ვლადიმერ სვანაძე

შეერთებული შტატების კიბერშესაძლებლობები

შეერთებული შტატები არის მოწინავე ქვეყანა კიბერუსაფრთხოების საკითხებში და ის წარმოადგენს ერთერთ ძირითად მოთამაშეს მსოფლიოში. ყველაზე დიდი კიბერშეტევების პროცენტული მაჩვენებელი მოდის შეერთებული შტატების კიბერსივრცესა და მის ინფრასტრუქტურაზე.

ობამას ადმინისტრაციამ ქვეყნის 2015 წლის საფინანსო ბიუჯეტში კიბერუსაფრთხოების სფეროსთვის გამოყო 14 მილიარდი ამერიკული დოლარი[1]. არსებული ინფორმაციით ეს არის ბიუჯეტის ოფიციალური ნაწილი, თუმცა ექსპერტები ვარაუდობენ, რომ შეერთებული შტატები კიბერუსაფრთხოების უზრუნველყოფისთვის აპირებს დახარჯოს უფრო მეტი[2].

თავდაპირველად შეერთებულმა შტატებმა კიბერუსაფრთხოების თემაზე მუშაობა დაიწყო 2001 წლის 11 სექტემბრის ტერორისტული აქტის შემდეგ. თუმცა მანამდე, 1991 წელს ერაყში „უდაბნოს ქარიშხალში“ სამხედრო - საჰაერო ძალების მიერ აქტიურად გამოიყენებოდა უახლესი ინფორმაციული ტექნოლოგიები, ხოლო მის დაცვას უზრუნველყოფდა სპეციალურად შექმნილი ქვედანაყოფი.

უკვე 2011 წლის მაისში[3] შეერთებულმა შტატებმა გამოაქვეყნა თავისი სტრატეგია კიბერსივრცის დაცვაზე. სტრატეგიას საფუძვლად უდევს მთავრობას, საერთაშორისო პარტნიორებსა და კერძო სექტორს შორის თანამშრომლობის მოდელი, სადაც აღწერილია მთელი რიგი ღონისძიებები, რომლებიც აუცილებელია გატარდეს შემდეგი შვიდი მიმართულებით:

- ეკონომიკა - საერთაშორისო სტანდარტებისა და ინოვაციების მოზიდვა, ღია და ლიბერალური ბაზარი;
- ეროვნული ქსელის დაცვა - უსაფრთხოების ამაღლება, სანდოობა და მდგრადობა;
- სამართალებრივი მხარე - თანამშრომლობისა და სამართლებრივი ნორმების გაფართოება;
- სამხედრო სფერო - უსაფრთხოების თანამედროვე გამოწვევებზე მზადყოფნა;

[1] გასულ წელს ეს მაჩვენებელი შეადგენდა 12,8 ამერიკულ დოლარს.

[2] არაოფიციალური ხარჯვითი ნაწილი არის ეროვნული უსაფრთხოების სააგენტოს, ცენტრალური სადაზვერვო სააგენტოსა და იუსტიციის სამინისტროს უფლებამოსილებაში;

[3] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

- სამთავრობო ინტერნეტის ქსელი - სამთავრობო სტრუქტურების ეფექტურობისა და მრავალმომცველობის გაფართოება;
- საერთაშორისო განვითარება - უსაფრთხოების ორგანიზება, საერთაშორისო კომპეტენციების განვითარება და ეკონომიკური აყვავება;
- თავისუფლება ინტერნეტში - მოქალაქეთა კერძო ცხოვრების ხელშეუხებლობისა და თავისუფლების მხარდაჭერა.

შეერთებული შტატების კიბერუსაფრთხოების სფეროში 2015 წელი არის მნიშვნელოვანი ცვლილებების წელი. კერძოდ, პირველი 2015 წლის თებერვალში აშშ-ის პრეზიდენტის ადმინისტრაციაში მიიღეს გადაწყვეტილება, რომ ეროვნული დაზვერვის დირექტორის (Director of National Intelligence, DNI)[4] უშუალო დაქვემდებარებაში შეიქმნას ახალი სპეციალური სამსახური - კიბერსაფრთხეებზე სადაზვერვო მონაცემების ინტეგრაციის ცენტრი (Cyber Threat Intelligence Integration Center, CTIIC). უწყების ფუნქციებში შედის სახელმწიფო უწყებებიდან და კერძო სექტორიდან მიღებული სადაზვერვო მონაცემების შეგროვება, ანალიზი და რეკომენდაციების გაცემა. ასევე უწყებათაშორისო კოორდინაცია; მეორე, ცენტრალურმა სადაზვერვო სააგენტომ (the Central Intelligence Agency, CIA)[5] ერთერთ პრიორიტეტულ მიმართულებად გამოაცხადა კიბერსაფრთხეების შეკავება, პრევენცია და შეტევითი ღონისძიებების განხორციელება, რისთვისაც სააგენტოში სპეციალურად შეიქმნა კიბერ - ოპერაციების დირექტორატი, რომლის მიზანია კიბერ ოპერაციებისთვის უპირველესი პრიორიტეტის მინიჭება და სადაზვერვო ინფორმაციის შეგროვებისას ციფრული ინოვაციების გამოყენება; და მესამე, ამ წელს დაგეგმილია 30 ათასი პროგრამისტის/ჰაკერის დასაქმება სახელმწიფო სექტორში. ასევე პენტაგონი აპირებს აწარმოოს უფრო აგრესიული პოლიტიკა კიბერუსაფრთხოების მიმართულებით, რაც მოიცავს არამარტო არმიის კრიტიკული ინფრასტრუქტურის დაცვით ღონისძიებებს, არამედ ასევე კიბერ თავდასხმების და სპეციალური კიბერ შეტევითი ოპერაციების განხორციელებას პოტენციურ მოწინააღმდეგეზე.

ზოგადად, შეერთებული შტატების კიბერუსაფრთხოების სისტემა არის სამდონიანი. კერძოდ:

<u>პირველი დონე</u> არის ფედერალური უწყებები

- *თავდაცვის სამინისტრო;*
- *შიდა უსაფრთხოების სამინისტრო* (Department of Homeland Security, DHS)[6]

[4] http://www.dni.gov/index.php
[5] https://www.cia.gov/index.html
[6] http://www.dhs.gov/

- კიბერუსაფრთხოების და კომუნიკაციების ოფისი (Office of Cyber Security and Communications);

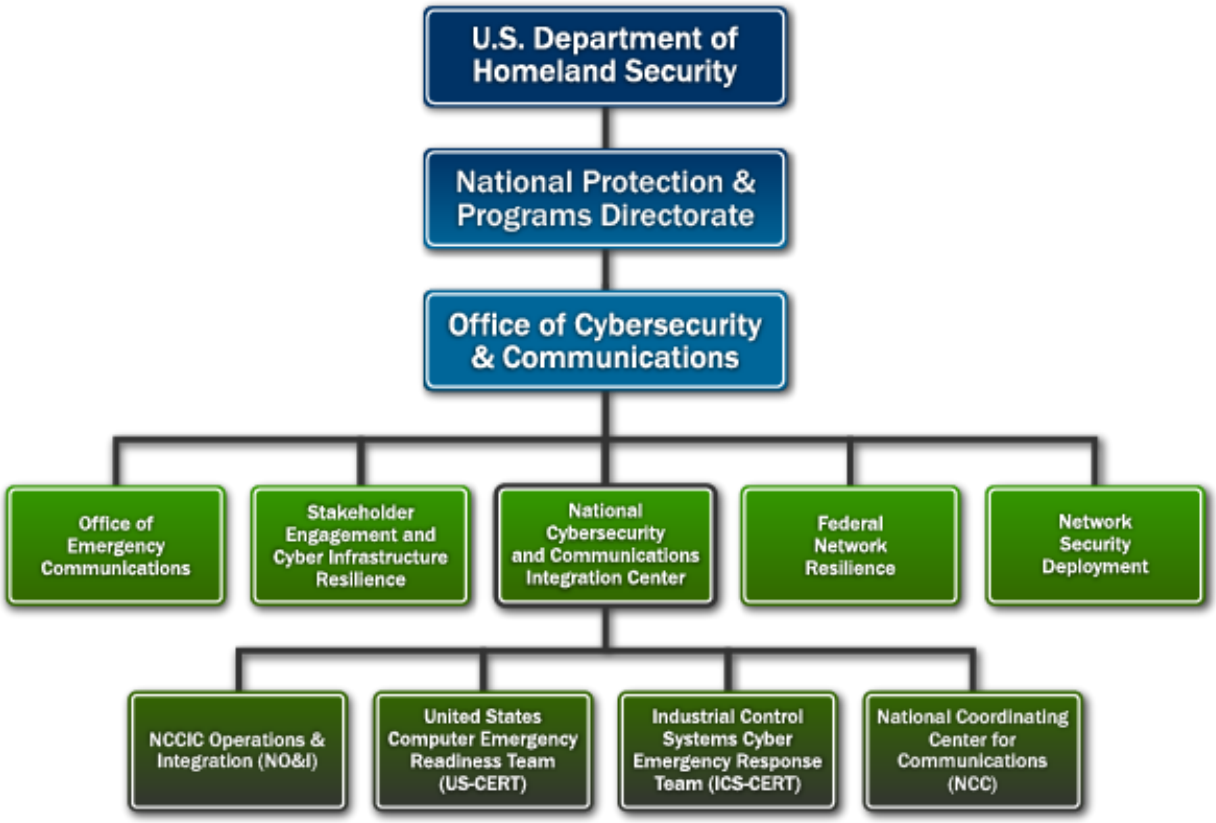
- *იუსტიციის დეპარტამენტი* (United States Department of Justice, DOJ)[7]
  - გამოძიების ფედერალური ბიუროს (Federal Bureau of Investigation, FBI)[8] კიბერგამოძიების ეროვნული გაერთიანებული ძალები (National Cyber Investigative Joint Task Force, NCIJTF);

<u>მეორე დონე</u> - პირველ დონის რომელიმე სტრუქტურაში შემავალი

- კომპიუტერული უსაფრთხოების ინციდენტებზე რეაგირების ჯგუფი (United States Computer Emergency response Team, US-CERT)[9];
- კიბერუსაფრთხოების ეროვნული ცენტრი (National Cyber Security Division, NCSD);
- კიბერდანაშაულთან ბრძოლის ცენტრი (Cyber Crimes Center);
- კიბერსაფრთხეების საოპერაციო ცენტრი (NSA/CSS Threat Operations Center, NTOC);
- შეიარაღებული ძალების კიბერსარდლობა (United States Cyber Command, USCYBERCOM)[10].

<u>მესამე დონე</u> - ლოკალური და რეგიონალური სტრუქტურული ქვედანაყოფები. მათ საქმიანობაზე ზედამხედველობასა და კონტროლს ახორციელებენ ზემოთ ნახსენები ორგანიზაციები.

[7] http://www.justice.gov/
[8] http://www.fbi.gov/
[9] https://www.us-cert.gov/
[10] http://www.stratcom.mil/factsheets/2/Cyber_Command/



შეერთებული შტატების კიბერუსაფრთხოების ორგანიზაციულ - სტრუქტურული სქემა

კიბერუსაფრთხოების სამხედრო ასპექტების გამოყოფა პენტაგონის პრიორიტეტებში დაიწყო ჯერ კიდევ ჯორჯ ბუში - უმცროსის პრეზიდენტობის დროს. იმავდროულად, დაიწყო მკაცრი კონკურენცია შეერთებული შტატების სპეციალურ სამსახურებს შორის მოცემულ სფეროში უფლებამოსილების თაობაზე. მაშინ დადგა საკითხი ერთიანი გაერთიანებული კიბერსარდლობის (USCYBERCOM) შექმნის შესახებ, რომელიც ხელს შეუწყობდა კიბერსივრცეში სამხედროების მოქმედებას, თუმცა იმ დროს პენტაგონი ამისთვის მზად არ აღმოჩნდა და საკითხი ისევ ღიად დარჩა. ამიტომ საერთო პასუხისმგებლობა კიბერომის პრობლემატიკასთან დაევალა შეიარაღებული ძალების სტრატეგიულ სარდლობას, ხოლო კიბერსივრცეში საბრძოლო ოპერაციების ფაქტიური განხორციელება დაევალა სამხედრო - საჰაერო ძალებს. შემდგომში ეს პროცესი უფრო განვითარდა და 2007 წელს შეერთებული შტატების სამხედრო - საჰაერო ძალებში შეიქმნა კიბერსარდლობა, რომელმაც ამ სტატუსით იარსება 2008 წლის ბოლომდე, რის შემდეგაც ეს ფუნქციები გადაეცა სამხედრო - საჰაერო ძალების კოსმოსურ (სტრატეგიულ) სარდლობას[11], სადაც 2009

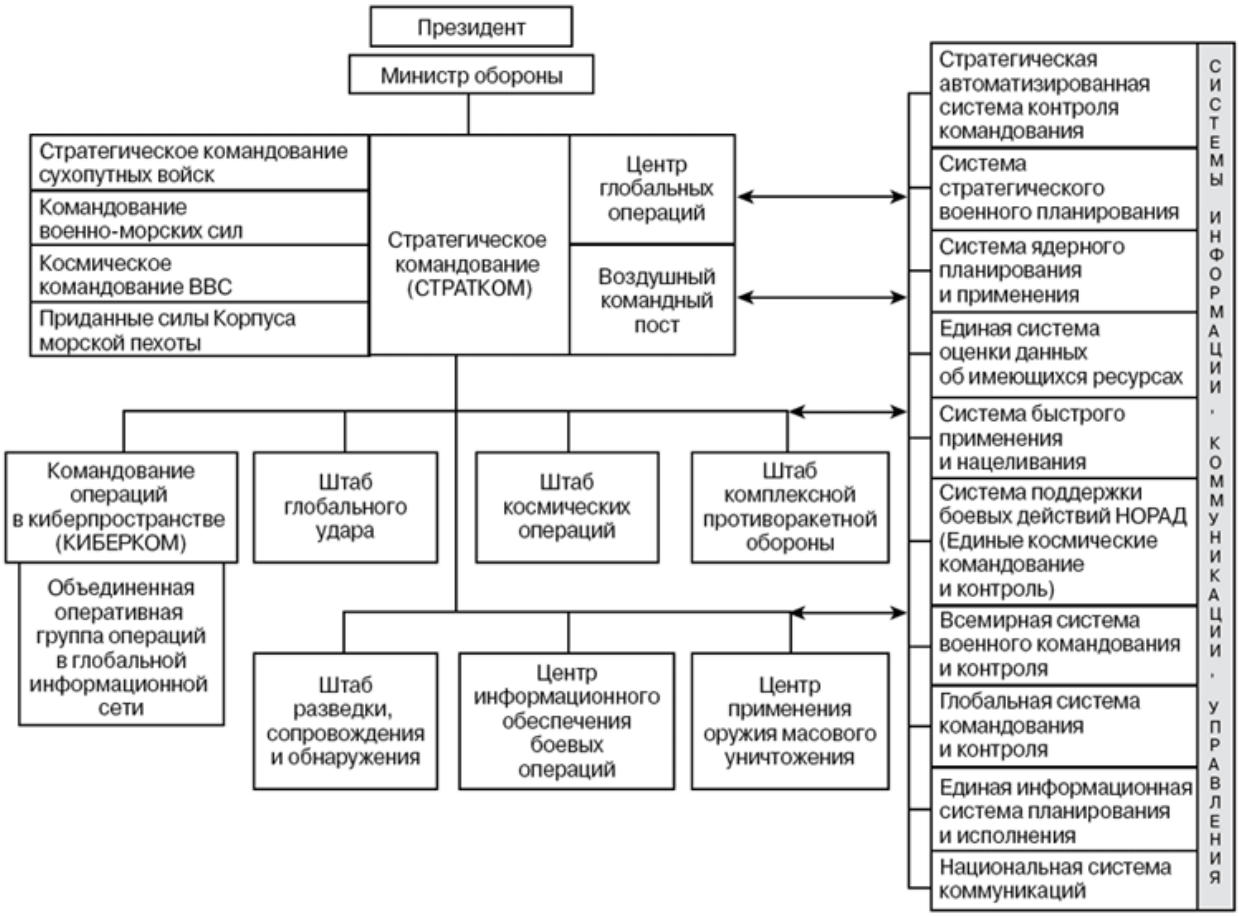
[11] პასუხისმგებელია ასევე ამერიკის ბირთვულ შეიარაღებასა და მართვაზე;

წლის ივნისში შეიქმნა კიბერსარდლობის განახლებული სტრუქტურული ერთეული. ფაქტიურად,

შეერთებული შტატების შეიარაღებული ძალების ხელმძღვანელობამ კიბერუსაფრთხოების უზრუნველყოფა მოაქცია ერთი სტრუქტურული ერთეულის ქვეშ, წინააღმდეგ შემთხვევაში კოორდინაციისა და ოპერატიულობის ხარისხი იქნებოდა ძალზედ დაბალი[12].

შეერთებული შტატების გამოცდილება აჩვენებს, რომ ორგანიზაციულ - სტრუქტურული თვალსზრისით, აუცილებელია შეიარაღებული ძალებისა და სამოქალაქო სექტორის (მათ შორის სპეციალური სამსახურების) ფუნქციების ერთმანეთისგან გამიჯვნა. კიბერსარდლობა თავის ამოცანებს ახორციელებს ცენტრალური სადაზვერვო სააგენტოს, საშინაო უსაფრთხოების სამინისტროს, ეროვნული უსაფრთხოების სააგენტოსა და სახელმწიფოს სხვა სტრუქტურული ერთეულების პარალელურად ან ერთობლივად, ამიტომ აუცილებელია კიბერსაფრთხეების წინააღმდეგ ერთობლივი ბრძოლა. ამ მიმართულებით, საინტერესო პრაქტიკა არის ის გარემოება, რომ სტრუქტურული ერთეულების მიერ ურთიერთგადამკვეთი ამოცანების გადაჭრა თავმოყრილია ერთი პიროვნების უფლებამოსილებაში, კერძოდ კიბერსარდლობის ამჟამინდელი ხელმძღვანელი ამავდროულად არის ეროვნული უსაფრთხოების სააგენტოს (NSA)[13] და უსაფრთხოების ცენტრალური სამსახურის დირექტორი.

[12] ეს სტრუქტურა მოქმედებს დღემდე და ანალოგიურის შექმნაზე მუშაობს რუსეთიც, რაც სტრუქტურის ეფექტიანობაზე მიუთითებს;
[13] https://www.nsa.gov/



შეიარაღებული ძალების სტრატეგიული სარდლობის ორგანიზაციულ- სტრუქტურული სქემა