კიბერუსაფრთხოების სფეროში არსებული ზოგიერთი ქვეყნის ორგანიზაციული სტრუქტურების მოკლე აღწერა. საქართველოში არსებული სუბიექტები

შესავალი

ბოლო ათწლეულში ინტერნეტ - სივრცის და მასთან დაკავშირებული პროცესების სწრაფმა განვითარებამ, ასევე მომხმარებელთა რაოდენობის მოკლე დროში კოლოსალურმა ზრდამ, გამოიწვია ახალი სახელმწიფო სუბიექტების შექმნისა და განვითარების საჭიროება. ყველა ქვეყანა ცდილობს მაქსიმალურად ეფექტური, მოქნილი და დახვეწილი ისეთი ორგანიზაციული სტრუქტურის ჩამოყალიბებას, რომელიც მაქსიმალურად უზრუნველყოფს კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვას, გაატარებს ეფექტურ ღონიძიებებს მიმართულს კიბერუსაფრთხოების უზრუნველყოფაზე, ასევე მაქსიმალურად დაიცავს პიროვნების პერსონალურ ინფორმაციას და არსებულ მონაცემთა ბაზებს. პირველ რიგში, ყველა ქვეყნის ხელისუფლება მოცემულ საკითხს განიხილავს როგორც ეროვნული უსაფრთხოების ერთერთ მნიშვნელოვან შემადგენელ ნაწილს, და შესაბამისად მსგავსი სუბიექტების დიდი ნაწილი იმყოფება თავდაცვის და შინაგან საქმეთა სამინისტროების, ან სადაზვერვო, უშიშროების ან სხვა სპეციალური სამსახურების კურატორობის ქვეშ.

მსგავს სუბიექტებს გააჩნიათ არსებობის მოკლე ისტორია. ფაქტიურად, არ არსებობდა არავითარი გამოცდილება და ყველა ქვეყანა ინდივიდუალურად ავითარებდა მოცემულ საკითხს. შეიძლება ითქვას, რომ კიბერუსაფრთხოების სფეროში სახელმწიფო თუ კერძო სუბიექტების შექმნა და მათი მომავალი განვითარება ეფუძნება იმ პრეცედენტებს, რომლებიც წარმოიშვა ინტერნეტ - სივრცეში და უკავშირდება ზოგადად, კიბერსივრცის დაცვის აუცილებლობას. ამიტომ, მოცემული სფეროს პარალელურად მუდმივად მიმდინარეობს სახელმწიფო თუ კერძო სექტორის სუბიექტების ორგანიზაციული სტრუქტურის განვითარების პროცესი.

ნაშრომში განხილულია ზოგიერთი ქვეყნის ორგანიზაციული სტრუქტურები დაკავშირებული კიბერუსაფრთხოებასთან და ის საერთო პრინციპები, რომლებიც გააჩნიათ და ახასიათებთ სხვადასხვა ქვეყნების სახელმწიფო თუ კერძო სუბიექტებს მოცემულ სფეროში. აქვე წარმოდგენილია საქართველოში არსებული ის სუბიექტები, რომლებიც პასუხისმგებელნი არიან კომპიუტერული ქსელებისა და კიბერსივრცის, ასევე პერსონალური მონაცემების დაცვაზე და ებრძვის კიბერდანაშაულს როგორც ლოკალურ ისე საერთაშორისო დონეზე.

ზოგიერთი ქვეყნის ორგანიზაციული სტრუქტურების მოკლე მიმოხილვა

ქვემოთ მოცემული მასალა ქმნის გარკვეულ წარმოდგენას კიბერუსაფრთხოების სფეროში არსებული სახელმწიფო სუბიექტების შესახებ. კერძოდ, აქ მოკლედ არის განხილულია ევროკავშირის ზოგიერთი წევრი ქვეყნისა და სხვა ქვეყნების იმ სახელმწიფო სუბიექტების ორგანიზაციული სტრუქტურა, ფუნქციები და უწყებრივი დაქვემდებარებულობა, რომლებიც პასუხისმგებელნი არიან თავიანთ ქვეყნებში უზრუნველყონ კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვა და კიბერუსაფრთხოება, გაატარონ ყველა ის საჭირო ღონისძიებები, რომლებიც საშუალებას იძლევა მაქსიმალურად იყოს დაცული ინტერნეტის სივრცე, მონაცემთა ბაზები და მოქლაქეთა პერსონალური ინფორმაცია, ასევე ეფექტურად აწარმოონ ბრძოლა კიბერდანაშაულის წინააღმდეგ. კერძოდ, განხილულ ქვეყნებს განეკუთვნება:

- **ესტონეთი** - კიბერუსაფრთხოების სტრატეგია გამოქვეყნდა 2008 წელს. მოცემულ დოკუმენტში[1] აღწერილია სახელმწიფოში კიბერუსაფრთხოების სფეროში არსებული ვითარება და განსაზღვრავს ეროვნულ პოლიტიკას მოცემული მიმართულებით. ქვეყანაში არ არსებობს ერთიანი სახელმწიფო ორგანო, რომელიც პასუხისმგებელი იქნებოდა კიბერსივრცის დაცვის უზრუნველყოფაზე. ამ პროცესში უშუალოდ მონაწილეობს რამდენიმე სამინისტრო და მათი ქვედანაყოფი. ინფორმაციული უსაფრთხოების უზრუნველყოფაში მთავარი როლი ეკუთვნის ეკონომიკისა და კავშირგაბმულობის სამინისტროს (MEAC)[2]. სამინისტროს დაქვემდებარებაში არის ცენტრალური აღმასრულებელი ხელისუფლების ორი ორგანო, რომლებიც ახდენენ კიბერუსაფრთხოების სახელმწიფო პოლიტიკის რეალიზაციას. ეს ორგანოებია: ინფორმაციული სისტემების სახელმწიფო დეპარტამენტი (RISO)[3], რომელიც არის მთავარი მაკოორდინირებელი ორგანიზაცია ინფორმაციისა და საკომუნიკაციო ტექნოლოგიების სფეროში (ICT)[4], და ესტონეთის ინფორმატიკის ცენტრი (RIA)[5], რომელიც პასუხისმგებელია მთლიანი ქსელის უსაფრთხოების უზრუნველყოფაზე, კრიტიკული ინფორმაციული ინფრასტრუქტურის სახელმწიფო სუბიექტების ტექნიკურ უსაფრთხოებაზე, ასევე სახელმწიფო ორგანიზაციების ინტერესებიდან გამომდინარე მონაცემთა გადაცემის სისტემის დამუშავება და მართვა. მოცემული ცენტრის შემადგენლობაში ფუნქციონირებს ესტონეთის საგანგებო სიტუაციებზე რეაგირების ოპერატიული ჯგუფი (CERT)[6]. უშუალოდ კრიტიკული ინფრასტრუქტურის დაცვასა (CIIP) და

[1] https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf
[2] https://www.mkm.ee/en
[3] http://www.riso.ee/en/
[4] Information and Communication Technology
[5] https://www.ria.ee/en/
[6] https://www.ria.ee/cert-estonia

კიბერუსაფრთხოებას უზრუნველყოფს შინაგან საქმეთა და თავდაცვის სამინისტროების სპეციალური სტრუქტურული ერთეულები. ორივე სამინისტრო პასუხისმგებელია ქვეყნის შიდა უსაფრთხოებასა და კრიზისების მართვაზე. საფოსტო და საბაზრო ელექტრონული კავშირის მომსახურების სფეროს კოორდინირებას უწევს კავშირგაბმულობის ეროვნული საბჭო. სახელმწიფოსა და კერძო სექტორს შორის პარტნიორობისთვის შეიქმნა პროექტი „კომპიუტერული უსაფრთხოება 2009“, რომელიც მიმართულია ინფორმაციული უსაფრთხოების გაძლიერებისკენ;

- **დიდი ბრიტანეთი** - 2009 წელს[7] მიღებული კიბერუსაფრთხოების სტრატეგია ხაზს უსვამს კიბერუსაფრთხოების უზრუნველყოფის საკითხთან კომპლექსური მიდგომის აუცილებლობას, რომლის რეალიზაციაში უნდა მონაწილეობდნენ სახელმწიფო სუბიექტები, მრეწველობის ყველა დარგის წარმომადგენლები, სამოქალაქო საზოგადოებრივი ორგანიზაციები და საერთაშორისო პარტნიორები. სტრატეგია ითვალისწინებს ორი ახალი ორგანიზაციის შექმნას[8]. პირველ რიგში ეს არის მინისტრთა კაბინეტის სტრუქტურაში შემავალი კიბერუსაფრთხოების სამმართველო (OCS)[9], რომელიც უზრუნველყოფს სტრატეგიულ ხელმძღვანელობასა და უწყებათაშორის დონეზე შეთანხმებულ მოქმედებას. ის იქნება ასევე დაკავებული კიბერდანაშაულის შესახებ საკოორდინაციო საქმიანობით. ამასთან ერთად გამოყენებული იქნება არსებული შესაძლებლობები, რომელიც გააჩნია თავდაცვის სამინისტროს, სადაზვერვო სამსახურებს და პოლიციას (ლონდონის პოლიციის ელექტრონულ დანაშაულებებთან ბრძოლის განყოფილება, ინტერნეტის ქსელის დაცვისა და ბავშვთა ექსპლუატაციის წინააღმდეგ ქმედებების ცენტრი, ასევე განსაკუთრებით საშიში და ორგანიზებული დანაშაულის სააგენტო). მეორე, ეს არის კიბერუსაფრთხოების ოპერატიული ცენტრი (CSOC), რომელიც ფუნქციონირებს სახელმწიფო კავშირგაბმულობის შტაბის[10] ბაზაზე ქ. ჩელტენჰემში. ეს არის ახალი ცენტრი, სადაც თავმოყრილია სხვადასხვა უწყებების არსებული ფუნქციები კიბერსივრცის მდგომარეობის მონიტორინგისა და ღონისძიებების კოორდინაცია ექსტრემალურ რეაგირებაზე. ცენტრი ასევე გააკეთებს ანალიზს იმ საფრთხეებზე, რომელიც ემუქრება დიდი ბრიტანეთის კომპიუტერულ ქსელებსა და მათ მომხმარებლებს, გამოიმუშავებს შესაბამის რეკომენდაციებსა და საინფორმაციო სახელმძღვანელოებს. ეროვნული ინფრასტრუქტურის დაცვის ცენტრის (CPNI)[11] შემადგენლობაშია კომპიუტერების დახმარების სასწრაფო სამსახური (CERT Service)[12];

[7] 2011 წელს მოხდა სტრატეგიის განახლება https://www.cpni.gov.uk/advice/cyber/cir/

[8] ორივე ორგანიზაციამ დაიწყო ფუნქციონირება 2010 წელს

[9] https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance

[10] http://www.gchq.gov.uk/Pages/homepage.aspx

[11] http://www.cpni.gov.uk/Templates/CPNI/pages/Default.aspx

[12] https://www.cpni.gov.uk/advice/cyber/cir/

- **შვედეთი** - კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვით ღონისძიებებში მონაწილეობას იღებს ბევრი ორგანიზაცია. 2009 წელს შვედეთის თავდაცვის სამინისტროსთან არსებულ სამოქალაქო თავდაცვის სააგენტოს (MSB)[13] დაევალა 2010 წლის იანვრამდე წინადადებების მომზადება კომპიუტერულ ქსელებში დანაშაულებების აღკვეთის თაობაზე. გადაწყდა სააგენტოს შემადგენლობაში შექმნილიყო კიბერუსაფრთხოების ეროვნული ოპერატიული საკოორდინაციო ცენტრი, რომელიც უწყებათაშორის დონეზე, გაუწევდა კოორდინაციას ერთობლივ ღონისძიებებს და შეასრულებდა ცენტრალური ელემენტის როლს კრიზისული მენეჯმენტის სისტემაში. ამ პროცესში მთავარი როლი ეკუთვნის ასევე თავდაცვის სამინისტროსთან არსებულ საგანგებო სიტუაციების სააგენტოს (SEMA)[14]. გარდა ამისა, სამოქალაქო თავდაცვის სააგენტოს (MSB) ხელმძღვანელობით, არსებობს ინფორმაციული უსაფრთხოების სფეროში ერთობლივი ოპერაციების ჯგუფი (SAMFI)[15], სადაც შედიან შვედეთის შეიარაღებული ძალების, რადიოტექნიკური თავდაცვის ეროვნული სამსახური (FRA)[16], ფოსტისა და ტელეკომუნიკაციის ეროვნული სააგენტო (PTS)[17] და პოლიციის ეროვნული დეპარტამენტის წარმომადგენლები. უწყებათაშორისო თანამშრომლობის ფარგლებში, მინისტრთა კაბინეტის დონეზე ტარდება სპეციალური სამუშაოები მიმართული საგანგებო სიტუაციების სააგენტოს (SEMA) რეკომენდაციებსა და კრიტიკული ინფორმაციული ინფრასტრუქტურის ეროვნული სისტემის მოდერნიზირებაზე. რაც შეეხება სახელმწიფოსა და კერძო სექტორის პარტნიორულ დონეზე თანამშრომლობას, აქ ხორციელდება საგანგებო სიტუაციების სააგენტოს (SEMA) მიერ მომზადებული ისეთი ინიციატივები და პროექტები, როგორებიცაა მოცემულ სფეროში სახელმწიფო და კერძო სექტორებს შორის თანამშრომლობის გაღრმავების, „სამრეწველო უსაფრთხოების

[13] https://www.msb.se/en/

[14] The Swedish Emergency Management Agency (SEMA) co-ordinates the work to develop the preparedness of Swedish society to manage serious crises. SEMA works together with municipalities, county councils and government authorities, as well as the business community and several organizations, to reduce the vulnerability of society and improve the capacity to handle emergencies. The Swedish Emergency Management Agency (SEMA) supports the bodies responsible for emergency management, especially county administrative boards and municipalities, which have a special role with overall geographic area responsibility. SEMA should be able to give support to other public actors, i.e. municipalities, county councils and government authorities. SEMA does not have an operative role and does not take over any responsibility from other authorities. The support that SEMA is able to provide in the event of a crisis may include advice and expert support within areas such as crisis communication and management methodoligy. SEMA should also assist the Government Offices with updated situation reports. To carry out this task, the authority has an established network of county administrative boards, central authorities and others that may be affected by or have knowledge of an emergency situation. SEMA also co-ordinates the planning, resource allocation, follow-up and evaluation of work within the area of crisis management. Furthermore, SEMA collects knowledge through horizon scanning, strategic analyses and research to develope sociaty's emergency management.

[15] http://rib.msb.se/Filer/pdf/26177.pdf

[16] http://www.fra.se/snabblankar/english.10.html

[17] http://www.pts.se/en-GB/

დელეგაციისა“ (NSD) და „ინფორმაციის დამუშავების საზოგადოების“ (DFS) პროექტები;

- **ფინეთი** - აქ კიბერუსაფრთხოება განიხილება, როგორც მონაცემთა უსაფრთხოების პრობლემა, აგრეთვე როგორც ეკონომიკური პირობა, რომელიც მჭიდროდ არის დაკავშირებული ქვეყნის ინფორმაციული საზოგადოების განვითარებასთან. კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის საკითხებით დაკავებულია შემდეგი სამი სახელმწიფო ორგანო: ტრანსპორტისა და კავშირგაბმულობის სამინისტროს შემადგენლობაში არსებული კავშირგაბმულობის რეგულირების სამსახური (FICORA)[18], რომელიც ხელს უწყობს ინფორმაციული საზოგადოების განვითარებას და ეწევა ტექნიკური საკითხებისა და სტანდარტიზაციის რეგულირებას; მეორე, საგანგებო სიტუაციების ეროვნული სააგენტო (NESA)[19], ეწევა კრიტიკული ინფორმაციული ინფრასტრუქტურის საფრთხეებისა და რისკების შეფასებასა და ანალიზს; და მესამე, სახელმწიფო ადმინისტრაციასთან არსებული მონაცემთა უსაფრთხოების მთავარი სამმართველო (VAHTI)[20], რომელიც ინფორმაციული უსაფრთხოების უზრუნველყოფის მიზნით ამუშავებს პრინციპებისა და პრაქტიკულების სახელმძღვანელოებს. გარდა ამისა, მოცემულ სფეროში სახელმწიფოსა და კერძო სექტორს შორის პარტნიორული ურთიერთობის მიზნით შექმნილია შემდეგი სამი ორგანიზაცია საგანგებო სიტუაციების ეროვნული საბჭო (NESC), ინფორმაციული

[18] https://www.viestintavirasto.fi/en/

[19] http://www.nesa.fi/

[20] The Government Information and Cyber Security Management Board (VAHTI), appointed by the Ministry, is responsible for Government cooperation, steering and development efforts in this area. VAHTI sets all the main policy guidelines for information and cyber security in central government. Different administrative branches and levels of administration are represented in VAHTI.

A Government Resolution on the development of information security in central government was issued on 26 November 2009. The Resolution provides guidance to central government in developing information security as an integral part of leadership, expertise, risk management and administrative development and functions. VAHTI's effective cooperation, steering and development of information security in central government will be reinforced. The present Government has discussed the earlier government resolutions and made a decision that this resolution is to be kept in force.

VAHTI guidelines and instructions are also important reference materials for the public authorities, local government, the private sector and civil society. In addition, the results of the work are used in such international information security forums as the OECD and the EU. VAHTI publications are considered to be of high quality in international comparison.

The role and tasks of VAHTI in the development, coordination, cooperation and steering of government information and cyber security have been further developed and strengthened. VAHTI deals with all significant central government information and cyber security guidance and policy matters.

VAHTI has received several awards for improving information security in Finland. The latest OECD report on the development of the global information security culture makes several references to the operations and results of VAHTI.

საზოგადოების საკითხთა საკონსულტაციო საბჭო და ფინეთის ინფორმაციული საზოგადოების განვითარების ცენტრი (TIEKE)[21];

- **ნიდერლანდები** - კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვისა და კიბერუსაფრთხოების უზრუნველყოფის მაკოორდინირებელ ორგანოს წარმოადგენს შინაგან საქმეთა და სამეფო საქმეთა სამინისტრო. გარდა ამისა, ამ სამინისტროში არსებული კრიზისების ეროვნული ცენტრი კურირებს სხვა უწყებების საქმიანობას, ასევე საერთაშორისო პოლიტიკასა და კრიზისების მართვას.ინფორმაციული უსაფრთხოების დაცვით ღონისძიებებში ასევე მონაწილეობს საერთო დაზვერვისა და უსაფრთხოების სამსახური (AIVD)[22];
- **გერმანია** - კრიტიკული ინფრასტრუქტურის უსაფრთხოების ეროვნული სტრატეგია განსაზღვრავს მთავრობის მიზნებსა და ამოცანებს მოცემულ სფეროში, რომელიც თავის მხრივ ასახულია ინფორმაციული ინფრასტრუქტურის უსაფრთხოების სახელმწიფო პროგრამაში (NPSI). კიბერუსაფრთხოების საკითხებში მთავარი როლი ეკუთვნის შინაგან საქმეთა სამინისტროსთან არსებულ ინფორმაციული უსაფრთხოების ფედერალურ სააგენტოს (BSI), რომელიც სამოქალაქო თავდაცვისა და საგანგებო სიტუაციების ფედერალურ სააგენტოსთან (BBK), კრიმინალური პოლიციის ფედერალურ სააგენტოსთან (BKA), ფედერალურ პოლიციასთან (BPOL) და ფედერალური ინსტიტუტების ტექნიკური მხარდაჭერის სამსახურთან ერთად ახორციელებს შეფასებასა და ანალიზს, ასევე ფორმულირებას უკეთებს კიბერსივრცის დაცვის კონცეფციას. კრიტიკული ინფრასტრუქტურის დაცვის მიზნით და ამ მიმართულებით კოორდინირებული მოქმედებისთვის შექმნილი არის სამუშაო ჯგუფი (AG KRITIS)[23]. სტრატეგიის შემუშავებისა და მისი შემდგომი რეალიზების საქმიანობა მიმდინარეობს კოორდინირებულად სხვა ფედერალურ სამინისტროებთან, სააგენტოებთან და სამსახურებთან ერთად (ეკონომიკისა და ტექნოლოგიის სამინისტრო, ფედერალური კანცლერის ადმინისტრაცია, იუსტიციის, საგარეო საქმეთა და თავდაცვის ფედერალური სამინისტროები, ელექტრონული ქსელების ფედერალური სააგენტო). გარდა ამისა, წარმოებს კონსულტაციები კერძო სექტორის სტრატეგიულ პარტნიორებთან;
- **საფრანგეთი** - კრიტიკული ინფრასტრუქტურის დაცვაზე მთელი პასუხისმგებლობა ეკისრება პრემიერ - მინისტრის ადმინისტრაციასთან არსებულ ეროვნული თავდაცვის გენერალურ სამდივნოს (SGDN). ქვეყანაში კიბერუსაფრთხოება ამავდროულად განიხილება როგორც მაღალტექნოლოგიური დანაშაულის საკითხი და როგორც პრობლემა, რომელიც ხელს უშლის და ეწინააღმდეგება ინფორმაციული საზოგადოების ნორმალურ განვითარებას.

[21] http://www.tieke.fi/display/English/Home
[22] https://www.aivd.nl/english/
[23] file:///C:/Users/Admin/Downloads/doc_263_259_en.pdf

მოცემულ სფეროში დანაშაულის გამოძიებაზე პასუხისმგებელი ორგანოებია 2000 წლის მაისში შექმნილი ინფორმაციისა და საკომუნიკაციო ტექნოლოგიების სფეროში დანაშაულთან ბრძოლის ცენტრალური ოფისი (OCLCTIC) და სასამართლო პოლიციის მთავარი სამმართველოს ეკონომიკური და ფინანსური საგამოძიებო განყოფილება. 2009 წლის ივლისის თვეში, თავდაცვის სამინისტროში შეიქმნა ინფორმაციული სისტემების უსაფრთხოების ეროვნული სააგენტო (Anssi)[24], რომელიც პასუხისმგებელია კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვისა და კიბერუსაფრთხოების უზრუნველყოფაზე. გარდა ამისა, ასევე ფუნქციონირებს ინფორმაციული სისტემების უსაფრთხოების უწყებათაშორისი კომისია (CISSY). სახელმწიფოსა და კერძო სექტორს შორის პარტნიორობის ფარგლებში შექმნილია ინფორმაციული ტექნოლოგიების სტრატეგიული საკონსულტაციო საბჭო (CSTI), რომელიც აერთიანებს სახელმწიფო ჩინოვნიკებს, ბიზნესისა და საწარმოთა მაღალი მმართველი რგოლისა და სამეცნიერო წრეების წარმომადგენლებს;

- **ნორვეგია** - სამოქალაქო თავდაცვისა და კრიზისების მართვის სამმართველო (DSB) არის მთავარი მაკოორდინირებელი ორგანიზაცია, რომელიც პასუხისმგებელია კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვითი საქმიანობის უზრუნველყოფაზე. სამმართველო იმყოფება იუსტიციისა და პოლიციის სამინისტროს დაქვემდებარებაში. ინფორმაციისა და ქსელების კავშირის უსაფრთხოება თავმოყრილია სახელმწიფო მართვისა და რეფორმების სამინისტროში. თავდაცვის სამინისტრო პასუხიმგებელია მხოლოდ სამხედრო კომპიუტერულ ქსელზე. ტრანსპორტისა და კავშირგაბმულობის სამინისტრო პასუხს აგებს კავშირგაბმულობის სექტორზე, ასევე ინფორმაციული ქსელების უსაფრთხოების ასპექტებზე. ნორვეგიის ეროვნული უსაფრთხოების სამსახური (NSA) კოორდინირებას უწევს კომპიუტერული ქსელების უსაფრთხოების უზრუნველყოფის ღონისძიებებს. ინფორმაციული უსაფრთხოების საკითხთა სახელმწიფო საკოორდინაციო საბჭო (KIS) უფლებამოსილი არ არის მიიღოს გადაწყვეტილებები, თუმცა ის უწევს კონსულტაციებს სამინისტროებსა და უწყებებს იმ საკითხებში, რომლებიც დაკავშირებულია კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვასა და კიბერუსაფრთხოებასთან. მის შემადგენლობაში შედის ექვსი სამინისტრო, პრემიერ - მინისტრის აპარატი და ათამდე სხვადასხვა სამმართველო;
- **ავსტრია** - ქვეყანაში არ არსებობს ერთიანი მაკოორდინირებელი ორგანო, რომელიც პასუხისმგებელი იქნება კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვით ღონისძიებებზე. ყოველი სამინისტრო და უწყება თავად ახორციელებს საკუთარი უსაფრთხოების ღონისძიებებს მიმართულს საგარეო კიბერშეტევებსა მონაცემთა არასანქცირებული გამოყენების გაუვნებელყოფაზე. კრიტიკული

[24] http://www.ssi.gouv.fr/en/

ინფორმაციული ინფრასტრუქტურის დაცვას ახორციელებს შინაგან საქმეთა სამინისტროს (BMI)[25] ზოგიერთი ქვედანაყოფი, კერძოდ, აწარმოებს მონავემთა უსაფრთხოების უზრუნველყოფასა და ბრძოლას კიბერდანაშაულებასთან. კრიმინალური პოლიციის ფედერალური სამმართველოს საზოგადოებრივი უსაფრთხოების მთავარ სამმართველოსთან ფუნქციონირებს ბავშვთა პორნოგრაფიის გავრცელების საწინააღმდეგო საინფორმაციო ცენტრი. სახელმწიფო დაცვისა და ტერორიზმთან ბრძოლის ფედერალური სააგენტო (BVT)[26] პასუხს აგებს პიროვნებისა და ობიექტების უსაფრთხოების საკითხებზე. თავდაცვის სამინისტროს მეორე სამმართველო აწარმოებს თავის საქმიანობას ინფორმაციული ომის ყველა მიმართულებით და ამასთანავე მჭიდროდ თანამშრომლობს სპეციალურ სამსახურებთან. ერთერთი არის Abwehramt[27], რომელსაც გააჩნია ელექტრონული თავდაცვის სპეციალური დეპარტამენტი. ტრანსპორტის, ინოვაციებისა და ტექნოლოგიების სამინისტრო (BMVIT)[28] პასუხისმგებელია სახელმწიფო ინფორმაციული ინფრასტრუქტურის უსაფრთხოებაზე. იგივე სამინისტრო უწევს კოორდინაციას უსაფრთხოების სფეროში სამეცნიერო კვლევებისა და განვითარების ეროვნულ პროგრამებს. კიბერუსაფრთხოების სფეროში არსებული სახელმწიფო პროგრამების[29] გათვალისწინებით, ავსტრიაში კიბერუსაფრთხოება ძირითადად განიხილება მონაცემთა დაცვის ფარგლებში;

- **პოლონეთი** - კრიტიკული ინფორმაციული ინფრასტრუქტურასა და მის უსაფრთხოებაზე პასუხისმგებელია სახელმწიფო ორი უწყება. კერძოდ, მეცნიერებისა და უმაღლესი განათლებისა და შინაგან საქმეთა და ადმინისტრაციის სამინისტროები. მთავარი სუბიექტი და ერთადერთი მაკოორდინირებელი ორგანო, რომელიც მონაწილეობს სამეცნიერო - ტექნიკური სახელმწიფო პოლიტიკის ყველა სტრატეგიის შემუშავებასა და განსაზღვრაში დაკავშირებული კრიტიკული ინფორმაციული ინფრასტრუქტურისა და მისი უსაფრთხოების უზრუნველყოფასთან, არის მეცნიერებისა და უმაღლესი განათლების სამინისტრო. ეს სამინისტრო ამუშავებს სტრატეგიულ

[25] http://www.bmi.gv.at/cms/bmi/_news/bmi.aspx

[26] The Federal Office for the Protection of the Constitution and Counterterrorism (Bundesamt für Verfassungsschutz und Terrorismusbekämpfung, "BVT") is an Austrian police organization that acts as a domestic intelligence agency. It is tasked with the protection of constitutional organs of the Republic of Austria and their ability to function. The agency was created from the Austrian State police, as well as various special task forces targeting organized crime and terrorism that were under the direction of the Directorate General for Public Security (Generaldirektion für die öffentliche Sicherheit, "GDföS"), which itself is a department of the Federal Ministry of the Interior. The BVT publishes the Verfassungsschutzbericht, an annual report on the status of the protection of the constitution

[27] ავსტრიის საგარეო დაზვერვა

[28] http://www.bmvit.gv.at/en/

[29] ელექტრონული მთავრობის პროგრამა, ინფორმაციული უსაფრთხოების სახელმწიფო პროგრამა, მოქალაქის ელექტრონული ინტელექტუალური ბარათის შექმნის საპილოტე პროგრამა

რეკომენდაციებს ყველა დანარჩენი სამინისტროსა და უწყებებისთვის, ასევე უზრუნველყოფს სახელმწიფო კომპიუტერული ქსელების თავსებადობას. შინაგან საქმეთა და ადმინისტრაციის სამინისტრო პასუხს აგებს სახელმწიფო კომპიუტერულ ინფრასტრუქტურაზე, სახელმწიფო სატელეკომუნიკაციო და ინფორმაციული ქსელების მართვის სისტემებზე;

- **შვეიცარია** - კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვით დაკავებულია რამოდენიმე ორგანიზაცია. ამ სფეროში ერთერთი მთავარი ორგანიზაცია არის ინფორმაციული ტექნოლოგიების ფედერალური სტრატეგიული ქვედანაყოფი (FSUIT)[30]. მოცემული ორგანიზაცია არის ფინანსთა ფედერალური დეპარტამენტის სტრუქტურულ შემადგენლობაში და ის ამუშავებს ინფორმაციულ უსაფრთხოებაში ინსტრუქციებს, მეთოდოლოგიასა და პროცედურებს, ასევე კურირებას უწევს ინფორმაციული უზრუნველყოფის სპეციალურ სამუშაო ჯგუფს (SONIA) და ინფორმაციული უსაფრთხოების საკითხთა საინფორმაციო - ანალიტიკურ ცენტრს (MELANI)[31], რომელიც ახორციელებს კიბერდანაშაულთან ბრძოლის საკოორდინაციო ჯგუფის საქმიანობას (KOBIK)[32]. ორივე ეს ქვედანაყოფი იმყოფება პოლიციის ფედერალური სამმართველოს (FEDPOL)[33] უწყებრივ დაქვემდებარებაში. ინფორმაციული ტექნოლოგიების, ქსელებისა და ტელეკომუნიკაციების ფედერალური სამმართველო (FOITT)[34] ასევე წარმოადგენს ფინანსთა ფედერალური დეპარტამენტის სტრუქტურულ ქვედანაყოფს და პასუხისმგებელია ოპერატიულ დონეზე ინფორმაციული ტექნოლოგიების ფედერალური სისტემების უსაფრთხოებასა და ექსტრემალურ მზადყოფნაზე. ინფორმაციული უსაფრთხოების სფეროში ასევე მოქმედებს ეკონომიკური რესურსების ფედერალური უწყების შემადგენლობაში არსებული ინფორმაციული და სატელეკომუნიკაციო ინფრასტრუქტურის სამმართველო, სამოქალაქო თავდაცვის ფედერალური სამმართველო (FOCP)[35] და ინფორმაციულ ქსელებში საგანგებო სიტუაციებზე რეაგირების სახელმწიფო ჯგუფი. სამხედრო კომპიუტერული ქსელების უსაფრთხოებაზე პასუხისმგებელია შეიარაღებული ძალების სამეთაურო მხარდაჭერის სამსახური (FUB)[36]. შვეიცარიის კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის პოლიტიკის რეალიზებაში დიდ როლს თამაშობს სახელმწიფო და კერძო სექტორს შორის არსებული საპარტნიორო ურთიერთობა;

[30] http://www.isb.admin.ch/index.html?lang=en
[31] http://www.melani.admin.ch/?lang=en
[32] https://www.cybercrime.admin.ch/kobik/en/home.html
[33] https://www.fedpol.admin.ch/fedpol/en/home.html
[34] http://www.bit.admin.ch/index.html?lang=en
[35] http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/das_babs.html
[36] http://www.vtg.admin.ch/internet/vtg/en/home/schweizerarmee/organisation/fub.html

- **რუსეთი** - ინფორმაციული უსაფრთხოების სფეროში მთავარ ორგანიზაციებად ითვლება უშიშროების საბჭო, უშიშროების ფედერალური სამსახური (ФСБ), დაცვის ფედერალური სამსახური, ტექნიკისა და ექსპერტის კონტროლის ფედერალური სამსახური და ინფორმაციული ტექნოლოგიებისა და კავშირგაბმულობის სამინისტრო. თითოეულ ორგანიზაციულ უწყებას გააჩნია თავისი კომპეტენციის ფარგლები და დაკისრებული პასუხისმგებლობა. კერძოდ, უშიშროების საბჭო განსაზღვრავს ინფორმაციულ სფეროში რუსეთის ეროვნულ ინტერესებს, ობიექტებს, სუბიექტებსა და სხვა რესურსებს, რომლებიც უნდა იყოს დაცული, ასევე კოორდინირებას უწევს ინფორმაციული უსაფრთხოების სტრატეგიის დამუშავებას. უშიშროების ფედერალური სამსახური (ФСБ)[37] პასუხისმგებელია რუსეთის ფედერაციის უსაფრთხოებასა და კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის უზრუნველყოფაზე. კონტრდაზვერვის სამსახურის[38] ფუნქციონირებს კომპიუტერული და ინფორმაციული უსაფრთხოების სამმართველო. იგივე უშიშროების ფედერალური სამსახური (ФСБ) აწარმოებს ინფორმაციული უსაფრთხოების სფეროში სახელმწიფოს სამეცნიერო - ტექნიკური პოლიტიკის დაგეგმვასა და რეალიზებას, უზრუნველყოფს კომპიუტერული ქსელების კრიპტოგრაფიულ და საინჟინრო - ტექნიკურ დაცვას, იცავს სახელმწიფო საიდუმლოებასა და კავშირგაბმულობის ყველა სახეობას. დაცვის ფედერალური სამსახურის შემადგენლობაშია ინფორმაციისა და სპეციალური კავშირების სამსახური, რომელმაც 2003 წლის შემდეგ აიღო იმ ფუნქციების დიდი ნაწილი, რომელიც ადრე შედიოდა ინფორმაციისა და სამთავრობო კავშირების ფედერალური სააგენტოს (ФАПСИ)[39] კომპეტენციაში. ФАПСИ - ს დანარჩენი ფუნქციები გადანაწილდა შეიარაღებული ძალების გენერალური შტაბის, უშიშროების ფედერალური სამსახურისა (ФСБ) და დაცვის სამსახურს შორის. ტექნიკისა და ექსპერტის კონტროლის ფედერალური სამსახური იმყოფება თავდაცვის სამინისტროს დაქვემდებარებაში. მოცემული სამსახურის კომპეტენციის ფარგლებში შედის უცხოეთის სახელმწიფოების ტექნიკურ ჯაშუშობასთან ბრძოლა, საიდუმლო ინფორმაციის დაცვა და კომპიუტერული ქსელებისა და სისტემების უსაფრთხოების უზრუნველყოფა. ინფორმაციული ტექნოლოგიებისა და კავშირგაბმულობის სამინისტრო რეალიზებას უკეთებს სახელმწიფო პოლიტიკასა და ახორციელებს ზედამხედველობას კავშირგაბმულობის სექტორში;
- **კანადა** - კომპიუტერულ ქსელებში საგანგებო სიტუაციებზე ოპერატიული რეაგირების ცენტრი (CCIRC)[40] ახორციელებს მონიტორინგსა და კონსულტირებას

[37] http://www.fsb.ru/

[38] სტრუქტურულად შედის უშიშროების ფედერალურ სამსახურში (ФСБ)

[39] http://www.agentura.ru/dossier/russia/fso/specvyaz/

[40] http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx

დაკავშირებულს კიბერსაფრთხეებისგან დაცვით საკითხებს, ასევე სახელმწიფო დონეზე კოორდინირებას უწევს ნებისმიერი საგანგებო სიტუაციებზე რეაგირების ოპერატიულ ღონისძიებებს, რომლებიც პირველ რიგში უკავშირდება კრიტიკული ინფორმაციული ინფრასტრუქტურის სახელმწიფო ობიექტებს. მოცემულ ღონისძიებებში ჩართული არის სხვადასხვა სახელმწიფო უწყება, მათ შორისაა კანადის ცხენოსანთა სამეფო პოლიცია, კავშირგაბმულობის უსაფრთხოების სააგენტო და უშიშროებისა და დაზვერვის სამსახური. 2010 წელს სახელმწიფომ ბოლო ათი წლის განმავლობაში მესამედ მიიღო კიბერუსაფრთხოების ეროვნული სტრატეგია;

- **ავსტრალია** - კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვითი საკითხებით დაკავებულია კიბერუსაფრთხოების ოპერატიული მართვის ცენტრი, რომელიც შეიქმნა 2009 წელს კიბერუსაფრთხოების სახელმწიფო სტრატეგიის ფარგლებში და შედის თავდაცვის სამინისტროს კავშირგაბმულობის სამმართველოს შემადგენლობაში (DCD). ცენტრის საშტატო განაკვეთი დაკომპლექტებულია შეიარაღებული ძალების, სამხედრო დაზვერვის სამსახურის, ფედერალური პოლიციის, უშიშროებისა და დაზვერვის სამსახურების სპეციალისტებით. ცენტრი მთავრობას უწევს კონსულტაციას დაკავშირებულს კიბერსაფრთხეებისგან ქვეყნის დაცვაზე, ასევე ცოდნის, გამოცდილებისა და სადაზვერვო მონაცემების ინტეგრაციის გზით, უზრუნველყოფს კოორდინირებულ საქმიანობას. თუმცა ცენტრის საქმიანობა და მასთან დაკავშირებული საკითხები მთლიანობაში გასაიდუმლოებულია;
- **იაპონია** - კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვისა და ინფორმაციული უსაფრთხოების უზრუნველყოფის სფეროში მთავარ მოქმედ პირს წარმოადგენს მინისტრთა კაბინეტის სამდივნო. მის სტრუქტურულ შემადგენლობაში ფუნქციონირებს ინფორმაციული ტექნოლოგიების განვითარების სტრატეგიის საბჭო, სადაც შედის 20 ავტორიტეტული ექსპერტი. 2005 წელს მინისტრთა კაბინეტის სამდივნოს სტრუქტურაში შეიქმნა ინფორმაციული უსაფრთხოების პოლიტიკის საბჭო (ISPC) და ინფორმაციული უსაფრთხოების ეროვნული ცენტრი (NISC), რომლებსაც დღეს უკავიათ წამყვანი ადგილი ეროვნული პოლიტიკის კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის სფეროში. ინფორმაციული უსაფრთხოების პოლიტიკის საბჭო (ISPC) წარმოადგენს მთავარ სახელმწიფო ორგანოს უსაფრთხოების პოლიტიკისა და სტრატეგიის მოდერნიზაციისა და დამუშავების საკითხებში. საბჭოს ხელმძღვანელობს მინისტრთა კაბინეტის სამდივნოს უფროსი და ის შედის ინფორმაციული ტექნოლოგიების სტრატეგიულ შტაბში, სადაც ასევე შედიან სხვადასხვა სამინისტროებისა და კერძო სექტორის წარმომადგენლები. ინფორმაციული უსაფრთხოების ეროვნული ცენტრი (NISC) წარმოადგენს ინფორმაციული ტექნოლოგიების უსაფრთხოების საკითხებში აღმასრულებელი

ხელისუფლების ცენტრალურ ორგანოს. მინისტრთა კაბინეტის სამდივნო მოქმედებს ეკონომიკის, ვაჭრობისა და მრეწველობის სამინისტროს (METI)[41], ეროვნული პოლიციის სააგენტოს (NPA)[42] და შინაგან საქმეთა და კომუნიკაციების სამინისტროს მხარდაჭერით. ინფორმაციული ტექნოლოგიების სტრატეგიული შტაბის ხელმძღვანელობით, METI ახორციელებს ინფორმაციული პოლიტიკის დაგეგმვასა და რეალიზებას, ასევე დაკავებულია ელექტრონული ვაჭრობის საკითხებით, მონაცემთა დაცვით, ინფორმაციული ტექნოლოგიების სფეროში კვლევებითა და განვითარებით. ეროვნული პოლიციის სააგენტო (NPA) უზრუნველყოფს კომპიუტერულ და ქსელურ უსაფრთხოებას, ასევე აწარმოებს კიბერდანაშაულებების საგამოძიებო საქმიანობას. ამ მიზნით, სააგენტოს ფარგლებში მოქმედებს მაღალტექნოლოგიური დანაშაულებების სამმართველო (HTCTD), რომელიც ებრძვის მსხვილმასშტაბიან კომპიუტერულ ინციდენტებს, ასევე უფლებამოსილია განახორციელოს მოკვლევა და დაკავება. სამმართველოს ერთერთ ქვედანაყოფს წარმოადგენს ტექნიკური მხარდაჭერის მობილური ჯგუფი, რომელიც განლაგებულია ქვეყნის მთელ ტერიტორიაზე და იმყოფება კიბერსარდლობის ცენტრის დაქვემდებარებაში. სახელმწიფოსა და კერძო სექტორს შორის პარტნიორობის ფარგლებში მოქმედებს ფინანსების დაცვის, ტექნიკური ექსპლუატაციის, ანალიზისა და რეაგირების ცენტრი (CEPTOAR), რომლის მთავარი მიზანია სახელმწიფო და კერძო სუბიექტებს შორის ინფორმაციის გაცვლის გაუმჯობესება;

- **კორეის რესპუბლიკა** - კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვით ღონისძიებებს ახორციელებს ყველა სახელმწიფო ორგანიზაცია და მათი სტრუქტურული ქვედანაყოფები. მოცემულ სფეროში ყველა სამინისტროსი და უწყების საქმიანობას კოორდინაციას უწევს კიბერუსაფრთხოების ეროვნული ცენტრი (NCSC)[43], რომელიც მუშაობს დაზვერვის ეროვნული სამსახურის (NIS)[44] ეგიდით. გარდა ამისა, კიბერუსაფრთხოების ეროვნული ცენტრი (NCSC) კიბერსაფრთხეებთან ბრძოლაში აერთიანებს კერძო, საჯარო და სამხედრო სექტორებს, ცენტრი ასევე წარმოადგენს კიბერშეტევების გამოვლენის, გაუვნებელყოფისა და კიბერსაფრთხეებზე ოპერატიული რეაგირების საკითხებში აღმასრულებელი ხელისუფლების ცენტრალურ ორგანოს. კიბერდანაშაულის პროფილაქტიკურ და საგამოძიებო საქმიანობის კოორდინაციას აწარმოებს გენერალური პროკურატურის სპეციალური სგამოძიებო ორგანო. ელექტრონიკისა და ტელეკომუნიკაციის სამეცნიერო - კვლევითი ინსტიტუტი (ETRI)[45] ახორციელებს შესაბამისი ტექნოლოგიების განვითარებასა და კრიტიკული

[41] http://www.meti.go.jp/english/
[42] http://www.npa.go.jp/english/index.htm
[43] http://service1.nis.go.kr/eng/intro/NCSCInfo.jsp
[44] http://eng.nis.go.kr/svc/index.do
[45] https://www.etri.re.kr/eng/main/index.etri

ინფორმაციული ინფრასტრუქტურის დაცვით ღონისძიებებს. მოცემულ სფეროში ინტერნეტისა და სატელეკომუნიკაციო ქსელის უსაფრთხოების კულტურის ფორმირებაზე პასუხისმგებელია ასევე სახელმწიფო მართვისა და უსაფრთხოების სამინისტრო (MOPAS)[46], კავშირგაბმულობის კომისია, ცოდნისა და ეკონომიკის სამინისტრო, ინფორმაციული უსაფრთხოების სააგენტოს (KISA)[47] შემადგენლობაში არსებული ინტერნეტის უსაფრთხოების ცენტრი (KrCERT/CC)[48]. KISA - ში შედის აგრეთვე ინფორმაციული ინფრასტრუქტურის დაცვის განყოფილება, რომელიც შედგება კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვითი ღონისძიებების დაგეგმვის, კრიტიკული ინფრასტრუქტურის უსაფრთხოების მართვისა და სერტიფიკაციის ჯგუფებისგან. ინფორმაციული უსაფრთხოების ეროვნული ალიანსი (NISA), სადაც გაერთიანებულია 22 სახელმწიფო ორგანიზაცია, 17 საწარმოს[49] ინფორმაციული უსაფრთხოების სამსახურების ხელმძღვანელი პირები, ასევე სპეციალისტები სამრეწველო და სამეცნიერო წრეებიდან, წარმოადგენს სახელმწოფოსა და კერძო სექტორებს შორის პარტნიორობას, რომელიც მიმართულია ინფორმაციის გაცვლის გზით, ინფორმაციული უსაფრთხოების ამაღლებასა და განვითარებაზე.

საქართველოში არსებული სუბიექტები

საქართველოში არ არსებობს ერთიანი ორგანო, რომელიც კოორდინაციას გაუწევს ქვეყნის კიბერსივრცის დაცვასა და უზრუნველყოფს კიბერუსაფრთხოებასთან დაკავშირებულ ღონისძიებებს სამინისტროებსა და უწყებებს შორის. განხორციელებულმა საკონსტიტუციო ცვლილებებმა და უშიშროების საბჭოს ალტერნატიული ორგანოს უსაფრთხოებისა და კრიზისების მართვის საბჭოს შექმნამ გამოიწვია მოცემული საკითხის დროებით ღიად დატოვება. კერძოდ, უშიშროების საბჭომ, რომელმაც თავის დროზე შეიმუშავა კიბერუსაფრთხოების სტრატეგია, და რომლის ფარგლებშიც უნდა ყოფილიყო კიბერსივრცის დაცვის საკითხებზე მომუშავე უწყებათაშორისი კომისია[50], თავისი ფუნქციები მოცემულ სფეროში გადასცა უსაფრთხოებისა და კრიზისების მართვის საბჭოს, სადაც ჯერჯერობით ამ მიმართულებით წინსვლა არ არის. მიუხედავად ამისა, კანონში „ინფორმაციული უსაფრთხოების შესახებ“ განსაზღვრულია კიბერუსაფრთხოებაზე პასუხიმგებელი და მაკოორდინირებელი სახელმწიფო ორგანო. კერძოდ, კანონის მე - 3 თავში „კიბერუსაფრთხოების უზრუნველყოფა“ ვკითხულობთ, რომ „საქართველოს კიბერსივრცეში ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვას, ასევე

[46] http://www.iclei.org/
[47] http://www.kisa.or.kr/eng/main.jsp
[48] http://eng.krcert.or.kr/krcert_cc/welcome.jsp
[49] ინფორმაციული ქსელების სახელმწიფო კომპანიები და ოპერატორები
[50] კომისიაში შედიოდა ყველა სამინისტროსა და უწყებების წარმომადგენლები

ინფორმაციული უსაფრთხოების კოორდინაციისკენ მიმართულ სხვა, მასთან დაკავშირებულ საქმიანობას, რომელიც კიბერუსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრას ემსახურება, ახორციელებს მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი - CERT.GOV.GE"[51]. მოცემული ჯგუფის მოვალეობებში შედის კრიტიკული ინფორმაციული სისტემის ინფორმაციული უსაფრთხოების დაცვის შესახებ რეკომენდაციების გაცემა, კომპიუტერული ინციდენტების ანალიზი, აღრიცხვა, მათი დროული გამოვლენა, რეაგირება და კოორდინაციის უზრუნველყოფა და სხვა. ასევე, ჯგუფი პასუხისმგებელია მოცემულ სფეროში ცნობიერების ამაღლებაზე, საგანმანათლებლო პროცესზე და სხვა[52].

საქართველოში კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვაზე, კიბერუსაფრთხოებით ღონისძიებების უზრუნველყოფასა და კიბერდანაშაულთან ბრძოლას წარმართავს იუსტიციის, თავდაცვისა და შინაგან საქმეთა სამინისტროები, რომლებსაც განსაზღვრული აქვთ და მოქმედებენ თავიანთი კომპეტენციის ფარგლები. კერძოდ:

- მოცემული სამინისტროებიდან ქვეყნის კრიტიკული ინფორმაციული ინფრასტრუქტურის სისტემებისა და სუბიექტების დაცვაზე პასუხისმგებელია იუსტიციის სამინისტროს სსიპ „მონაცემთა გაცვლის სააგენტო"[53], სადაც ასევე გაერთიანებულია ზემოთ ნახსენები კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი - CERT.GOV.GE. სააგენტო ასევე განსაზღვრავს ინფორმაციული უსაფრთხოების პოლიტიკას[54], კოორდინაციასა და მონიტორინგს უწევს სამინისტროებსა და უწყებებში ინფორმაციული უსაფრთხოების მიმართულებით გასატარებელ ყველა ღონისძიებას. მონაცემთა გაცვლის სააგენტო ასევე აქტიურად თანამშრომლობს საერთაშორისო დონეზე, კერძოდ ევროკავშირის წევრ ქვეყნებთან და ნატო - ს შესაბამის სტრუქტურულ ერთეულებთან. გარდა ამისა, სააგენტო წარმატებით ახორციელებს E – Governmant[55] სისტემის დანერგვის პროცესს;

[51] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, თავი III, მუხლი 8, გვ. 7

[52] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, თავი III, მუხლი 8, გვ. 7, 8

[53] http://dea.gov.ge/uploads/legal_acts/1/monacemta%20gacvlis%20saaagento_geo.pdf

[54] http://dea.gov.ge/uploads/legal_acts/8/Inf._Security.pdf

[55] E-government (short for electronic government, also known as e-gov, Internet government, digital government, online government, or connected government) consists of the digital interactions between a citizen and their government (C2G), between governments and government agencies (G2G), between government and citizens (G2C), between government and employees (G2E), and between government and businesses/commerce (G2B). Essentially, e-government delivery models can be briefly summed up as (Jeong, 2007):
G2G (government to governments)
G2C (government to citizens)
G2E (government to employees)
G2B (government to businesses)

- 2014 წლის თებერვალში[56] თავდაცვის სამინისტროს ფარგლებში შეიქმნა სსიპ „კიბერუსაფრთხოების ბიურო“[57], რომლის მიზანია კიბერდანაშაულთან ბრძოლის ერთიანი სახელმწიფო პოლიტიკის განხორციელება, ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავება და მისი განხორციელების ხელშეწყობა, ბიუროს კომპეტენციას მიკუთვნებული სფეროს მარეგულირებელი კანონმდებლობის შემუშავება და სრულყოფა და კანონმდებლობით დადგენილი სხვა საქმიანობის განხორციელება. ბიუროს ძირითადი საქმიანობა წარიმართება ინფორმაციული და კომუნიკაციების ტექნოლოგიების დეპარტამენტის მიერ, რომლის სტრუქტურული ერთეულებია: პროექტების მართვის სამმართველო; კომპიუტერულ ინციდენტებზე რეაგირების საკოორდინაციო სამმართველო CSIRT/CC); კომპიუტერულ ინციდენტებზე რეაგირების სამმართველო (CSIRT); კომპიუტერულ ინციდენტებზე რეაგირების საკომუნიკაციო მომსახურების განყოფილება;
- ინტერნეტ - სივრცეში კიბერდანაშაულების გამოვლენას, აღკვეთას, მოკვლევით და საგამოძიებო საქმიანობას, ასევე საჭიროების შემთხვევაში დაკავებას, ახორციელებს შინაგან საქმეთა ცენტრალური კრიმინალური პოლიციის დეპარტამენტის კიბერდანაშაულთან ბრძოლის სამმართველო[58]. გარდა ამისა, შინაგან საქმეთა სამინისტროში საექსპერტო–კრიმინალისტიკური მთავარი სამმართველოს შემადგენლობაში ჩამოყალიბდა კომპიუტერულ–ციფრული ექსპერტიზის ქვეგანყოფილება, რომელიც უშუალოდ ახორციელებს ციფრული მტკიცებულებების პირველად მოპყრობასა და მათ შემდგომ ექსპერტიზას. სამინისტროს შემადგენლობაში ასევე ფუნქციონირებს ოპერატიულ - ტექნიკური დეპარტამენტი, რომელიც ახორციელებს სამინისტროში ინოვაციური ინფორმაციული ტექნოლოგიების, ციფრული სატელეკომუნიკაციო სისტემების დანერგვას და ოპერირებას, აღნიშნულ სფეროებში სხვა სახელმწიფო დაწესებულებების კონსულტირებას, სამინისტროსა და მისი სტრუქტურული ქვედანაყოფების სატელეკომუნიკაციო უზრუნველყოფას და კანონმდებლობით დადგენილი წესის შესაბამისად, საგამოძიებო ღონისძიებების განხორციელების შედეგად მოპოვებული ციფრული მტკიცებულებების საექსპერტო - კრიმინალისტიკურ გამოკვლევას.

[56] https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=2235212&lang=ge

[57] კიბერუსაფრთხოების ბიუროს მიზნები და ფუნქციების დიდი ნაწილი წარმოადგენს მონაცემთა გაცვლის სააგენტოს მიზნებისა და ფუნქციების ანალოგიას, რაც ყოვლად დაუშვებელია, ვინაიდან მოხდება მოცემულ სფეროში უწყებრივი ფუნქციების აღრევა და სამუშაო პროცესის წარმართვა პარალელურ რეჟიმში

[58] 2012 წელს საქართველო შეუერთდა კიბერდანაშაულთან ბრძოლის შესახებ ევროსაბჭოს კონვენციას. ამავე წელს შსს-ს ცენტრალური კრიმინალური პოლიციის დეპარტამენტში შეიქმნა კიბერდანაშაულთან ბრძოლის სამმართველო, რომელსაც ევალება კიბერ სივრცეში ჩადენილი მართლსაწინააღმდეგო ქმედებების გამოვლენა, აღკვეთა და პრევენცია.

რეზუმე

ნაშრომში მოკლედ, ზოგად ფორმებში არის განხილული ევროკავშირის ზოგიერთი წევრი ქვეყნისა და სხვა ქვეყნების სუბიექტები, რომლებიც პასუხისმგებელნი არიან კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვასა და კიბერუსაფრთხოების მიმართულებით აუცილებელი ღონისძიებების განხორციელებაზე. კიბერსივრცეში არსებული საფრთხები და რისკები არცთუ ისე დიდი ხნის წინ წარმოიშვა, თუმცა ინტერნეტისა და ტექნოლოგიების სწრაფმა განვითარებამ, დადებითი პროცესების პარალელურად, გამოიწვია ასევე კიბერდანაშაულის სწრაფი ზრდა. კიბერსივრცეში საფრთხეების მაქსიმალური შემცირების მიზნით, მსოფლიო საზოგადოებამ დაიწყო ორგანიზაციული სტრუქტურული ერთეულების შექმნისა და განვითარების პროცესი, რაც პირდაპირ კავშირშია ახალი ტექნოლოგიებისა და კიბერდანაშაულის ზრდასთან, მის ახალ გამოვლინებებთან. ფაქტიურად, მოცემულ სფეროში მუდმივად მიმდინარეობს და ვითარდება ინსტიტუციონალიზმის პროცესი.

საქართველო აქტიურად მიისწრაფვის ევროინტეგრაციისკენ, ქვეყანა ცდილობს გახდეს ევროკავშირისა და ჩრდილოეთ ალიანსის სრულუფლებიანი წევრი, ხელი მოეწერა ასოცირების ხელშეკრულებას. ყოველივე ეს ნიშნავს, რომ ქვეყანა თავის თავზე იღებს ყველა იმ ვალდებულებას, რაც უზრუნველყოფს არამარტო საქართველოს უსაფრთხოებას, არამედ ევროკავშირის როგორც ცალკეული წევრი ქვეყნებისა ისე მთლიანად ევროკავშირის უსაფრთხოების შესაბამისი ნორმების დაცვას, სადაც ასევე იგულისხმება კიბერსივრცის მაქსიმალური დაცვის უზრუნველყოფა. ეს არის ქვეყნისთვის სერიოზული გამოწვევა, რადგან საქართველომ უნდა შექმნას ეროვნული კანონმდებლობა, წესრიგში მოიყვანოს და საერთაშორისო სტანდარტებს შეუსაბამოს ქვეყნის კრიტიკული ინფორმაციული ინფრასტრუქტურის სისტემისა და ცალკეული სუბიექტების დაცვა, გაზარდოს საერთაშორისო თანამშრომლობა და რისკების შემცირების მიზნით, უნდა მოახდინოს საზოგადოების ცნობიერების ამაღლება და საგანმანათლებლო სისტემის შემუშავება. მოცემულ სფეროში აქტუალური და აუცილებელი ხდება საქართველოს სუბიექტების, ევროკავშირის წევრი და სხვა ქვეყნების ანალოგიურ სუბიექტებთან ინტეგრაციის პროცესის სწორი მიმართულებით წარმართვა, მათი ცოდნისა და გამოცდილების გაზიარება, რაც ხელს შეუწყობს კიბერუსაფრთხოების სფეროში ქვეყნის ორგანიზაციულ სტრუქტურული სუბიექტების განვითარებას, მათ საერთაშორისო სტანდარტებთან შესაბამისობაში მოყვანას, კოორდინირებული მუშაობის ამაღლებასა და ეფექტური ღონისძიებების გატარებას კრიტიკული ინფორმაციული ინფრასტრუქტურისა და პერსონალური თუ სხვა სახის მონაცემთა დაცვის მიმართულებით.

ლიტერატურა

1) Democratic Governance Challenges of Cyber Security, *Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler*, DCAF 2010, DCAF Horizon 2015 Working Paper Series http://genevasecurityforum.org/files/DCAF-GSF-cyber-Paper.pdf; http://www.dcaf.ch/Publications/Democratic-Governance-Challenges-of-Cyber-Security;
2) კანონი „ინფორმაციული უსაფრთხოების შესახებ“, 19/06/2012 http://www.economy.ge/uploads/kanonmdebloba/kavshirgabmuloba/informaciuli_usafrtxoeba.pdf;
3) საჯარო სამართლის იურიდიული პირის – კიბერუსაფრთხოების ბიუროს დებულების დამტკიცების შესახებ, *საქართველოს თავდაცვის მინისტრის ბრძანება №8*, 2014 წლის 6 თებერვალი https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=2235212&lang=ge.