დიდი ბრიტანეთის კიბერშესაძლებლობები

2009 წელს[1] 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[2]. პირველ რიგში ეს არის მინისტრთა კაბინეტის სტრუქტურაში შემავალი კიბერუსაფრთხოების სამმართველო (OCS)[3], 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[4] 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)[5] შემადგენლობაშია კომპიუტერების დახმარების სასწრაფო სამსახური (CERT Service)[6].

[1] 2011 წელს მოხდა სტრატეგიის განახლება https://www.cpni.gov.uk/advice/cyber/cir/
[2] ორივე ორგანიზაციამ დაიწყო ფუნქციონირება 2010 წელს;
[3] https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance
[4] http://www.gchq.gov.uk/Pages/homepage.aspx
[5] http://www.cpni.gov.uk/Templates/CPNI/pages/Default.aspx
[6] https://www.cpni.gov.uk/advice/cyber/cir/

გაერთიანებული სამეფოს მიდგომა ასევე მიმართულია კიბერუსაფრთხოების განვითარებაზე. სტრატეგიის მთავარი მიზანია გაიყვანოს დიდი ბრიტანეთი მოწინავე პოზიციებზე ინფორმაციული და სატელეკომუნიკაციო ტექნოლოგიების სფეროში ინოვაციების, ინვესტიციებისა და ხარისხიანი მომსახურების მიხედვით. ასევე მთლიანად ისარგებლოს კიბერსივრცის ყველა უპირატესობებითა და მიღწევებით. 2011 წელს შემოღებული სტრატეგია ასახავს მაქსიმალური რისკების შემცირებას დამნაშავეთა (მათ შორის ტერორისტების) და სხვა სახელმწიფოთა მხრიდან კიბერშეტევების მიმართ, რაც მიმართულია კიბერსივრცეში თითოეული მოქალაქის, საზოგადოებისა და ეკონომიკის უსაფრთხოებისკენ.

2014 წლის დეკემბერში[7] პრემიერ - მინისტრის ოფისმა გამოაქვეყნა მოხსენება კიბერუსაფრთხოების სფეროში მიმდინარე სამუშაოებისა და მომავალი გეგმების შესახებ. ეს წარმოადგენს 2011 წლის სტრატეგიის მხარდამჭერ დოკუმენტს, სადაც ასახულია სტრატეგიის მიზნების განხორციელების გზები და საშუალებები, კერძოდ:

- დიდი ბრიტანეთი გახდეს მსოფლიოში ერთერთი უსაფრთხო ადგილი კიბერსივრცეში ბიზნესის საწარმოებლად;
- დიდი ბრიტანეთი გახდეს უფრო სტაბილური კიბერშეტევების მიმართ და უკეთ დაიცვას ქვეყნების ინტერესები კიბერსივრცეში;
- ღია, გამჭვირვალე და სტაბილური კიბერსივრცის ფორმირება, რომელიც მხარს უჭერს ღია საზოგადოებას;
- დიდ ბრიტანეთში კიბერუსაფრთხოების ცოდნის, უნარებისა და შესაძლებლობების გაზრდა.

მოცემული მიზნების მისაღწევად დიდი ბრიტანეთის მთავრობა მუშაობს კიბერუსაფრთხოების ეროვნული პროგრამის[8] ფარგლებში, კერძოდ:

- უმაღლესი კლასის კიბერ საფრთხეების აღმოჩენისა და აღმოფხვრის მიზნით, ეროვნული შესაძლებლობების შემდგომი განმტკიცება;
- კიბერდანაშაულის დაძლევისა და ინტერნეტში ბიზნესის საწარმოებლად აუცილებელი ნდობის შენარჩუნების მიზნით, სამართალდამცავი ორგანოების უნარებისა და შესაძლებლობების გაზრდა;
- დიდი ბრიტანეთის კრიტიკული სისტემებისა და ქსელების უზრუნველყოფა სანდოობითა და სტაბილურობით;
- კიბერ ცნობიერებისა და ბრიტანული ბიზნესის რისკების მართვის გაუმჯობესება;

[7] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf

[8] the National Cyber Security Programme (NCSP).

- საზოგადოების წევრების თავის დაცვასა და მათ მიერ მოხმარებული სერვისების კიბერუსაფრთხოების შესახებ ცნობიერების ამაღლების უზრუნველყოფა;
- კიბერუსაფრთხოების მიმართულებით სამეცნიერო კვლევებისა და განათლების გაძლიერება, მაღალკვალიფიცირებული კადრების ყოლა და ახალ ტექნოლოგიებზე მუშაობის მუდმივი პროცესის უზრუნველყოფა;
- საერთაშორისო პარტნიორებთან მუდმივი მუშაობა და მათთან საერთაშორისო დიალოგის წარმოება, რაც ხელს შეუწყობს ღია, დინამიური და უსაფრთხო კიბერსივრცის ჩამოყალიბებას.

მოცემული სამუშაოები ტარდება კიბერუსაფრთხოების ეროვნული პროგრამის (the National Cyber Security Programme (NCSP)) მხარდაჭერით. პროგრამის მიზნობრივი დაფინანსება მომავალი ორი წლის განმავლობაში შეადგენს 860 მილიონ ფუნტ სტერლინგს. პროგრამის მიზანია ხელი შეუწყოს ისეთ პროექტებს, რომლებიც განავითარებენ კიბერუსაფრთხოების შესაძლებლობებს და სტიმულს მისცემენ დიდი ბრიტანეთის კიბერუსაფრთხოების ბაზარს.

მინისტრთა კაბინეტის ოფისსა და ეროვნული უსაფრთხოების საბჭოს მხარდამჭერია კიბერუსაფრთხოებისა და ინფორმაციული უზრუნველყოფის ოფისი[9], რომელიც მთავრობისთვის უზრუნველყოფს კიბერუსაფრთხოების სტრატეგიულ მიმართულებასა და კოორდინაციას უწევს პროგრამებს. ოფისის ხელმძღვანელია James Quinault და ის მუშაობს სხვა სახელმწიფო დეპარტამენტებთან და სააგენტოებთან, კერძოდ:

- მთავარი ოფისი[10];
- თავდაცვის სამინისტრო[11];
- სამთავრობო კავშირის მთავარი ოფისი[12];
- კომუნიკაციებისა და ელექტრონული უსაფრთხოების დეპარტამენტი[13];
- ეროვნული ინფრასტრუქტურის დაცვის ცენტრი[14];
- საგარეო და ბრიტანეთის თანამეგობრობის ოფისი[15];

[9] The Office of Cyber Security & Information Assurance (OCSIA) https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance
[10] https://www.gov.uk/government/organisations/home-office
[11] https://www.gov.uk/government/organisations/ministry-of-defence
[12] Government Communications Headquarters (GCHQ) http://www.gchq.gov.uk/Pages/homepage.aspx
[13] the Communications-Electronics Security Department (CESG) http://www.cesg.gov.uk/Pages/homepage.aspx
[14] the Centre for the Protection of National Infrastructure (CPNI) http://www.cpni.gov.uk/
[15] the Foreign & Commonwealth Office (FCO) https://www.gov.uk/government/organisations/foreign-commonwealth-office

- ბიზნესის, ინოვაციებისა და უნარების დეპარტამენტი[16].

საერთაშორისო ურთიერთობების ფარგლებში დიდი ბრიტანეთი აგრძელებს ორმხრივ და მრავალმხრივ თანამშრომლობას ევროკავშირთან, NATO - სთან, ბრიტანეთის თანამეგობრობისა და სხვა ქვეყნებთან. ორმხრივი თანამშრომლობა გაძლიერდა კორეის რესპუბლიკასთან, ისრაელთან, სინგაპურთან და იაპონიასთან. კერძოდ, ხელი მოეწერა ურთიერთგაგების მემორანდუმებს კორეის რესპუბლიკასთან და ისრაელთან; ხოლო სინგაპურთან და იაპონიასთან დაწყებულია მოლაპარაკებები კიბერუსაფრთხოების სფეროში მრავალმხრივი თანამშრომლობის შესახებ, რომელიც ამა წლის მარტის თვეში დასრულდება; 2015 წელს ასევე იგეგმება დიალოგის დაწყება ინდოეთთან და ჩინეთთან.

დიდი ბრიტანეთი წარმატებით ეხმარება ევროკავშირს კიბერუსაფრთხოების სტრატეგიის ფორმირებაში, სადაც ასევე განსაზღვრულია ევროკავშირის ცალკეულ წევრ ქვეყნებთან მჭიდრო თანამშრომლობა. ასევე ქვეყანა არის აქტიური მონაწილე ევროპაში უსაფრთხოებისა და თანამშრომლობის ორგანიზაციის (ეუთო)[17] კიბერსივრცეში ნდობის აღდგენის ღონისძიებების[18] მიმართულებით.

2014 წლის ივნისში დიდი ბრიტანეთი გახდა NATO - ს კიბერ თავდაცვის ცენტრის[19] სრულუფლებიანი წევრი. ქვეყანა ცენტრის მუშაობაში შეიტანს მნიშვნელოვანს წვლილს და წარმოდგენილი იქნება განათლების, სასწავლო პროგრამების, კონსულტაციების, კვლევებისა და განვითარების (R&D) მიმართულებით. ასევე დიდი ბრიტანეთის ინიციატივა სამრეწველო კიბერ პარტნიორობის[20] შესახებ მოწონებული იქნა ალიანსის წევრი ქვეყნების მიერ და აღინიშნა უელსის სამიტის დეკლარაციაში, კერძოდ „technological innovations and expertise from the private sector are crucial to enable NATO and Allies to achieve the Enhanced Cyber Defence Policy"s objectives".

კიბერუსაფრთხოების ეროვნული პროგრამის (the National Cyber Security Programme (NCSP)) ფარგლებში ასევე ფინანსდება დიდი ბრიტანეთის თანამეგობრობის ქვეყნების სატელეკომუნიკაციო ორგანიზაციები, რათა მათ შეძლონ განვითარება და ეროვნული კიბერუსაფრთხოების მოდელის იმპლიმენტაცია.

მთავრობა აგრძელებს კიბერუსაფრთხოების გაძლიერებას შეიარაღებულ ძალებში, სადაც სამხედრო ოპერაციების დაგეგმვასა და განხორციელებაში სულ უფრო

[16] the Department for Business, Innovation & Skills (BIS) https://www.gov.uk/government/organisations/department-for-business-innovation-skills
[17] the Organisation for Security and Cooperation in Europe (OSCE);
[18] Confidence Building Measures (CBMs) for cyberspace at the OSCE;
[19] the NATO Cooperative Cyber Defence Centre of Excellence;
[20] NATO Industry Cyber Partnership (NICP);

აქტიურად გამოიყენება კიბერშესაძლებლობები. შეიარაღებულ ძალებში ჩამოყალიბდა კიბერ თავდაცვის პარტნიორობა[21], რომლის მიზანია ინფორმაციული უსაფრთხოების უზრუნველყოფა, საუკეთესო პრაქტიკის გაზიარება, ცნობიერების ამაღლება და სტანდარტების დანერგვა. პარტნიორობა თავისთან მოიცავს კერძო ბიზნესის ცამეტ წარმომადგენელს, რომელთა შორის ყველაზე მსხვილი არის ADS[22] და techUK[23]. თავდაცვის კიბერუსაფრთხოების მოდელი ოფიციალურად იმპლიმენტირებული იქნება 2015 წელს. თუმცა უნდა ითქვას, რომ დიდ ბრიტანეთში ისევე როგორც ბევრ წამყვან ქვეყანაში კიბერუსაფრთხოების სფეროში სამოქალაქო და სამხედრო მიმართულებები მკაცრად არის ერთმანეთისგან გამიჯნული. თავდაცვის სამინისტროში კიბერუსაფრთხოების უზრუნველყოფასა და ოპერაციებზე პასუხისმგებელია სამინისტროს გაერთიანებული ძალების სარდლობა[24]. აღსანიშნავია, რომ 2015 წელს დაგეგმილია 200 - მდე ინფორმაციული ტექნოლოგიების სპეციალისტისა და პროგრამისტის გაწვევა. ასევე ყოფილი სამხედროებისგან იქმნება რეზერვისტთა ჯგუფი კიბერუსაფრთხოების მიმართულებით.

2014 წლის მარტში შეიქმნა ახალი ორგანიზაცია CERT - UK[25], რომლის მიზანია კიბერ ინციდენტებზე რეაგირება და ინფორმაციის გაზიარება NATO - ს წევრ ქვეყნებთან, ასევე თავად ალიანსთან.

დიდ ბრიტანეთში დიდი ყურადღება ეთმობა კიბერ სფეროში საჭირო უნარების, განათლების მიღებისა და პროფესიული განვითარების პროცესს. ასევე დარგის სამეცნიერო და კვლევით საქმიანობას. შეიძლება ითქვას, რომ ამ მიმართულებით დიდი ბრიტანეთი არის ერთერთი წამყვანი ქვეყანა, რომელსაც საკმაოდ მოქნილი და ეფექტური საგანმანათლებლო სისტემა აქვს შექმნილი[26] მთავრობა ეძებს ახალ ტალანტებს და უქმნის მათ ყველა საჭირო პირობას, რათა ისინი ჩამოყალიბდნენ მაღალი კვალიფიკაციის სპეციალისტებად. ქვეყნის ხელისუფლებამ შემოიღო საინტერესო ინიციატივა, კერძოდ კიბერუსაფრთხოება სხვადასხვა დონეზე ისწავლება ყველა სასწავლებელში დაწყებული 11 წლის ასაკიდან[27]. ეს ინიციატივა იძლევა იმის საშუალებას, რომ ქვეყნის მოქალაქეს ადრეული ასაკიდან აქვს გარკვეული ზოგადი წარმოდგენა კიბერუსაფრთხოებაზე და კიბერსივრცეში არსებულ საფრთხეებზე[28].

---

[21] the Defence Cyber Protection Partnership (DCPP).

[22] https://www.adsgroup.org.uk/

[23] http://www.techuk.org/

[24] Joint Forces Command at MOD of UK https://www.gov.uk/government/organisations/joint-forces-command/about

[25] https://www.cert.gov.uk/

[26] ამ მიმართულებით ბიუროსთვის კარგი იქნება ბრიტანელ კოლეგებთან თანამშრომლობა;

[27] ჩვენი ქვეყნისთვისაც საინტერესო ინიციატივა იქნებოდა;

[28] ამით იზრდება ქვეყნის კიბერსივრცის დაცულობა და მცირდება რისკები;

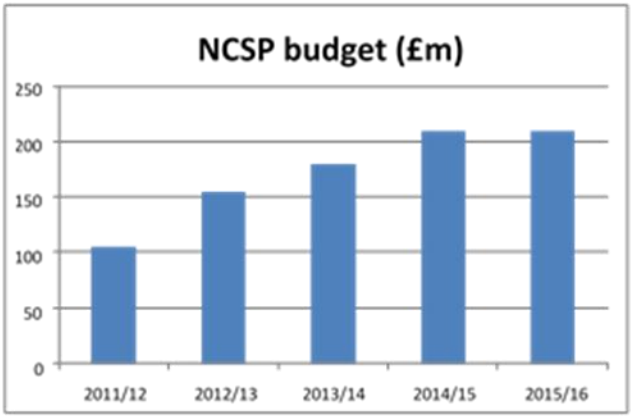
სკოლებში მოქმედებს პროგრამა Make IT Happy[29] და არსებობს სპეციალური სასწავლო მასალა Behind the screen[30]. კიბერუსაფრთხოების მიმართულებით საგანმანათლებლო პროგრამები ხორციელდება უშუალოდ მთავრობის, კერძოდ სამთავრობო კავშირის მთავარი ოფისის (GCHQ) მიერ, რომელიც პროფესიული განვითარების კუთხით თანამშრომლობს Tech Partnership - თან[31], ხოლო დარგის აკადემიურ დონეზე შესწავლისა და კვლევების მიმართულებით ოფისი პარტნიორობს 11 უმაღლეს სასწავლებელთან[32]. ცალკე არის გამოყოფილი სამაგისტრო პროგრამები[33], სადაც შერჩეულია ხუთი უმაღლესი სასწავლებელი და ისევ ოფისის პატრონაჟით ხორციელდება სასწავლო პროგრამები.

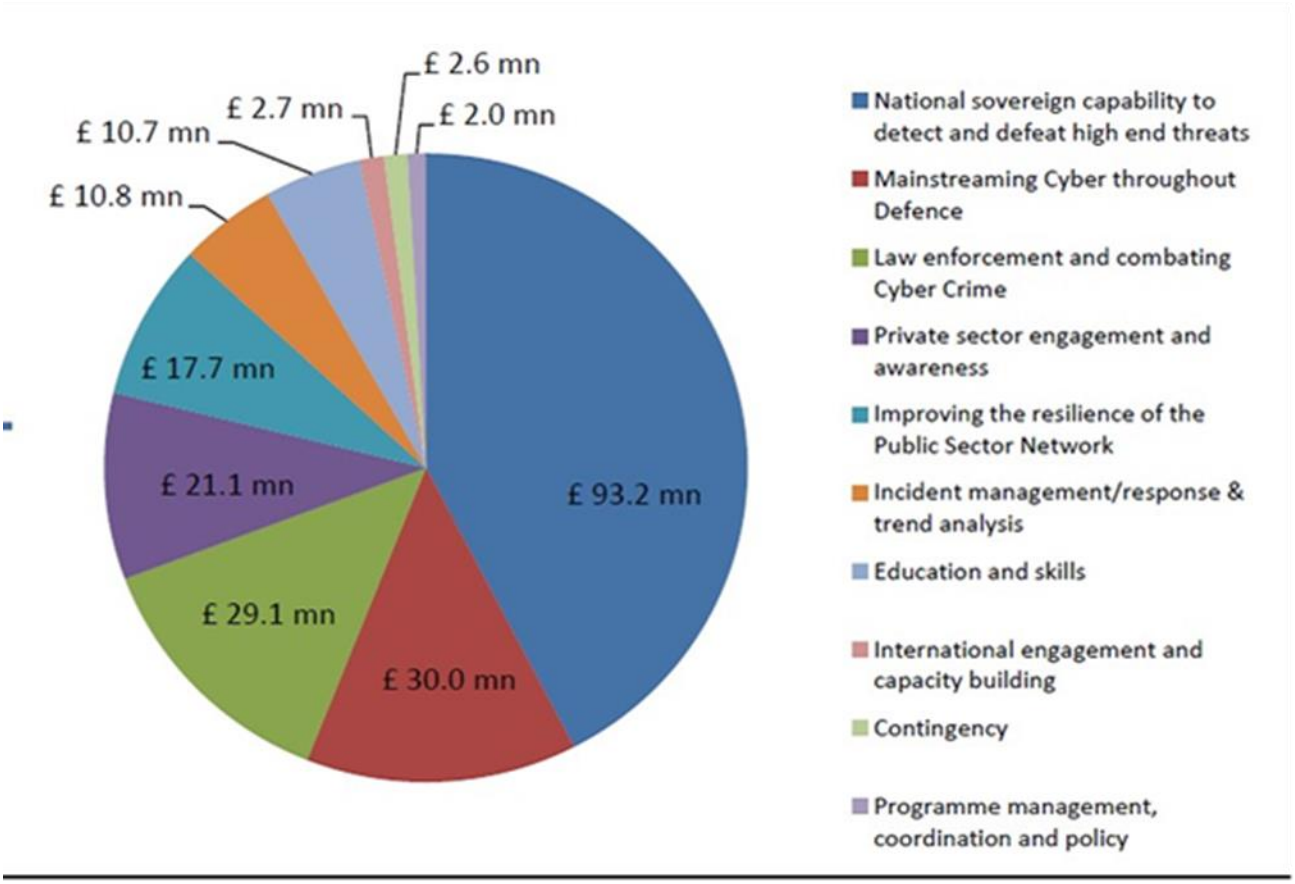
ექსპერტთა აზრით, მსგავსი საგანმანათლებლო სისტემა, რომელიც მთავრობის მკაცრი კონტროლის ქვეშ იმყოფება, სხვა წამყვან ქვეყნებთან მიმართებაში დიდ ბრიტანეთს უახლოეს მომავალში საშუალებას მისცემს იყოლიოს მაღალი კვალიფიკაციისა და პროფესიონალი ადამიანური რესურსი, და გახდეს დარგის ერთერთი ლიდერი ქვეყანა.

[29] http://makeithappy.cc4g.net/
[30] http://www.techfutureclassroom.com/
[31] http://www.thetechpartnership.com/
[32] https://www.cesg.gov.uk/awarenesstraining/academia/Pages/Academic-Centres.aspx
[33] http://www.gchq.gov.uk/press_and_media/press_releases/Pages/GCHQ-certifies-Masters-Degrees-in-Cyber-Security.aspx

NATIONAL CYBER SECURITY FUNDING

The allocation of NCSP funding for 2014/15 is set out below. These figures do not include spending in support of cyber objectives funded outside the NCSP. The chart demonstrates the spread of spend across the full range of cyber security activity. The sp end on „sovereign capabilities", not broken down here, supports activity across the Programme.





ეროვნული კიბერუსაფრთხოების დაფინანსება

დიაგრამებზე ნაჩვენებია NCSP - ის 2014/15/16 წლების ბიუჯეტი, სადაც კიბერ თავდაცვითი ღონისძიებებისთვის გამოყოფილია 30 მილიონი ფუნტი სტერლინგი. სქემა არ აჩვენებს სხვა დაფინანსების ოდენობას, რომელიც ხორციელდება არა NCSP - ის ფარგლებში.