CRC GCSD

საარჩევნო პროცესების კიბერუსაფრთხოება

საუკეთესო პრაქტიკა

საარჩევნო პროცესების კიბერუსაფრთხოება - საუკეთესო პრაქტიკა

ავტორი: ანდრო გოცირიძე, კიბერუსაფრთხოების კონსულტანტი. კიბერუსაფრთხოების საგანმანათლებლო კვლევითი ცენტრის CYSEC დამფუძნებელი, თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიუროს დირექტორი 2014-2017 წლებში.

აბსტრაქტი

არჩევნები, როგორც დემოკრატიული წყობის ძირითადი ატრიბუტი რუსული ჰიბრიდული ომის ერთ ერთი მნიშვნელოვანი სამიზნეა. ევროპის სახელმწიფოთა თუ აშშ-ის საარჩევნო პროცესები, რეფერენდუმი ან მოსახლეობის ნების გამოხატვის სხვა პროცესი მრავალჯერ გახდა რუსული კიბეროპერაციების სამიზნე.

არჩევნების შედეგებით მანიპულირებას რუსეთი როგორც ტექნიკური, ისე ფსიქოლოგიური ეფექტის მქონე კიბეროპერაციებით ცდილობს. ტექნიკურ ეფექტს იძლევა სტანდარტული კიბერშეტევა, ხოლო ფსიქოლოგიურ ზემოქმედებას: ამომრჩევლის აღქმის შეცვლას, მანიპულაციას, პროცესისადმი ნდობის შერყევას კი კრემლის მიერ მხარდაჭერილი აქტორები საინფორმაციო ოპერაციების მეშვეობით ახორციელებენ.

კიბერშეტევა ხშირად საინფორმაციო ოპერაციის ჩასატარებელ სერიოზულ ინსტრუმენტს წარმოადგენს და ინფორმაციული უპირატესობის მოპოვებას ისახავს მიზნად. ზოგჯერ, კიბერშეტევა საინფორმაციო ოპერაციის პარალელურად ხორციელდება. მაგალითად, კიბერშეტევის შედეგად ხდება ელექტრონული ფოსტიდან ან სოციალური ქსელის ანგარიშიდან ინფორმაციის არასანქცირებული მოპოვება, ხოლო შემდგომ, მოპოვებული მაკომპრომეტირებელი მასალა ორიგინალის ან ფაბრიკაციის სახით ვრცელდება ინტერნეტში.

სტატიაში განხილულია საარჩევნო პროცესებში ხშირად გამოყენებული კიბერშეტევებისა და საინფორმაციო ოპერაციების ტექნიკები, საფრთხეები, საფრთხის აქტორები და რისკების მართვის საუკეთესო პრაქტიკა. დასასრულს, მოყვანილია რამდენიმე პრაქტიკული რჩევა საარჩევნო პროცესების ადმინისტრირებაში ჩართულ პირთა კიბერჰიგიენისთვის. ნაშრომი ძირითადად ორ მიზანს ემსახურება: არჩევნების კიბერუსაფრთხოების, კიბერშეტევებისა და საინფორმაციო ოპარაციების შესახებ ცნობიერების ამაღლებას საარჩევნო პროცესში ჩართული ნებისმიერი მხარისათვის და საარჩევნო ადმინისტრაციის თანამშრომლებისათვის რისკების შემცირების სტრატეგიის შეთავაზებას.

საარჩევნო პროცესების კიბერუსაფრთხოება - საუკეთესო პრაქტიკა

არჩევნები, ხალხის მიერ საკუთარი ნების გამოხატვა, დემოკრატიის ფუძემდებლური პრინციპია. ხალხის ნდობას მხოლოდ არჩევნების გზით მოსახლეობის მიერ მხარდაჭერილი მთავრობა იმსახურებს, შესაბამისად, უმნიშვნელოვანესია არჩევნების პროცესისა და მისი შედეგების მიმართ ნდობის მაღალი ხარისხი. სწორედ ამიტომ, არჩევნები, როგორც დემოკრატიული წყობილების ძირითადი ატრიბუტი რუსული ჰიბრიდული ომის ერთ ერთი მნიშვნელოვან სამიზნეს წარმოადგენს. უკანასკნელ პერიოდში რუსული კიბეროპერაციების შედეგებს ტექნიკურ, კინეტიკურ ეფექტთან ერთად ფსიქოლოგიური ზემოქმედებაც დაემატა და სახელმწიფოთა საარჩევნო სისტემები, რეფერენდუმი ან მოსახლეობის ნების გამოხატვის სხვა პროცესი მრავალჯერ გახდა რუსული კიბეროპერაციების სამიზნე.

ხშირად, არჩევნების კიბერუსაფრთხოებაზე საუბარი ხმის მიცემის ელექტრონულ პროცედურების გამართულობაზე დაიყვანება, თუმცა ეს ასე არ არის. კიბერუსაფრთხოების პერსპექტივიდან, საარჩევნო პროცესის ნებისმიერი ეტაპი, რომელიც მოიცავს ელექტრონული მოწყობილობის ან სივრცის გამოყენებას, რისკის შემცველია. კომპიუტერული სისტემები და პროგრამული უზრუნველყოფა საარჩევნო პროცესის ყველა კომპონენტშია წარმოდგენილი, რაც ამ პროცესებში სისუსტეების არსებობასაც გულისხმობს. კიბერშეტევის პოტენციური ვექტორი შესაძლოა იყოს როგორც ტექნიკური, ასევე ადამიანური ფაქტორი და მოიცავდეს როგორც თავად საინფორმაციო სისტემას, ასევე მათ, ვინც ქმნის ან მართავს ამ მას. სახელმწიფო სექტორზე, ბიზნესსა თუ ინდუსტრიაზე განხორციელებულ თავდასხმებში, კიბერინციდენტების უმეტესობა ძირითადად, მავნე აქტორების მიერ ადამიანური ფაქტორის გამოყენებითაა განპირობებული. კომპიუტერული სისტემებისა და პროგრამული უზრუნველყოფის ვენდორები ასევე წარმოადგენენ მეტად მოწყვლად სამიზნეს. ამ მხრივ გამონაკლისს არც საარჩევნო სისტემების კიბერუსაფრთხოება წარმოადგენს.

არჩევნების კიბერუსაფრთხოების კონტექსტში, კიბერშეტევის[1] გავრცელებული სახეებია ფიშინგი, DDoS შეტევა, Defacement, MITM და სხვა. კიბერშეტევა ხშირად **საინფორმაციო ოპერაციის**[2] ჩასატარებელ მნიშვნელოვან ინსტრუმენტს წარმოადგენს და **ინფორმაციული**

[1] ქსელზე თავდასხმის ერთ ერთი ფორმა, რომლის მიზანს კომპიუტერის ან კომპიუტერული ქსელის მწყობრიდან გამოყვანა, შეფერხება, განადგურება, მასზე არასანქცირებული კონტროლის მოპოვება, მასში არსებული კონტროლირებადი ინფორმაციის მთლიანობის დარღვევა ან მისი არაავტორიზებული დაუფლება წარმოადგენს.

[2] წარმოადგენს საინფორმაციო კონტენტის გავრცელებას საზოგადოებრივი აზრის მანიპულაციის ან საზოგადოების ქცევაზე გავლენის მოხდენის მიზნით. **კონტენტი** *ცრუ და ნამდვილი ინფორმაციის ნაზავია, რომელიც მიმართულია სამიზნე აუდიტორიის დაბნევის, დემორალიზაციისა და მასზე გავლენის მოპოვებისკენ.* **სამიზნე აუდიტორია** *ზოგჯერ საკუთარი მოსახლეობა და ქვეყნის შიდა პოლიტიკური ელიტაა, თუმცა, არცთუ იშვიათად, სამიზნეს სხვა ქვეყნების მოსახლეობის გარკვეული ჯგუფები, ეთნიკური, რელიგიური უმცირესობა და პოლიტიკური ელიტა წარმოადგენს.*

უპირატესობის[3] მოპოვებას ისახავს მიზნად. საინფორმაციო ოპერაციების კიბერელემენტი მოიცავს დაინტერესების ობიექტების ქსელების კომპრომეტაციას ისეთი ინფორმაციის მოპოვების მიზნით, რომელიც შესაძლოა გამოყენებულ იქნას დაშინების, შანტაჟის, დისკრედიტაციის ან ფალსიფიკაციის მიზნით, ასევე მასმედიის საშუალებებში კონტროლირებადი გავრცელებისთვის.

ციფრული ტექნოლოგიების ბუმმა, შემტევი კიბერშესაძლებლობების განვითარებამ სახელმწიფოებს უპრეცენდენტო მასშტაბის საინფორმაციო ოპერაციების განხორციელების საშუალება მისცა, რადგან ამგვარი ოპერაციებისათვის საჭირო კიბერინსტრუმენტები უკიდურესად იაფი და ხელმისაწვდომია. საინფორმაციო ოპერაციების ტაქტიკა გულისხმობს მცდარი ან შეცდომაში შემყვანი ინფორმაციის გავრცელებას, მოპარული ინფორმაციის კონტროლირებად გაჟონვას ინტერნეტში, სოციალური ქსელების გამოყენებას ანტაგონისტული განწყობების გასაღვივებლად, პოლარიზაციის გასაღრმავებლად და პოლიტიკური კონფლიქტის გასაჩაღებლად.[i]

როგორც უკვე აღინიშნა, კიბერშეტევა, ხშირად, საინფორმაციო ოპერაციის უმნიშვნელოვანესი ინსტრუმენტია. მაგალითად, კიბერშეტევის შედეგად ხდება ელექტრონული ფოსტიდან ან სოციალური ქსელის ანგარიშიდან ინფორმაციის არასანქცირებული მოპოვება, ხოლო შემდგომ, მოპოვებული მაკომპრომეტირებელი მასალა ორიგინალის ან ფაბრიკაციის სახით ვრცელდება ინტერნეტში, სადაც, ისევ კიბერტექნოლოგიების - ტროლინგის ან ბოტების მეშვეობით ხდება სასურველი აზრის ფორმირება.

კიბერშეტევების ან საინფორმაციო ოპერაციების საშუალებით არჩევნებზე ზეგავლენის მოხდენის, დემოკრატიული პროცესების დისკრედიტაციის მისწრაფება და შესაძლებლობა ბევრ აქტორს შეიძლება ჰქონდეს როგორც ქვეყნის შიგნით, ასევე მის ფარგლებს გარეთ. ესენია:

- სახელმწიფოები;
- ორგანიზებული კიბერკრიმინალი ან ცალკეული ჰაკერები;
- ტერორისტული ორგანიზაციები;
- ინსაიდერები;
- პოლიტიკურად მოტივირებული ჯგუფები;
- ჰაქტივისტები.

აქტორებისათვის მოტივაციას არჩევნებში ჩარევისათვის შესაძლოა წარმოადგენდეს:

- სახელმწიფოს ეროვნული ან გეოპოლიტიკური ინტერესები;
- ფინანსური მოგება;
- რეპუტაციის გამყარება;
- ანარქიის და ქაოსის პროვოცირება;

---

[3] რუსულ სამხედრო და პოლიტიკურ წრეებში დამკვიდრებული ტერმინია და გულისხმობს ინფორმაციის მიღების, დამუშავებისა და გავრცელების შესაძლებლობას, რომელიც ხელს უშლის მოწინააღმდეგეს იმავე ფუნქციის განხორციელებაში.

- შურისძიება;
- პოლიტიკური ოპოზიციის სუბვერსია;
- დემოკრატიული პროცესებისა და წყობისადმი ნდობის შესუსტება.

ჰაკერები თუ ორგანიზებული კიბერკრიმინალური დაჯგუფებები სერიოზულ საფრთხეს წარმოადგენენ არჩევნებისთვის. კიბერდამნაშავეები წარმატებით ახორციელებენ საცალო ბიზნესისა და ფინანსური ინსტიტუტების ქსელებში შეღწევას, რათა მოიპოვონ ფინანსური ინფორმაცია, პერსონალური მონაცემები, საცხოვრებელი თუ ელექტრონული ფოსტის მისამართები და სამედიცინო ჩანაწერები, რაც წარმოადგენს საბაზისო ინფორმაციას კრიმინალური ოპერაციებისათვის. უკანასკნელ პერიოდში ჰაკერების კიბერშეტევათა ვექტორმა საარჩევნო სისტემებისკენაც გადაინაცვლა, სადაც დიდი რაოდენობით ძვირადღირებული ინფორმაციაა დეპონირებული. ამგვარი თავდასხმების მოტივაცია მრავალგვარია: ფინანსური სარგებელი, თავის გამოჩენის სურვილი თუ უბრალოდ საკუთარი შესაძლებლობების გამოცდა.

თუმცა, არჩევნებზე ზეგავლენის მოხდენის მსურველთა შორის ყველაზე დიდ საფრთხეს, როგორც კიბერშეტევის პოტენციალის, ასევე დაინტერესების მხრივ, მაინც სახელმწიფოები და მათთან აფილირებული კიბერაქტორები წარმოადგენენ. შემტევი კიბერპოტენციალის თვალსაზრისით, რუსეთი ერთ ერთ მოწინავე პოზიციას იკავებს მსოფლიოში[ii] და საქართველოსადმი მტრულად განწყობილ ერთადერთ ქვეყანას წარმოადგენს. კრემლი საქართველოს მისი გავლენის სფეროდ მოიაზრებს, რის გამოც ჩვენი ქვეყანა რუსეთის ჰიბრიდული ომის სამიზნეა, ამ ომის არეალი კი გარდა დიპლომატიური, ეკონომიკური, სამხედრო, პოლიტიკური, კულტურული, სოციალური, რელიგიურ თუ საინფორმაციო სფეროებისა, მოწინააღმდეგე ქვეყნების მთავრობების ან ინსტიტუტების დელეგიტიმიზაცია, დემოკრატიული პროცესების ძირგამომთხრელი საქმიანობაცაა.

არჩევნების შედეგებით მანიპულირებას რუსეთი როგორც ტექნიკური, ისე ფსიქოლოგიური ეფექტის მქონე კიბეროპერაციებით ცდილობს. ტექნიკურ ეფექტს იძლევა სტანდარტული კიბერშეტევა, ხოლო ფსიქოლოგიურ ზემოქმედებას: ამომრჩევლის აღქმის შეცვლას, მანიპულაციას, პროცესისადმი ნდობის შერყევას კი კრემლის მიერ მხარდაჭერილი აქტორები საინფორმაციო ოპერაციების მეშვეობით ახორციელებენ. უკანასკნელი ათწლეულის მანძილზე, ევროპისა თუ აშშ-ის საარჩევნო პროცესები მრავალჯერ გახდა ამგვარი ზემოქმედების სამიზნე.[iii]

რუსეთის კიბერაქტივობების მასშტაბი მზარდია, როგორც სირთულის, ისე მრავალფეროვნების თვალსაზრისით. გარდა მოწინააღმდეგის ქსელის მწყობრიდან გამოყვანის ან მისი ექსპლოატაციის მიზნით წარმოებული კიბერთავდასხმებისა, რუსეთი კიბერსივრცეს იყენებს ფსიქოლოგიური ეფექტის მისაღწევად, რაც კრემლის სასარგებლოდ ადმიანების ქცევის ან ცნობიერების შეცვლის მცდელობებს გულისხმობს.

ამრიგად, რუსული კიბეროპერაციების შედეგი, ერთის მხრივ, შეიძლება იყოს მნიშვნელოვანი ზარალი და მსხვერპლიც კი, მეორეს მხრივ კი ამ ოპერაციებს შესაძლოა კრემლის სასარგებლოდ ცნობიერების შეცვლა, პრორუსული ელიტის ფორმირება-გაძლიერება, არჩევნების შედეგებით მანიპულირება, პოლარიზაცია, არჩეული ხელისუფლების ლეგიტიმაციის შემცირება და სხვა ძირგამომთხრელი ეფექტი ჰქონდეს.

რუსულ კიბეოპერაციებში, სხვა აქტორებთან ერთად, მნიშვნელოვან როლს თამაშობს საგარეო დაზვერვის სამსახურისა (Служба Внешней Разведки) და თავდაცვის სამინისტროს

გენერალური შტაბის მთავარი სადაზვერვო სამმართველოს (Главное Разведывательное Управление) კიბერდანაყოფები. ეს უწყებები სხვა რეზონანსულ კიბერშეტევებთან ერთად, პასუხისმგებელნი არიან აშშ საპრეზიდენტო არჩევნების პროცესში დემოკრატიული პატრიის სერვერებიდან ინფორმაციის დაუფლებაზე.

სამხედრო დაზვერვის მთავარი სამმართველო, რომლის კიბერდანაყოფი ბოლო ატრიბუციამდე APT 28 -ის სახელით იყო ცნობილი, 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, საგარეო დაზვერვის სამსახურის კიბერდანაყოფს, მისი სახელი უკავშირდება აშშ სახელმწიფო დეპარტამენტის, თეთრი სახლის, პენტაგონის და სხვა სახელმწიფო უწყებების სისტემებიდან არასაიდუმლო ინფორმაციის გაჟონვას. არჩევნებთან დაკავშირებულ პროცესებში ორივე დაჯგუფება ფიგურირებს: არსებული მონაცემებით საგარეო დაზვერვის სამსახურს თითქმის 1 წელი ჰქონდა წვდომა აშშ-ის დემოკრატიული პარტიის კომუნიკაციის საშუალებებზე, ელექტრონულ ფოსტასა და ჩატის კონტენტზე. [iv]

არასასურველ კანდიდატთა მაკომპრომეტირებელი ინფორმაციის ან მათ საზიანოდ დეზინფორმაციის გავრცელება დაზვერვის წყაროების ან კონტროლირებადი მედიის საშუალებით სათავეს ჯერ კიდევ ცივი ომის დროიდან იღებს. უკანასკნელი წლების მოვლენებმა კი ცხადყო, რომ კიბერსივრცე რუსეთის მიერ ხშირად არის გამოყენებული მოწინააღმდეგე ქვეყნების მთავრობების ან ინსტიტუტების დელეგიტიმიზაციის მიზნით და გადაიქცა ძირგამომთხრელი საქმიანობის ასპარეზად: არჩევნებში ჩარევის მიზნით კიბეროპერაციების გამოყენების პრეცედენტი რუსეთმა ჯერ კიდევ უკრაინის კონფლიქტისას შექმნა, როდესაც 2014 წელს უკრაინის საარჩევნო ინფრასტრუქტურაზე განახორციელა მასირებული შეტევა.

პრეზიდენტ იანუკოვიჩის გაქცევის შემდგომ უკრაინაში ჩატარდა საპრეზიდენტო არჩევნები. არჩევნებადე 4 დღით ადრე პრორუსულმა დაგჯუფებამ „კიბერბერკუტმა“ მოახერხა ცენტრალური საარჩევნო კომისიის პროგრამის სისტემური ფაილების წაშლა. კომისიამ შეძლო სარეზერვო ასლებიდან მასალების აღდგენა, თუმცა ინციდენტმა ოცსაათიანი შეფერხება გამოიწვია და დაგვიანდა არჩევნების შედეგების გამოცხადება. **ინფრასტრუქტურის ექსპლოატაციის**[4] შედეგად კიბერბერკუტმა არჩევნებამდე ოთხი თვით ადრე მოიპოვა წვდომა საარჩევნო კომისიის ადმინისტრაციულ მონაცემებსა და შიდა ელექტრონულ ფოსტაზე. სარჩევნო კომისიის კომპრომეტირებული საიტი აჩვენებდა **ფაბრიკაციას,** თითქოსდა არჩევნებში გაიმარჯვა ულტრამემარჯვენე კანდიდატმა. მიუხედავად ოფიციალური უარყოფისა, რუსული მედია ავრცელებდა აღნიშნულ ინფორმაციას. უკრაინის კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფის მონაცემებით, ინციდენტის გამომწვევ მალვეარს[5] ადრე რუსული სამხედრო დაზვერვა იყენებდა.

---

[4] კიბერშეტევის ან კიბერშპიონაჟის შედეგად საინფორმაციო არხებიდან სადაზვერვო ინფორამციის მოხსნის და შეგროვების აქტი. განმარტებულია Office of the Director of National Intelligence, Cyber Threat Intelligence Integration Center. Cyber Threats to Elections – a Lexicon.

[5] **მავნე პროგრამული უზრუნველყოფა** - Malware, მალვეარი; კომპიუტერული პროგრამა, რომელიც გამოიყენება ინფორმაციულ სისტემებზე არასანქცირებული შეღწევის, სენსიტიური ინფორმაციის

2016 წელს, აშშ-ის საპრეზიდენტო საარჩევნო მარათონისას რუსული კიბერაქტორების მიერ განხორციელდა მრავალმხრივი კამპანია დემოკრატიული პროცესებისადმი ხალხის რწმენის შესარყევად, საპრეზიდენტო კანდიდატის საქმიანი რეპუტაციის შესალახად და საარჩევნო პოტენციალის შესამცირებლად. ამ კამპანიაში გამოყენებულ იქნა როგორც საინფორმაციო ოპერაციები (პოლიტიკური პროცესის დელეგიტიმიზაციის მიზნით სოციალური მედიის ყალბი ანგარიშების მეშვეობით პოლარიზაციის გაზრდის 2014 წლიდან დაწყებული კამპანია), ისე, კიბერთავდასხმები, რომელთა საშუალებითაც ორმა რუსულმა აქტორმა, სამხედრო დაზვერვის მთავარმა სამმართველომ და საგარეო დაზვერვის სამსახურმაარაავტორიზებული წვდომა მოპიოვა დემკრატიული პარტიის სერვერებსა და ელექტრონულ ფოსტაზე. მოპოვებული ინფორმაცია “Guccifer 2.0”-ის სახელით გამოქვეყნდა პლატფორმებზე DCLeaks.com და WikiLeaks, IRA-ს[6] მიერ მოხდა ამერიკის მოქალაქეების ათასობით ყალბი ანგარიშის შექმნა, რომელთა დისკუსიებმაც მოახდინეს გარემოს უკიდურესი პოლარიზაცია, ამავდროულად, ამავე ორგანზაციამ გაავრცელა ყალბი კონტენტი, რომელიც თითქოსდა მრჩეველი კანდიდატ კლინტონს ბენღაზის ინციდენტისას ამერიკელების მსხვერპლზე აკისრებდა პასუხისმგებლობას. ცხადია, არ არსებობს პირდაპირი მტკიცებულებები საარჩევნო ხმებით მანიპულირებისა პრეზიდენტ ტრამპის სასარგებლოდ, თუმცა რუსულმა ჩარევამ გააღრმავა სოციალურ-პოლიტიკური უთანხმოება, მოახდინა საარჩევნო გარემოს პოლარიზაცია და განაპირობა მოსახლეობის რწმენის შერყევა არჩევნების შედეგებისადმი. DNC hack განიხილება, როგორც რუსეთის ხელისუფლების უმაღლეს დონეზე სანქცირებული ჩარევა აშშ-ის არჩევნებში, დემოკრატიულ პროცესების რწმენის შესუსტების და კონკრეტული კანდიდატის კომპრომეტაციის მიზნით. [v]

2017 წლის 5 მაისს, საფრანგეთის პრეზიდენტის არჩევნებამდე ორი დღით ადრე მიზანმიმართული ფიშინგის გზით მოპოვებულ იქნა მაკრონის საარჩევნო გუნდის კუთვნილი რამდენიმე გიგაბაიტი ინფორმაცია, რომლის ავთენტურობა ან ცალსახა სიყალბე რთული დასადგენია. მასალა სპეციალურად შექმნილ პლატფორმაზე გამოქვეყნდა უშუალოდ არჩევნების წინ, რამაც გაართულა მაკრონის შტაბის მხრიდან რეაგირება. ამავდროულად, სოციალურ ქსელში გასავრცელებლად და ნეგატიური განწყობების გასამძაფრებლად ბოტების მიერ წარმოებულმა კამპანიამ დიდი როლია შეასრულა. ჩარევის მიზანი რუსეთისამდი პოზიტიურად განწყობილი კანდიდატის მხარდაჭერა იყო, რომელიც ამ შემთხვევაში უშედეგოდ დასრულდა.

გერმანიის ბუნდესტაგის არჩევნების წინ, 2015 წელს განხორციელდა ელექტრონული ფოსტის კონტენტის მოპარვა ბუნდესტაგის სერვერებიდან და კანცლერ მერკელის ქრისტიან-დემოკრატიული პარტიის საინფორმაციო სისტემებიდან, თუმცა ამ ინფორმაციის გამოქვეყნება არ მომხდარა. ამავდროულად, ნეგატიური განწყობების გაღვივების მიზნით, გერმანულენოვანმა რუსულმა გამოცემებმა სოციალურ ქსელში ბოტებისა და ტროლების ჩართულობით გააჩაღეს ანტისაიმიგრაციო აქცენტებზე დაფუძნებული კამპანია, რომელიც მიზნად ისახავდა პოლიტიკურ პოლარიზაციას, და საარჩევნო პროცესისადმი ნდობის

შეგროვების, მოპარვის, განადგურების, შეცვლის, კრიპტაციის ან კომპიუტერზე უკანონო წვდომის მოსაპოვებლად.

[6] Internet Research Agency იგივე Trolls from Olgino. სანკტ-პეტერბურგში ბაზირებული რუსული კომპანია, რომელიც ჩართულია გავლენის ოპერაციებში რუსული ბიზნესისა და პოლიტიკური ინტერესების სასარგებლოდ. მისი რამდენიმე წევრი ოფიციალურად მხილებულია აშშ-ის 2016 წლის საპრეზიდენტო არჩევნებში ცარევის მცდელობებში.

შემცირებას და არჩევნების შედეგების დელეგიტიმიზაციას. პარალელურად, ხდებოდა ყალბი **კონტენტის** გავრცელება, რომელიც ემყარებოდა გერმანელი გოგონას არაბი მიგრანტის მიერ გაუპატიურების გამოგონილ ამბავს. გერმანული სპეცსამსახურების აზრით, რუსეთის მხრიდან არჩევნებში ჩარევა, შესაძლოა, არც იყო რომელიმე კანდიდატის ან პარტიის მხარდასაჭერად განხორციელებული, არამედ, რაც უფრო სარწმუნოა, მიზნად ისახავდა დემოკრატიული პროცესების და ზოგადად არჩევნების ინსტიტუტის დისკრედიტაციას. ამგვარი ჩარევის მთავარი მიზანი დემოკრატიული ინსტიტუტების გრძელვადიანი დისკრედიტაცია და ნებისმიერი მომავალი მმართველობისადმი მხარდაჭერის შესუსტებაა, რაც რუსული გეოპოლიტიკური ინტერესების რეალიზაციას უწყობს ხელს. აღნიშნულის დასტურად ის ფაქტიც გამოდგება, რომ თუმცა მერკელის პარტიამ არჩევნებში გაიმარჯვა, მაგრამ მან მიიღო საკუთარ ისტორიაში ყველაზე ნაკლები ხმა.

ამრიგად, ზემოაღნიშნული საარჩევნო ინციდენტების ანალიზი ცხადყოფს, რომ მოქმედებს სქემა, რომლის მიხედვითაც კიბერთავდასხმის შედეგად ხდება საინფორმაციო სისტემების პენეტრაცია, არსებული სენსიტიურ ინფორმაციაზე წვდომის მოპოვება და შემდგომ პოლიტიკური ფიგურების ან ინსტიტუტების დისკრედიტაციის მიზნით მისი კონტროლირებადი გავრცელება. ნეგატიური განწყობების გაღრმავების მიზნით, ბოტებისა და ტროლების მიერ ყალბი პროფაილებისა ან ბლოგების გამოყენებით გავრცელებული ინფორმაციის კომენტირებით ხდება რუსული ნარატივის დამკვიდრება, ცრუ ინფორმაციის გავრცელება და სასურველი საზოგადოებრივი აზრის ჩამოყალიბება.[vi]

თუკი რუსეთის მხრიდან საქართველოს შიდაპოლიტიკური პროცესებით დაინტერესების ხარისხს, ქართული სახელმწიფო თუ კერძო სექტორის ქსელების მოწყვლადობას და რუსული დესტრუქციული კიბერაქტორების მიერ პენეტრაციის მასშტაბებს გავითვალისწინებთ, ცხადია, ქართულ საარჩევნო კამპანიაში რუსული ჩარევის ალბათობა ცალსახად ყურადსაღებია. ცნობილი ფაქტია, რომ კრემლთან დაკავშირებულ აქტორებს, ხანგრძლივი დროის განმავლობაში ჰქონდა არასანქცირებული წვდომა ქართულ სახელმწიფო, საკომუნიკაციო თუ ბიზნეს-ქსელებთან, რის შედეგადაც, სავარაუდოდ დიდი მოცულობა სენსიტიური ინფორმაციისა წლების მანძილზე ხვდებოდა რუსული სპეცსამსახურების ხელში[7vii]. ჩვენს არჩევნებში, გარდა არალეგალურად მოპოვებული მაკომპრომეტირებელი მასალებისა, გასავრცელებელი კონტენტის კიდევ ერთი წყაროდ იქცევა ხოლმე ღია რესურსებსა და სოციალურ ქსელებში არსებული ამა თუ იმ კანდიდატის ან მათი მხარდამჭერი პოლიტიკური ძალების მოსაზრებები თუ გამონათქვამები სენსიტიურ თემებსა და პროცესებზე.

შესაბამისად, უკიდურესად მნიშვნელოვანია მოხდეს არჩევნებში რუსული ჩარევის მაგალითების განხილვის შედეგად შეტევების ხშირად გამოყენებული ტექნიკების, კიბერსაფრთხეების, მეთოდიკების კლასიფიკაცია და რისკების მიტიგაციისათვის რეკომენდაციების შემუშავება.

7

დღემდე არსებული მონაცემებით, რუსეთი არჩევნებში ჩასარევად ყველაზე ხშირად კიბერთავდავსხმებისა და სანფორმაციო ოპერაციების შემდეგ მეთოდებს იყენებს:

სოციალური ინჟინერია - ინტერნეტ-თაღლითობის ერთ-ერთი ტექნიკა, რომელიც იწვევს მანიპულირების გზით მომხმარებლის მიერ გაუცნობიერებლად კონფიდენციალური მონაცემების ჰაკერისთვის გამჟღავნებას, მის ინფიცირებულ ლინკზე გადასვლას ან/და კომპიუტერში მავნე პროგრამული უზრუნველყოფის ინსტალაციას. ეს მეთოდი წარმატებით გამოიყენება იმ მომხმარებლის მიმართ, ვინც ბოლომდე ვერ აცნობიერებს პერსონალური მონაცემების მნიშვნელობას ან მისი დაცვის ხერხებს.

ფიშინგი - კიბერკრიმინალის გავრცელებული ფორმა, რომლის მიზანია მსხვერპლს მოტყუების გზით მოპაროს სენსიტიური ინფორმაცია ან/და მოახდინოს კომპიუტერის კომპრომეტაცია. გამოიყენება მეილი, რომელიც წარმოჩენილია როგორც სანდო წყაროსგან მიღებული შეტყობინება, როგორიცაა ბანკი ან ნებისმიერი სხვა ორგანიზაცია თუ პირი ვისთანაც მსხვერპლს შესაძლოა ქონდეს ურთიერთობა. მეილი შენიღბულია როგორც სასწრაფო შეტყობინება, რომელშიც დამატებითი ინფორმაციისთვის მოთავსებულია ვებ-ბმულები ან მიმაგრებული დოკუმენტები. ფიშინგ მეილში მოთავსებულ ბმულზე გადასვლის, ან ფაილის გახსნის შედეგად შესაძლებელია მოხდეს მსხვერპლის კომპიუტერში შეღწევა ან მისგან დამატებით სენსიტიური ინფორმაციის მოთხოვნა (პაროლი, მომხმარებლის სახელი, ბარათის ინფორმაცია და სხვა). ფიშინგ მეილები იგზავნება მასიურად, მაქსიმალურად მეტ ადრესატთან, რაც მათი წარმატების ალბათობას რეალურს ხდის.

ფიშინგის განსაკუთრებულ ფორმას წარმოადგენს ე.წ. **Spear-Phishing,** რომელიც განკუთვნილია მომხმარებლის ვიწრო და სპეციფიური წრისათვის (მმართველობა, გარკვეული ცოდნის, ინფორმაციის მატარებელი ჯგუფი). საჭიროებს კარგად მომზადებულ კონტექსტს ნდობის მოსაპოვებლად. გარდა ფინანსურად მოტივირებული კიბერკრიმინალისა, ფიშინგის სხვადასხვა ფორმა აქტიურად გამოიყენება სახელმწიფოთაშორის დესტრუქციულ კიბეროპერაციებში მოწინააღმდეგის ქსელის კომპრომეტაციისათვის.

SQL-injection - შეტევის ტექნიკა, რომელიც პროგრამულ უზრუნველყოფაში არსებული სისუსტეების გამოყენებით გზით უზრუნველყოფს კოდის „ინექციას“ და მონაცემთა ბაზაზე არასანქცირებულ წვდომას ან მანიპულირებას (მავნე კოდის დაგზავნა, მონაცემთა წაშლა, საწყისი გვერდის შეცვლა).

პორტების სკანირება - თავდამსხმელების მიერ ხშირად გამოყენებული ტექნიკა სამიზნე სისტემების სისუსტეების გამოსავლენად, ძირითადად გამოიყენება არასათანადოდ დაცულ სერვერებსა და ქსელებზე არაავტორიზებული წვდომის მოსაპოვებლად.

MITM (Man in the Middle) - შეტევის სახე, როდესაც თავდამსხმელი არაავტორიზებულად ერთვება ორი ან რამდენიმე მხარის კომუნიკაციაში და მოიპოვებს წვდომას მათ შორის მიმოცვლილ ინფორმაციაზე.

DDoS (A distributed-denial-of-service) - კომპრომეტირებული კომპიუტერების მეშვეობით გენერირებული დიდი რაოდენობით მონაცემთა მოთხოვნის ნაკადის მიმართვა სერვერისკენ, რომელიც მიმართულია ქსელის გამტარობის და ოპერატიული მეხსიერების

გადასავსებად, რასაც შესაძლოა შედეგად მოჰყვეს სამიზნე სისტემის მწყობრიდან გამოყვანა და ბიზნეს-პროცესის მოშლა.

ინსაიდერული შეტევა - შეტევა, რომლის დროსაც ყოფილი ან მოქმედი თანამშრომელი, ვენდორი, კონტრაქტორი ან სხვა ავტორიზებული პირი უფლებამოსილებას იყენებს მავნე ზემოქმედებისათვის.

საინფორმაციო ოპერაციები - პროპაგანდა, დეზინფორმაცია და სხვა საშუალებები, რომელთა გამოყენებაც ხდება ამომრჩევლის აზრის მანიპულირებისათვის, კიბერსივრცის ამ მიზნით გამოყენებამ წარმოუდგენლად გააფართოვა ამგვარი ოპერაციების შესაძლებლობები როგორც მასშტაბის, ასევე ეფექტის თვალსაზრისითაც. არჩევნების კონტექსტში ამგვარი ოპერაციები გამოიყენება არჩევნების შედეგებისადმი უნდობლობის დასათესად, ამა თუ იმ პოლიტიკური ძალის დისკრედიტაციისათვის, ასევე დემოკრატიული წყობის და მთავრობების დელეგიტიმიზაციისათვის.

ინფორმაციის კონტროლირებადი გაჟონვა - თავამსხმელები, ახდენენ რა სამიზნე ქსელის პენეტრაციას, განათავსებენ მოპარულ სენსიტიურ ინფორმაციას სოციალურ ქსელში ან სპეციალურ პლატფორმაზე. საარჩევნო სუბიექტების ბიუჯეტის, სპონსორების, საარჩევნო სისტემის სისუსტეებისა და სენსიტიური პროცესების შესახებ ინფორმაციის ან ფაბრიკაციის გაჟონვა არჩევნების შედეგებისადმი უნდობლობას იწვევს.

ცრუ ან შეცდომაში შემყვანი ინფორმაციის გავრცელება - სოციალური ქსელის თავდამსხმელის მიერ მიტაცებული ოფიციალური ანგარიშიდან ან სოციალური მედიისა და დაფინანსებული რეკლამის მეშვეობით მცდარი ან შეცდომაში შემყვანი ინფრმაციის გავრცელება არჩევნების დროის, ადგილის, შედეგების შესახებ, კანდიდატის, პოლიტიკური ჯგუფის დისკრედიტაცია ან არჩევნების შედეგებით მანიპულირება,

ანტაგონისტური განწყობების გაღვივება - ხშირად პოლარიზაციის გასამძაფრებლად გამოიყენება არსებული უთანხმოებები, სამეზობლო დავები, ეთნიკური, რელიგიური ან სხვა სახის უმცირესობების პრობლემატიკა. ადგილი აქვს ტრადიციული, ხშირად ყოფითი სამეზობლო დავის სახელმწიფოთაშორისი ურთიერთობების კონტექსტში გადატანას, ან ერთაშორისი ურთიერთობის უკიდურესად ნეგატიურ ჭრილში წარმოჩენას, ტრადიციულად სენსიტიურ საკითხებზე აქცენტირებას, ნეგატიურ პრიზმაში ნაჩვენები პრობლემატიკის ტირაჟირებას სოციალური ქსელებით და შემდგომ ამაზე დისკუსიის გამართვას ტროლების, „სასარგებლო იდიოტების“, თუ სხვა საშუალებების ჩართულობით, რაც, საბოლოო ჯამში ერთაშორისი ან სახელმწიფოთაშორისი ურთიერთობების რანგში აიყვანება.

მიუხედავად არჩევნების ტიპისა, კანონმდებლობისა თუ სისტემების მრავალფეროვნებისა, არსებობს საუკეთესო პრაქტიკა, რომელიც უზრუნველყოფს პროცესის კიბერუსაფრთხოებას, არჩევნების შედეგების მთლიანობის და სანდოობის დაცულობას, როგორც ტექნიკური ასევე შინაარსობრივი თვალსაზრისით. განვიხილოთ ზოგიერთი მათგანი და მათ დასამკვიდრებლად განსახორციელებელი ღონისძიებები[8]:

[8] ტექნიკური რჩევების ნაწილის საფუძვლად აღებულია Defending Digital Democracy Project. Belfer Center for Science and International Affairs. Harvard Kennedy School. The State and Local Election

1. კიბერუსაფრთხოების პროაქტიული კულტურის დანერგვა

წარმატებული კიბერშეტევების დიდი უმრავლესობა ადამიანურ ფაქტორთან - მომხმარებლის შეცდომასთან არის დაკავშირებული, ამიტომ კიბერუსაფრთხოების კულტურის დანერგვა, „ზემოდან-ქვემოთ“ პოლიტიკა რისკების შემცირების უმნიშვნელოვანესი ინსტრუმენტია. კიბერუსაფრთხოების ფესვგადგმული კულტურა, მომხმარებლის კიბერჰიგიენის გაცნობიერებული ჩვევები ასევე დიდწილად განაპირობებს თავდამსხმელის მხრიდან სისტემის სამიზნედ შერჩევის ალბათობის ხარისხს, განხორციელებული თავდასხმის წარმატებულობის მინიმიზაციას ან ფსიქოლოგიური ზემოქმედების მიზნით წარმატების აღქმის შექმნის შესაძლებლობას.

- ტოპ-მენეჯმენტის ჩართულობა კიბერუსაფრთხოების საკითხებში;
- ინციდენტების მართვის დეტალური გეგმის შემუშავება/იმპლემენტაცია;
- არჩევნების ადმინისტრირებაში მონაწილე პირთა სანდოობის შემოწმება;
- გარე რესურსების გამოყენება უწყებათაშორისი და საჯარო-კერძო თანამშრომლობის ფარგლებში.

2. სისტემის კიბერუსაფრთხოებისადმი კომპლექსური მიდგომა

საარჩევნო სისტემის ნებისმიერი სეგმენტის კომპრომეტაციამ შესაძლოა გამოიწვიოს მთლიანად სისტემის პენეტრაცია. თავდამსხმელები ეძებენ სუსტ წერტილებს, რომელთა მეშვეობითაც ხდება სისტემაში შეღწევა. ინტერნეტთან კავშირის არმქონე სისტემის კომპრომეტაციაც კი შესაძლებელია გარე მეხსიერების და სხვა მობილური მოწყობილობების საშუალებით.

- პროცესთან შემხებლობაში მქონე ყველა კომპიუტერის და მოწყობილობის დაცვა, მიუხედავად მათი კუთვნილებისა;
- კიბერუსაფრთხოების მენეჯმენტის ოპტიმიზაცია და ცენტრალიზება.

3. ძლიერი პასვორდისა და ორმაგი ავთენთიფიკაციის პოლიტიკის დანერგვა

თავდამსხმელები სისტემის კომპრომეტირებისათვის ხშირად იყენებენ მომხმარებლის საავტორიზაციო მონაცემებს. რადგან პასვორდის გატეხვის ძირითადი მეთოდი ამ პასვორდის კომპონენტთა კომბინაციათა შესაძლო რიცხვზეა დამოკიდებული, მიზანშეწონილია 8 ან მეტსიმბოლოიანი, სათანადო წესით შედგენილი პასვორდის სავალდებულო გამოყენება. ასევე, აუცილებელია ორფაქტორიანი ავტორიზაციის პოლიტიკის დანერგვა.

4. წვდომის კონტროლი და მენეჯმენტი

Cybersecurity Playbook. 2018. ზოგიერთი ღონისძიება საქართველოს საარჩევნო სისტემაში გატარებულია.

ნებისმიერი ავტორიზებული მომხმარებელი წარმოადგენს თავდამსხმელთა სამიზნეს და ხშირად, ერთი მომხმარებლის კომპრომეტაცია საკმარისია ქსელზე სრული წვდომის მოსაპოვებლად. შესაბამისად, რაც უფრო მეტ ადამიანს აქვს წვდომა სისტემასთან და რაც უფრო ფართოა მათი წვდომის არეალი, მით მეტია სისტემის კომპრომეტაციის საფრთხე.

- სისტემაზე ავტორიზებული წვდომის მქონე პირთა რაოდენობის შეზღუდვა;
- ავტორიზებულ პირთათვის წვდომის მინიჭება მხოლოდ აუცილებელ მონაცემებზე, „მინიმალური უფლებების“ პრინციპით;
- მომხმარებლის წვდომის ავტომატური გაუქმება პოზიციის, კომპეტენციის სფეროს შეცვლისას ან სამსახურიდან დათხოვნისას.

5. მგრძნობიარე მონაცემების და სისტემების გამიჯვნა

სისტემის ნებისმიერი სეგმენტი მნიშვნელოვანია, თუმცა აუცილებელია პრიორიტეტების განსაზღვრა მონაცემთა სენსიტიურობის თვალსაზრისით, რადგან დაცვის დამატებითი ღონისძიებები მოითხოვს დანახარჯებს და საოპერაციო პროცედურებს.

- სენსიტიური მონაცემების შემცველი მოწყობილობების კონფიგურირება მხოლოდ კონკრეტული ქმედების განხორციელების შესაძლებლობით;
- მობილური მოწყობილობების გამოყენების სისტემური აკრძალვა.

6. მონიტორინგის, ლოგირების და სარეზერვო ასლების სისტემის შექმნა

მონიტორინგი, ლოგების ჟურნალი და სარეზერვო ასლების სისტემა შესაძლებლობას გვაძლევს მოვახდინოთ შეტევის დეტექცია და ინციდენტის შემდგომ სისტემის აღდგენა.

- მონაცემთა ბაზების ნებისმიერი ცვლილების ლოგირება და მონიტორინგი ადამიანური რესურსით თუ ანომალიის აღმომჩენი პროგრამული უზრუნველყოფით;
- სარეზერვო ასლების რეგულარული შექმნის ავტომატური პროცესის იმპლემენტაცია. ასლი შექმნის მომენტიდან უნდა იყოს Read only და მისგან მონაცემთა სრული აღდგენის შესაძლებლობის ტესტირება უნდა ხდებოდეს რეგულარულად.

7. ვენდორის/კონტრაქტორის კიბერუსაფრთხოების ხარისხის გათვალისწინება

საარჩევნო პროცესის პროგრამული უზრუნველყოფის, საოპერაციო სისტემის, სხვადასხვა სერვისის მომწოდებლის ან ავტორიზებული წვდომის მქონე კონტრაქტორის არასათანადო დაცულობა რეალური ინსაიდერული საფრთხეა სისტემისათვის, რადგან წარმოადგენს მონაცემთა განადგურების, შეცვლის ან გაჟონვის ერთ ერთ ყურადსაღებ მიმართულებას. რისკის შემცველია **მტრული სახელმწიფოს წარმოებული პროგრამებისა და აპლიკაციების გამოყენება**.

8. კიბერჰიგიენის კულტურის დანერგვა სარჩევნო პროცესის მონაწილე ყველა რგოლში

კიბეროპერაციების დიდი უმრავლესობა, მიუხედავად იმისა, რომ ისინი მტრული სახელმწიფოს სტრატეგიული ამოცანის - არჩევნებზე ზეგავლენის მოხდენის განხორციელებას ემსახურებიან **ადამიანური ფაქტორით, მომხმარებლის შეცდომითაა განპირობებული.** ფიშინგის, სოციალური ინჟინერიის სხვა შეტევების გამანადგურებელი შედეგების თავიდან აცილება მომხმარებლის კიბერჰიგიენის წესების დაცვითაა შესაძლებელი. **კიბერჰიგიენა** არის საუკეთესო პრაქტიკა და აქტივობები კიბერუსაფრთხოების ასამაღლებლად, რომელიც **ემყარება მომხმარებლის გაცნობიერებულ ჩვევებს.**

9. **საერთაშორისო, უწყებათაშორისი და კერძო-საჯარო თანამშრომლობა**

ინფორმაციის გაზირების, კიბერსავარჯიშოების, დეზინფორმაციასთან და რუსულ პროპაგანდასთან ბრძოლის მიმართულებებზე.

---

[i] Sebastian Bay, Guna Šnore, Protecting Elections: a strategic communications approach. NATO Strategic Communications Centre of Excellence, 2019

[ii] Defence Intelligence Agency. Russia Military Power - Building a Military to Support Great Power Aspirations. Report, 2017. ხელმისაწვდომია www.dia.mil/Military-Power-Publications

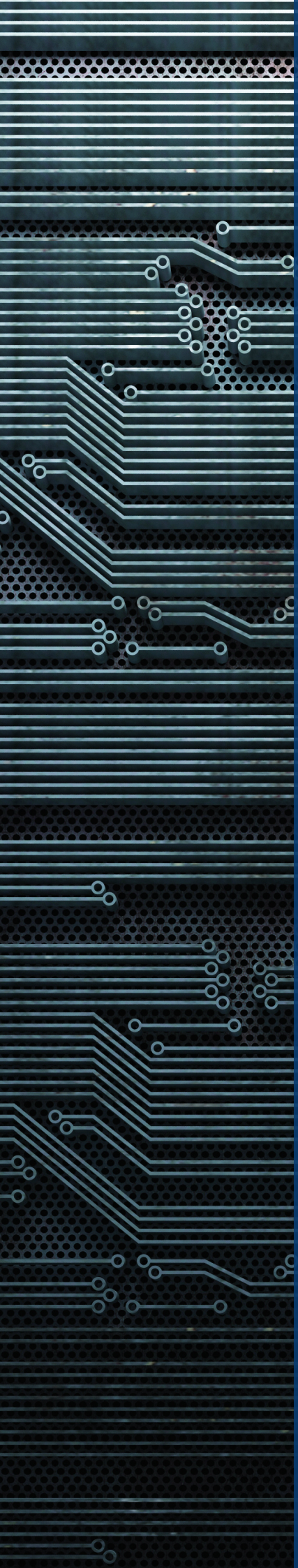
[iii] Laura Galante, Shaun Eee. Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents. Atlantic Councis Issue Brief. September, 2018

iv Intelligence Community Assesment. Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution. ICA 2017-01D, 6 January 2017

v Dr Andrew Foxall. Putin's Cyberwar: Russia's Statecraft in the Fifth Domain. Russia Studies Centre Policy Paper No. 9 (2016). The Henry Jackson Society May 2016

[vi] ა.გოცირიძე. კიბერსაფრთხეები და მათთან ბრძოლის სტრატეგიული მიმართულებები საქართველოს პერსპექტივიდან. თ.ხიდაშელი "ჰიბრიდული ომების ანატომია"-ში. გვ. 365-395. გამომცემლობა პალიტრა L.

[vii] Fire eye special report, 2014. APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS?. ხელმისაწვდომია https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf



CRC GCSD