Scientific and Practical Cyber Security Journal (SPCSJ) 7(4): 111 – 116 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

რუსული კიბერაქტორების მოკლე დახასიათება უკრაინაში სრულმასშტაბიანი შეჭრის წინ

ანდრო გოცირიძე[1]

[1]ბიზნესისა და ტექნოლოგიების უნივერსიტეტის პროფესორი

აბსტრაქტი. ზღვარი სახელმწიფო და არასახელმწიფო კიბერაქტორებს შორის რუსეთში წაშლილია. ეს აქტორები ინტენსიურად თანამშრომლობენ ერთმანეთთან, მოქმედებენ კოორდინირებულად, ხშირად იყენებენ კრიმინალური ჯგუფების საფარს და ახორციელებენ რუსეთის სახელმწიფო ინტერესებს, რაც საფრთხეს უქმნის საქართველოს და მთელ დასავლურ საზოგადოებას. სტატიაში დახასიათებულია ჩვენთვის ცნობილი კიბერ ჯგუფები, რომლებიც პირდაპირ ან ირიბად არიან დაკავშირებული რუსულ სახელმწიფო სისტემასთან. აღწერილია მათი პასუხისმგებლობის ზონები, მოტივაცია, შეტევის მეთოდები უკრაინაში სრულმასშტაბიანი შეჭრის წინ. აღნიშნულის ცოდნა დაგვეხმარება საქართველოში ეფექტური კიბერთავდაცვის მოდელების ჩამოყალიბებაში.

საკვანძო სიტყვები: კიბერ მსახიობები, თავდასხმის მეთოდები, კიბერთავდაცვა, კიბერ ომი

ABSTRACT. Distinguishing between state and non-state actors within Russia is often difficult, especially when these actors actively collaborate, cooperate, and condone criminal activity that pose a threat to the security of Georgia and the entire western society. This article covers principal cyber groups, directly or indirectly connected to the Russian special services or state institutions, their responsibilities, motivation, and attack methods before a full-scale invasion of Ukraine. This knowledge will help us build efficient cyber defense models established in Georgian defense institutions.

KEYWORDS: cyber actors, attack methods, cyber defense, cyber war

1. შესავალი

შემტევი კიბერპოტენციალის თვალსაზრისით, რუსეთი ერთ- ერთ მოწინავე პოზიციას იკავებს მსოფლიოში. საქართველოსთან 2008 წლის ომის, არაბული გაზაფხულისა და 2011 წელს რუსული ოპოზიციის მიერ სოციალური ქსელებით ორგანიზებული მასშტაბური გამოსვლების შედეგების ანალიზზე დაყრდნობით, კრემლმა განახორციელა ორგანიზაციულ-დოქტრინალური ცვლილებები და გააქტიურა კიბერსივრცის კონტროლი.

რუსული კიბერაქტორების ჩამონათვალი მოიცავს როგორც სახელმწიფო უწყებებს, რომელთაგან მნიშვნელოვანი წილი სპეცსამსახურებზე მოდის, (Galeotti 2016) ასევე კრემლთან აფილირებულ კერძო დაჯგუფებებს, კიბერკრიმინალურ ორგანიზაციებს, ჰაქტივისტებს თუ „პატრიოტ ჰაკერთა“ ჯგუფებს. უნდა აღინიშნოს, რომ კერძო სტრუქტურების დიდ ნაწილს კრემლთან დაახლოებული ოლიგარქები აფინანსებენ და მართავენ.

თანამედროვე რუსული სპეცსამსახურებისთვის დამახასიათებელია უკიდურესი პოლიტიზირება, წაშლილი ზღვარი პარტიასა და სახელმწიფოს შორის, მმართველი რეჟიმის უსაფრთხოებაზე ზრუნვა, უწყებათაშორისი კონკურენცია კრემლის კეთილგანწყობისა და შესაბამისად რესურსების მოსაპოვებლად, ასევე პოლიტიკურ იარაღად მათი გამოყენება.

უსაფრთხოების ფედერალური სამსახური (ФСБ, Федеральная Служба Безопасности) საბჭოთა კავშირის სახელმწიფო უშიშროების კომიტეტის მემკვიდრე და რუსეთის უძლიერესი სპეცსამსახურია. მიუხედავად მკაფიო კონტრდაზვერვითი ფუნქციისა, უწყება ხშირად საზღვარგარეთ, განსაკუთრებით კი ე.წ. „პოსტსაბჭოთა სივრცეში“ ახორციელებს ოპერაციებს, რადგან რუსეთი ამ რეგიონს საკუთარ გავლენის სფეროდ მოიაზრებს და მის დასავლურ ინტეგრაციას კონტრდაზვერვით საფრთხედ აღიქვამს. **ФСБ**, საზედამხედველო უწყებებთან და პროფილურ სამინისტროსთან ერთად, მნიშვნელოვან როლს თამაშობს რუსეთის საინფორმაციო სფეროს უსაფრთხოების დაცვაში. მაგალითად, იგი, ინტერნეტ-პროვაიდერების მონიტორინგის ფარგლებში, უფლებამოსილია აწარმოოს სატელეფონო მოსმენები და ინტერნეტის ტრაფიკის კონტროლი. თუმცა, მისთვის არც შემტევი კიბეროპერაციებია უცხო: სწორედ ФСБ-ს უკავშირდება ცნობილი მაღალტექნოლოგიური ჰაკერული ჯგუფი Turla (Snake, Uroburos, Venomous Bear). იგი ერთ ერთი უძველესი ჰაკერული ჯგუფია, რომლის კვალიც აღმოჩენილ იქნა ჯერ კიდევ 2008 წელს აშშ-ის სამხედრო ქსელებსა თუ ირანელი ჰაკერების სერვერების კომპრომეტაციაში მათი შემდგომი გამოყენების მიზნით.

სამხედრო დაზვერვის მთავარი სამმართველო - ГРУ ან ГУ (Главное Разведывательное Управление, Главное Управление Генерального Штаба Вооружённых Сил РФ) წარმოადგენს საგარეო დაზვერვის განმახორციელებელ უწყებას. კიბეროპერაციების ადრეულ ეტაპზე, მაგალითად 2007-2008 წლებში ესტონეთისა და საქართველოს წინააღმდეგ განხორციელებულ კიბერშეტევებში ГРУ-ს შედარებით მეორეხარისხოვანი როლი ჰქონდა, თუმცა მოგვიანებით, ეს უწყება გადაიქცა შემტევი კიბეროპერაციების ფლაგმანად. დასავლური სპეცსამსახურები სწორედ მას მიაწერენ მნიშვნელოვან გახმაურებულ კიბერშეტევებს საინფორმაციო-ტექნიკური თუ საინფორმაციო-ფსიქოლოგიური ეფექტით, რომლებიც ფართოდ არის აღწერილი სხვადასხვა წყაროს მიერ. მიუხედავად სპეცსამსახურისთვის დამახასიათებელი მკაცრი კონსპირაციისა, ცნობილია კიბეროპერაციების განმახორციელებელი ГРУ-ს რამდენიმე დანაყოფი:

- **85-ე სპეციალური უზრუნველყოფის ცენტრი** (ს/ნ 26165[1]) - ნომინალურად პასუხისმგებელია რადიოელექტრონულ დაზვერვასა და კრიპტოგრაფიაზე თუმცა სწორედ მას უკავშირდება ბოლო დრომდე APT28-ის (Fancy Bear, Pawn Storm, Sofacy, Strontium) სახელით ცნობილი აქტივობები. იგი წარმოადგენს ერთ ერთ ყველაზე აქტიურ, მაღალტექნოლოგიურ, მეტად დესტრუქციულ კიბერაქტორს და პასუხისმგებელია საჰაერო სივრცეზე, თავდაცვის და ენერგეტიკის სფეროებსა თუ სახელმწიფო და მედიასექტორზე განხორციელებულ კიბერთავდასხმებზე. თავდასხმების არეალი ფართოა და მოიცავს აშშ-ს, დასავლეთ ევროპას, ირანს, იაპონიას, საქართველოს, მალაიზიასა და სამხრეთ კორეას. APT28 ცნობილია თავდაცვის სექტორსა და სხვა სამხედრო მიზნებზე განხორციელებული კიბერშპიონაჟის გახმაურებული ფაქტებით. (FireEye 2014) ცნობილ შეტევებს მიეკუთვნება 2014 წ. უკრაინის და 2016 წ. აშშ-ის საპრეზიდენტო, 2015 წ. ბუნდესთაგის საარჩევნო სისტემებზე თავდასხმა, ფრანგულ ტელემაუწყებელ TV5Monde -ზე

[1] ს/ნ - სამხედრო ნაწილი. საბჭოთა დროიდან შეორჩენილი საიდუმლო სარეჟიმო ობიექტების აღრიცხვის მიღებული ფორმა.

კიბერშეტევა კიბერხალიფატის საფარქვეშ და 2018 წელს ფხენიანის ზამთრის ოლიმპიურ თამაშებზე თავდასხმა. ცნობილია კარგად ორგანიზებული ფიშინგ-შეტევებით.

- **სპეციალური ტექნოლოგიების მთავარი ცენტრის** (ს/ნ 74455) ძირითადი აქტივობები კომპიუტერულ ტექნოლოგიებზე დაფუძნებულ ოპერაციების უკავშირდება. მისი ქოლგის ქვეშ მოქმედებს ჰაკერული ჯგუფი **Sandworm** (Telebots, Voodoo Bear, Iron Viking), რომელიც გამოირჩევა განსაკუთრებით მაღალტექნოლოგიური და დესტრუქციული კიბერშეტევებით. იგი წარმოადგენს ტექნიკურ ეფექტზე ორიენტირებულ აქტორს და პასუხისმგებელია აშშ-ის 2016 წლის საპრეზიდენტო არჩევნებში ჩარევის ტექნიკურ მხარეზე, NotPetya-სა[2] და უკრაინის ენერგეტიკული სექტორის წინააღმდეგ 2015-2016 წლებში გამოყენებული KillDisk და Industroyer შექმნა-გავრცელებაზე. Sandworm-ის ანგარიშზეა ასევე 2018 წელს ფხენიანის ზამთრის ოლიმპიურ თამაშებზე განხორციელებული კიბერშეტევა.
- **72-ე სპეციალური ღონისძიებების ცენტრი (ს/ნ 54777)** წარმოადგენს ГРУ-ს ფსიქოლოგიური ომის ბირთვს, მინიმუმ 2014 წლიდან წარმართავს კიბერშეტევებს საინფორმაციო ოპერაციების განსახორციელებლად. აღნიშნული დანაყოფი მჭიდროდ თანამშრომლობს შეფარების უწყებებთან და პროქსი-ორგანიზაციებთან.
- სამხედრო დაზვერვის მთავარი სამმართველოს კიბეროპერაციების კიდევ ერთი ინსტრუმენტია დაჯგუფება **„კიბერბერკუტი“ (Киберберкут)**, რომელიც თითქოსდა ჰაქტივისტური მოტივით ახორციელებს რუსული სამხედრო ოპერაციებისა და სტრატეგიული ამოცანების მხარდაჭერას როგორც ტექნიკურ, ისე ფსიქოლოგიურ ეფექტზე გათვლილი კიბერშეტევებით. კიბერბერკუტი 2014 წლიდან აქტიურადაა ჩართული კიბერშპიონაჟის აქტებსა თუ DDoS -ს შეტევებში ნატოსა და უკრაინის, ასევე - გერმანიის სამთავრობო საიტების წინააღმდეგ. ფოკუსირება ხდება ჰაკერული გზით მოპოვებული დოკუმენტაციის ონლაინ გამოქვეყნებაზე, რაც ძირითადად ემსახურება მთავრობების დისკრედიტაციას, არჩევითი ორგანოებისადმი ნდობის შემცირებას, მოწინააღმდეგის დემორალიზებას, დაშინებას.

საგარეო დაზვერვის სამსახური (CBP) აწარმოებს სტრატეგიულ სადაზვერვო ოპერაციებს, მათ შორის კიბერსივრცეშიც. სამხედრო დაზვერვის მთავარი სამმართველოსგან განსხვავებით, რომლის ამოცანასაც კიბერშპიონაჟთან ერთად, საბოტაჟი და საინფორმაციო ოპერაციებიც შეადგენს, საგარეო დაზვერვის სამსახური ძირითადად კონცენტრირებულია კიბერშპიონაჟის ტრადიციულ მიზნებზე პოლიტიკურ დაზვერვასა და საიდუმლო ინფორმაციის მოპოვებაზე. CBP-თან არის დაკავშირებული ცნობილი APT29 (Cozy Bear/The Dukes)-ის აქტივობები. ეს მაღალტექნოლოგიური ჯგუფი კიბერშეტევებისთვის იყენებს ძვირ და კომპლექსურ ინფრასტრუქტურას. ახლო წარსულში CBP -მა განახორციელა წარმატებული კიბერშეტევები თეთრ სახლზე, სახელმწიფო დეპარტამენტსა და აშშ-ის გაერთიანებულ შტაბებზე. გარდა აღნიშნულისა, დაჯგუფების სამიზნეებს წარმოადგენს თავდაცვისა და ენერგეტიკის სექტორი,

[2] რუსეთის სამხედრო დაზვერვის მთავარი სამმართველოს კიბერდაჯგუფება Sandworm -ის მიერ 2017 წელს განხორციელებული მაღალტექნოლოგიური შეტევა რომელმაც გაანადგურა მონაცემები უკრაინის საბანკო და ენერგეტიკული სექტორის, სახელმწიფო უწყებებისა და აეროპორტების სერვერებზე. მოგვიანებით, მალვეარი გავრცელდა ევროპაშიც და მილიარდობით ზარალი მიაყენა ლოგისტიკურ კომპანიებს, ფარმაცევტულ სექტორს და სახელმწიფო უწყებებს.

საფინანსო და სადაზღვევო სფერო, ფარმაცევტული სფერო, ინდუსტრიულ-ტექნოლოგიური კვლევები, მედია და ანალიტიკური ცენტრები. აღწერილია თავდასხმები დასავლეთ ევროპის, ჩინეთის, ბრაზილიის, მექსიკის, იაპონიის, თურქეთის და სხვა სახელმწიფოების ქსელებზე. ცნობილია Spear-Phishing ტექნიკის მიზანმიმართული ფიშინგ-შეტევებით.

ГРУ-სთან ერთად CBP-ის კიბერდანაყოფები არიან პასუხისმგებელი 2016 წლის აშშ-ის საპრეზიდენტო არჩევნებში ჩარევაზე. ამ უკანასკნელს უკავშირდება ასევე აშშ-ის, გაერთიანებული სამეფოსა და კანადის COVID -ვაქცინაციის ცენტრებზე თავდასხმები და კიბერშპიონაჟის ბოლო წლების უმსხვილესი კამპანია 2020 წელს აშშ-ის სამთავრობო ქსელების, უსაფრთხოების სექტორის და კრიტიკული ინფრასტრუქტურის წინააღმდეგ, რომელიც „SolarWinds hack“-ის სახელითაა ცნობილი.

საინფრომაციო კონფრონტაცია[3] და მისი თანმხლები კიბეროპერაციები რუსეთის სახელისუფლებო ვერტიკალში სპეცსასმსახურების პასუხისმგებლობის ზონად ითვლება. აშშ-ის ეროვნული დაზვერვის დირექტორის ინფორმაციით, ეს სამსახურები აქტიურად ავითარებენ კრიტიკული ინფრასტრუქტურის ICS-ზე (**Industrial Control Systems - ICS**)[4] დისტანციური წვდომის საშუალებებს: ჯერ კიდევ 2015 წლის მონაცემებით, უცნობმა რუსმა აქტორებმა წარმატებულად განახორციელეს რამდენიმე ICS მწარმოებლის პროგრამის კომპრომეტაცია, ლეგალური პროგრამული უზრუნველყოფის განახლებებში **მავნე პროგრამული კოდის** ჩანერგვა და ამ გზით მომხმარებლის სისტემასთან პირდაპირი წვდომის დამყარება. მოგვიანებით, „SolarWinds" კიბერშეტევამ დაადასტურა რუსული სპეცსამსახურების ეს შესაძლებლობა, როდესაც ათასობით კომპანია თუ სახელმწიფო უწყება დაინფიცირდა პროგრამული განახლებების ლეგალური სერვერიდან გადმოწერილი რუსული მალვეარის შედეგად.

რუსეთის შეიარაღებული ძალების პასუხისმგებლობის სფეროა რადიოელექტრონული ბრძოლის საშუალებები და კიბეროპერაციების მათთან მომიჯნავე ველი. 2014 წელს რუსეთის თავდაცვის მინისტრმა ს. შოიგუმ დააანონსა კიბერსარდლობის შექმნა, თუმცა მოგვიანებით, 2017 წლის თებერვალში გაცხადდა საინფორმაციო ოპერაციების ჯარების შექმნის შესახებ, რომელიც პასუხისმგებელია, როგორც ტექნიკური ეფექტის მქონე კიბეროპერაციების წარმოებაზე, ისე საბრძოლო მოქმედებებისას პროპაგანდის გავრცელებასა და საინფორმაციო კონფრონტაციის სხვა ელემენტებზე.

---

[3] **საინფრომაციო კონფრონტაცია** - დაპირისპირება საინფორამციო სფეროში, რომელიც მოიცავს კომპლექსურ დესტრუქციულ ზემოქმედებას მოწინააღმდეგე მხარის ინფორმაციაზე, საინფორმაციო სისტემებსა და ინფრასტრუქტურაზე, ამავდროულად საკუთარი ინფორამციის, საინფორმაციო სისტემებისა და ინფრასტრუქტურის დაცვის გათვალისწინებით. ინფორამაციული კონფრონტაციის საბოლოო მიზანს ინფორმაციული უპირატესობის მოპოვება წარმოადგენს.

[4] **ICS (Industrial control system)** - კოლექტიური ტერმინი, რომელიც გამოიყენება კონტროლის სისტემებისა და მათთან დაკავშირებული ინსტრუმენტების აღსაწერად და აერთიანებს ინდუსტრიული პროცესების ავტომატიზაციისა და ოპერირებისათვის გამოყენებულ მოწყობილობებს, სისტემებს, ქსელებს და კონტროლის მექანიზმებს. დღეისათვის ფართოდ გამოიყენება კრიტიკული ინფრასტრუქტურის თითქმის ყველა მიმართულებაზე, როგორიცაა ინდუსტრია, ტრანსპორტი, ენერგეტიკა, ჰიდრომეურნეობა და სხვა, რის გამოც წარმოადგენს დესტრუქციული კიბეროპერაციების სამიზნეს. ICS-ს გავრცელებულ სახეობას წარმოადგენს ე.წ. **SCADA (Supervisory Control and Data Acquisition) და DCS (Distributed Control Systems) სისტემები.**

რუსეთის თავდაცვის სამინისტროს კიბერდანაყოფები მონაწილეობენ შემტევი კიბეროპერაციების, საინფორმაციო-ფსიქოლოგიური ეფექტის მქონე კიბერღონისძიებებისა და მოწინააღმდეგის მართვისა და კონტროლის სისტემებში მავნებელი პროგრამული უზრუნველყოფის ჩანერგვაში. რუსეთის მაღალი რანგის სამხედრო პირებზე დაყრდნობით, საინფორმაციო ოპერაციების ჯარებმა 2016 წლის სექტემბერში პირველად მიიღეს მონაწილეობა სამეთაურო-საშტაბო სწავლებაში „Кавказ-2016“.

საინფორმაციო კონფრონტაციის პროცესში დომინირებისათვის რუსეთი გარდა სახელმწიფო აქტორებისა, აქტიურად იყენებს კიბერკრიმინალის შესაძლებლობებს, რაც მას საშუალებას აძლევს დაუსჯელად და იაფად დააზიანოს მოწინააღმდეგე ქვეყნის კრიტიკული ინფრასტრუქტურა. ლიეტუვას და საქართველოს წინააღმდეგ 2008 წელს განხორციელებულ კიბერშეტევებში მნიშვნელოვანი როლი შეასრულა ძლიერი ტექნიკური შესაძლებლობების მქონე კიბერკრიმინალურმა ორგანიზაციამ RBN (Russian Business Network), რომელმაც ინტენსიური თავდასხმა განახორციელა ქართულ ქსელებზე.

2020 წელს აშშ- ის ერთ-ერთ უმსხვილეს ნავთობსადენზე განხორციელებული “Ransomware”[5] კიბერშეტევის შედეგად, კომპანია Colonial Pipeline- მა ნავთობსადენის მუშაობა დროებით შეაჩერა. ჰაკერებმა მილსადენის კომპიუტერულ სისტემაში შეაღწიეს და ხელში თითქმის 100 GB-ის მოცულობის მონაცემები ჩაიგდეს, ხოლო დაშიფრული მონაცემების გასახსნელად კომპანიისგან გამოსასყიდად რამდენიმე მილიონი დოლარის ღირებულების ბიტკოინები მიიღეს. თავდამსხმელი, DarkSide რუსეთში ბაზირებული კიბერკრიმინალური დაჯგუფებაა, რომელმაც 2019 წლიდან დასავლეთის ქვეყნებს უკვე მილიარდობით ზარალი მიაყენა. აშშ-ის მთავრობა იძულებული გახდა საგანგებო მდგომარეობა გამოეცხადებინა. მილსადენის გაჩერებამ საწვავის ფასის ზრდა გამოიწვია. რამდენიმედღიანი შეფერხების შედეგად, საწვავის ფასმა 2014 წლის ოქტომბრის შემდეგ ყველაზე მაღალ ნიშნულს მიაღწია.

ოდნავ მოგვიანებით, იმავე წლის ივნისის დასაწყისში განხორციელებულმა მორიგმა „Ransomware“ შეტევამ ხორცპროდუქტების უმსხვილეს მწარმოებელზე „JBS”-ზე აშშ-ის, კანადისა და ავსტრალიის ოპერაციებში მნიშვნელოვანი შეფერხება და ხორცპროდუქტებზე ფასების ზრდა გამოიწვია. შეტევის უკან რუსული კიბერკრიმინალური დაჯგუფება „REvil“ იდგა. „REvil“, იგივე Sodinokibi ცნობილი კიბერკრიმინალური ჯგუფია. იგი მინიმუმ 2019 წლიდანაა აქტიური და მისი წევრები რუსეთისა და პოსტსაბჭოთა ქვეყნების მოქალაქეები არიან.

გართულებული ატრიბუციის გამო, რუსული სადაზვერვო სამსახურები აარსებენ კონსპირაციის მაღალი დონის მქონე ჰაქტივისტურ ჯგუფებს ან მოქმედებენ უკვე არსებულთა საფარქვეშ. ჰაქტივისტური კიბერშეტევები წარმოადგენდა ერთ-ერთ ელემენტს რუსეთის მთავრობის მიერ მხარდაჭერილ კიბერშეტევებში 2007 წელს ესტონეთის, 2008 წელს კი

[5] „Ransomware“კიბერშეტევის ფორმაა, რომლის დროსაც კრიმინალები, არასანქცირებული წვდომის შედეგად მათ მიერვე დაშიფრული ან ბლოკირებული ინფორმაციის გასახსნელად გამოსასყიდს ითხოვენ. ამ ტიპის შეტევის გამოყენება, როგორც ფინანსურად მოტივირებული კიბერკრიმინალის, ასევე სახელმწიფოთა მიერ მხარდაჭერილი შეტევებისას დრამატულად გაიზარდა, რაც აშშ-ის უსაფრთხოების სამსახურების მზარდ შეშფოთებას იწვევს. ანონიმურობის და ქსელის დაცულობის მაღალი ხარისხის გამო, კიბერკრიმინალი გადახდის საშუალებად ხშირად კრიპტოვალუტას იყენებს. ატრიბუციის გარდა, გართულებულია ბიტკოინის ტრანზაქციის შეჩერება, მისი ამოღება, წართმევა ან უკან დაბრუნება.

საქართველოს წინააღმდეგ, ასევე მუდმივად იყო გამოყენებული რუსეთ-უკრაინის კონფლიქტში მეიდანზე განვითარებული პროცესებისას თუ ყირიმის ანექსიისას.
რუსეთი კიბერშეტევებს ე.წ. false flag ოპერაციებითაც ახორციელებს. პარტნიორი სპეცსამსახურების დადასტურებული მონაცემებით, სწორედ რუსეთი იდგა "ისლამურ სახელმწიფოსთან" ასოცირებული კიბერხალიფატის ("Cyber Chaliphate") მიერ ჰაქტივიზმის საფარვეშ საფრანგეთის სატელევიზიო არხ TV5 Monde-ზე 2015 წლის აპრილში განხორციელებული თავდასხმის უკან. შეტევა კარგად იყო ორგანიზებული და დაიწყო არხის თანამშრომლებისათვის ფიშინგ-წერილების დაგზავნის კამპანიით, რამაც კიბერკრიმინალებს შესაძლებლობა მისცა 3 თვის შემდგომ მოეპოვებინათ კონტროლი ათამდე საინფორმაციო არხსა და მათ სოციალურ მედიაარხებზე, გაევრცელებინათ ჯიჰადისტური პროპაგანდა და გამოექვეყნებინათ სირიაში დისლოცირებული ფრანგი სამხედროების პერსონალური მონაცემები.

3. დასკვნა

საინფორმაციო კონფრონტაციის მიზნების მისაღწევად რუსეთი ფართოდ იყენებს ანაზღაურებად კომენტატორთა არმიას - ე. წ. ტროლებს. ტროლები წარმოადგენენ შედარებით ღია, თუმცა მაინც გართულებული ატრიბუციის ინსტრუმენტს ანტირუსული ინფორმაციის დისკრედიტაციისა და პროკრემლისტური განწყობების ჩამოსაყალიბებლად. კონკრეტული ტროლი ხშირად მართავს მრავალრიცხოვან ონლაინპროფაილსა და ბლოგს. რუსული ტროლინგის მიზანი ყოველთვის რუსული თვალსაზრისის სისწორეში აუდიენციის დარწმუნება კი არ არის, არამედ, მათ მისიას წარმოადგენს სოციალური მედიის წალეკვა ყალბი კონტენტით, ეჭვის, შიშის, არასტაბილურობის განცდის შექმნა და ინტერნეტის დემოკრატიულ სივრცედ გამოყენების ხელისშეშლა.

ბიბლიოგრაფია:

1. Janne Hakala, Jazlyn Melnychuk. Russia's strategy in Cyberspace. e NATO StratCom COE. Riga, June 2021. ISBN: 978-9934-564-90-1
2. Joint Cybersecurity Advisory co-authored by authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom. Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. April 20. 2020.
3. Defence Intelligence Agency. Russia Military Power - building a military to support great power aspirations. dia-11-1704-161. www.dia.mil/military-power-publications
4. UK Foreign and Commonwealth Office Report "UK exposes Russian involvement in SolarWinds cyber compromise" 2021
5. Hearing: Worldwide Cyber Threats (Open). Testimony of The Honorable James Clapper, Director of National Intelligence. September 10, 2015. https://docs.house.gov/meetings/IG/IG00/20150910/103797/HHRG-114-IG00-Wstate-ClapperJ-20150910.PDF
6. Nakashima E. and Timberg C. Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce, The Washington Post, 14 December 2020
7. Russia's Cyber Tactics: Lessons Learned in 2022 — SSSCIP analytical report on the year of Russia's full-scale cyberwar against Ukraine. 2023