ვლადიმერ სვანაძე

რუსეთის კიბერუსაფრთხოების შესაძლებლობები

შესავალი

საქართველოს ეროვნული უსაფრთხოების კონცეფციის მიხედვით, ქვეყნისთვის დიდი საფრთხის შემცველია რუსეთი და მისი ქმედებები. 2014 წლის კვლევების მიხედვით, მსოფლიოში კიბერშეტევებში ერთერთ მთავარ მოთამაშედ, ისევე როგორც 2013 წელს, დასახელებული არის რუსეთი.

რუსეთში ინფორმაციული უსაფრთხოების სფეროში მთავარ ორგანიზაციებად ითვლება უშიშროების საბჭო, უშიშროების ფედერალური სამსახური (ФСБ), დაცვის ფედერალური სამსახური, ტექნიკისა და ექსპერტის კონტროლის ფედერალური სამსახური, თავდაცვისა და ინფორმაციული ტექნოლოგიებისა და კავშირგაბმულობის სამინისტროები.

თითოეულ დასახელებულ 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) პასუხისმგებელია რუსეთის ფედერაციის უსაფრთხოებასა და კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის უზრუნველყოფაზე. კონტრდაზვერვის სამსახურში ფუნქციონირებს კომპიუტერული და ინფორმაციული უსაფრთხოების სამმართველო, რომელიც ასევე კურირებს ჰაკერთა დაჯგუფებებს.

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) კომპეტენციაში.

ФАПСИ - ს დანარჩენი ფუნქციები გადანაწილდა თავდაცვის სამინისტროს შეიარაღებული ძალების გენერალური შტაბის, უშიშროებისა (ФСБ) და დაცვის ფედერალურ სამსახურებს 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.

<u>რუსეთის ინფორმაციული უსაფრთხოების სტრატეგია</u>

გასული 2014 წლის იანვარში, რუსეთის ფედერალურმა საბჭომ ფართო განხილვისათვის წარმოადგინა „რუსეთის ფედერაციის კიბერუსაფრთხოების სტრატეგიის კონცეფცია“, რომელიც მიმართულია თანამედროვე ინფორმაციულ სამყაროში ახალი საფრთხეების განსაზღვრაზე. კონცეფციამ დარგის ექსპერტთა შორის გამოიწვია აზრთა სხვადასხვაობა, თუმცა მათ მიერ ჩამოყალიბებულ იქნა <u>საერთო რეკომენდაციები</u>, კერძოდ:

1) ინფორმაციული უსაფრთხოების არსებულ ტერმინოლოგიასთან კიბერუსაფრთხოებისა და კიბერსივრცის თანხვედრი ტერმინოლოგიის შემუშავება;
2) კიბერსივრცის დაცვის კომპლექსური სისტემების შემუშავება;
3) კიბერსივრცის მოდელისა და იმ ძირითადი ფაქტორების შემუშავება, რაც გავლენას ახდენს მის ფუნქციონირებაზე. ასევე სავარაუდო საფრთხეების მათემატიკური მოდელების შექმნა;
4) კიბერსივრცის მდგრადობის უზრუნველყოფის სპეციალური მეთოდების შექმნა:
   - კრიპტოგრაფიული დაცვის ახალი მეთოდების რეალიზება;
   - ტოპოლოგიური სტრუქტურის ანალიზი და შესაბამისი რეკომენდაციების შემუშავება;
   - სპეციალური პროცედურების გამოყენებით ინფორმაციული უსაფრთხოების მეთოდების შემუშავება;
5) კიბერუსაფრთხოების უზრუნველყოფის ინტელექტუალური მეთოდები, კერძოდ:
   - მომხმარებლის ინტელექტუალური იდენტიფიკაცია;
   - ინტელექტუალური მეთოდებით ვირუსებისა და სხვა შეტევების გაუვნებელყოფა;
   - არასანქცირებული შეღწევისა და შეტევის გამოვლენის ინტელექტუალური მეთოდები;

- ინფორმაციული უსაფრთხოების მდგომარეობის ანალიზი;
- ნეიროქსელურ ტექნოლოგიებზე დაფუძნებული კრიპტოგრაფიული დაცვის ახალი მეთოდები.

თავად სტრატეგიის მიზანს წარმოადგენს საგარეო და საშინაო პოლიტიკაში პრიორიტეტების, პრინციპებისა და ღონისძიებების სისტემების განსაზღვრის საფუძველზე პიროვნების, ორგანიზაციებისა და სახელმწიფოს კიბერუსაფრთხოების უზრუნველყოფა.

სტრატეგიის პრიორიტეტებია:

1) ეროვნული სისტემებისა და ქსელების დაცვის განვითარება;
2) კრიტიკული ინფორმაციული ინფრასტრუქტურის სანდოობის განვითარება და მუდმივი განახლება;
3) კიბერსივრცეში სახელმწიფო რესურსების უსაფრთხოების უზრუნველყოფის სრულყოფის ღონისძიებების გატარება;
4) კიბერუსაფრთხოების სფეროში სახელმწიფო, კერძო სექტორისა და სამოქალაქო საზოგადოების საპარტნიორო მექანიზმების შემუშავება;
5) კიბერსივრცეში უსაფრთხო ქცევის კულტურის შემუშავება და მოქალაქეთა ცნობიერების ამაღლება;
6) გლობალურ დონეზე კიბერუსაფრთხოების ამაღლების მიზნით საერთაშორისო თანამშრომლობის განვითარება.

კიბერუსაფრთხოების სტრატეგიას საფუძვლად უდევს შემდეგი ძირითადი პრინციპები:

1) ინფორმაციის მიღებისა და გამოყენების სფეროში ადამიანისა და მოქალაქის კონსტიტუციური უფლებებისა და თავისუფლების გარანტიის პრინციპი;
2) კიბერსივრცეში პიროვნებისა და ორგანიზაციების მაქსიმალური დაცულობის პრინციპი;
3) კიბერუსაფრთხოების უზრუნველყოფის ფარგლებში, ინფორმაციული საზოგადოების ყველა სუბიექტის (პიროვნება, კერძო და სახელმწიფო სექტორი) კონსტრუქციული თანამშრომლობის პრინციპი;
4) კიბერუსაფრთხოების მოთხოვნების დაცვაზე დადგენილი პასუხისმგებლობის ბალანსის შენარჩუნების პრინციპი;
5) საფრთხეების პრიორიტეტების განსაზღვრის პრინციპი;
6) კიბერუსაფრთხოების უზრუნველყოფის საშუალებებისა და მეთოდების სისტემური აქტუალიზაციის პრინციპი.

კონცეფციის მიხედვით, რუსეთის კიბერუსაფრთხოებითი უზრუნველყოფა უნდა განხორციელდეს შემდეგი მიმართულებებით:

1) კიბერუსაფრთხოების უზრუნველყოფაზე საერთო სისტემური ზომების მიღება;
2) კიბერუსაფრთხოების უზრუნველყოფაზე სამართლებრივ - ნორმატიული ბაზისა და სამართლებრივი ღონისძიებების სრულყოფა;
3) კიბერუსაფრთხოების სფეროში სამეცნიერო - კვლევითი სამუშაოების წარმოება;
4) კიბერუსაფრთხოების უზრუნველყოფის საშუალებების შემუშავებისთვის, წარმოებისა და გამოყენებისთვის პირობების შექმნა;
5) საკადრო და საორგანიზაციო ღონისძიებების სრულყოფა;
6) ადგილობრივი და საერთაშორისო თანამშრომლობის ორგანიზება;
7) კიბერსივრცეში უსაფრთხო ქცევის კულტურის ფორმირება და განვითარება.

ექსპერტთა აზრით, 2014 და 2015 წელი კიბერუსაფრთხოების სფეროში, რუსეთისთვის იქნება გადამწყვეტი პერიოდი, რომლის დროსაც გამოიკვეთება სახელწიფო პოლიტიკის ახალი დოქტრინალური საფუძვლები და საგარეო კონტურები, ასევე სტარტს აიღებს ახალი გრძელვადიანი პროგრამები და პროექტები. იგივე ექსპერტები ვარაუდობენ, რომ ამ პერიოდში ძალზედ მოწყვლადი იქნება რუსეთის კიბერსივრცე, რომელიც გარკვეული რისკების შემცველია ქვეყნის ეროვნული უსაფრთხოებისთვის. შეიძლება ითქვას, რომ კიბერუსაფრთხოების პოლიტიკა რუსეთში კრიზისულ ფაზაში შედის, თუმცა მიიჩნევენ, რომ ეს იქნება პოზიტიური პროცესის დასაწყისი.

კონცეპტუალური შეხედულებები რუსეთის შეიარაღებული ძალების ინფორმაციულ სივრცეში მოქმედებებზე

რუსეთის შეიარაღებული ძალების მოღვაწეობას ინფორმაციულ სივრცეში საფუძვლად უდევს შემდეგ პრინციპთა ერთობლიობა:

1) კანონიერება - მოითხოვს რუსეთის კანონმდებლობის, აგრეთვე აღიარებული და არსებული საერთაშორისო სამართლის ნორმების დაცვას. ყველა გადაწყვეტილებას დაკავშირებულს აქტიურ მოქმედებებთან ქვეყნის შიგნით თუ მის ფარგლებს გარეთ იღებს რუსეთის პრეზიდენტი. საერთაშორისო

სამართლის თანახმად, რუსეთის შეიარაღებული ძალები გლობალურ ინფორმაციულ სივრცეში აღიარებს შემდეგ ნორმებსა და პრინციპებს:

- სახელმწიფო სუვერენიტეტის პატივისცემა;
- სხვა სახელმწიფოების საშინაო საქმეებში ჩაურევლობა;
- ძალისა და შეტევითი ღონისძიებების გამოუყენებლობა;
- ინდივიდუალურ და კოლექტიურ თავდაცვაზე უფლება.

2) პრიორიტეტულობა - წარმოებს საფრთხეების შესახებ აქტუალური და სანდო ინფორმაციის შეგროვება, მისი ოპერატიულ დონეზე დამუშავება, ღრმა ანალიზი, რეალიზაცია და დაცვითი ღონისძიებების დროული განხორციელება. მოცემული პროცესის ერთობლიობა ქმნის არმიის ეფექტური მართვის ხელსაყრელ გარემო პირობებს.
3) კომპლექსურობა - ინფორმაციულ სივრცეში მოიცავს შტაბებისა და შენაერთების ისეთი ღონისძიებების ერთობლიობას, როგორებიცაა სამხედრო დაზვერვა, ოპერატიული შენიღბვა, რადიოელექტრონული ბრძოლა, კავშირგაბმულობა, ავტომატიზირებული მართვა, შტაბების ინფორმაციული მუშაობა, აგრეთვე საკუთარი ინფორმაციული სისტემების დაცვა.
4) ურთიერთქმედება - ინფორმაციულ სივრცეში თავისი ქმედებები თავდაცვის სამინისტრომ უნდა შეუთანხმოს აღმასრულებელი ხელისუფლების სხვა ფედერალურ სამსახურებსა და ორგანოებს.
5) თანამშრომლობა - მოითხოვს მეგობარ ქვეყნებთან და საერთაშორისო ორგანიზაციებთან თანამშრომლობას.
6) ინოვაცია - რუსეთის შეიარაღებული ძალებისგან მოითხოვს ინფორმაციულ სივრცეში გამოიყენოს მოწინავე ტექნოლოგიები, საშუალებები და მეთოდები. ასევე ინფორმაციული უსაფრთხოების ამოცანების გადაწყვეტის პროცესში მოიზიდოს მაღალკვალიფიციური პირადი შემადგელობა.

შეიარაღებული ძალები ინფორმაციულ სივრცეში თავისი ამოცანების გადაჭრისას ხელმძღვანელობს კიბერ კონფლიქტების შეკავების, აღკვეთისა და გადაჭრის უფლებათა ერთობლიობით. კერძოდ, შეკავებისა და აღკვეთის უფლებები მოიცავს:

- შეიარაღებულ ძალებში ინფორმაციული უსაფრთხოების სისტემების განვითარება;
- ინფორმაციული უსაფრთხოების ძალებისა და საშუალებების მუდმივი მზადყოფნა;
- პრიორიტეტულ საფუძვლებზე თანამშრომლობის განვითარება კოლექტიური უსაფრთხოებისა და შანხაის ორგანიზაციების ქვეყნებთან, ასევე დსთ - ს წევრ - ქვეყნებთან. აგრეთვე, პარტნიორი ქვეყნების წრის გაფართოება და თანამშრომლობის განვითარება;

- ინფორმაციულ სივრცეში არსებული და აღიარებული საერთაშორისო ნორმების საფუძველზე გლობალური ინფორმაციული უსაფრთხოების უზრუნველყოფა;
- კიბერ კონფლიქტების აღმოცენებისა და ესკალაციის ფაქტორების დადგენა და მათზე კონტროლის დაწესება;
- კიბერ კონფლიქტის საერთაშორისო დონეზე გავრცელების აღკვეთა;
- კიბერ კონფლიქტების ფაქტორების ნეიტრალიზაცია და მათი კონსტრუქციული თანამშრომლობის პირობებში გადაყვანა;
- საჯაროდ, ობიექტურად და დროულად მსოფლიო საზოგადოების ინფორმირება და მიზეზების განმარტება.

ინფორმაციულ სივრცეში კონფლიქტების გადაჭრა:

- მშვიდობიანი საშუალებები;
- კონფლიქტის ესკალაციისა და მისი კრიზისულ ფაზაში გადასვლის შემთხვევაში, ინდივიდუალური და კოლექტიური თავდაცვითი ძალების გამოყენება;
- ინდივიდუალური და კოლექტიური თავდაცვის ფარგლებში საპასუხო დარტყმის პოტენციალის განსაზღვრა;
- ინდივიდუალური და კოლექტიური თავდაცვის ინტერესებიდან გამომდინარე ინფორმაციული უსაფრთხოების უზრუნველყოფის მიზნით, საკუთარი ძალებისა და საშუალებების განლაგება უცხო ქვეყნის ტერიტორიაზე, ამ უკანასკნელთან შესაბამისი შეთანხმების საფუძველზე;
- კონფლიქტის მსვლელობისას ქვეყნისა და საერთაშორისო მასობრივი საინფორმაციო საშუალებების მუდმივი ინფორმირება.

ინფორმაციულ სივრცეში რუსეთის შეიარაღებული ძალები მუდმივად ცდილობენ ნდობითი ღონისძიებების გამყარებას. კერძოდ:

- ინფორმაციულ სივრცეში უსაფრთხოების უზრუნველსაყოფად ეროვნული კონცეფციების გაცვლა;
- ინფორმაციულ სივრცეში კრიზისული მოვლენებისა და საფრთხეების, და მათი ნეიტრალიზაციის შესახებ ოპერატიული ინფორმაციის გაცვლა;
- ინფორმაციულ სივრცეში მოღვაწეობის შესახებ კონსულტაციები, და თანამშრომლობა კონფლიქტების მოგვარების სფეროში.

თანამედროვე პირობებში რუსეთის შეიარაღებული ძალების თავდაცვისუნარიანობა ბევრად არის დამოკიდებული ინფორმაციულ სივრცეში მათ

ეფექტურ მოქმედებაზე. შეიარაღებული ძალები გეგმავენ გადაჭრან მათ წინაშე არსებული ამოცანები თავდაცვისა და უსაფრთხოების უზრუნველყოფაზე, ინფორმაციულ სივრცეში შეიარაღებული ძალების მოქმედების ძირითადი პრინციპებისა და უფლებების გამოყენებით.

მოცემული კონცეპტუალური შეხედულებების რეალიზებისას, რუსეთის შეიარაღებული ძალები მაქსიმალურად გამოიყენებს ინფორმაციულ სივრცეს შემდეგი მიმართულებებით:

- ქვეყნის თავდაცვისუნარიანობის გასაძლიერებლად;
- სამხედრო კონფლიქტების შეკავებისა და აღკვეთისათვის;
- სამხედრო თანამშრომლობის განვითარებისათვის;
- საერთაშორისო საზოგადოების ინტერესებიდან გამომდინარე, გლობალური ინფორმაციული უსაფრთხოების სისტემის ფორმირებისათვის.

<u>შეიარაღებული ძალები, სპეციალური სამსახურები და ინფორმაციული უსაფრთხოება</u>

2010 წლის თებერვალში, რუსეთის ფედერაციამ გამოუშვა თავისი ახალი სამხედრო დოქტრინა, სადაც განხილულია პოლიტიკური და საინფორმაციო საშუალებების გამოყენება მიმართული რუსეთისა და მისი მოკავშირეების ეროვნული ინტერესების დაცვაზე. დოქტრინა განსაზღვრავს თანამედროვე სამხედრო კონფლიქტისთვის დამახასიათებელ თავისებურებებს, რაც მოიცავს სამხედრო ძალებისა და საინფორმაციო ომის წარმოების კომპლექსურ ერთობლიობას. ფაქტიურად, დოქტრინა შეიცავს კიბერუსაფრთხოების გააქტიურების საშუალებებს.

2012 წლის მარტის თვეში, დიმიტრი როგოზინმა გააკეთა განცხადება შეიარაღებულ ძალებში შეერთებული შტატების მსგავსი (U.S.CYBERCOM) „კიბერ სარდლობის“ შექმნაზე, რაც პრაქტიკულად ნიშნავს ინფორმაციული უსაფრთხოების საკითხებში სპეციალურ სამსახურებზე სრულ დომინირებას. აქვე უნდა ითქვას, რომ ადრე თავდაცვის სამინისტროს პრიორიტეტულ ამოცანებში ეს საკითხები არ შედიოდა. იმავე წლის ბოლოსთვის დასრულდა არაკომერციული სტრუქტურის პერსპექტიული კვლევების ფონდის შექმნა, რომლის ბიუჯეტი განისაზღვრა 3 მილიარდი რუბლით. ფაქტიურად, ფონდის შექმნა განხორციელდა დაჩქარებული წესით.

საინტერესოა, რომ 2012 წლის ოქტომბერში, თავდაცვის სამინისტრომ სტრატეგიული ინიციატივების სააგენტოსთან, რუსეთის განათლებისა და

მეცნიერების სამინისტროსთან და პროგრამირებისა და კომპიუტერული ტექნოლოგიების სფეროში წამყვან უმაღლეს სასწავლებელთან (МГТУ им. Баумана) ერთად საფუძველი ჩაუყარა ყოველწლიურ კონკურსს (უკვე გამოცხადებულია 2015 – 2016 წლებზე), რომლის მთავარი თემა იყო ანტივირუსული სისტემების გვერდის ავლის საშუალებები და მეთოდები, ასევე ქსელის დაცვა. არსებობს მოსაზრება, რომ ამ კონკურსის ფარგლებში წარმოებს საბრძოლო შემტევი ვირუსების შემუშავება. ეს კარდინალურად ცვლის სურათს დაკავშირებულს კიბერ დაპირისპირების სფეროში თავდაცვითი სტრატეგიის შესახებ, რაც სამხედრო დოქტრინით არის გაწერილი.

საყურადღებოა ის ფაქტი, რომ 2013 წლის 13 თებერვალს რუსეთის შეიარაღებული ძალების გენერალურ შტაბში შეიქმნა რამოდენიმე ახალი ნახევრად საიდუმლო სტრუქტურა, რომლებიც პასუხისმგებელნი არიან ინფორმაციულ უსაფრთხოებაზე, რაც მიანიშნებს შეიარაღებული ძალების გააქტიურებას დაკავშირებულს კიბერსივრცესთან და მის დაცულობასთან. არსებული ინფორმაციით, ახლადშექმნილი სტრუქტურები ამუშავებენ ასევე შემტევ ვირუსებს და მათი თანამშრომლების ნაწილს შეადგენს ზემოთნახსენები კონკურსის მონაწილეები.

მიუხედავად თავდაცვის სამინისტროს მზარდი ინტერესისა სამხედრო - სტრატეგიული ხასიათის კიბერსაფრთხეებზე, რუსეთის სპეციალური სამსახურები (ФСБ, ФСО და ФСТЭК) მაინც ინარჩუნებენ წამყვან როლს ქვეყნის კიბერუსაფრთხოების უზრუნველყოფის საკითხებში. 2013 წლის 15 იანვარს, კასპერსკის ლაბორატორიის მიერ კიბერჯაშუშური ქსელის Red October - ის (არსებობს მოსაზრება, რომ ეს ქსელი მუშაობდა რუსეთის სპეციალური სამსახურების დავალებებზე) გახსნის შემდეგ რამოდენიმე დღეში, ვლადიმერ პუტინმა ხელი მოაწერა ბრძანებას, რომლის თანახმად რუსეთის ფედერალური უშიშროების სამსახურს (ФСБ) ავალდებულებს შექმნას სახელმწიფო სისტემები მიმართული ქვეყნის კრიტიკული ინფრასტრუქტურისა და მთლიანად კომპიუტერული ქსელის კიბერშეტევებისგან დაცვის უზრუნველყოფაზე. დარგის ექსპერტები მიიჩნევენ, რომ პუტინის ეს ბრძანება რუსეთის ინფორმაციული უსაფრთხოების პოლიტიკის განვითარებაში არის გადამწყვეტი მნიშვნელობის მქონე.

ამავდროულად, 2012 წლის ბოლოს, სენატორ რუსლან გატაროვის მიერ ინიცირებული წინადადება რუსეთის კიბერუსაფრთხოების სტრატეგიის კომპლექსური მიდგომის საკითხების შემუშავების შესახებ, არ წარმოადგენს პრიორიტეტულს, ვინაიდან რუსეთის ფედერაციის საბჭოს არ გააჩნია საჭირო კომპეტენცია მოცემული მიმართულებით.

საინტერესოა, რომ კიბერუსაფრთხოების საკითხის პარალელურ რეჟიმში განვითარება, მომავალში გამოიწვევს გარკვეულ დაპირისპირებას სამხედროებსა და

სპეციალურ სამსახურებს შორის უფლებამოსილებების შესახებ. ეს პროცესი დიდ გავლენას იქონიებს რუსეთის კიბერ სარდლობის ჩამოყალიბების საბოლოო შედეგზე, ვინაიდან ჯერ ბოლომდე არ არის გარკვეული მსგავსი სტრუქტურის შექმნით როგორ გადანაწილდება უფლებამოსილებები და პროცესში ჩართულობა, არ არსებობს ასევე სტრუქტურულ - ორგანიზაციული სქემა.

ქვეყნის ინფორმაციული უსაფრთხოების უზრუნველყოფაში ყველა სპეციალურ სამსახურს (ФСБ, ФСО და ФСТЭК) თავისი ინტერესი და ფუნქცია გააჩნია, რაც გარკვეულწილად ეწინააღმდეგება შეერთებული შტატების მსგავსი „კიბერ სარდლობის“ (U.S.CYBERCOM) შექმნის იდეასა და ინიციატივას, რომელიც თავის დროზე როგოზინმა წამოაყენა და მხარდაჭერილ იქნა როგორც ყოფილი მინისტრის სერდუკოვის, ისე ამჟამინდელი მინისტრის შოიგუს მიერ. ვერ ხერხდება ერთმანეთისგან სამხედროებისა და სპეციალური სამსახურების ფუნქციონალურ - სტრუქტურული გამიჯვნა. ფაქტიურად, რუსეთი კიბერუსაფრთხოების საერთო სტრატეგიის საკითხებში მიდის სამხედროებისა და სპეციალური სამსახურების სინქრონიზაციის პროცესისკენ, რაც გარკვეული რისკების შემცველი იქნება თავად ქვეყნისთვის, ვინაიდან დარგი დაუბრუნდება ძველ ჩარჩოებს, სადაც კიბერუსაფრთხოების თემას ექნება მეორეხარისხოვანი როლი საგარეო სტრატეგიული საფრთხეების შეფასებისას და ზოგადად, ეროვნული უსაფრთხოების საკითხებში.

მიუხედავად ზემოაღნიშნულისა, რუსეთის უშიშროების ფედერალური სამსახური (ФСБ) უკვე აქტიურად მუშაობს ქვეყნის ერთიანი სისტემის შექმნაზე, რომელიც მიმართული იქნება კიბერ შეტევების აღმოჩენასა და გაფრთხილებაზე. ასევე არაოფიციალური ინფორმაციით, ФСБ - ს 16 - ე დირექტორატის კონტროლის ქვეშ იმყოფება რუსეთის ჰაკერთა მთელი რესურსები. სამსახური აგრეთვე მუდმივად მუშაობს ჰაკერთა ახალი რესურსების მოძიებასა და თავის სასარგებლოდ პროცესში ჩართვაზე არა მარტო ქვეყნის შიგნით, არამედ უცხოეთშიც, რაშიც ასევე აქტიურად მონაწილეობს რუსეთის საგარეო დაზვერვის სამსახური (СВР).

განხორციელებული ცნობილი კიბერშეტევები

რუსეთის მიერ განხორციელებულ ცნობილ კიბერშეტევებს შეიძლება მივაკუთვნოთ:

1) 2007 წლის აპრილ - მაისში, რუსეთსა და ესტონეთს შორის არსებული დაპირისპირება გადაიზარდა სერიოზულ კიბერშეტევაში, რომლის დროსაც გარკვეული დროის განმავლობაში მიუწვდომელი იყო ესტონური ინტერნეტ რესურსები.

2) 2008 წლის აპრილში რუსეთის მხრიდან განხორციელდა მასირებული კიბერ შეტევა რადიო თავისუფალ ევროპასა და რადიო თავისუფლებაზე.

3) 2008 წლის ივნისსა და ივლისში ლიტვის კიბერსივრცეზე განხორციელებული კიბერშეტევები.

4) 2008 წლის ივლის - აგვისტოში რუსეთის მხრიდან მოხდა კიბერ შეტევა საქართველოს კიბერსივრცეზე, რაც ზოგიერთი ექსპერტების მიერ შეფასდა ასევე როგორც მასშტაბური ხასიათის „საინფორმაციო ომი“ მიმართული საქართველოს წინააღმდეგ.

5) 2008 – 2014 წლებში რუსეთის მხრიდან სისტემატურად ხორციელდებოდა კიბერშეტევა საქართველოს შინაგან და საგარეო საქმეთა სამინისტროების, აღმოსავლეთ ევროპის ქვეყნების სახელისუფლებო, სამხედრო წარმომადგენლობების, NATO - სა და OSCE - ს საიტებზე, რაც წარმოდგენილია ცხრილში.

Malware	Targeting	Russian Attributes
Evolves and Maintains Tools for Continued, Long-Term Use • Uses malware with flexible and lasting platforms • Constantly evolves malware samples for continued use • Malware is tailored to specific victims' environments, and is designed to hamper reverse engineering efforts • Development in a formal code development environment **Various Data Theft Techniques** • Backdoors using HTTP protocol • Backdoors using victim mail server • Local copying to defeat closed/air gapped networks	**Georgia & the Caucasus** • Ministry of Internal Affairs • Ministry of Defense • Journalist writing on Caucasus issues • Kavkaz Center **Eastern European Governments & Militaries** • Polish Government • Hungarian Government • Ministry of Foreign Affairs in Eastern Europe • Baltic Host exercises **Security-related Organizations** • NATO • OSCE • Defense attaches • Defense events and exhibitions	**Russian Language Indicators** • Consistent use of Russian language in malware over a period of six years • Lure to journalist writing on Caucasus issues suggests APT28 understands both Russian and English **Malware Compile Times Correspond to Work Day in Moscow's Time Zone** • Consistent among APT28 samples with compile times from 2007 to 2014 • The compile times align with the standard workday in the UTC + 4 time zone, which includes major Russian cities such as Moscow and St. Petersburg

წყარო: Chart by FireEye

ეს კიბერშეტევები ხორციელდებოდა რუსული ჰაკერული დაჯგუფება APT 28 - ის მიერ, რომელსაც არაოფიციალური ინფორმაციით, კოორდინაციას უწევს რუსეთის ფედერალური უშიშროების სამსახური (ФСБ). დაჯგუფებისთვის დამახასიათებელია ორშაბათიდან პარასკევის ჩათვლით, დილის 8 საათიდან საღამოს 6 საათამდე მუშაობა. პირველად APT 28 ეგონათ ჩინური წარმოშობის, მაგრამ შემდეგ ექსპეტთა უმრავლესობა დარწმუნდა, რომ APT 28 არის რუსული ჰაკერული დაჯგუფება, რომლის სავარაუდო ადგილმდებარეობაა სანქტ - პეტერბურგი;

6) 2011 – 2014 წლებში რუსეთის მხრიდან განხორციელდა პერმანენტული კიბერშეტევები შეერთებული შტატების თავდაცვისა და უსაფრთხოების სტრუქტურულ ქვედანაყოფებზე. მათ შორის იყო პენტაგონისა და ეროვნული უსაფრთხოების სააგენტოს (NSA) დეპარტამენტები მოცემული კიბერშეტევების დროს გამოყენებული იქნა მავნებლური პროგრამა (malware) "Uroburos", რომლის შესახებ პირველი განცხადება გააკეთა გერმანულმა უსაფრთხოების კომპანიამ G Data Security - მ;
7) შეერთებული შტატების ფედერალური საგამოძიებო ბიუროს (FBI) განცხადებით, 2014 წლის აგვისტოს შუა რიცხვებში განხორციელდა მასირებული შეტევა უმსხვილეს ბანკზე JPMorgan Chase & Co. - ზე. კიბერ შეტევის წყარო მოდიოდა რუსეთიდან.

დასკვნა

რუსეთი მსოფლიოს ინფორმაციულ სივრცეში წარმოადგენს ერთერთ მთავარ მოთამაშეს, რომელიც მუდმივად ანვითარებს თავის შესაძლებლობებს. ქვეყანას გააჩნია მუდმივი ინტერესები და მიზნები, რომელთა მიღწევისთვის ის სამხედრო და პოლიტიკური შესაძლებლობების პარალელურად სულ უფრო აქტიურად იყენებს ინფორმაციულ სივრცეს.

რუსეთში ინფორმაციული უსაფრთხოების მიმართულება ამ ეტაპზე იმყოფება ახლის ჩამოყალიბებისა და არსებულის რეფორმირების სტადიაში. ქვეყანაში ეს სფერო ისევ რჩება სპეციალური სამსახურების კონტროლის ქვეშ, რის პარალელურად იწყება დარგის განვითარება შეიარაღებულ ძალებში, სადაც უკვე არსებობს ნახევრად საიდუმლო ქვედანაყოფები, რომლებიც მუშაობენ არამარტო კიბერ შეტევის შეკავებასა და აღკვეთაზე, არამედ თავადაც ახორციელებენ კიბერ შეტევებს. რუსეთმა დაიწყო საკითხის მიმართ კომპლექსური მიდგომა, რაც ნიშნავს ნებისმიერი სამხედრო თუ სხვა სახის გააქტიურება (პოლიტიკური, ეკონომიკური, სოციალური) მიმდინარეობს

ინფორმაციულ სივრცეში შესაბამისი ღონისძიებების გატარებით, კიბერშეტევითი ოპერაციების ჩათვლით.

ზემოაღნიშნულიდან გამომდინარე, შეიძლება ზოგადად ჩამოვაყალიბოთ რუსეთის ინფორმაციული უსაფრთხოების პოლიტიკის შემდეგი <u>ძირითადი მიმართულებები</u>:

- ქვეყნის საერთო ქსელის, კრიტიკული ინფორმაციული ინფრასტრუქტურის, კომპიუტერული სისტემებისა და მომხმარებელთა დაცვა;
- სამართლებრივ - ნორმატიული ბაზისა და სამართლებრივი ღონისძიებების სრულყოფა;
- სამეცნიერო - კვლევითი სამუშაოების წარმოება, რაც ასევე მოიცავს სემინარების, კონფერენციებისა და კონკურსების ჩატარებას;
- კიბერუსაფრთხოების უზრუნველყოფის ტექნოლოგიური საშუალებების შემუშავებისთვის, წარმოება/დანერგვისა და გამოყენებისთვის საჭირო პირობების შექმნა;
- საკადრო პოლიტიკის განვითარებისა და საორგანიზაციო ღონისძიებების სრულყოფა;
- ადგილობრივი კერძო სექტორის წარმომადგენლებთან და საერთაშორისო დონეზე თანამშრომლობის ორგანიზება და გაფართოება;
- ინფორმაციულ სივრცეში მომხმარებელთა უსაფრთხო ქცევის კულტურის ფორმირება და განვითარება;
- შეიარაღებულ ძალებში ინფორმაციული უსაფრთხოების სისტემების განვითარება;
- ინფორმაციული უსაფრთხოების ძალებისა და საშუალებების მუდმივი მზადყოფნა.

საქართველოს ეროვნული უსაფრთხოების კონცეფციის თანახმად, რუსეთი ისევ წარმოადგენს საფრთხეს საქართველოს სუვერენიტეტისთვის და მისი ეროვნული უსაფრთხოებისთვის. ასევე რუსეთის შემტევითი აქტიურობა ინფორმაციულ სივრცეში გარკვეული საფრთხის შემცველია საქართველოს კიბერსივრცისთვის. სტატისტიკა აჩვენებს, რომ საქართველოს კიბერსივრცე არის ერთერთი პრიორიტეტული რუსი ჰაკერული დაჯგუფებებისთვის, რომელთა ძირითად ობიექტებს წარმოადგენს არამარტო სამთავრობო, არამედ ასევე კერძო თუ სამოქალაქო სექტორის საიტები. მსგავსი კიბერ შეტევების ძირითადი მოტივი არის სამუშაო პროცესის პარალიზება და ინფორმაციის შეგროვება.

ბიბლიოგრაფია

1) Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space, *by NATO Research Center*, February, 2014;
2) "Information Troops" – a Russian Cyber Command?, *by Keir Giles, Conflict Studies Research Centre Oxford, UK,* 2013;
3) "The Battlefield On Your Laptop", *K. Mshvidobadze,* Radio Free Europe/Radio Liberty 21 March 2011;
4) "Russian Views on Information-based Warfare", *by T.L. Thomas*, Foreign Military Studies Office (FMSO), July 1996;
5) "Electronic Warfare", *US Joint Publication 3-13.1;*
6) http://www.dia.mil/News/SpeechesandTestimonies/ArticleView/tabid/11449/Article/570863/statement-for-the-record-worldwide-threat-assessment.aspx
7) КОНЦЕПЦИЯ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ, *Проект,* 2014;
8) Киберпространство. Американская и российская концепции, *Фатех Вергасов,* 2013;
9) INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS, *by Eneken Tikk, Kadri, Kaska, Liis Vihul,* 2010;
10) *https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf.*