რუსეთის ფედერაციის თავდაცვითი და შემტევი კიბერ შესაძლებლობები

ბექა კახელი, გიორგი მარტიაშვილი
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილულია რუსეთის ფედერაციის თავდაცვითი და შემტევი კიბერშესაძლებლობების კვლევითი პროექტის ოფიციალური მასალები. ანალიზიდან გამომდინარე აშკარაა, რომ რუსეთის მთავრობა აქტიურად არის ჩართული კიბერუსაფრთხოებისა და კიბერშეტევების განვითარებაში, რაზეც მეტყველებს მათ მიერ ჩადებული ინვესტიციები და ჰაკერული ჯგუფების მფარველობა. ნაშრომში მოყვანილი მაგალითებიდან ცხადი ხდება, რომ კიბერშესაძლებლობების გამოყენება ინფორმაციულ ომში რუსეთის ფედერაციისთვის ერთ–ერთი წამყვანი თემაა. ბოლო წლებში მომხდარ დაპირისპირებათა მაგალითზე ჩანს, რომ რუსეთის ფედერაცია კიბერ შესაძლებლობებს აქტიურად იყენებს საკუთარი მიზნების მისაღწევად.

საკვანძო სიტყვები: კიბერ-დანაშაული. ინფორმაციული უსაფრთხოება. კიბერ-ტერორიზმი. ორგანიზებული დანაშაული.

1. შესავალი

ინფორმაციული ტექნოლოგიების როლი ჩვენს ყოველდღიურ ცხოვრებაში თანდათან იზრდება, რამაც გამოიწვია კიბერუსაფრთხოების საკითხების მნიშვნელობის გაზრდა ქვეყნის მასშტაბით. კომპიუტერული სისტემების და ქსელების დაცვას სტრატეგიული მნიშვნელობა აქვს სახელმწიფოს თავდაცვისუნარიანობაში.

კიბერ-ძალები რუსეთმა ჯერ კიდევ 2000-იან წლების მოვლენებამდე მოიკრიბა. 1990-იანი წლების ბოლოდან ქვეყანა ჰაკერობის და სხვა ქსელური ხულიგნობის სახეობების ცენტრი გახდა. ინტერნეტ-დანაშაულები, კიბერ-ძარცვა, სისტემებში შეღწევა, ბოლო ათი წლის განმავლობაში რუსეთის იმიჯის განუყოფელ ნაწილად იქცა, 2000-იანი წლების დასაწყისში საინფორმაციო სამართალდარღვევების რიცხვი განუხრელად მატულობს: 2001 წელს 3000-დან 6000-მდე, 2002 წელს 12000, 2003 წელს 15000 და ა.შ. 2008 წელს ამ ტიპის დანაშაულებზე სისხლის სამართლის 8000 საქმე აღიძრა. გაეროში რუსეთის წარმომადგენელმა ამ ორგანიზაციის ეგიდით კიბერ-კრიმინალთან ბრძოლისათვის საერთაშორისო კონვენციის შექმნისკენ მოწოდება გააკეთა. 1999 წელს შეიქმნა ფედერალური უსაფრთხოების ბიუროს სპეციალური განყოფილება, რომლის ამოცანაც კიბერ-უსაფრთხოების სფეროში დოქტრინის შემუშავება და რუსეთის არმიასთან მჭიდრო თანამშრომლობით კიბერ-ომის დოქტრინის შემუშავება გახდა.

კვლევა მოიცავს რუსეთის ფედერაციის თავდაცვით და შემტევ კიბერ შესაძლებლობებს. კვლევა მომზადებულია ღია წყაროებზე დაყრდნობით. ქვემოთ განხილული იქნება რუსეთის ფედერაციის სპეცსამსახურები, კერძო ორგანიზაციები, პოლიტიკური მოძრაობები, რომლებსაც მნიშვნელოვანი როლი აქვთ ქვეყნის თავდაცვით და შემტევ კიბერ შესაძლებლობებში. ასევე განხილული იქნება რუსეთის მიერ ესტონეთზე (2007), საქართველოზე (2008) და ყირგიზეთზე (2009) განხორციელებული კიბერ შეტევები. ასევე, შევეხებით კიბერდაზვერვის და კიბერშეტევის ტექნიკურ საშუალებებს.

2. რუსეთის ფედერაციის სპეცსამსახურები, კერძო ორგანიზაციები, პოლიტიკური მოძრაობები და ორგანიზებული კრიმინალი

მრავალი ქვეყნის და ორგანიზაციის მუშაობაში განსაკუთრებული ადგილი უკავია კომპიუტერული სისტემებისა და ინტერნეტის გამოყენებას. შესაბამისად მათი მუშაობის შეფერხება ან რაიმე სახის დაზიანება, სერიოზულად მოქმედებს ნებისმიერ პროცესზე, რასაც აღნიშნული ორგანიზაცია, კომპანია თუ სახელმწიფო სტრუქტურა ახორციელებს.

ინტერნეტი და კომპიუტერული სისტემები გამოიყენება სხვადასხვა ინფრასტრუქტურის სამართავად: სამხედრო და სატელიტური სისტემები, კომუნიკაციის არხები, წყლის, გაზის, ელექტრო და ატომური ენერგიის, ნავთობმომპოვებელი და გადამამუშავებელი ინფრასტრუქტურის ელემენტები. რომელიმე მათგანის დაზიანება ან მწყობრიდან გამოსვლა სერიოზული ზიანის მომტანია როგორც კომპანიის, ისე სახელმწიფოსათვის.

აღსანიშნავია რუსეთის ფედერაციის ძალისხმევის გაძლიერება კიბერმიმართულებით. ღია წყაროებიდან ნათელი ხდება განსაკუთრებით დიდი რესურსების მიმართვის ფაქტები. 2014 წლის შემოდგომაზე კიდევ ერთ დიდ პროექტს ჩაეყარა საფუძველი, კერძოდ, რუსეთის ფედერაციის თავდაცვის სამინისტროში შეიქმნა კიბერთავდაცვის ცენტრი, გენერალ-პოლკოვნიკ პავლოვის დაქვემდებარებაში. აღნიშნული ცენტრის გასავითარებლად გამოყოფილ იქნა 500 მლნ აშშ დოლარი [1]. აქვე უნდა აღინიშნოს, რომ ცენტრი წარმოდგენილია ქვეყნის მასშტაბით სამხედრო დანაყოფებში და სარგებლობს საკუთარი დაცული ქსელით, რომელიც არ არის დაკავშირებული გლობალურ ქსელთან. აღნიშნული გარეომოება ფაქტობრივად შეუძლებელს ხდის გარედან კიბერშეტევას. რუსეთის ფედერაციის გლობალური ქსელიდან მოწყვეტის შემთხვევაშიც კი, ცენტრს შეუძლია გააგრძელოს ფუნქციონირება შეუფერხებლად.

საბჭოთა კავშირის დაშლის შემდეგ, KGB Eighth (Encoding) -ის ბაზაზე შეიქმნა სამთავრობო კომუნიკაციების და ინფორმაციის საიდუმლო ფედერალური სააგენტო FAPSI. იგი პრეზიდენტის დაქვემდებარებაშია. მას სათავეში KGB-ს გენერალი ალექსანდრე სტაროვოიტოვი ჩაუდგა [2]. სააგენტოს ფუნქციებში შედის როგორც სამთავრობო კომუნიკაციების დაცვა, ასევე რადიო შპიონაჟი და რადიო ჩახშობა. აღსანიშნავია, რომ სააგენტოს საკუთარი საბრძოლო ერთეული ჰყავს. მისი შემადგენლობა რამდენიმეჯერ აღემატება FSB-ს თანამშრომელთა რაოდენობას. ასევე, საბჭოთა მემკვიდრეობით ერგო რუსეთის ფედერაციას საიდუმლო სადაზვერვო ბაზა Lourdes [Cuba] Signals Intelligence (SIGINT) facility კუბაზე. ბაზა ოფიციალურად დახურულია, თუმცა, არსებობს გონივრული ეჭვი, რომ ის ისევ განაგრძობს ფუნქციონირებას. Lourdes-ს შესაძლებლობა აქვს დაიჭიროს რადიოსიგნალები და მიიღოს ინფორმაცია აშშ-ს სამთავრობო და კომერციული სექტორიდან. როგორც ფიდელ კასტრომ აღნიშნა, რუსეთი სამხედრო სტრატეგიული ინფორმაციის 75%-ს Lourdes-დან იღებს [3].

რუსეთის ფედერაცია ასევე აქტიურად იყენებს კერძო ორგანიზაციებს. ამის ნათელი მაგალითია კასპერსკი. კასპერსკის ყოფილმა თანამშრომლებმა ინტერვიუ მისცეს Bloomberg-ს, სადაც ადასტურებენ, რომ ორგანიზაცია აქტიურად თანამშრომლობს ქვეყნის სპეცსამსახურებთან. გასათვალისწინებელია ის გარეომოება, რომ kaspersky-ს 400 მლნ მომხმარებელი ჰყავს მსოფლიოს მასშტაბით [4], რაც საშუალებას აძლევს რუსეთს,

აწარმოოს კიბერსადაზვერვო და შემტევი აქტივობები სხვადასხვა ქვეყნის და კომპანიების წინააღმდეგ. ბაზარზე საკმაოდ პოპულარული მწარმოებლები დღემდე იყენებენ კასპერსკის ანტივირუსს თავიანთ FireWall-ში, რაც თავისთავად გზას უხსნის რუსეთის სპეც-სამსახურებს.

რუსეთის ანტიტერორისტული კანონი ავალდებულებს უცხოურ ინტერნეტ-სერვისის მომწოდებლებს, შეინახონ მომხმარებელთა აქტივობის ლოგები ნახევარი წლის განმავლობაში და აუცილებლად რუსეთის ტერიტორიაზე. აღნიშნული კანონი ხელს უწყობს სპეცსამსახურებს, მოიპოვონ წვდომა მილიონობით სოციალური ქსელის, ელექტრონული ფოსტის და მესენჯერის მომხმარებლის აქტივობის ჩანაწერებზე.

აღსანიშნავია რუსული ჰაკერული დაჯგუფებების (energy bear, dragonfly) გააქტიურება, რომელთაც საკმაოდ დიდი შესაძლებლობები გააჩნია. მათ მიერ განხორციელებული შეტევები დასავლეთის ნავთობის, გაზის და ელექტრო კომპანიებზე ცხადყოფს რუსეთის დაინტერესებას აღნიშნულ მიმართულებაზე. არსებობს ეჭვი, რომ ჰაკერთა ჯგუფები მჭიდრო კავშირში არიან რუსეთის სამთავრობო ორგანიზაციებთან და ფინანსდებიან მათ მიერ. შეტევების უმრავლესობა ხორციელდება რუსეთის დროით სამუშაო საათებში [5]. ყველა ხვდება, რომ რუსული ჰაკერული შეტევების (დასავლეთის ენერგო სისტემები, ესტონეთი, საქართველო, ყირგიზეთი, უკრაინა) უკან კრემლი დგას, თუმცა ამის დადასტურება ვერავინ შეძლო. ესტონეთსა და საქართველოზე კიბერ შეტევების ორგანიზება თავის თავზე აიღო რუსულმა ახალგაზრდულმა მოძრაობამ Nashi.

Russian Business Network (RBN) არის კარგად ცნობილი რუსული ორგანიზებული კიბერ-კრიმინალური ორგანიზაცია. მათი საქმიანობაა - ჰაკერული ინსტრუმენტების გაყიდვა, კრიმინალური ორგანიზაციებისთვის web hosting, მავნებლური პროგრამები (malware), ჯაშუშური პროგრამები (spyware), DDOS შეტევები, ფსევდო ანტივირუსები, ონლაინ კაზინოები, ბავშვების პორნო და სხვ. RNB მაგალითია, თუ როგორ იყენებს ტრადიციული ორგანიზებული დანაშაული კიბერსაშუალებებს. რუსეთის ფედერაციის ხელისუფლება თვალს ხუჭავს ასეთ ორგანიზაციებზე და ისინი იარსებებენ მანამ, სანამ იარსებებს მოთხოვნა აღნიშნულ პროდუქტებზე [6,7]. ეს ორგანიზაცია აქტიურად იყო ჩართული ესტონეთსა და საქართველოზე კიბერშეტევებში.

3. დასკვნა

მოცემული დოკუმენტი წარმოადგენს „რუსეთის ფედერაციის თავდაცვითი და შემტევი კიბერშესაძლებლობების“ კვლევით პროექტს. ზემოთქმულიდან გამომდინარე, რუსეთის მთავრობა აქტიურად არის ჩართული კიბერუსაფრთხოებისა და კიბერშეტევების განვითარებაში, რაზეც მეტყველებს მათ მიერ ჩადებული ინვესტიციები და ჰაკერული ჯგუფების მფარველობა. ზემოთ მოყვანილი მაგალითებიდან ცხადი ხდება, რომ კიბერშესაძლებლობების გამოყენება ინფორმაციულ ომში რუსეთის ფედერაციისთვის ერთ–ერთი წამყვანი თემაა. ბოლო წლებში მომხდარ დაპირისპირებათა მაგალითზე ჩანს, რომ რუსეთის ფედერაცია კიბერ შესაძლებლობებს აქტიურად იყენებს საკუთარი მიზნების მისაღწევად. 2007 წელს ესტონეთზე კიბერშეტევა გამოწვეული იყო მთავრობის გადაწყვეტილებით, გადაეტანათ რუსი ჯარისკაცის ძეგლი ტალინიდან, რასაც მოჰყვა რუსეთის გაღიზიანება და დაიწყო DDOS შეტევები ესტონეთის მთავრობის, ფინანსური

ინსტიტუტების და კერძო კომპანიების წინააღმდეგ. მოსკოვი უარყოფდა მის მონაწილეობას მიმდინარე მოვლენებში, თუმცა მოგვიანებით დადასტურდა RNB-ის მონაწილეობა და ასევე რამდენიმე სამთავრობო უწყების ჩართულობაც. მოსკოვმა პასუხისმგებლობა აირიდა და განაცხადა, რომ ჰაკერების მიერ განზრახ იყო გამოყენებული სამთავრობო უწყებების ქსელი, რადგან გამოჩენილიყო კავშირი ოფიციალურ მოსკოვსა და DDOS შეტევებს შორის [8-10]. ანალოგიური ტექნოლოგია გამოიყენა რუსეთმა საქართველოს წინააღმდეგ 2008 წელს. DOS შეტევები სამთავრობო ვებ გვერდებზე წინ უძღვოდა სამხედრო კონფლიქტს. მოგვიანებით, 2009 წელს, რუსეთმა კიბერ შეტევები გამოიყენა ყირგიზეთის წინააღმდეგაც. აღნიშნულმა კიბერ თავდასხმებმა ცხადყო, რომ კიბერ იარაღი შესაძლებელია გამოყენებული იყოს შეიარაღებულ ოპერაციებში.

ლიტერატურა – References – Литература:

1. SC Magazine UK. http://www.scmagazineuk.com/500-million-for-new-russian-cyber-army/article/381720/

2. Moscow Novaya Gazeta No. 37, 15-21 Sep 97

3. fas Intelligence Resource Program, http://www.fas.org/irp/imint/c80_04.htm

4. РБК политика. 03.19.2015, 20:18

5. The Wire. http://www.thewire.com/technology/2014/07/russian-hackers-go-after-oil-companies/373785/

6. wired. http://www.wired.com/2009/03/pro-kremlin-gro/

7. Cener for Stategic & International STUDIES

8 . McAfee Proven Security. http://web.archive.org/web/20060823090948/

http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_akapoor_rootkits1_en.pdf

9. CNET. http://www.cnet.com/news/security-firm-claims-russian-government-makes-mal-ware/

10. G Data Software AG. https://www.gdata.de/rdk/dl-en-rp-Uroburos

DEFENSIVE AND OFFENSIVE CYBER CAPABILITIES OF THE RUSSIAN FEDERATION

Kakheli Beka, Giorgi Martiashvili

Georgian Technical University

Summary

The article deals with the Russian Federation, Official materials of the Cyber Capability Research Project. Based on the analysis, it is clear that the Russian government is actively involved in the development of cyber security and cyber attacks, which indicates investments and protection of hacker groups. From the examples outlined in the work, it is clear that the use of cyber attacks is one of the leading topics for the Russian Federation. The example of controversy in recent years shows that the Russian Federation is actively using cyber opportunities to achieve its goals.