**დესტრუქციული აქტორების მოკლე მიმოხილვა**

რუსეთის ფედერაცია. შემტევი კიბერპოტენციალის თვალსაზრისით, რუსეთი ერთ- ერთი ძლიერი სახელმწიფოა მსოფლიოში.

2014 წლის დეკემბერში რუსეთში ჩამოყალიბდა თავდაცვის მართვის ეროვნული ცენტრი (Национальный центр управления обороной РФ, NDMC), რომელიც წარმოადგენს რუსეთის ფედერაციის თავდაცვის სამინისტროსა და შეიარაღებული ძალების მართვისა და კონტროლის უმაღლეს ორგანოს.

2017 წლის თებერვალში რუსეთმა შექმნა საინფორმაციო ოპერაციების ჯარები, რომელიც პასუხისმგებელია, როგორც ტექნიკური ეფექტის მქონე კიბეროპერაციების წარმოებაზე, ისე პროპაგანდის გავრცელებასა და საინფორმაციო კონფრონტაციის სხვა ელემენტებზე.

რუსეთის თავდაცვის სამინისტროს კიბერდანაყოფები, რომლებიც პასუხისმგებელნი არიან შემტევი კიბეროპერაციების ჩატარებაზე, საინფორმაციო-ფსიქოლოგიური ეფექტის მქონე კიბერღონისძიებებსა და მოწინააღმდეგის მართვისა და კონტროლის სისტემებში მავნებელი პროგრამული უზრუნველყოფის ჩანერგვაზე, სერიოზული და ყველაზე რეალური საფრთხის შემცველია საქართველოსთვის.

რუსეთის სპეცსამსახურები აქტიურად ავითარებენ კრიტიკული ინფრასტრუქტურის ინდუსტრიის კონტროლის სისტემებზე დისტანციური წვდომის საშუალებებს: უცნობმა რუსმა აქტორებმა წარმატებულად განახორციელეს რამდენიმე მწარმოებლის პროგრამის კომპრომეტაცია, ლეგალური პროგრამული უზრუნველყოფის განახლებებში **მავნე პროგრამული კოდის** ჩანერგვა და ამ გზით მომხმარებლის სისტემასთან პირდაპირი წვდომის დამყარება.

საქართველოსათვის საფრთხის შემცველი კიდევ ერთი მიმართულება რუსეთის კიბერჯაშუშობის შესაძლებლობებია. წლების განმავლობაში რუსული აქტორების მიერ ჩანერგილი ჯაშუშური პროგრამის მსხვერპლი გახდა სამთავრობო და ძალოვან სტრუქტურათა რესურსები, სამხედრო ატაშეების ოფისები, ნატო-საქართველოს ურთიერთობასთან დაკავშირებული დოკუმენტაცია და სხვა სენსიტიური მასალები, სამხედრო – სამრეწველო სფეროს საიდუმლო პროექტები.

გარდა მწყობრიდან გამოყვანის ან გამოყენების მიზნით მოწინააღმდეგის ქსელზე წარმოებული თავდასხმებისა, რუსეთი კიბერსივრცეს იყენებს ფსიქოლოგიური ეფექტის მისაღწევად, რაც კრემლის სასარგებლოდ ადმიანების ქცევის ან ცნობიერების შეცვლის მცდელობებს გულისხმობს.

ინფორმაციული კონფრონტაციის პროცესში დომინირებისათვის რუსეთი მრავალფეროვან საშუალებებს მიმართავს: საქართველოს წინააღმდეგ 2008 წელს განხორციელებულ კიბერშეტევაში მნიშვნელოვანი როლი შეასრულა ძლიერი ტექნიკური შესაძლებლობების მქონე კიბერკრიმინალურმა ორგანიზაციამ RBN (Russian Business Network), რომელმაც ინტენსიური თავდასხმა განახორციელა ქართულ ქსელებზე.

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 საქართველოს წინააღმდეგ, ასევე მუდმივად იყო გამოყენებული რუსეთ-უკრაინის კონფლიქტში მეიდანზე განვითარებული პროცესებისას თუ ყირიმის ანექსიისას.

რუსულ კიბეოპერაციებში მნიშვნელოვან როლს თამაშობს ორი ჰაკერულმა დაჯგუფება: APT 28 (Fancy Bear) და APT 29 (Cozy Bear), რომლებიც რუსეთის ფედერაციის გენერალური შტაბის სამხედრო დაზვერვასთან ასოცირდებიან და სხვა რეზონანსულ კიბერშეტევებთან ერთად, პასუხისმგებელნი არიან აშშ საპრეზიდენტო არჩევნების პროცესში დემოკრატიული პატრიის სერვერებიდან ინფორმაციის დაუფლებაზე (ე.წ. DNC Hack). DNC hack განიხილება, როგორც რუსეთის ხელისუფლების უმაღლეს დონეზე სანქცირებული ჩარევა აშშ-ის არჩევნებში, დემოკრატიულ პროცესების რწმენის შესუსტების და კონკრეტული კანდიდატის კომპრომეტაციის მიზნით.

APT 28 პასუხისმგებელია ასევე ევროპის ქვეყნების თავდაცვის სექტორის საინფორმაციო სისტემებიდან ინფორმაციის მოპარვასა და საქართველოს სახელმწიფო სტრუქტურების და ჟურნალისტური წრეების წინააღმდეგ 2008-14 წლებში განხორციელებულ კიბერჯაშუშობის კამპანიაზე. რაც შეეხება APT 29-ს, ამ დაჯგუფების სახელი უკავშირდება აშშ სახელმწიფო დეპარტამენტის, თეთრი სახლის, პენტაგონის და სხვა სახელმწიფო უწყებების სისტემებიდან არასაიდუმლო ინფორმაციის გაჟონვას. DNC Hack პროცესში ორივე დაჯგუფება ფიგურირებს: არსებული მონაცემებით APT 29-ს თითქმის 1 წელი ჰქონდა წვდომა დემოკრატიული პარტიის კომუნიკაციის საშუალებებზე, ელექტრონულ ფოსტასა და ჩატის კონტენტზე.

უკრაინის ენერგოსისტემაზე 2014 -15 წლებში რუსეთის მიერ განხორციელებულმა კიბერშეტევებმა გააჩინა განცდა, რომ რუსეთი მომავალ კონფლიქტში არ შემოიფარგლება მხოლოდ DDoS და Defacement შეტევებით ან კიბერშპიონაჟის ოპერაციებით და არ არსებობს გარანტია, რომ იგი არ განახორციელებს კრიტიკული ინფრასტრუქტურის წინააღმდეგ მიმართულ აქციას, რასაც, გარკვეულ ეტაპზე, შესაძლოა ნგრევა და მსხვერპლი მოჰყვეს.

ირანის ისლამური რესპუბლიკა. ირანმა თანხების სწორი განაწილებით მოახერხა შეექმნა ძლიერი კიბერშესაძლებლობები და გამხდარიყო ერთ ერთი სერიოზული კიბერაქტორი. მისი კიბერპოტენციალი რუსეთის და ჩინეთისას ჩამოუვარდება, თუმცა იგი წარმოადგენს ჩრდილოეთ კორეის დონის აქტორს და რეალური საფრთხეა განვითარებული ქვეყნის კრიტიკული ინფრასტრუქტურისთვის.

ისრაელსა და საუდის არაბეთთან წლების განმავლობაში მიმდინარე დაპირისპირებამ ირანის კიბერპოტენციალის განვითარებას შეუწყო ხელი. ირანმა, რუსეთისა და ჩინეთისაგან მიღებული ტექნოლოგიური დახმარების ხარჯზე, მოახერხა კიბერშესაძლებლობების განვითარება.

დღესდღეობით, კიბეროპერაციები ირანის სამხედრო ძალის მნიშვნელოვანი შემადგენელია. კიბერშეტევებისას გამოყენებული ინსტრუმენტები ძირითადად კრიმინალურ ბაზარზე არსებული მოდიფიცირებული მალვეარია, რომელიც, დესტრუქციული პოტენციალით ჩამოუვარდება რუსულ ანალოგებს მაგრამ მნიშვნელოვანი ზიანის მომტანია ნებისმიერი ქვეყნის ინფრასტრუქტურისათვის.

მცირე ბანკების, ლოკალური მნიშვნელობის ენერგეტიკული კომპანიების ან ნავთობსადენის კონტროლის სისტემებისათვის ირანის დესტრუქციული კიბერპოტენციალი რეალურ საფრთხეს წარმოადგენს. უფრო მაღალტექნოლოგიური შეტევებისათვის ირანის კიბერშესაძლებლობები დღეისათვის მზად არ არის.

ირანისათვის დამახასიატებელია კიბეროპერაციების განხორციელება რამდენიმე მიმართულებით:

* DDoS შეტევა
* კიბერშპიონაჟი საჰაერო და კოსმოსური ტექნოლოგიების კომპანიების, თავდაცვის სფეროს კონტრაქტორების, ენერგეტიკისა და ბუნებრივი რესურსების სექტორისა და სატელეკომუნიკაციო სფეროს წარმომადგენლების წინააღმდეგ
* პიროვნების თრეკინგი ტერორისტული აქტისათვის საჭირო მონაცემების მოსაპოვებლად
* მონაცემთა წაშლა
* საინფორმაციო ოპერაცია მაკომპრომეტირებელი მასალების გამოქვეყნებით

2012 წელს თეირანმა კიბერშეტევა განახორციელა საუდის არაბეთის Aramco -სა და ყატარის RasGas-ზე. გამოყენებულმა მაღალტექნოლოგიურმა მალვეარმა ათასობით კომპიუტერის მწყობრიდან გამოსვლა გამოიწვია. 2012-13 წლებში ირანელმა ჰაკერებმა DDoS შეტევა განახორციელეს ამერიკული ბანკებისა და საფონდო ბირჟის წინააღმდეგ, ხოლო 2014 წელს - მონაცემების წაშლა ამერიკული Las Vegas Sands კაზინოდან. იმავე 2014 წელს, ღაზას სექტორში მიმდინარე ესკალაციისას ირანული DDoS შეტევის სამიზნე გახდა ისრაელის თავდაცვის ძალების ინფრასტრუქტურა. 2016-2017 წლებში ირანმა კიდევ ერთი მაღალტექნოლოგიური შეტევა განახორციელა საუდის არაბეთის წინააღმდეგ, რამაც ათეულობით ობიექტიდან ინფორმაციის წაშლა გამოიწვია. ამჯერად სამიზნეს სამოქალაქო ავიაციის, ცენტრალური ბანკისა და სახელმწიფო უწყებების ქსელები წარმოადგენდა.

საქართველოსთვის ირანის კიბერშესაძლებლობები შესაძლოა საფრთხეს წარმოადგენდეს იმდენად, რამდენადაც ჩვენს ტერიტორიაზე განთავსებულია ირანის ხედვით, მისდამი მტრულად განწყობილი სახელმწიფოების ინფრაქსტრუქტურა. ასევე, თანამედროვე ტენდენციების გათვალისწინებით, სავსებით რეალურია ირანის მიერ მხარდაჭერილი ტერორისტული ორგანიზაციების მხრიდან ქართული კიბერქსელების პროპაგანდისტული მიზნებით გამოყენება.

ჩინეთი. ჩინეთის კიბეროპერაციები ძირითადად კომერციულ მიზნებს ემსახურება და, შესაბამისად, საქართველოსთვის პირდაპირი საფრთხის შემცველი არ არის. აქ, თუმცა არ უნდა გამოგვრჩეს ჩვენთან არსებული განვითარებული ქვეყნების სამთავრობო თუ კომერციული სტრუქტურების ქსელები და მათ მონაცემთა ბაზებში არსებული ინფორმაცია. მიუხედავად კიბერსეფროში თანამშრომლობის შესახებ მათ შორის გაფორმებული მემორანდუმისა, ჩინეთის კიბერშპიონაჟის მთავარ სამიზნედ კვლავ რჩება აშშ. დაინტერესების საკითხების სპექტრი ფართოა, ეროვნულ უსაფრთხოებასთან დაკავშირებული ინფორმაციით დაწყებული, სენსიტიური ეკონომიკური მონაცემებითა და აშშ-ის კომპანიების ინტელექტუალური საკუთრებით დამთავრებული. ცხადია, საქართველომ განსაკუთრებული ყურადღება უნდა მიაქციოს იმ მნიშვნელოვანი პროექტების კიბერუსაფრთხოებას, რომელიც აშშ ჩართულობით ან მისი პატრონაჟით ხორციელდება ქართულ სახელმწიფო თუ კომერციულ სტრუქტურებში.

ჩრდილოეთ კორეა კიდევ ერთი აქტორია, რომელიც კიბერშესაძლებლობებს პოლიტიკური მიზნებისთვის იყენებს. სპეციფიური პოლიტიკური რეჟიმის გათვალისწინებით, ამ სახელმწიფოს კიბერდანაყოფების სამიზნე ძირითადად აშშ-ის კრიტიკული ინფრასტრუქტურა ან თავისუფალი მედიაა.  ეს სახელმწიფო პასუხისმგებელია 2014 წლის ნოემბერში Sony Pictures Entertainment-ის წინააღმდეგ განხორციელებულ კიბერშეტევაზე, რომლის დროსაც ქსელურ ინფრასტრუქტურაში მავნე კოდის შეღწევის შედეგად, განადგურდა სენსიტიური ინფორმაცია. თავდასხმა დაემთხვა ჩრდილოეთ კორეის სახელმწიფოს მეთაურის შესახებ კრიტიკული ფილმის გამოსვლის სავარაუდო თარიღს და მისთვის ხელის შეშლას ისახავდა მიზნად. 2017 წელს 150 ქვეყნის ასეულობით ათასი კომპიუტერი დაინფიცირდა ჩრდილოკორეული მალვეარით WannaCry. ჩრდილოეთ კორეას ასევე მიაწერენ ონლაინ ბირჟებიდან ორ მილიარდამდე დოლარის ღირებულების კრიპტოვალუტის მოპარვას მასობრივი განადგურების იარაღის შესაქმნელი სამუშაოების შესასრულებლად.