროდუქტებს** და ასევე, რა გავლენა შეიძლება ქონდეს ამ სერვისებს სუბიექტების უსაფრთხოებაზე.

კვლევის ფარგლებში ყურადღება გამახვილდა რამდენიმე მნიშვნელოვანი შესყიდვების კატეგორიის მიხედვით, როგორიც არის:

- **30200000** -კომპიუტერული მოწყობილობები და აქსესუარები
- **32300000** - ტელე და რადიოსიგნალის მიმღებები და აუდიო ან ვიდეოგამოსახულების ჩამწერი ან აღწარმოების აპარატურა
- **32400000** - ქსელური მოწყობილობები და სერვისი
- **48200000** - ქსელის, ინტერნეტისა და ინტრანეტის პროგრამული პაკეტები
- **72200000** - პროგრამული უზრუნველყოფის შესყიდვა და შემუშავება

თითოეული მიმართულებით აღმოჩენილი მნიშვნელოვანი მიგნებები წარმოდგენილია ცალკეულ ქვეთავებში.

წინამდებარე კვლევის ფარგლებში დეტალურად გაანალიზდა კრიტიკული ინფორმაციული სისტემის სუბიექტების (საჯარო უწყებების) მიერ ტენდერისა და პირდაპირი შესყიდვის გზით **2021-2023 წლებში განხორციელებული შესყიდვები. თუმცა, შესყიდვის და ICT სფეროს სპეციფიკიდან გამომდინარე სრული სურათისათვის, რიგ შემთხვევებში გამოყენებულ იქნა წინა პერიოდის მონაცემებიც.**

3.1. მართვის ელექტრონული სისტემების შემუშავება და შესყიდვა

მართვის ელექტრონული სისტემები (Management Information Systems) მნიშვნელოვან როლს თამაშობს სამთავრობო პროცესების ავტომატიზაციასა და ეფექტიანობის გაზრდაში. რაც უფრო მეტად იზრდება ორგანიზაციის დამოკიდებულება ელექტრონულ სისტემებზე, მით მეტად იზრდება ამ სისტემებთან დაკავშირებული კიბერრისკების პოტენციური გავლენა. შესაბამისად,

წინამდებარე თავებში წარმოდგენილია რამდენი მნიშვნელოვანი კატეგორიის მართვის ელექტრონული სისტემები და შესაბამისი მონაცემების ანალიზი. კერძოდ, წინამდებარე თავებში განხილული იქნება:

- ***Enterprise Resource Planning (ERP) სისტემები;***
- ***Law Enforcement Systems (LES);***
- ***Global Navigation Satelite Systems (GNSS);***

3.1.1. ERP სისტემები

პირველი კატეგორიის კრიტიკული ინფორმაციული ინფრასტრუქტურის უსაფრთხოებისთვის, მნიშვნელოვანია, სუბიექტების მიერ შესყიდული და გამოყენებული **ERP პროგრამული პროდუქტებისა** და **ფინანსური აღრიცხვის სისტემების** ანალიზი.

საქართველოს ბაზარზე, ერთ-ერთი ყველაზე გავრცელებული ERP სისტემაა[22] - „1C“ და „FMG Soft“, თავისი დაბალი ფასისა და შედარებით მარტივი დანერგვის პროცესის გათვალისწინებით.

3.1.1.1. 1C შესყიდვების ანალიზი

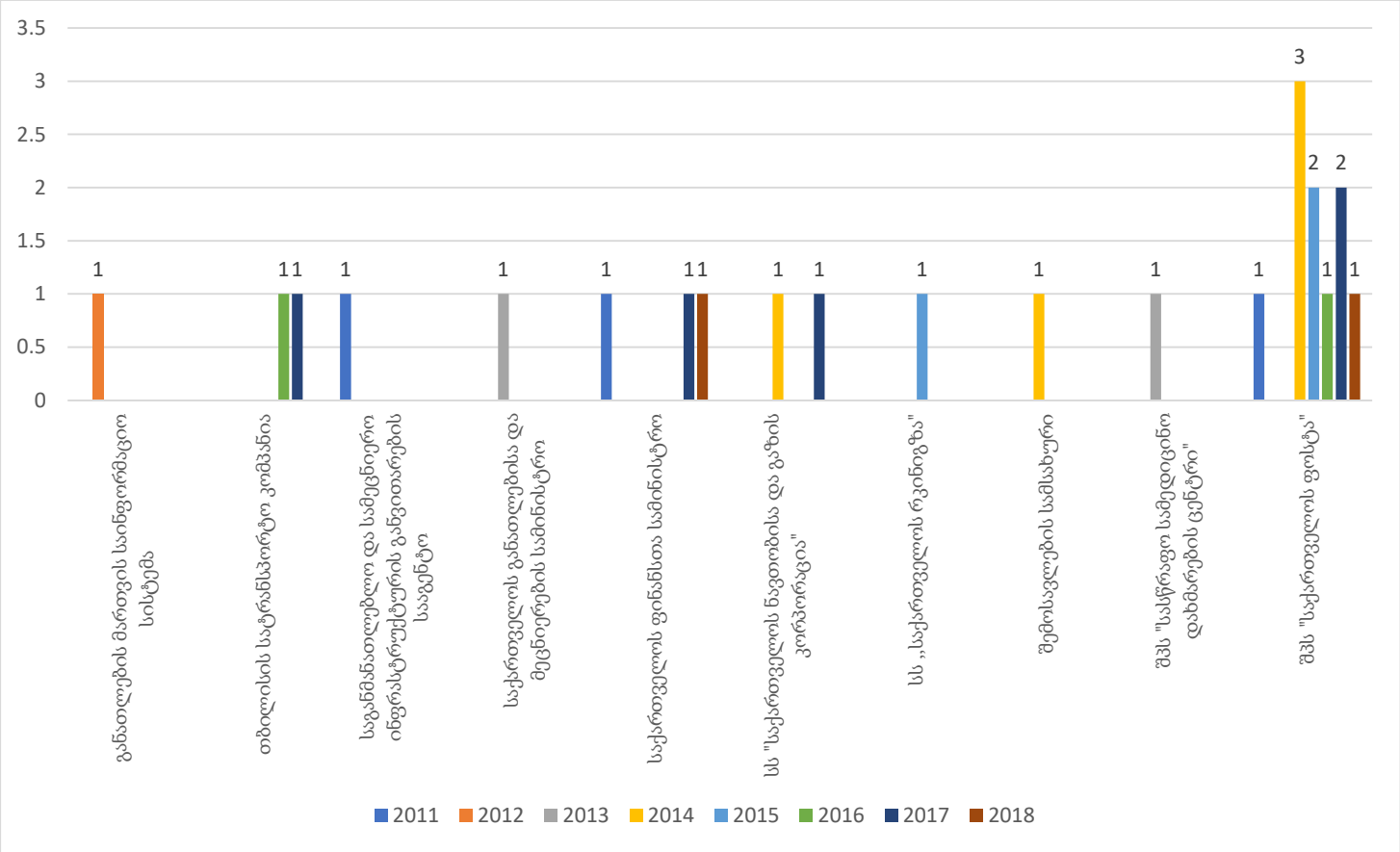
„1C“ წარმოადგენს რუსული წარმომავლობის ERP პროგრამულ უზრუნველყოფას, რომლის **პროგრამული მხარდაჭერა და განახლებები იმართება რუსული კომპანიის** მიერ. კვლევაში წარმოდგენილია პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტებში აღნიშნული პროდუქტის მოხმარება.

ანალიზის შედეგად გამოვლინდა, რომ „1C“ სისტემის მომხმარებლებს წარმოადგენს შემდეგი კრიტიკული ინფორმაციული სისტემის სუბიექტები:

1. ***შპს "საქართველოს ფოსტა";***
2. ***სს ,,საქართველოს რკინიგზა";***
3. ***სსიპ განათლების მართვის საინფორმაციო სისტემა;***
4. ***საქართველოს ფინანსთა სამინისტრო;***
5. ***სსიპ შემოსავლების სამსახური;***
6. ***საქართველოს განათლებისა და მეცნიერების სამინისტრო;***
7. ***სსიპ საგანმანათლებლო და სამეცნიერო ინფრასტრუქტურის განვითარების სააგენტო.***

[22] „BDO დიჯიტალი“ წარმოადგენს 1C-ის ყველაზე მსხვილ მიმწოდებელს საჯარო სექტორისთვის.

წლების მანძილზე, პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების მიერ „1C” სისტემის შესყიდვის ტენდენცია:



3.1.1.2. FMG Soft შესყიდვების ანალიზი

FMG Soft არის რუსული წარმომავლობის ბუღალტრულ/ERP სისტემა, რომელსაც საქართველოში წარმოადგენს კომპანია „ეფემჯი სოფტი“. აღნიშნული კომპანია იყენებს რუსული მწარმოებლის „ნოვა სოფტის“ მიერ წარმოებულ „ინფო საწარმოს“. წლების მანძილზე კრიტიკული ინფორმაციული სისტემის სუბიექტების მიერ „ეფემჯი სოფტთან“ განხორციელებული შესყიდვების სტატისტიკა შემდეგია:

შემსყიდველი	2011	2012	2013	2014	2015	2016	2017	2018	2019	2021	2022	2023	ჯამი
აღსრულების ეროვნული ბიურო										2			**2**
კონკურენციისა და სახელმწიფო შესყიდვების სააგენტო										2			**2**

მასწავლებელთა პროფესიული განვითარების ეროვნული ცენტრი				1									**1**
საქართველოს პარლამენტის აპარატი									1	2			**3**
საქართველოს პრეზიდენტის ადმინისტრაცია							1						**1**
საქართველოს ფინანსთა სამინისტრო									1	1			**2**
საქართველოს შინაგან საქმეთა სამინისტრო		1											**1**
საქართველოს შსს. დაცვის პოლიციის დეპარტამენტი	1	4	2	1	2	2	1						**13**
საქართველოს ცენტრალური საარჩევნო კომისია						1				1	1		**3**
სახმელეთო ტრანსპორტის სააგენტო										2	1		**3**
სსიპ საქართველოს შსს მომსახურების სააგენტო								1					**1**
სურსათის ეროვნული სააგენტო												1	**1**
ქ. თბილისის მერია					1								**1**
ქ.თბილისის საკრებულოს აპარატი						1				2			**3**
სსიპ - "112"		3	1							2			**6**

3.1.2. სხვადასხვა სისტემები

გარდა ERP სისტემებისა ცხრილში წარმოდგენილია სხვდასხვა მმართველობითი სისტემების შესყიდვის მიმართულებით იდენტიფიცირებული სარისკო შესყიდვები:

შესყიდვის #	შემსყიდველი	მიმწოდებელი	აღწერა	მწარმოებელი	ქვეყანა

NAT230017233	ქ. თბილისის მერია	ნეოტექი	ვიდეო-სამეთვალყურეო კამერებისთვის ლიცენზიები	Hangzhou Hikvision Digital Technology Co. Ltd	**ჩინეთი**
NAT230009413	საქართველოს შინაგან საქმეთა სამინისტრო	შპს საექსპერტო სისტემები	ფონოსკოპიური ექსპერტიზის სისტემა	Speech Tech GmbH - IKAR Lab 3 Hardware and Software	**რუსეთი**
NAT220019926	საქართველოს შინაგან საქმეთა სამინისტრო	მაი მობაილ +	ჰაბიტოსკოპიური სისტემის - "POLYFACE"-ის პროგრამული უზრუნველყოფის არსებული ვერსიის განახლებ	Papilon Savunma Teknoloji ve Ticaret A.Ş.	**თურქული წარმომადგენლობა, რუსული კომპანია Papilon AO.**

3.1.3. სამართალდამცავი პროგრამული უზრუნველყოფა (LES)

ძალოვანი უწყებებისთვის, რომლებიც კლასიფიცირებულია, როგორც პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტები, და ეროვნული უსაფრთხოებისთვის, კრიტიკულად მნიშნელოვანია უზრუნველყოფილი იქნეს უსაფრთხო ICT მიწოდების ჯაჭვი. შესაბამისად, კვლევის ფარგლებში შესწავლილი იქნა **სამართალდამცავი პროგრამული უზრუნველყოფის (Law Enforcement Software – LES) შესყიდვები**.

3.1.3.1. ჰაბიტოსკოპიური სისტემის შესყიდვა

ღია მონაცემების ანალიზისას შესწავლილი იქნა **შინაგან საქმეთა სამინისტროს შესყიდვები**[23]**.** შინაგან საქმეთა სამინისტრო **სახის ამოცნობისათვის იყენებს ჰაბიტოსკოპიურ საექსპერტო-კრიმინალისტურ სისტემას „PolyFace”**. აღნიშნული სისტემა არის შემუშავებული რუსული მწარმოებლის მიერ.

სისტემის პირველადი შესყიდვა განხორციელდა 2013 წელს. **2022 წლამდე,** სისტემის განახლებებისა და მომსახურების შესყიდვის დოკუმენტებში ფიქსირდება **რუსული** კომპანია - „Papillon AO”, როგორც სისტემის მწარმოებელი. თუმცა, **2022 წლიდან,** იმავე სისტემის

[23] კვლევაში არ არის იდენტიფიცირებული სახელმწიფო საიდუმლო შესყიდვები. შესაბამისად, წარმოდგენილი მიგნებები შეიძლება სრულად არ ასახავდეს სამინისტროში არსებული პროგრამული უზრუნველყოფის პორტფელს.

განახლებებისა და სერვისების შესყიდვის დოკუმენტებში მწარმოებელ კომპანიად მითითებული **თურქული** კომპანია „Papilon Savunma Teknoloji ve Ticaret A.Ş.“. ზემოხსენებული სისტემის შესყიდვების შესახებ დეტალური ინფორმაცია მოცემულია წინამდებარე ცხრილში:

წელი	შესყიდვის #	აღწერა	ღირებულება (ლარი)	მწარმოებელი	დოკუმენტაციით განსაზღვრული ქვეყანა
2013	**SPA130017726**	ჰაბიტოსკოპიური საიდენტიფიკაციო სისტემის პროგრამული უზრუნველყოფის შესყიდვა	125,000	Papillon Polyface	**რუსეთი**
2017	**SPA170005270**	Polyface სისტემის პროგრამული განახლება	96,970	Papillon Polyface	**რუსეთი**
2018	**NAT180012028**	Polyface სისტემის პროგრამული განახლება	91,750	Papillon AO.	**რუსეთი**
2020	**NAT200009157**	Polyface სისტემის პროგრამული განახლება	146,856	Papillon AO.	**რუსეთი**
2022	**NAT220019926**	Polyface სისტემის პროგრამული განახლება	340,000	Papilon Savunma Teknoloji ve Ticaret A.Ş.	**თურქეთი**

3.1.3.2. ფონოსკოპიური სისტემის შესყიდვა

საქართველოს შინაგან საქმეთა სამინისტროს იყენებს **ფონოსკოპიური ექსპერტიზის სისტემას**, რომელიც **გამოიყენება ხმის და მეტყველების ფონოგრამების კრიმინალისტიკური გამოკვლევისათვის**. აღნიშნული მიზნებისათვის, შსს იყენებს **რუსულ პროგრამულ უზრუნველყოფას „IKAR Lab 3“,** რომლის მიმწოდებელია საქართველოში რეგისტრირებული კომპანია შპს „საექსპერტო სისტემები[24]“.

3.1.3.3. დაქტილოსკოპიური სისტემის შესყიდვა

შინაგან საქმეთა სამინისტროს მიერ შპს „საექსპერტო სისტემებთან“-თან გაფორმებული ხელშეკრულებებიდან ასევე, საყურადღებოა შემდეგი შესყიდვები:

თარიღი	შესყიდვის #	ღირებულება	პროდუქტი	მწარმოებლის ქვეყანა

[24] 2023 წლის 1 ივნისს გაფორმებული ხელშეკრულება.

2024-01-25	**NAT230026968**	414,920	დაქტილოსკოპიურ ავტომატურ საძიებო-საიდენტიფიკაციო სისტემა "DACTO 2000"-სთან თავსებადი სკანერების (კომპლექტში - ინსტალაციით) შესყიდვა.	თურქეთი/რუსეთი	Papilon Savunma Teknoloji ve Ticaret A.Ş
			მომხმარებლის პროგრამული უზრუნველყოფა	ბელორუსია	TODES Ltd
2023-02-27	**NAT230003 397**	377,200	დაქტილოსკოპიური სკანერი - ანაბეჭდების სკანერი დაქტილოსკოპიურ ავტომატურ საძიებო-საიდენტიფიკაციო სისტემა "DACTO 2000"-სთან თავსებადი სკანერების (კომპლექტში - ინსტალაციით) შესყიდვა.	თურქეთი/რუსეთი	Papilon Savunma Teknoloji ve Ticaret A.Ş
			მომხმარებლის პროგრამული უზრუნველყოფა (User)	ბელორუსია	TODES Ltd

3.1.3.4. ბალისტიკური სისტემის შესყიდვა

შინაგან საქმეთა სამინისტრომ 2018 წელს პირველად შეიძინა (NAT180001965) **ბალისტიკური ავტომატური საძიებო საიდენტიფიკაციო სისტემა - „არსენალი“,** საქართველოში რეგისტრირებული კომპანიისაგან „სოლემარტი“. აღნიშნული სისტემაც წარმოებულია რუსეთის ფედერაციაში, ს.ს. „პაპილონის“ მიერ.

2022 წელს შინაგან საქმეთა სამინისტრომ „არსენალის“ განახლებისათვისა და სკანერის დამატებისათვის ხელშეკრულება კვლავ კომპანია „სოლემარტთან“ გააფორმა. თუმცა, **2022 წელს გაფორმებულ ხელშეკრულებაში, პროგრამული უზრუნველყოფის წარმომავლობის ქვეყნად მითითებულია თურქეთი.**

შსს საექსპერტო კრიმინალისტიკური დეპარტამენტის მოთხოვნის უზრუნველსაყოფად, ბალისტიკური ავტომატური საძიებო საიდენტიფიკაციო სისტემა "ARSENAL"-სთვის დამატებითი სკანერების (კომპლექტში - ინსტალაციით) შესყიდვა განხორციელდა 2023 წელსაც თურქულ კომპანიასთან.

3.1.4. გლობალური ნავიგაციის სატელიტური სისტემები (GNSS)

გლობალური ნავიგაციის სატელიტური სისტემები (GNSS) უზრუნველყოფს სატელიტური კავშირის საშუალებით ადგილმდებარეობის განსაზღვრას, ნავიგაციასა და განრიგის სერვისებს. შვეიცარიული კომპანიის „Leica Geosystems“-ის მიერ წარმოებული GNSS სისტემები ფართოდ გამოიყენება საქართველოს სახელმწიფო უწყებების მიერ. აღნიშნულ სისტემებს აქვს შესაძლებლობა შემდეგი თანამგზავრული სიგნალების ტიპების მხარდაჭერის: **GPS, GLONASS, GALILEO**.

კვლევის ფარგლებში გაანალიზდა „Leica Geosystems“-ის მიერ წარმოებული GNSS სისტემებისა და სხვადასხვა ლაზერული მანძილმზომების შესყიდვები. **კერძოდ, 2012 წლიდან 2024 წლამდე, ზემოხსენებული სისტემები შესყიდული აქვს შემდეგ კრიტიკული ინფორმაციული სისტემის სუბიექტებს:**

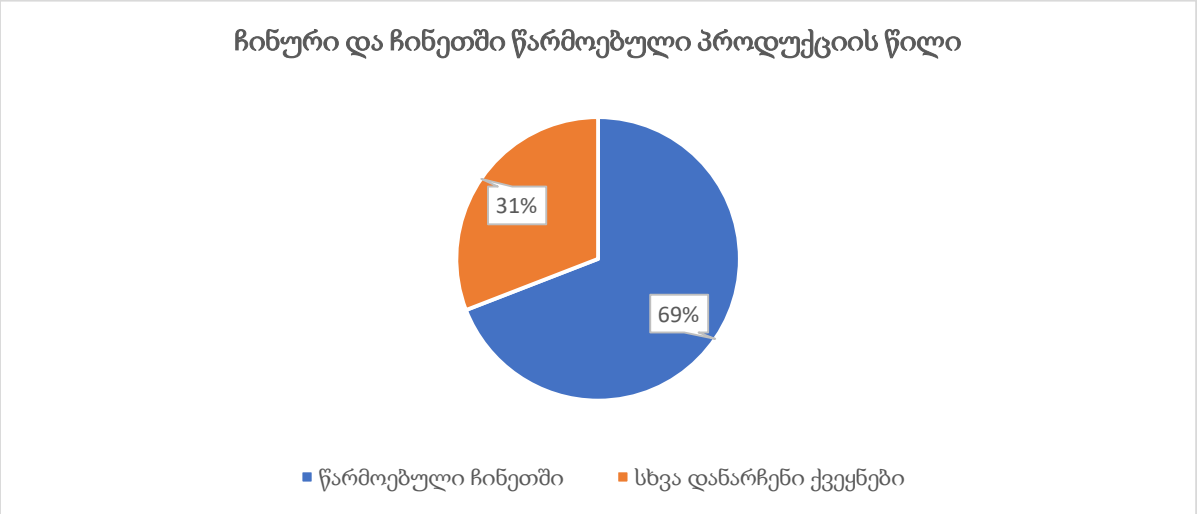
1. *ქ. თბილისის მერია;*
2. *სსიპ გარემოს ეროვნული სააგენტო;*
3. *სსიპ საჯარო რეესტრის ეროვნული სააგენტო;*
4. *საქართველოს შინაგან საქმეთა სამინისტრო;*
5. *საქართველოს თავდაცვის სამინისტრო;*
6. *სსიპ შემოსავლების სამსახური.*

ყველა მათგანში, აღნიშნულია, რომ შესყიდულ სისტემას აქვს ***GPS (აშშ), GLONASS (რუსეთი), GALILEO (ევროკავშირი)*** თანამგზავრული სიგნალების მხარდაჭერა. შესყიდვების დოკუმენტაციის დეტალური ანალიზისას გაირკვა, რომ მხოლოდ **ქ. თბილისის მერიის მიერ განხორციელებულ 2021 წლის შესყიდვაში** მერიამ დამატებით შეისყიდა **GLONASS** ლიცენზია (**NAT21012630**). კერძოდ, შესყიდვის ფარგლებში, მერიამ მოითხოვა ***აღნიშნული სმარტ ანტენისთვის რუსული გლობალური პოზიციონერების სისტემის GLONASS ლიცენზიის განახლება.***

3.2. აპარატურული უზრუნველყოფის შესყიდვები

3.2.1. კომპიუტერული მოწყობილობების შესყიდვა

წინამდებარე თავში განხილულია **კომპიუტერების, პლანშეტების და სხვა კომპიუტერული მოწყობილობების სახელმწიფო შესყიდვები (**CPV 302000 კოდი). აღნიშნული CPV კოდით შესყიდულ აპარატურაში ლიდერობს ჩინეთში წარმოებული პროდუქცია.



აღნიშნული შესყიდვების ფარგლებში განსაკუთრებით საყურადღებო და სარისკო შესყიდვებს წარმოადგენს **<u>საქციერებული მწარმოებელი კომპანიებისა და რუსული წარმომადგენლობისგან შეძენილი პროდუქცია:</u>**

შემსყიდველი	შესყიდვის #	თარიღი	მიმწოდებელი	მწარმოებელი	ქვეყანა	პროდუქტი
საქართველოს შინაგან საქმეთა სამინისტრო	NAT230010258	2023	ჯი ეს სი	Zhejiang Dahua Vision Technology Co.,	ჩინეთი	მონიტორი კომპიუტერისათვის
საქართველოს შინაგან საქმეთა სამინისტრო	NAT230001772	2023	ჯი ეს სი	Zhejiang Dahua Vision Technology Co.,	ჩინეთი	მონიტორები
საზღვაო ტრანსპორტის სააგენტო	NAT210020469	2021	პისიშოპ.ჯი	Huawei	ჩინეთი	პლანშეტები

სურსათის ეროვნული სააგენტო	NAT210020278	2021	შპს "ომეგა"	Samsung Electronics Rus Company	ჩინეთი - დოკუმენტაციით რუსული წარმომადგენლობა	პლანშეტები
საქართველოს შსს. დაცვის პოლიციის დეპარტამენტი	NAT210017368	2021	ჯიტეკი	Hangzhou Hikvision Digital Technology Co. Ltd	ჩინეთი	ვიდეო ჩამწერები
საქართველოს შინაგან საქმეთა სამინისტრო	NAT220002873	2022	ჯი ეს სი	Zhejiang Dahua Vision Technology Co.,	ჩინეთი	მონიტორი

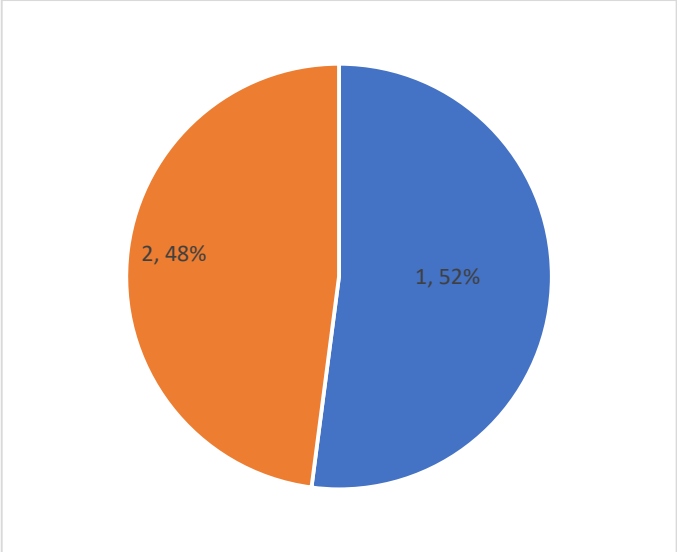
კონსოლიდირებული ტენდერები და ძირითადი გამარჯვებულები:

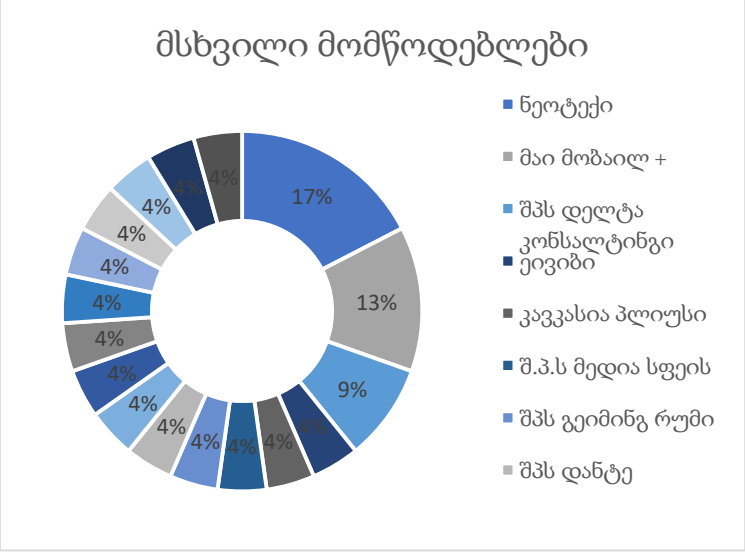
თარიღი	**შესყიდვის #**	**მიმწოდებელი**	**კომპანია**	**ქვეყანა**	**პროდუქტი**
2023-12-20	CON230000579	იუჯითი	acer	პროდუქცია - ჩინეთი MAF - ყაზახეთი	კომპიუტერები
2023-12-20	CON230000580	იუჯითი	Dell	MAF უკრაინა	კომპიუტერები
2023-11-22	CON230000368	იუჯითი	HP	ამსტერდამის წარმომადგენლობა	პრინტერი
2023-11-22	CON230000369	ბედი ჯი	EAST GROUP CO., LTD	ჩინეთი	UPS
2023-09-27	CON230000315	იუჯითი	Acer	პროდუქცია - ჩინეთი MAF - ყაზახეთი	კომპიუტერები
2023-06-13	CON230000278	Smartmatic International Holding B.V.	Smartmatic International Holding B.V.	ნიდერლანდები	ამომრჩეველთა ვერიფიკაციის აპარატი
2023-02-16	CON230000090	ბედი ჯი	EAST GROUP CO., LTD	ჩინეთი	UPS
2022-11-29	CON220000355	იუჯითი	Acer	პროდუქცია - ჩინეთი MAF - ყაზახეთი	კომპიუტერები

2022-11-29	CON220000356	იუჯითი	Acer	პროდუქცია - ჩინეთი MAF - ყაზახეთი	კომპიუტერები
2022-11-03	CON220000305	იუჯითი	Acer	პროდუქცია - ჩინეთი MAF - ყაზახეთი	კომპიუტერები

3.2.2. ვიდეო სათვალთვალო კამერების შესყიდვა

ვიდეო სათვალთვალო კამერების მოხმარება უფრო და უფრო აქტუალური ხდება საჯარო სივრცეებში და ადმინისტრაციულ შენობებში. აღნიშნული პროდუქტების შესყიდვა აქტუალური და მნიშვნელოვანია საჯარო სექტორის კრიტიკული ინფორმაციული სისტემის სუბიექტებისთვისაც.





2021-2023 წლების მანძილზე შესყიდული **<u>კამერების უმრავლესობის წილი მოდის ამერიკის მიერ სანქცირებულ კომპანიებზე, კერძოდ Hangzhou Hikvision Digital Technology Co. Ltd და Zhejiang Dahua Vision Technology.</u>**

3.2.3. აშშ-ს მიერ სანქცირებული მწარმოებლებისა და პროდუქტების შესყიდვები

2021- 2023 წლებში კრიტიკული ინფორმაციული სისტემის სუბიექტების მიერ შეძენილი პროდუქტების ჩინეთის სანქცირებული მომწოდებლებისგან.

შემსყიდველი	შესყიდვის #	თარიღი	GEL	მიმწოდებელი	პროდუქტი	მწარმოებელი	ქვეყანა
შეფასებისა და გამოცდების ეროვნული ცენტრი	NAT230006075	2023-03-17	86,100.00	ნეოტექი	ვიდეოსათვალთვალო კამერა	Hangzhou Hikvision Digital Technology Co. Ltd	ჩინეთი
საქართველოს მთავარი პროკურატურა	NAT210021585	2021-11-16	11,213.00	ჯი ეს სი	ვიდეოსათვალთვალო კამერა	Dahua Technology Company	ჩინეთი
საქართველოს მთავარი პროკურატურა	NAT210010162	2021-06-07	5,900.00	ნეოტექი	ვიდეოსათვალთვალო კამერები	Hangzhou Hikvision Digital Technology Co. Ltd	ჩინეთი
შემოსავლების სამსახური	NAT210008827	2021-05-18	46,410.00	შპს დელტა კონსალტინგი	ვიდეოსათვალთვალო კამერა	Hangzhou Hikvision Digital Technology Co.,Ltd	ჩინეთი
შპს "საქართველოს ფოსტა"	SPA210001184	2021-04-22	17,875.82	ნეოტექი	ვიდეოსათვალთვალო კამერა	Hangzhou Hikvision Digital Technology Co.	ჩინეთი
შეფასებისა და გამოცდების ეროვნული ცენტრი	NAT220015150	2022-08-02	47,560.00	ნეოტექი	ვიდეოსათვალთვალო კამერა	Hangzhou Hikvision Digital Technology Co.	ჩინეთი
საქართველოს ცენტრალური საარჩევნო კომისია	CMR200104806	2020 – 09-01	164,515.00	ნეოტექი	ვიდეოსათვალთვალო კამერა	Hangzhou Hikvision Digital Technology Co.	ჩინეთი

აღსანიშნავია, რომ **<u>2019 და 2018 წლებშიც საკმაოდ მოცულობითია სანქცირებული კომპანიების მიერ წარმოებული პროდუქციის წილი საჯარო სექტორში ქსელური კამერების შესყიდვის კუთხით</u>**:

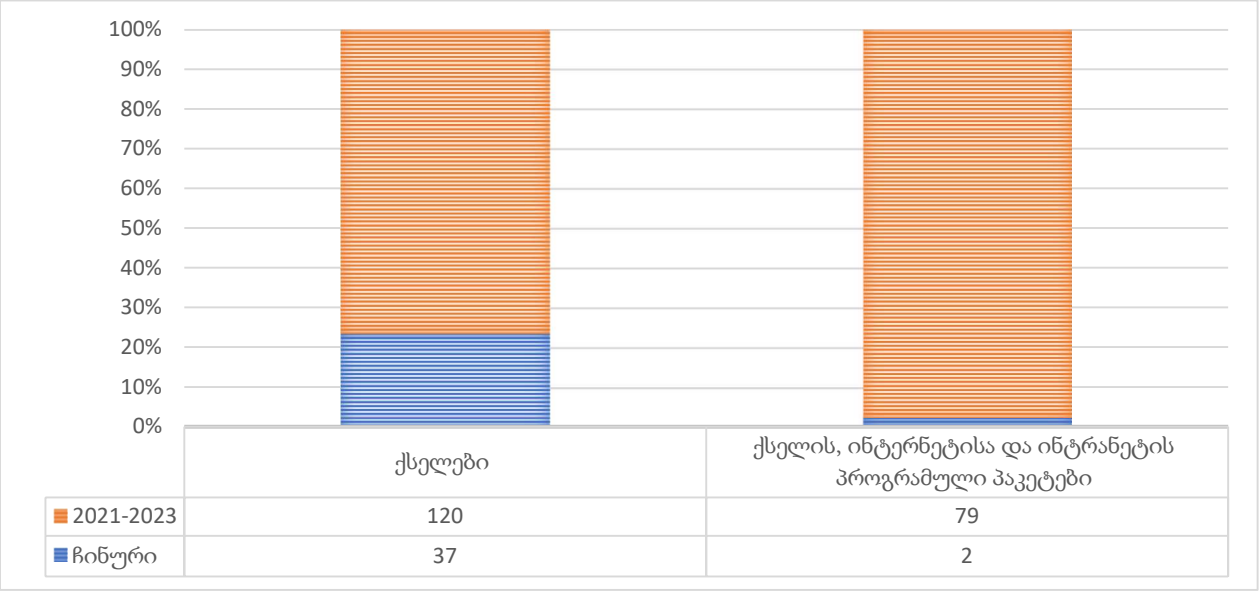
შემსყიდველი	შესყიდვის #	მიმწოდებელი	თარიღი	თანხა	მწარმოებელი
შპს "საქართველოს ფოსტა"	NAT190024043	ნეოტექი	10.12.2019	4,254.00	Hangzhou Hikvision Digital Technology Co.
ქ. თბილისის მერია	NAT190023978	ნეოტექი	09.12.2019	189,886.00	Hangzhou Hikvision Digital Technology Co.

საფინანსო-ანალიტიკური სამსახური	NAT190023720	ნეოტექი	06.12.2019	45,600.00	Hangzhou Hikvision Digital Technology Co.
საქართველოს ეროვნული ბანკი	SPA190005343	ნეოტექი	12.11.2019	27,000.00	Hangzhou Hikvision Digital Technology Co.
შემოსავლების სამსახური	NAT190018012	ნეოტექი	12.09.2019	22,541.00	Hangzhou Hikvision Digital Technology Co.
შემოსავლების სამსახური	NAT190014564	ნეოტექი	22.07.2019	164,160.00	Hangzhou Hikvision Digital Technology Co.
შეფასებისა და გამოცდების ეროვნული ცენტრი	SPA190001711	ნეოტექი	21.03.2019	21,973.00	Hangzhou Hikvision Digital Technology Co.
საქართველოს ეროვნული ბანკი	SPA190001045	ნეოტექი	15.02.2019	112,600.00	Hangzhou Hikvision Digital Technology Co.
შემოსავლების სამსახური	NAT190001617	ნეოტექი	24.01.2019	12,960.00	Hangzhou Hikvision Digital Technology Co.
საქართველოს შსს. დაცვის პოლიციის დეპარტამენტი	NAT180016034	ნეოტექი	08.10.2018	46,777.00	Hangzhou Hikvision Digital Technology Co.
სახელმწიფო სერვისების განვითარების სააგენტო	SPA180007844	ნეოტექი	04.10.2018	23,642.00	Hangzhou Hikvision Digital Technology Co.
საქართველოს შსს. დაცვის პოლიციის დეპარტამენტი	NAT180016034	ნეოტექი	08.10.2018	46,777.00	Hangzhou Hikvision Digital Technology Co.
საქართველოს ცენტრალური საარჩევნო კომისია	SPA180005511	ნეოტექი	15.06.2018	185,000.00	Hangzhou Hikvision Digital Technology Co.
შპს "საქართველოს ფოსტა"	NAT180008813	ნეოტექი	11.06.2018	46,180.00	Hangzhou Hikvision Digital Technology Co.
შპს "საქართველოს ფოსტა"	NAT180008812	ნეოტექი	11.06.2018	160,869.00	Hangzhou Hikvision Digital Technology Co.
საქართველოს შინაგან საქმეთა სამინისტრო	NAT190019759	ჯი ეს სი	11.10.2019	33,245.00	Dahua Technology Company

საქართველოს სახელმწიფო უსაფრთხოების სამსახური	SPA190003937	ჯი ეს სი	31.07.2019	2,043.00	Dahua Technology Company
საქართველოს შინაგან საქმეთა სამინისტრო	NAT190019759	ჯი ეს სი	11.10.2019	33,245.00	Dahua Technology Company
საქართველოს უზენაესი სასამართლო	NAT190012220	ჯი ეს სი	20.06.2019	25,736.00	Dahua Technology Company
საქართველოს სახელმწიფო უსაფრთხოების სამსახური	SPA190002972	ჯი ეს სი	31.05.2019	15,298.00	Dahua Technology Company

3.2.4. ქსელური მოწყობილობები

ქსელური მოწყობილობები მნიშვნელოვან ვექტორს წარმოადგენს კიბერშეტევის ორგანიზებისათვის. კვლევის ფარგლებში შესწავლილი იქნა ქსელური მოწყობილობების (CPV 32400000) და ქსელის, ინტერნეტისა და ინტრანეტის პროგრამული პაკეტების (CPV 48200000) შესყიდვები.



გრაფიკი 1: 2021-2023 წლებში ქსელების მიმართულებით განხორციელებული შესყიდვები

საქართველოს პირველი კატეგორიის კრიტიკული ინფორმაციული ინფრასტრუქტურისთვის პოტენციურად საფრთხის შემცველი ქსელური მოწყობილობების შესყიდვებიდან

მნიშვნელოვანი ყურადღება გამახვილდა ისეთ შესყიდვებზე, რომელიც **მოიცავს ამერიკისა და ევროკავშირის წევრი ქვეყნების მიერ სანქცირებულ პროდუქტებს:**

შემსყიდველი	შესყიდვის #	თარიღი	მიმწოდებელი	პროდუქტი	ქვეყანა	მწარმოებელი
საქართველოს მთავრობის ადმინისტრაცია	NAT210014102	2021-07-29	ჯი ეს სი	სახის ამომცნობი ტერმინალი[25]	ჩინეთი	Zhejiang Dahua Vision Technology Co., Ltd.
შემოსავლების სამსახური	NAT220021399	2022-10-20	ნეოტექი	კომუტატორები	ჩინეთი	Hangzhou Hikvision Digital Technology Co. Ltd
შინაგან საქმეთა სამინისტროს საქვეუწყებო დაწესებულება სასაზღვრო პოლიცია	NAT220012627	2022-06-29	ინდივიდუალური მეწარმე რევაზ 84	კომპიუტერული ქსელის კაბელი	ჩინეთი	Hangzhou Hikvision Digital Technology Co. Ltd
შემოსავლების სამსახური	NAT220008435	2022-04-29	ნეოტექი	ქსელის კაბელი	ჩინეთი	Hangzhou Hikvision Digital Technology Co. Ltd
ქ. თბილისის მერია	NAT230017233	2023-08-22	ნეოტექი	ვიდეო-სამეთვალყურეო კამერებისთვის ლიცენზიები[26]	ჩინეთი	Hangzhou Hikvision Digital Technology Co. Ltd

კერძოდ, კრიტიკული ინფორმაციული სისტემის სუბიექტების მიერ არის შესყიდული, ამერიკის შეერთებული შტატების მიერ „Secure and Trusted Communications Networks Act of 2019“ ფარგლებში დასანქცირებული მწარმოებლები, როგორიც არის: Hangzhou Hikvision Digital Technology Co. Ltd და Zhejiang Dahua Vision Technology. აღნიშნული შესყიდვები განხორციელებულია, შემდეგი კრიტიკული ინფორმაციული სისტემის სუბიექტების მიერ:

- სსიპ „შემოსავლების სამსახური“;
- შსს საქვეუწყებო დაწესებულება სასაზღვრო პოლიცია

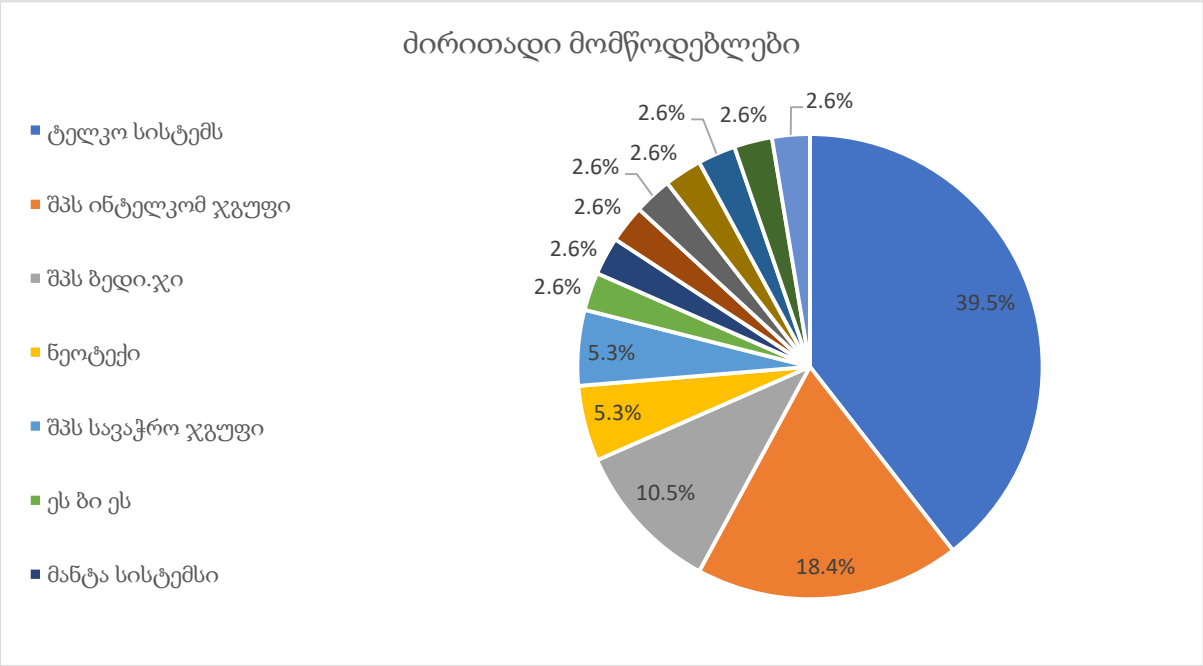
[25] აღნიშნული არ წარმოადგენს ქსელურ მოწყობილობას, თუმცა, შესყიდვა განხორციელდა ქსელური მოწყობილობების CPV კოდით, რაც კიდევ ერთხელ მიუთითებს იმაზე, რომ ზოგიერთ შემთხვევაში CPV კატეგორია შეიძლება ზუსტად არ ასახავდეს შესყიდვის საგანს.

[26] აღნიშნული არ წარმოადგენს ქსელურ მოწყობილობას, თუმცა, შესყიდვა განხორციელდა ქსელური მოწყობილობების CPV კოდით, რაც კიდევ ერთხელ მიუთითებს იმაზე, რომ ზოგიერთ შემთხვევაში CPV კატეგორია შეიძლება ზუსტად არ ასახავდეს შესყიდვის საგანს.

- ქალაქ თბილისის მერია.

3.2.5. სატელეკომუნიკაციო მოწყობილობები და აქსესუარები

სატელეკომუნიკაციო მოწყობილობების შესყიდვის ფარგლებში განხილული იყო VoIP ტელეფონების, შესაბამისი საკომუნიკაციო მოწყობილობების და აქსესუარების შესყიდვა. აღნიშნული მიმართულებით **<u>2021-2023 წლებში განხორციელებული შესყიდვების ფარგლებში ჩინეთში წარმოებული და ჩინური პროდუქციის წილმა 78% შეადგინა.</u>** ცხრილში წარმოდგენილი პროცენტული განაწილება და მნიშვნელოვანი მომწოდებლების გადანაწილება:



აღნიშნული მიმართულებით **2021-2023 წლებში მოხდა ამერიკის მიერ სანქცირებული მომწოდებლების შემდეგი პროდუქტების შესყიდვა:**

შემსყიდველი	შესყიდვის #	მიმწოდებელი	პროდუქტი	კომპანია
საქართველოს შინაგან საქმეთა სამინისტრო	NAT230004024	ნეოტექი	ვიდეო დომოფონი	Hangzhou Hikvision Digital Technology Co.,Ltd/
შინაგან საქმეთა სამინისტრო საჯარო სამართლის იურიდიული პირი საზოგადოებრივი	NAT210021971	ნეოტექი	კომუტატორი	Hangzhou Hikvision Digital Technology Co.,Ltd

უსაფრთხოების მართვის ცენტრი „112“				

კრიტიკული ინფორმაციული სისტემის სუბიექტების მიერ 2021-2023 წლებში **შესყიდული IP ტელეფონების 50% ჩინური წარმოების მოწყობილობებია:**

შემსყიდველი		**თარიღი**	**მიმწოდებელი**	**კომპანია**
საქართველოს შინაგან საქმეთა სამინისტრო	NAT230021734	2023-11-15	ტელკო სისტემს	Fanvil Technology Co., Ltd
საქართველოს შინაგან საქმეთა სამინისტრო	NAT230011937	2023-06-20	ტელკო სისტემს	Fanvil Technology Co., Ltd
სსიპ „ინფორმაციული ტექნოლოგიების სააგენტო“	NAT230011610	2023-06-09	შპს ემ კა ეს	Fanvil Technology Co., Ltd
საქართველოს შინაგან საქმეთა სამინისტრო	NAT230008266	2023-04-24	შპს მკს	Yealink Network Technology Co.,
საქართველოს შინაგან საქმეთა სამინისტრო	NAT230006420	2023-04-03	ტელკო სისტემს	Fanvil Technology Co., Ltd
სპეციალური პენიტენციური სამსახური	NAT230005893	2023-03-24	ტელკო სისტემს	Fanvil Technology Co., Ltd
სახელმწიფო სერვისების განვითარების სააგენტო	SPA230000664	2023-03-22	ტელკო სისტემს	Fanvil Technology Co., Ltd
საქართველოს განათლებისა და მეცნიერების სამინისტრო	NAT230003142	2023-02-24	ტელკო სისტემს	Fanvil Technology Co., Ltd
საქართველოს სახელმწიფო უსაფრთხოების სამსახურის სსიპ - საქართველოს ოპერატიულ-ტექნიკური სააგენტო	SPA230000350	2023-02-16	შპს ინტელკომ ჯგუფი	YEALINK (XIAMEN) NETWORK TECHNOLOGY CO., LTD
საქართველოს შინაგან საქმეთა სამინისტრო	NAT210022032	2021-12-03	შპს ინტელკომ ჯგუფი	YEALINK (XIAMEN) NETWORK TECHNOLOGY CO., LTD
საქართველოს შინაგან საქმეთა სამინისტრო	NAT210010456	2021-07-05	შპს ინტელკომ ჯგუფი	YEALINK (XIAMEN) NETWORK TECHNOLOGY

საქართველოს მთავარი პროკურატურა	NAT210009279	2021-06-02	შპს ინტელკომ ჯგუფი	YEALINK (XIAMEN) NETWORK TECHNOLOGY
საქართველოს შინაგან საქმეთა სამინისტრო	NAT210008148	2021-05-17	შპს გეიმინგ რუმი	YEALINK (XIAMEN) NETWORK TECHNOLOGY
სპეციალური პენიტენციური სამსახური	NAT210006782	2021-04-22	ტელკო სისტემს	Fanvil Technology Co., Ltd
სპეციალური პენიტენციური სამსახური	NAT220018200	2022-09-14	ტელკო სისტემს	Fanvil Technology Co., Ltd
საქართველოს შინაგან საქმეთა სამინისტრო	NAT220006883	2022-04-18	შპს ინტელკომ ჯგუფი	YEALINK (XIAMEN) NETWORK TECHNOLOGY
საქართველოს სახელმწიფო უსაფრთხოების სამსახური	SPA220000707	2022-03-21	შპს ინტელკომ ჯგუფი	YEALINK (XIAMEN) NETWORK TECHNOLOGY
შინაგან საქმეთა სამინისტროს საქვეუწყებო დაწესებულება სასაზღვრო პოლიცია	NAT220003948	2022-03-07	ტელკო სისტემს	Fanvil Technology Co., Ltd
საქართველოს შინაგან საქმეთა სამინისტრო	NAT220001916	2022-02-09	შპს ინტელკომ ჯგუფი	YEALINK (XIAMEN) NETWORK TECHNOLOGY

3.3. სერვისების შესყიდვა

ICT მიწოდების ჯაჭვის უსაფრთხოების ერთ-ერთ მნიშვნელოვან მიმართულებას წარმოდგენს **მიწოდებული სერვისების უსაფრთხოება.** კერძოდ, სერვისებში შეიძლება მოიაზრებოდეს როგორც პროგრამული უზრუნველყოფის შე**მუშავება, ასევე, მზა პროგრამული უზრუნველყოფისთვის მხარდაჭერის სერვისების მიწოდება.** ამ მხრივ, გამოწვევას წარმოადგენს სერვისის მიმწოდებელი **კომპანიების წარმომავლობის დადგენა და ამ სერვისის გაწევაში ჩართული პირების იდენტიფიცირება.**

მაგალითისთვის, სახელმწიფო უწყებამ შესაძლოა შეისყიდოს დასავლური პროდუქტი (მაგ. Microsoft, Oracle, Norton, CISCO, VMware , etc.), თუმცა, დანერგვა განხორციელდეს ზემოხსენებული **კომპანიის მოსკოვის ოფისიდან, ადგილობრივი თანამშრომლობის ჩართულობით. ასევე, აღნიშნული თანამშრომლები შესაძლოა ხშირად ჩართული იყვნენ**

ინციდენტების ან სერვის მოთხოვნების მოგვარებაში. ***<u>აღნიშნული შემთხვევების იდენტიფიცირების საშუალება არ გვეძლევა სახელმწიფო შესყიდვების სისტემაში არსებული მონაცემების ანალიზით.</u>***

ზემოხსენებული შეზღუდვის გათვალისწინებით, კვლევის მიზნებისათვის შეირჩა რამდენიმე საქართველოში რეგისტრირებული კომპანია, რომელიც კლასიკური გაგებით არღვევს უსაფრთხო მიწოდების ჯაჭვის მოთხოვნებს. მაგალითისთვის, ICT სერვისების მიმართულებით, ერთ-ერთ მსხვილ მიმწოდებელ ორგანიზაციას წარმოადგენს შპს „სოფთლაინ საქართველო“, რომლის 90% წილი ეკუთვნის „Noventiq Holdings PLC“. აღნიშნული კომპანიის დამაარსებელი და ჰოლდინგის მფლობელი კი არის რუსი ბიზნესმენი იგორ ბოროვიკოვი. შპს „სოფთლაინ საქართველოს“ მიერ მიწოდებული სერვისები კრიტიკული ინფორმაციული სისტემის სუბიექტებისათვის:

შემსყიდველი	შესყიდვის #	მთავარი CPV	თარიღი	ღირებულება
საქართველოს ცენტრალური საარჩევნო კომისია	NAT230016576	დოკუმენტების, გრაფიკული გამოსახულებების შექმნის, გამოსახულების დამუშავების, დაგეგმვისა და წარმადობის გაზრდის პროგრამული პაკეტები (48300000)	2023-08-19	7700
საქართველოს ცენტრალური საარჩევნო კომისია	NAT230013649	დოკუმენტების, გრაფიკული გამოსახულებების შექმნის, გამოსახულების დამუშავების, დაგეგმვისა და წარმადობის გაზრდის პროგრამული პაკეტები (48300000)	2023-07-08	12872.86
საფინანსო-ანალიტიკური სამსახური	NAT230013463	მონაცემთა ბაზისა და ოპერაციული პროგრამული პაკეტები (48600000)	2023-07-07	73600
აჭარის ავტონომიური რესპუბლიკის მთავრობის აპარატი	NAT230011424	ქსელები (32400000)	2023-06-05	74820
საქართველოს შსს. დაცვის პოლიციის დეპარტამენტი	NAT230005091	პროგრამული უზრუნველყოფის შემუშავება და საკონსულტაციო მომსახურებები (72200000)	2023-03-17	22100

სსიპ საპენსიო სააგენტო	SPA210003302	მონაცემთა ბაზისა და ოპერაციული პროგრამული პაკეტები (48600000)	2021-12-11	319850
საზღვაო ტრანსპორტის სააგენტო	NAT210018053	კომპიუტერული მოწყობილობები და აქსესუარები (30200000)	2021-09-25	16740
საფინანსო-ანალიტიკური სამსახური	NAT210014481	საკომუნიკაციო და მულტიმედიის პროგრამული პაკეტები (48500000)	2021-08-09	22018
საფინანსო-ანალიტიკური სამსახური	NAT210014866	მონაცემთა ბაზისა და ოპერაციული პროგრამული პაკეტები (48600000)	2021-08-14	31000
შპს "საქართველოს ფოსტა"	GEO210000351	ქსელების, ინტერნეტისა და ინტრანეტის პროგრამული პაკეტები (48200000)	2021-06-27	131685
საქართველოს ცენტრალური საარჩევნო კომისია	SPA210001400	დოკუმენტების, გრაფიკული გამოსახულებების შექმნის, გამოსახულების დამუშავების, დაგეგმვისა და წარმადობის გაზრდის პროგრამული პაკეტები (48300000)	2021-05-25	16512
საქართველოს პრეზიდენტის ადმინისტრაცია	SPA210000911	დოკუმენტების, გრაფიკული გამოსახულებების შექმნის, გამოსახულების დამუშავების, დაგეგმვისა და წარმადობის გაზრდის პროგრამული პაკეტები (48300000)	2021-04-10	11583.96
საქართველოს პარლამენტის აპარატი	NAT210003840	დოკუმენტების, გრაფიკული გამოსახულებების შექმნის, გამოსახულების დამუშავების, დაგეგმვისა და წარმადობის გაზრდის პროგრამული პაკეტები (48300000)	2021-03-07	17782.5
საფინანსო-ანალიტიკური სამსახური	NAT220025464	ქსელების, ინტერნეტისა და ინტრანეტის პროგრამული პაკეტები (48200000)	2022-12-09	81000
სსიპ საპენსიო სააგენტო	SPA220002816	პროგრამული უზრუნველყოფის შემუშავება და საკონსულტაციო მომსახურებები (72200000)	2022-11-26	56000

საზღვაო ტრანსპორტის სააგენტო	NAT220020501	მონაცემთა ბაზისა და ოპერაციული პროგრამული პაკეტები (48600000)	2022-10-14	17280
საფინანსო-ანალიტიკური სამსახური	NAT220014822	საკომუნიკაციო და მულტიმედიის პროგრამული პაკეტები (48500000)	2022-08-07	56924
შპს "საქართველოს ფოსტა"	GEO220000366	ქსელების, ინტერნეტისა და ინტრანეტის პროგრამული პაკეტები (48200000)	2022-07-10	146999.7
საფინანსო-ანალიტიკური სამსახური	NAT220011476	მონაცემთა ბაზისა და ოპერაციული პროგრამული პაკეტები (48600000)	2022-06-24	28400
საქართველოს პრეზიდენტის ადმინისტრაცია	SPA220000944	დოკუმენტების, გრაფიკული გამოსახულებების შექმნის, გამოსახულების დამუშავების, დაგეგმვისა და წარმადობის გაზრდის პროგრამული პაკეტები (48300000)	2022-04-09	11104.98
საქართველოს პარლამენტის აპარატი	NAT220005686	დოკუმენტების, გრაფიკული გამოსახულებების შექმნის, გამოსახულების დამუშავების, დაგეგმვისა და წარმადობის გაზრდის პროგრამული პაკეტები (48300000)	2022-03-28	17820

3.3.1. ინტერნეტ სერვის პროვაიდერები

სერვისების მიმართულებით ასევე ერთ ერთი საყურადღებო ფაქტია, ინტერნეტ სერვის პროვაიდერები (ISP). ადგილობრივი ISP გლობალური ქსელზე დაერთებისათვის იყენებს სხვადასხვა რეგიონულ ISP, რომლის საშუალებითაც, საბოლოო მომხმარებელს/მოქალაქეს ან/და შესაბამის საჯარო სტრუქტურას აწვდის ინტერნეტსერვისს.

კვლევის ფარგლებში იდენტიფიცირდა ინტერნეტ სერვის პროვაიდერი შპს „ჯორჯიანაირლინკი“, რომელიც კომპანიის გლობალურ ქსელზე დაერთებისათვის იყენებს რუსულ ინტერნეტ პროვაიდერებს.

შემსყიდველი	შესყიდვის #	სერვისის დასახელება	მომწოდებელი	რისკი
სს ,,საქართველოს რკინიგზა"	NAT230009423	ინტერნეტ მომსახურება	შპს ჯორჯიანაირლინკი	BGP დაერთება რუსეთთან
სს ,,საქართველოს რკინიგზა"	NAT210025669	ინტერნეტ მომსახურება	შპს ჯორჯიანაირლინკი	BGP დაერთება რუსეთთან
საქართველოს ცენტრალური საარჩევნო კომისია	SPA230002579	ინტერნეტ მომსახურება	შპს ჯორჯიანაირლინკი	BGP დაერთება რუსეთთან
საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტრო	SPA210000409	ინტერნეტ მომსახურება	შპს ჯორჯიანაირლინკი	BGP დაერთება რუსეთთან
საქართველოს ცენტრალური საარჩევნო კომისია	SPA210003488	ინტერნეტ მომსახურება	შპს ჯორჯიანაირლინკი	BGP დაერთება რუსეთთან
საქართველოს ცენტრალური საარჩევნო კომისია	SPA210000315	ინტერნეტ მომსახურება	შპს ჯორჯიანაირლინკი	BGP დაერთება რუსეთთან

3.3.2. ტელეკომუნიკაციები

ტელეკომუნიკაციების სექტორი არ წარმოადგენდა წინამდებარე კვლევის სიღრმისეული შესწავლის ანალიზს, თუმცა გამოკვეთილი გარემოებები მნიშვნელოვან ასპექტს წარმოადგენს ქვეყნის ეროვნული უსაფრთხოების ჭრილში. კერძოდ, საყურადღებოა საჯარო სექტორის და მათ შორის CII დამოკიდებულება რუსულ კომპანიებზე ტელეკომუნიკაციების მიმართულებით.

ზემოაღნიშნული დამოკიდებულების მნიშვნელოვანი მაჩვენებელია საქართველოს მთავრობის მიერ 2018 წელს გამოცხადებული კონსოლიდირებული ტენდერი 2018-2019 წლებში მობილური სატელეფონო კავშირის მომსახურების შესყიდვის მიმართულებით. კონსოლიდირებული ტენდერის საფუძველზე გამარჯვებულად გამოცხადდა 3 კომპანია, მათ შორის იყო შპს „ვიონ საქართველო“. შპს „ვიონ საქართველო“ საქართველოს ბაზარზე ოპერირებდა რუსული კავშირგაბმულობის კომპანიის „ბილაინი“ სახელით და წარმოადგენდა VEON LTD

წარმომადგენლობას საქართველოში. 2022 წლამდე კომპანიის მმართველ საბჭოში იყო რუსი სანქცირებული ბიზნესმენი მიხეილ ფრიდმანი, რომელიც სანქცირების შემდგომ გადადგა დაკავებული პოზიციიდან.

აღსანიშნავია, რომ 2018 წელს გამოცხადებული კონსოლიდირებული ტენდერის საფუძველზე, შპს „ვიონ საქართველო“ („სილქნეტსა“ და „მაგთისთან“ ერთად) 2020 წლიდან 2022 წლამდე, უზრუნველყოფდა საქართველოს საჯარო სექტორისათვის ფიჭური კავშირგაბმულობის სერვისის მიწოდებას. მათ შორის აღსანიშნავია, რომ კონსოლიდირებული ტენდერის საფუძველზე გამარტივებული შესყიდვით, აღნიშნულ წლებში შესყიდვა გააკეთა ორმა კრიტიკული ინფორმაციული სისტემის სუბიექტმა, როგორიც არის, საქართველოს ფოსტა და სსიპ „საჯარო რეესტრის ეროვნული სააგენტო“.

კომპანია არსებული მდგომარეობით შპს „სელფი მობაილის“ (204450584) დასახელებით ოპერირებს და 2023 წელს რებრენდინგის საფუძველზე ბაზარზე ოპერირებს, როგორც „სელფი“. 2022 წელს კომპანიის შესყიდვა განახორციელა ქართველმა წარმომადგენლობამ.

4. თავი 4: საქართველოს კონტექსტი და რეკომენდაციები

4.1. საქართველოს კონტექსტი

4.1.1. ძირითადი რეგულაციები და აქტები

საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“ წარმოადგენს საქართველოს ინფორმაციული და კიბერუსაფრთხოების გარემოს ძირითად მარეგულირებელ დოკუმენტს. კანონის განახლებული (2020 წლის ვერსიის) მიხედვით, საქართველოში აღიარებულია კრიტიკული ინფორმაციული ინფრასტრუქტურის 3 სექტორი:

- *პირველი კატეგორია* - ***სახელმწიფო უწყებები***
- *მეორე კატეგორია* - ***სატელეკომუნიკაციო სექტორი***
- *მესამე კატეგორია* - ***ჯერძო სექტორი***

ზემოხსენებულ სექტორებს ევალდებულებათ ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დაკმაყოფილება. აღნიშნული მოთხოვნები, თავის მხრივ, ეფუძნება ISO/IEC 27001:2013 ინფორმაციული უსაფრთხოების მართვის სისტემის სტანდარტს. გარდა ამისა, საკუთარი მანდატის ფარგლებში, **მარეგულირებელი ორგანოები გამოსცემენ ინფორმაციული და კიბერუსაფრთხოების რეგულაციებს,** რომელიც ასევე სავალდებულოა შესასრულებლად კრიტიკული ინფორმაციული სისტემის სუბიექტებისთვის.

4.1.2. სამთავრობო უწყებების როლი

სსიპ ოპერატიულ-ტექნიკური სააგენტო

> **პირველი და მეორე კატეგორიის** კრიტიკული ინფორმაციული სისტემის სუბიექტების ზედამხედველობაზე პასუხისმგებელია სახელმწიფო უსაფრთხოების სამსახურის ქვე-უწყება სსიპ „ოპერატიულ-ტექნიკური სამსახური“. სააგენტო გამოსცემს კანონქვემდებარე აქტებს და უზრუნველყოფს სექტორის ზედამხედველობას.

სსიპ ციფრული მმართველობის სააგენტო

> **მესამე კატეგორიის** კრიტიკული ინფორმაციული სისტემის სუბიექტების ზედამხედველობაზე პასუხისმგებელია იუსტიციის სამინისტროს ქვე-უწყება სსიპ „ციფრული მმართველობის სააგენტო“.

საქართველოს ეროვნული ბანკი

> **საფინანსო სექტორის ზედამხედველობას** უზრუნველყოფს საქართველოს ეროვნული ბანკი, რომელიც შეიმუშავებს როგორც საოპერაციო რისკების, ასევე, კიბერრისკების შესახებ სპეციფიურ რეგულაციებს, რომელიც სავალდებულოა საფინანსო უწყებებისთვის.

4.1.3. გამოწვევები და სისუსტეები

საქართველოს კიბერუსაფრთხოების გარემოს ანალიზი საჭიროებს დამატებით, მიუკერძოებელ და სიღრმისეულ შესწავლას, თუმცა, **კვლევის მიზნებიდან გამომდინარე,** აქცენტი გაკეთდება რამდენიმე მნიშვნელოვან გამოწვევაზე:

#	გამოწვევა	განმარტება
1	კრიტიკული ინფრასტრუქტურის განსაზღვრა	საქართველოში არ არის განსაზღვრული კრიტიკული ინფრასტრუქტურა. არსებული მდგომარეობით, განსაზღვრულია მხოლოდ კრიტიკული ინფორმაციული ინფრასტრუქტურა.
2	კრიტიკული ინფორმაციული სისტემის სუბიექტების დაბალი სიმწიფე	მიუხედავად იმისა, რომ ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები დადგენილია 2012 წლიდან, საჯარო სექტორში (პირველ კატეგორიაში), 70 უწყებიდან მხოლოდ 2 უწყება არის სერტიფიცირებული.
3	უცხო ქვეყნის მიერ დაფინანსებული კიბერშეტევები	2007-2024 წლებში საქართველოში არაერთი მსხვილმასშტაბიანი კიბერშეტევა მოხდა, რომლის უკან, მიკუთვნების მაღალი სანდოობით, იდგა სახელმწიფოს მიერ დაფინანსებული ჰაკერული დაჯგუფებები.
4	კადრების დეფიციტი	კიბერუსაფრთხოების კვალიფიკაციური კადრების დეფიციტია როგორც გლობალურ, ასევე, ლოკალურ ბაზარზე. ხშირად, ერთმანეთს კონკურენციას უწევს საერთაშორისო კომპანია, ადგილობრივი კერძო ორგანიზაცია და საჯარო სექტორი.
5	სუსტი მარეგულირებელი ჩარჩო	ინფორმაციული უსაფრთხოების მოთხოვნების ძირითადი მარეგულირებელი მოთხოვნები დამტკიცდა 2012-2013 წელს და 2020 წლამდე თვისობრივად არ განახლებულა. ამასთან, არ არსებობს ICT **მიწოდების ჯაჭვის რეგულაციები არცერთი კრიტიკული სექტორისთვის.**
6	მრავალშრიანი მიდგომა	ეროვნული კიბერუსაფრთხოების უზრუნველყოფა არის კოლექტიური პასუხისმგებლობა. არ შეიძლება ჩაითვალოს, რომ აღნიშნული არის მხოლოდ ეროვნული მარეგულირებლის პასუხისმგებლობა. ICT მიწოდების ჯაჭვის უზრუნველყოფაში ჩართული უნდა იყოს ყველა მნიშვნელოვანი აქტორი.
7	სუსტი ეკოსისტემა	ადგილობრივ ბაზარზე წარმოდგენილია მცირე რაოდენობის IT კომპანია (არა-ინტეგრატორი კომპანია) და ანალიტიკური ორგანიზაცია (Think Tank), რაც ართულებს ეკოსისტემის განვითარებისთვის ქმედითი ნაბიჯების გადადგმას.

4.2. ხედვა და რეკომენდაციები

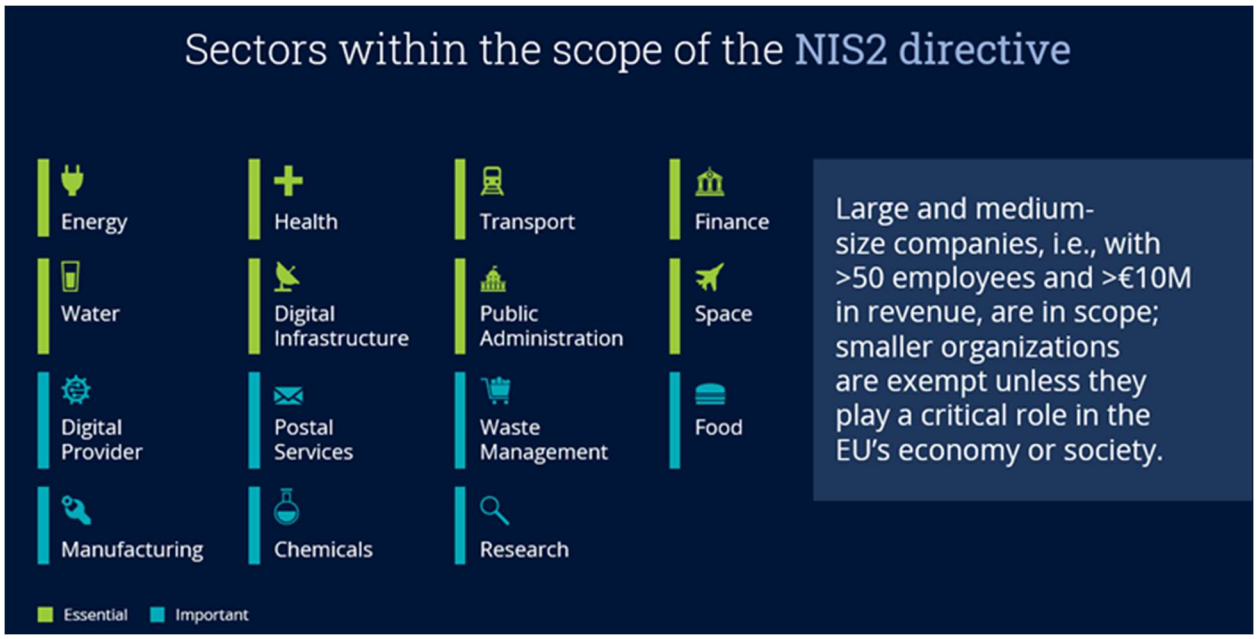
წინამდებარე თავში წარმოდგენილია ჩვენი ხედვა და რეკომენდაციების საქართველოს ICT მიწოდების ჯაჭვის უსაფრთხოების უზრუნველყოფისათვის. ამასთან, ჩვენი ხედვისა და რეკომენდაციების მომზადებისას, ***კრიტიკულად მნიშვნელოვანი ფაქტორია ევროკავშირის რეგულაციებთან ჰარმონიზაციის კომპონენტი.*** შედეგად, მომზადებული რეკომენდაციები მნიშვნელოვანი იქნება ევროკავშირში ქვეყნის ინტეგრაციის პროცესის წარმართვისას.

ამასთან, კრიტიკულად მნიშვნელოვანია, რომ **პირველ რიგში, უზრუნველყოფილი იქნეს კიბერუსაფრთხოების ეკოსისტემის სწორი, დაბალანსებული და ეფექტიანი არქიტექტურა, ადეკვატურად იქნეს გადანაწილებული როლები და პასუხისმგებლობები.** შესაბამისად, შემოთავაზებულ რეკომენდაციებში წარმოდგენილია არამხოლოდ ICT მიწოდების ჯაჭვებთან დაკავშირებული რეკომენდაციები.

4.2.1. კრიტიკული ინფრასტრუქტურისა და კრიტიკული სისტემების განსაზღვრა

კრიტერიუმი და საერთაშორისო პრაქტიკის მაგალითები

NIS2 დირექტივის შესაბამისად, ევროკავშირის წევრ ქვეყნებში განსაზღვრულია კრიტიკული სექტორები. ამასთან, გამიჯნულია მნიშვნელოვანი და ძირითადი კატეგორიის ორგანიზაციები სპეციფიური კრიტერიუმების საფუძველზე. ჯამურად, სახეზეა 15 სექტორი.



ევროკავშირის პრაქტიკის მსგავსად, აშშ განსაზღვრულია კრიტიკული სექტორები - 16 სექტორი.

მიუხედავად იმისა, რომ **თითოეულ სექტორს შეიძლება ყავდეს მარეგულირებელი, კიბერუსაფრთხოების სფეროში,** გამოყოფილია **ცენტრალური, მთავარი**

<u>მარეგულირებელი უწყება ეროვნულ დონეზე.</u> ევროკავშირის შემთხვევაში - **ევროკავშირის კიბერუსაფრთხოების სააგენტო (ENISA), ხოლო აშშ შემთხვევაში - კიბერუსაფრთხოების და ინფრასტრუქტურის უსაფრთხოების სააგენტო (CISA).**

<u>ფაქტობრივი მდგომარეობა და გამოწვევები</u>

კვლევის მიმდინარეობისას, არ არსებობს ეროვნულ დონეზე შეფასებული და განსაზღვრული კრიტიკული ინფრასტრუქტურა. ამასთან, განსაზღვრულია კრიტიკული **ინფორმაციული ინფრასტრუქტურის 3 სექტორი / კატეგორია, რაც არასაკმარისია.** გამოწვევას წარმოადგენს მეთოდოლოგიის შემუშავება და პრაქტიკაში იმპლემენტაცია. ამასთან, გამოწვევას წარმოადგენს კრიტიკული ინფორმაციული სისტემის სუბიექტების ერთიანად დადგენა და განსაზღვრა.

<u>რეკომენდაცია</u>

1. ყველა დაინტერესებული მხარის ჩართულობით, დამტკიცდეს საქართველოს კრიტიკული ინფრასტრუქტურის პირველადი სექტორული სია.
2. საწყის ეტაპზე, მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტებს გამოეყოს ყველა ის სექტორი, რომელიც სიმწიფის მაღალ დონეზეა და რომელსაც უკვე ყავს **<u>ინსტიტუციურად ძლიერი სექტორული მარეგულირებელი. საწყის ეტაპზე, ასეთი სექტორებია საფინანსო და ენერგო სექტორები.</u>**

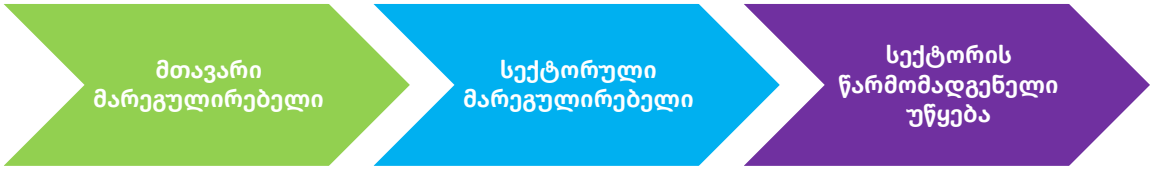
4.2.2. როლების გადანაწილება და კოორდინაცია

<u>მოდელი</u>

კიბერუსაფრთხოების არქიტექტურის შემუშავებისას, აუცილებელია, სწორად მოხდეს **როლებისა და პასუხისმგებლობების გადანაწილება.** ევროპულ პრაქტიკაზე დაყრდნობით, სექტორული მოდელი შეიძლება ჩამოყალიბდეს შემდეგნაირად:

კიბერუსაფრთხოების მთავარი მარეგულირებელი უწყება	•შეიმუშავებს ეროვნულ მიდგომას, პოლიტიკებსა და რეგულაციებს •უზრუნველყოფს კოორდინაციას
სექტორული მარეგულირებელი უწყება	•შეიმუშავებს სექტორისთვის მორგებულ პოლიტიკებსა და რეგულაციებს, რომელიც თანხვედრაშია მთავარი მარეგულირებლის მიერ შემუშავებულ რეგულაციებთან •უზრუნველყოფს სექტორული რეგულაციების აღსრულების ზედამხედველობას
კრიტიკული სუბიექტი / კრიტიკული სისტემა	•უზრუნველყოფს რეგულაციების შესრულებას

წინამდებარე ქვეთავებში წარმოდგენილი მიდგომა ეფუძნება ზემოხსენებულ მოდელს: **მთავარი მარეგულირებელი -> სექტორული მარეგულირებელი -> სექტორის წარმომადგენელი უწყება.** ანალოგიურად, **ძირითადი მარეგულირებელი პოლიტიკა -> სექტორისთვის სპეციფიური პოლიტიკა** (მაგალითად, NIS2 დირექტივა -> DORA).



4.2.2.1. როლი 1: კიბერუსაფრთხოების მთავარი მარეგულირებელი უწყება

<u>კრიტერიუმი და საერთაშორისო პრაქტიკის მაგალითები</u>

NIS2 დირექტივის შესაბამისად, აუცილებელია არსებობდეს ცენტრალური მაკოორდინირებელი უწყება და კომპიუტერულ ინციდენტებზე რეაგირების ეროვნული ჯგუფი (CSIRT). აღნიშნულის მიზანია, ეროვნული დონის კიბერშეტევებისას ან კრიზისებისას, **უზრუნველყოს უწყებათაშორისი კოორდინაცია და ასევე, საჭიროების შემთხვევაში ევროკავშირის კიბერუსაფრთხოების სააგენტოს (ENISA) კიბერკრიზისების ქსელთან (CyCLONe) ინფორმაციის გაზიარება.**

აშშ-სა და ევროკავშირის პრაქტიკის ანალიზი აჩვენებს, რომ კრიტიკული ინფრასტრუქტურის ძირითადი მარეგულირებელი და ზედამხედველი ორგანიზაცია არის **ძალოვანი უწყება, შესაბამისი მანდატითა და აღსრულების მექანიზმებით.**

აშშ-ს შემთხვევაში, აღნიშნულ როლს ასრულებს აშშ სამშობლოს უსაფრთხოების დეპარტამანეტის (Department of Homeland Security) ქვე-უწყება კიბერუსაფრთხოებისა და ინფრასტრუქტურის დაცვის სააგენტო (Cybersecurity and Infrastructure Security Agency – CISA). ანალოგიურად, **ევროკავშირის წევრი ქვეყნების უმრავლეს შემთხვევაში, აღნიშნულ როლს უზრუნველყოფენ ძალოვანი უწყებები** (შინაგან საქმეთა სამინისტრო, სახელმწიფო უსაფრთხოების სამსახური, თავდაცვის სამინისტრო).

#	Country	Ministry	Sub-ordinated Agency	CERT Name
1	Austria	Federal Chancellery	Federal Ministry of Interior	CERT.at
2	Belgium	Prime Minister's Office	Centre for Cybersecurity Belgium (CCB)	CERT.be
3	Bulgaria	Ministry of Transport, Information Technology and Communications	State e-Government Agency	CERT Bulgaria
4	Croatia	Ministry of the Interior	Croatian National CERT (CARNET)	CERT.hr
5	Cyprus	Ministry of Transport, Communications and Works	Office of the Commissioner of Electronic Communications and Postal Regulations (OCECPR)	CY-CERT
6	Czech Republic	Ministry of Interior	National Cyber and Information Security Agency (NÚKIB)	GOVCERT.CZ
7	Denmark	Ministry of Defence	Centre for Cyber Security (CFCS)	DK-CERT

8	Estonia	Ministry of Economic Affairs and Communications	Estonian Information System Authority (RIA)	CERT-EE
9	Finland	Ministry of Transport and Communications	Finnish Transport and Communications Agency (Traficom)	NCSC-FI
10	France	Prime Minister's Office	National Cybersecurity Agency of France (ANSSI)	CERT-FR
11	Germany	Federal Ministry of the Interior	Federal Office for Information Security (BSI)	CERT-Bund
12	Greece	Ministry of Digital Governance	Hellenic Cyber Security Authority	GR-CERT
13	Hungary	Ministry of Interior	National Cyber Security Center (NCSC)	GovCERT-Hungary
14	Ireland	Department of Environment, Climate and Communications	National Cyber Security Centre (NCSC)	IRL-CERT
15	Italy	Prime Minister's Office	National Cybersecurity Agency (ACN)	CERT-PA
16	Latvia	Ministry of Defence	Information Technology Security Incident Response Institution (CERT.LV)	CERT.LV
17	Lithuania	Ministry of National Defence	National Cyber Security Centre (NKSC)	CERT-LT
18	Luxembourg	Ministry of the Economy	Cybersecurity Competence Centre Luxembourg (C3)	CIRCL
19	Malta	Ministry for Finance and Financial Services	Malta Information Technology Agency (MITA)	MaltaCERT
20	Netherlands	Ministry of Justice and Security	National Cyber Security Centre (NCSC-NL)	CERT-EU
21	Poland	Ministry of the Interior and Administration	The Internal Security Agency (ABW)	CERT.PL
22	Portugal	Ministry of National Defence	National Cybersecurity Centre (CNCS)	CERT.PT
23	Romania	Ministry of Internal Affairs	National Cyber Security Directorate (DNSC)	RoCERTS
24	Slovakia	National Security Authority	National Security Authority (NBÚ)	SK-CERT
25	Slovenia	Ministry of Public Administration	Slovenian Information Security Administration (AKOS)	SI-CERT

26	Spain	Ministry of Economic Affairs and Digital Transformation	National Cybersecurity Institute of Spain (INCIBE)	CCN-CERT
27	Sweden	Ministry of Justice	Swedish Civil Contingencies Agency (MSB)	CERT-SE

ფაქტობრივი მდგომარეობა და გამოწვევები

NIS2 დირექტივის შესაბამისად, **ცალსახად იყოს განსაზღვრული როგორც ცენტრალიზებული / ძირითადი მარეგულირებელი, ასევე, ეროვნული ცერტის სტატუსიც.**

ინფორმაციული უსაფრთხოების შესახებ საქართველოს კანონის თანახმად, სსიპ **ოპერატიულ-ტექნიკური სააგენტო** წარმოადგენს პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების ზედამხედველ ორგანოს. ამასთან, ეროვნული კიბერკრიზისის დროს, **სააგენტო უფლებამოსილი ხდება უხელმძღვანელოს უწყებათაშორის კოორდინაციას.** შესაბამისად, აღნიშნული უფლებამოსილება ავტომატურად უნდა მოიაზრებდეს, რომ ოპერატიულ-ტექნიკური სააგენტოს ცერტი წარმოადგენს ეროვნულ ცერტს.

თუმცა, ბუნდოვანია ეროვნული CERT-ის სტატუსი. სოციალურ ქსელში (Facebook), საქართველოს ეროვნული CERT-ის გვერდზე მითითებულია სსიპ ციფრული მმართველობის სააგენტო. ასევე, ინფორმაციული უსაფრთხოების კანონი (სფეროს ძირითადი მარეგულირებელი დოკუმენტი) ცალსახად არ ადგენს ეროვნული ცერტის სტატუსს.

კვლევის მიმდინარეობისას, **არ არსებობს ICT მიწოდების ჯაჭვის უსაფრთხოებასთან დაკავშირებული სპეციფიური** რეგულაცია კრიტიკული ინფორმაციული სისტემის სუბიექტებისთვის. ასევე, გამოწვევას წარმოადგენს უწყების ორგანიზაციული და პოლიტიკური დამოუკიდებლობა, საზოგადოების ნდობა და ანგარიშვალდებულება.

რეკომენდაცია

1. კიბერუსაფრთხოების მთავარი მარეგულირებელი ორგანოს დეპოლიტიზირება, დამოუკიდებლობისა და ანგარიშვალდებულების გაზრდა. აღნიშნულისათვის, სსიპ „ოპერატიულ-ტექნიკური სააგენტოს“ სახელმწიფო ინფორმაციული და კიბერუსაფრთხოების ცენტრის გაძლიერება და ცალკეული უწყების - **ეროვნული კიბერუსაფრთხოების ცენტრის ჩამოყალიბება**. შედეგად, საკითხის მნიშვნელობის ხაზგასმა, ადექვატური რესურსების მობილიზება და საზოგადოებაში ნდობის ამაღლება, რაც ხელს შეუწყობს ეროვნული კრიტიკული ინფრასტრუქტურის დაცვას.
2. სსიპ **ოპერატიულ-ტექნიკური სააგენტოს ცერტს მიენიჭოს ეროვნული ცერტის სტატუსი და გამოირიცხოს გადაფარული** პასუხისმგებლობები.

3. სსიპ ოპერატიულ-ტექნიკურმა **სააგენტომ შეიმუშაოს და დაამტკიცოს ICT მიწოდების ჯაჭვის უსაფრთხოების პოლიტიკა,** რომელიც იქნება ძირითადი მარეგულირებელი დოკუმენტი საქართველოს კრიტიკული ინფრასტრუქტურისთვის.

4.2.2.2. როლი 2: საფინანსო სექტორის მარეგულირებელი უწყება

<u>კრიტერიუმი და საერთაშორისო პრაქტიკის მაგალითები</u>

ციფრული საოპერაციო მედეგობის აქტის (DORA) შესაბამისად, საფინანსო ინსტიტუციებს უჩნდებათ ვალდებულება, სხვა მოთხოვნებთან ერთად, **დაიცვან ICT მიწოდების ჯაჭვის უსაფრთხოების მოთხოვნები.** ამასთან, ინსტიტუციებისთვის ჩნდება ვალდებულება სხვა უწყებებთან ერთად, ცენტრალურ ბანკს გაუზიარონ ინციდენტების შესახებ ინფორმაცია. აღნიშნულში მოიაზრება როგორც ევროკავშირის ცენტრალური ბანკი, ასევე, ევროკავშირის კიბერუსაფრთხოების სააგენტო (ENISA), რაც თანხვედრაშია წინა თავში წარმოდგენილ მოდელთან. დამატებით, NIS2 დირექტივის თანახმად, საბანკო სფერო ექცევა რეგულაციის სფეროში.

<u>ფაქტობრივი მდგომარეობა და გამოწვევები</u>

ინფორმაციული უსაფრთხოების შესახებ საქართველოს კანონისა საფუძველზე, **მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტებად განისაზღვრა კომერციული ბანკების (საფინანსო ინსტიტუტების) ნაწილი.** შესაბამისად, სსიპ **ციფრული მმართველობის სააგენტოს მანდატი გავრცელდა** ამ ორგანიზაციებზე. თუმცა, მეორეს მხრივ, **საქართველოს ეროვნული ბანკი წარმოადგენს მთავარ მარეგულირებელ (კომპეტენტურ) ორგანოს** საფინანსო ინსტიტუტების ზედამხედველობისთვის.

აღსანიშნავია, **<u>რომ ეროვნულ ბანკს, განსხვავებით ციფრული მმართველობის სააგენტოსი,</u>** გააჩნია სფეროს რეგულირების უფრო ხანგრძლივი ინსტიტუციური გამოცდილება და ქმედითი მექანიზმები. არსებობს და პრაქტიკაში ქმედითია ეროვნული ბანკის რეგულაციები საოპერაციო რისკების მართვის, კიბერუსაფრთხოების ჩარჩოს, SWIFT სისტემასთან თავსებადობისა და შეღწევადობის ტესტირების მიმართულებით. ამასთან, **ეროვნული ბანკის ICT ინფრასტრუქტურა, საკუთარი უსაფრთხოების შესაძლებლობები (ერთ-ერთი საჯარო დაწესებულებაა რომელიც აკმაყოფილებს ISO/IEC 27001) და სიმწიფე უფრო განვითარებულია.**

კვლევის მიმდინარეობისას, არ არსებობდა **საქართველოს საფინანსო სექტორის ICT მიწოდების ჯაჭვის რეგულაცია**. ასევე, ბუნდოვანია რა როლი და დამოკიდებულება შეიძლება იყოს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების ზედამხედველს - სსიპ ციფრული მმართველობის სააგენტოსა და საფინანსო სექტორის მთავარ მარეგულირებელს - საქართველოს ეროვნულ ბანკს შორის. განსხვავებით ამერიკული და ევროპული პრაქტიკისგან, საქართველოს საფინანსო სექტორი არ წარმოადგენს ცალკეულ სექტორს კრიტიკული ინფორმაციული ინფრასტრუქტურის

განსაზღვრისას.

<u>რეკომენდაცია</u>

1. ევროკავშირის დირექტივებთან შესაბამისობისა და სექტორის საჭიროებების უზრუნველყოფისათვის, მნიშვნელოვანია, **<u>საფინანსო სექტორი გამოიყოს როგორც დამოუკიდებელი კრიტიკული სექტორი</u>**.
2. სექტორის რეგულირების ეფექტიანობის გაზრდისათვის, მიზანშეწონილია საფინანსო სექტორს **<u>ყავდეს კომპეტენტური მარეგულირებელი</u>**, რომელიც უზრუნველყოფს **სექტორზე მორგებული რეგულაციების შემუშავებას.** კერძოდ, გადაფარვების თავიდან აცილებისათვის, მიზანშეწონილია **<u>საფინანსო სექტორის კიბერრეგულაციებზე პასუხისმგებელი იყოს მხოლოდ საქართველოს ეროვნული ბანკი</u>**.
3. საფინანსო სექტორის ICT მიწოდების ჯაჭვის უსაფრთხოების უზრუნველყოფისათვის და ამასთან, ევროკავშირის დირექტივებთან ჰარმონიზაციის მიზნით, **ეროვნულმა ბანკმა მიიღოს DORA-სთან თავსებადი ICT მიწოდების ჯაჭვის უსაფრთხოების რეგულაციები.**

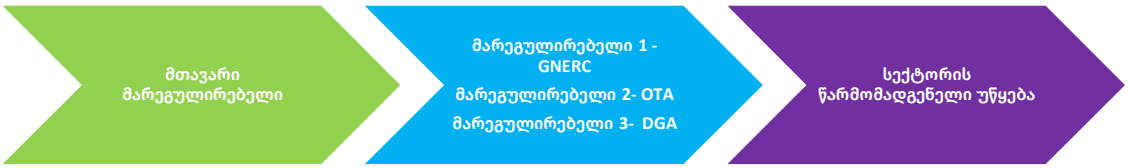
4.2.2.3. როლი 3: ენერგეტიკისა და წყალმომარაგების სექტორის მარეგულირებელი უწყება

<u>კრიტერიუმი და საერთაშორისო პრაქტიკის მაგალითები</u>

ევროკავშირისა და აშშ კრიტიკული ინფრასტრუქტურის მიმოხილვა აჩვენებს, რომ ენერგეტიკისა და წყალმომარაგების სექტორები წარმოადგენს ერთ-ერთ პრიორიტეტულ და დამოუკიდებელ სექტორს. მსგავსად საფინანსო სექტორისა, **ენერგეტიკისა და წყალმომარაგების სექტორს გააჩნია სექტორისთვის დამახასიათებელი საოპერაციო და კიბერუსაფრთხოების საჭიროებები. მაგალითისთვის, ფინანსური სექტორისგან განსხვავებით, ენერგო სექტორი აქტიურად იყენებს ინდუსტრიული კონტროლის სისტემებს (ICS) და შესაბამისად, შესაძლოა მეტი აქცენტი გააკეთოს საოპერაციო ტექნოლოგიების (OT) უსაფრთხოებაზე, ვიდრე ინფორმაციული ტექნოლოგიების (IT) დაცვაზე.** მნიშვნელოვანია, სექტორის მიმართ გამოყენებული იყოს ერთგვაროვანი მიდგომა და შემუშავებული იყოს სექტორზე მორგებული რეგულაციები.

<u>ფაქტობრივი მდგომარეობა და გამოწვევები</u>

კვლევის მიმდინარეობისას, საქართველოს კრიტიკული ინფორმაციული **ინფრასტრუქტურა არ ცნობდა ცალკეულად გამოყოფილ ენერგეტიკისა და წყალმომარაგების სექტორს.** სექტორებისა და შესაბამისი ორგანიზაციების განსაზღვრისას, რამდენიმე ენერგო **კომპანია განსაზღვრული იქნა როგორც მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი. თუმცა, მიმდინარე მდგომარეობით, სახელმწიფოს კუთვნილებაში / კონტროლის ქვეშ მყოფი ენერგო კომპანიების ნაწილი განსაზღვრულია, როგორც პირველი კატეგორიის სუბიექტები, ხოლო კერძო სექტორის მფლობელობაში არსებული ენერგო ორგანიზაციები მიეკუთვნება მესამე კატეგორიას.** ამასთან, არ არსებობს ენერგო სექტორის საჭიროებებზე მორგებული ICT მიწოდების ჯაჭვთან დაკავშირებული მოთხოვნები.



<u>რეკომენდაცია</u>

1. ენერგეტიკისა და წყალმომარაგების სექტორის კიბერუსაფრთხოების საჭიროებებისა და სფეროს მნიშვნელობის გათვალისწინებით, კრიტიკული ინფორმაციული სისტემის **სუბიექტებში ცალკეულ კატეგორიად გამოიყოს ენერგო და წყალმომარაგების** სექტორი.
2. სექტორის რეგულირების ეფექტიანობის გაზრდისათვის, მიზანშეწონილია ენერგეტიკისა და წყალმომარაგების სექტორს **<u>ყავდეს კომპეტენტური მარეგულირებელი</u>**, რომელიც უზრუნველყოფს **სექტორზე მორგებული რეგულაციების შემუშავებას.** კერძოდ, გადაფარვების თავიდან აცილებისათვის, მიზანშეწონილია **<u>ენერგეტიკისა და წყალმომარაგების სექტორის კიბერრეგულაციებზე პასუხისმგებელი იყოს მხოლოდ საქართველოს ენერგეტიკისა და წყალმომარაგების ეროვნული კომისია.</u>**

4.2.2.4. PFMS - ფინანსთა სამინისტრო და სახელმწიფო შესყიდვების სააგენტო

<u>კრიტერიუმი და საერთაშორისო პრაქტიკის მაგალითები</u>

აშშ გამოცდილება ცხადყოფს, რომ ფედერალური შესყიდვების უსაფრთხოების საბჭო (FASC) და კომერციის დეპარტამენტი ფლობს შესაბამის მანდატს დროულად უზრუნველყოს **რისკის შემცველი შესყიდვის იდენტიფიცირება და საჭიროების შემთხვევაში მიმდინარე ტრანზაქციის შეჩერება.**

<u>ფაქტობრივი მდგომარეობა და გამოწვევები</u>

კვლევის მიმდინარეობისას, სახელმწიფო შესყიდვების სააგენტოსა და საქართველოს ფინანსთა სამინისტროს არ გააჩნია ფორმალური როლი ICT და სერვისების მიწოდების ჯაჭვის უსაფრთხოების უზრუნველყოფაში.

<u>რეკომენდაცია</u>

1. სახელმწიფო შესყიდვების სააგენტომ უზრუნველყოს ICT მიწოდების ჯაჭვის უსაფრთხოებასთან დაკავშირებული მიღებული პოლიტიკებისა და სტრატეგიების აღსრულების მონიტორინგი **საკუთარი კომპეტენციის ფარგლებში.** კერძოდ, **უზრუნველყოს აკრძალული ICT და სერვისების შესყიდვების მცდელობის იდენტიფიკაცია და პრევენცია** სახელმწიფო შესყიდვების ერთიანი ელექტრონული სისტემის საშუალებით.
2. სახელმწიფო შესყიდვების სააგენტომ უზრუნველყოს ICT შესყიდვების შემთხვევაში სტანდარტული კონტრაქტუალური მოთხოვნების შემუშავება და იმპლემენტაციის მონიტორინგი.
3. საქართველოს ფინანსთა სამინისტრომ, **სახელმწიფო ხაზინასთან** ერთად, უზრუნველყოს იმ **ტრანზაქციების იდენტიფიცირება და პრევენცია,** რომელიც დაკავშირებულია ICT და სერვისის მიწოდების ჯაჭვის რეგულაციებით.

4.2.2.5. ეკონომიკის სამინისტრო და საგარეო საქმეთა სამინისტრო

<u>ფაქტობრივი მდგომარეობა და გამოწვევები</u>

კვლევის მიმდინარეობისას, საქართველოს ეკონომიკისა და მდგრადი განვითარების სააგენტოსა და საგარეო საქმეთა სამინისტროს არ გააჩნია არავითარი როლი ICT მიწოდების ჯაჭვის უსაფრთხოების უზრუნველყოფაში.

დამოუკიდებლობის მოპოვების შემდგომ, წლების მანძილზე, ერთ-ერთ მნიშვნელოვან გამოწვევას **წარმოადგენს რუსეთის ფედერაციის ICT ბაზარზე დამოკიდებულება**. კერძოდ, ICT და სერვისის მიმწოდებელი კომპანიების უმრავლესობა, საქართველოში პროდუქტებს ყიდდა რუსეთის (დსთ) ოფისის გავლით. ანალოგიურად, ICT პროდუქტების შესყიდვა, დანერგვა და მხარდაჭერა ძირითადად ხორციელდებოდა რუსეთის წარმომადგენლობის გავლით.

<u>რეკომენდაცია</u>

1. ICT და სერვისების მიწოდების ჯაჭვის უსაფრთხოების უზრუნველსაყოფად, **საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრომ, საქართველოს საგარეო სამინისტროს დახმარებით, უზრუნველყოფს მოლაპარაკება** დასავლურ კომპანიებთან უსაფრთხო ღირებულებათა და მიწოდების ჯაჭვების უზრუნველსაყოფად.

4.2.2.6. სახელმწიფო აუდიტის სამსახური

<u>კრიტერიუმი და საერთაშორისო პრაქტიკის მაგალითები</u>

სახელმწიფოს უმაღლესი მაკონტროლებელი კონსტიტუციური ორგანო, რომელიც ხელს უწყობს **საპარლამენტო ზედამხედველობის განხორციელებას.** აშშ გამოცდილება ცხადყოფს, რომ US Government Accountability Office აქტიურად მონაწილეობს ICT მიწოდების ჯაჭვის უსაფრთხოების უზრუნველყოფაში. მაგალითად, თავდაცვის ავტორიზაციის აქტში (NDAA), ისევე, როგორც სხვა აქტებში, მითითებულია, რომ აქტის მიღებიდან 150 დღის შემდეგ US GAO ჩაატარებს აუდიტს იმის დასადგენად თუ რამდენად ეფექტიანად შეასრულა თავდაცვის დეპარტამენტმა აქტით დაკისრებული ვალდებულება.

ევროკავშირის შემთხვევაში, NIS2 დირექტივა განსაზღვრავს ევროპის აუდიტორთა სასამართლოს (European Court of Auditors) უფლება-მოვალეობებს. ECA წარმოადგენს ევროკომისიისა და ევროპარლამენტის საზედამხედველო ინსტრუმენტს, რომელიც ამ ორგანოებს წარუდგენს დამოუკიდებელი, მიუკერძოებელ და პროფესიულ მოსაზრებებს.

<u>ფაქტობრივი მდგომარეობა და გამოწვევები</u>

კვლევის მიმდინარეობისას, სახელმწიფო აუდიტის სამსახურს არ გააჩნია ფორმალური როლი ICT და მიწოდების ჯაჭვის უსაფრთხოების უზრუნველყოფისათვის.

<u>რეკომენდაცია</u>

1. სახელმწიფო აუდიტის სამსახურმა უზრუნველყოს საქართველოს კონსტიტუციით დაკისრებული მოვალეობა, რაც სხვა დანარჩენთან ერთად, გულისხმობს **სახელმწიფო კრიტიკული ინფორმაციული ინფრასტრუქტურისა და სახელმწიფო მარეგულირებლების საქმიანობის შეფასებას.**
2. უზრუნველყოს **სახელმწიფო შესყიდვების რისკების რეესტრში ICT** და სერვისების მიწოდების რისკების გათვალისწინება და ყოველწლიური აუდირება.

4.2.2.7. საჯარო-კერძო თანამშრომლობა და Think Tank-ების გაძლიერება

<u>კრიტერიუმი და საერთაშორისო პრაქტიკის მაგალითები</u>

ევროკავშირისა და აშშ გამოცდილება ცხადყოფს, რომ **კერძო სექტორი წარმოადგენს ყველა მნიშვნელოვანი რეფორმის, სტრატეგიისა და პოლიტიკის განუყოფელ ნაწილს.** ამასთან, NIS2 და DORA მნიშვნელოვან ყურადღებას უთმობს საჯარო-კერძო თანამშრომლობის მექანიზმების შექმნასა და განვითარებას, რაც მოიცავს როგორც გამოცდილების გაზიარებას, ასევე, მნიშვნელოვანი ინციდენტების შესახებ ინფორმაციის გაზიარებასაც (cyber threat intelligence).

<u>ფაქტობრივი მდგომარეობა და გამოწვევები</u>

კიბერუსაფრთხოების საჯარო-კერძო თანამშრომლობის მექანიზმები განვითარების საწყის ეტაპზეა. მეორეს მხრივ, მნიშვნელოვანია, რომ ბაზარზე არ ხდება კიბერუსაფრთხოების Think Tank-ების ჩამოყალიბება და განვითარება. მსხვილ

საერთაშორისო პროექტებში მონაწილეობს საერთაშორისო კონსორციუმები ან ბაზარზე უკვე არსებული ტრადიციული კვლევითი ცენტრები. **მაგალითად, გამოწვევას წარმოადგენს შემთხვევები, როდესაც საჯარო-ფინანსების მართვის სფეროში გამოცდილი ორგანიზაცია ცდილობს კიბერუსაფრთხოების სფეროში არსებული პროექტებისა და თუ გრანტების მოპოვებას, რაც იმთავითვე კლავს ახალი კიბერუსაფრთხოების კვლევითი ორგანიზაციების გაჩენა-განვითარებას.**

<u>რეკომენდაცია</u>

1. კიბერუსაფრთხოების კვლევითი ორგანიზაციების განვითარებისა და ხელშეწყობის სტრატეგია. ქმედითი მექანიზმების დანერგვა, როგორიცაა საგრანტო ფონდები, კვლევითი პროექტებისა და მნიშვნელოვან პროექტებში ჩართულობის წახალისება, რაც უზრუნველყოფს საქართველოში შესაბამისი ექსპერტიზის შექმნასა და დაგროვებას.
2. ICT და სერვისების მიწოდების ჯაჭვის რეგულაციების შექმნაში აქტიურად ჩაერთოს ინდუსტრიის წარმომადგენელი ორგანიზაციები, მათ შორის, IT და კიბერ კომპანიები, კვლევითი ინსტიტუტები და არასამთავრობო ორგანიზაციები.

5. დანართები

დანართი #1: ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების ორგანოები

#	Country	Ministry	Sub-ordinated Agency	CERT Name
1	Austria	Federal Chancellery	Federal Ministry of Interior	CERT.at
2	Belgium	Prime Minister's Office	Centre for Cybersecurity Belgium (CCB)	CERT.be
3	Bulgaria	Ministry of Transport, Information Technology and Communications	State e-Government Agency	CERT Bulgaria
4	Croatia	Ministry of the Interior	Croatian National CERT (CARNET)	CERT.hr
5	Cyprus	Ministry of Transport, Communications and Works	Office of the Commissioner of Electronic Communications and Postal Regulations (OCECPR)	CY-CERT
6	Czech Republic	Ministry of Interior	National Cyber and Information Security Agency (NÚKIB)	GOVCERT.CZ
7	Denmark	Ministry of Defence	Centre for Cyber Security (CFCS)	DK-CERT
8	Estonia	Ministry of Economic Affairs and Communications	Estonian Information System Authority (RIA)	CERT-EE
9	Finland	Ministry of Transport and Communications	Finnish Transport and Communications Agency (Traficom)	NCSC-FI
10	France	Prime Minister's Office	National Cybersecurity Agency of France (ANSSI)	CERT-FR
11	Germany	Federal Ministry of the Interior	Federal Office for Information Security (BSI)	CERT-Bund
12	Greece	Ministry of Digital Governance	Hellenic Cyber Security Authority	GR-CERT
13	Hungary	Ministry of Interior	National Cyber Security Center (NCSC)	GovCERT-Hungary
14	Ireland	Department of Environment, Climate and Communications	National Cyber Security Centre (NCSC)	IRL-CERT
15	Italy	Prime Minister's Office	National Cybersecurity Agency (ACN)	CERT-PA

16	Latvia	Ministry of Defence	Information Technology Security Incident Response Institution (CERT.LV)	CERT.LV
17	Lithuania	Ministry of National Defence	National Cyber Security Centre (NKSC)	CERT-LT
18	Luxembourg	Ministry of the Economy	Cybersecurity Competence Centre Luxembourg (C3)	CIRCL
19	Malta	Ministry for Finance and Financial Services	Malta Information Technology Agency (MITA)	MaltaCERT
20	Netherlands	Ministry of Justice and Security	National Cyber Security Centre (NCSC-NL)	CERT-EU
21	Poland	Ministry of the Interior and Administration	The Internal Security Agency (ABW)	CERT.PL
22	Portugal	Ministry of National Defence	National Cybersecurity Centre (CNCS)	CERT.PT
23	Romania	Ministry of Internal Affairs	National Cyber Security Directorate (DNSC)	RoCERTS
24	Slovakia	National Security Authority	National Security Authority (NBÚ)	SK-CERT
25	Slovenia	Ministry of Public Administration	Slovenian Information Security Administration (AKOS)	SI-CERT
26	Spain	Ministry of Economic Affairs and Digital Transformation	National Cybersecurity Institute of Spain (INCIBE)	CCN-CERT
27	Sweden	Ministry of Justice	Swedish Civil Contingencies Agency (MSB)	CERT-SE

6. ბიბლიოგრაფია

რეგულაციები

United States

1. Cybersecurity Information Sharing Act (CISA) of 2015

- United States. Congress. Senate. 2015. *Cybersecurity Information Sharing Act*. Public Law 114-113. 129 Stat. 2242. https://www.congress.gov/bill/114th-congress/senate-bill/754

2. Executive Order on Improving the Nation's Cybersecurity (EO 14028)

- Biden, Joseph R. 2021. "Executive Order on Improving the Nation's Cybersecurity." *Federal Register* 86, no. 99 (May 17): 26633-26644. https://www.federalregister.gov/d/2021-10460

3. National Defense Authorization Act (NDAA)

- United States. Congress. 2021. *National Defense Authorization Act for Fiscal Year 2021*. Public Law 116-283. 134 Stat. 3388. https://www.congress.gov/bill/116th-congress/house-bill/6395

4. CISA's Information and Communications Technology Supply Chain Risk Management (ICT SCRM)

- Cybersecurity and Infrastructure Security Agency. 2020. *Information and Communications Technology Supply Chain Risk Management Task Force Year Two Report*. https://www.cisa.gov/publication/ict-scrm-task-force-year-two-report

5. White House Executive Order on America's Supply Chains (EO 14017)

- Biden, Joseph R. 2021. "Executive Order on America's Supply Chains." *Federal Register* 86, no. 40 (March 1): 11849-11854. https://www.federalregister.gov/d/2021-04280

6. Federal Acquisition Security Council (FASC) and Interim Final Rule

- Federal Acquisition Security Council. 2020. "Federal Acquisition Supply Chain Security Act of 2018: Interim Final Rule." *Federal Register* 85, no. 148 (July 31): 45335-45353. https://www.federalregister.gov/d/2020-15824

7. NIST SP 800-161 (Supply Chain Risk Management Practices)

- Boyens, Jon, Celia Paulsen, Nadya Bartol, Kristina Kemp, and James Smith. 2015. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. NIST Special Publication 800-161. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161

United Kingdom

1. National Cyber Security Centre (NCSC) Supply Chain Security Group

- National Cyber Security Centre. 2016. *Supply Chain Security*. https://www.ncsc.gov.uk/collection/supply-chain-security

2. Centre for the Protection of National Infrastructure (CPNI) Supply Chain Security Guidance

- Centre for the Protection of National Infrastructure. 2015. *Supply Chain Security Guidance*. https://www.cpni.gov.uk/supply-chain-security

3. UK Government's 5G Supply Chain Diversification Strategy Working Group

- UK Government. 2020. *5G Supply Chain Diversification Strategy*. https://www.gov.uk/government/publications/5g-supply-chain-diversification-strategy

4. Telecommunications Supply Chain Diversification Advisory Council

- UK Department for Digital, Culture, Media & Sport. 2020. "Telecommunications Supply Chain Diversification Advisory Council: Terms of Reference." https://www.gov.uk/government/publications/telecommunications-supply-chain-diversification-advisory-council-terms-of-reference

5. Defence Cyber Protection Partnership (DCPP) Supply Chain Working Group

- Ministry of Defence. 2013. *Defence Cyber Protection Partnership*. https://www.gov.uk/government/groups/defence-cyber-protection-partnership

6. British Standards Institution (BSI) Supply Chain Services and Solutions

- British Standards Institution. 1901. *BSI Supply Chain Services and Solutions*. https://www.bsigroup.com/en-GB/supply-chain-risk-management/

European Union

1. Directive on Security of Network and Information Systems (NIS Directive)

- European Parliament and Council. 2016. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union*. Official Journal of the European Union L194/1. https://eur-lex.europa.eu/eli/dir/2016/1148/oj

2. EU Cybersecurity Act

- European Parliament and Council. 2019. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*. Official Journal of the European Union L151/15. https://eur-lex.europa.eu/eli/reg/2019/881/oj

3. The Digital Operational Resilience Act (DORA)

- European Parliament and Council. 2022. *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union L333/1. https://eur-lex.europa.eu/eli/reg/2022/2554/oj

4. General Data Protection Regulation (GDPR)

- European Parliament and Council. 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)*. Official Journal of the European Union L119/1. https://eur-lex.europa.eu/eli/reg/2016/679/oj

1. ENISA's Guidelines and Reports on Supply Chain Security

- European Union Agency for Cybersecurity. 2010. *Supply Chain Security Recommendations*. https://www.enisa.europa.eu/publications/supply-chain-integrity

2. ENISA's Cloud Security and 5G Network Security Guidelines

- European Union Agency for Cybersecurity. 2013. *Cloud Computing Security Risk Assessment*. https://www.enisa.europa.eu/publications/cloud-computing-security-risk-assessment

- European Union Agency for Cybersecurity. 2016. *5G Network Security*. https://www.enisa.europa.eu/publications/5g-security

3. ENISA's Stakeholder Engagement and Working Groups

- European Union Agency for Cybersecurity. 2004. *Stakeholder Engagement Framework*. https://www.enisa.europa.eu/topics/working-groups

სახელმძღვანელოები და სამუშაო ჯგუფები

European Union

1. ENISA's Guidelines and Reports on Supply Chain Security

- European Union Agency for Cybersecurity. 2010. *Supply Chain Security Recommendations*. https://www.enisa.europa.eu/publications/supply-chain-integrity

2. ENISA's Cloud Security and 5G Network Security Guidelines

- European Union Agency for Cybersecurity. 2013. *Cloud Computing Security Risk Assessment*. https://www.enisa.europa.eu/publications/cloud-computing-security-risk-assessment

- European Union Agency for Cybersecurity. 2016. *5G Network Security*. https://www.enisa.europa.eu/publications/5g-security

3. ENISA's Stakeholder Engagement and Working Groups

- European Union Agency for Cybersecurity. 2004. *Stakeholder Engagement Framework*. https://www.enisa.europa.eu/topics/working-groups

United States

1. Cybersecurity and Infrastructure Security Agency (CISA) Supply Chain Risk Management Task Force

- Cybersecurity and Infrastructure Security Agency. 2018. *CISA Supply Chain Risk Management Task Force*. https://www.cisa.gov/supply-chain

2. National Institute of Standards and Technology (NIST) Cyber Supply Chain Risk Management Program

- Boyens, Jon, Celia Paulsen, Nadya Bartol, Kristina Kemp, and James Smith. 2015. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. NIST Special Publication 800-161. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161

3. Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Working Group

- Cybersecurity and Infrastructure Security Agency. 2018. *ICT Supply Chain Risk Management (SCRM) Working Group*. https://www.cisa.gov/ict-scrm

4. Federal Acquisition Security Council (FASC)

- Federal Acquisition Security Council. 2020. “Federal Acquisition Supply Chain Security Act of 2018: Interim Final Rule.” *Federal Register* 85, no. 148 (July 31): 45335-45353. https://www.federalregister.gov/d/2020-15824

5. Defense Industrial Base (DIB) Cybersecurity Program

- U.S. Department of Defense. 2007. *Defense Industrial Base (DIB) Cybersecurity Program*. https://dibnet.dod.mil

6. National Defense Industrial Association (NDIA) Supply Chain Security Committee

- National Defense Industrial Association. 1919. *NDIA Supply Chain Security Committee*. https://www.ndia.org/policy/committees/supply-chain-network

United Kingdom

1. National Cyber Security Centre (NCSC) Supply Chain Security Group

- National Cyber Security Centre. 2016. *Supply Chain Security*. https://www.ncsc.gov.uk/collection/supply-chain-security

2. Centre for the Protection of National Infrastructure (CPNI) Supply Chain Security Guidance

- Centre for the Protection of National Infrastructure. 2015. *Supply Chain Security Guidance*. https://www.cpni.gov.uk/supply-chain-security

3. UK Government's 5G Supply Chain Diversification Strategy Working Group

- UK Government. 2020. *5G Supply Chain Diversification Strategy*. https://www.gov.uk/government/publications/5g-supply-chain-diversification-strategy

4. Telecommunications Supply Chain Diversification Advisory Council

- UK Department for Digital, Culture, Media & Sport. 2020. "Telecommunications Supply Chain Diversification Advisory Council: Terms of Reference." https://www.gov.uk/government/publications/telecommunications-supply-chain-diversification-advisory-council-terms-of-reference

5. Defence Cyber Protection Partnership (DCPP) Supply Chain Working Group

- Ministry of Defence. 2013. *Defence Cyber Protection Partnership*. https://www.gov.uk/government/groups/defence-cyber-protection-partnership

6. British Standards Institution (BSI) Supply Chain Services and Solutions

- British Standards Institution. 1901. *BSI Supply Chain Services and Solutions*. https://www.bsigroup.com/en-GB/supply-chain-risk-management/