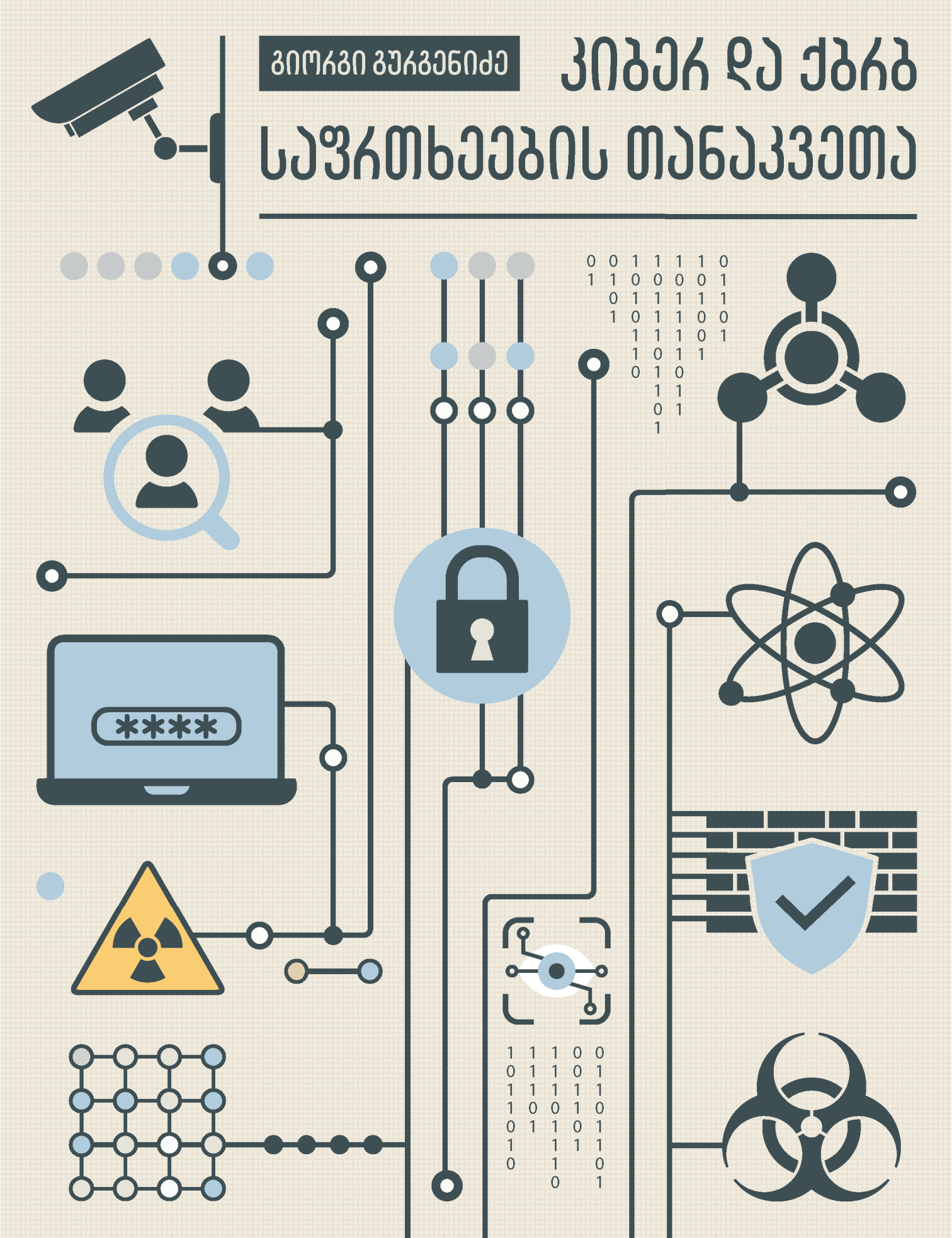
გიორგი გურგენიძე

კიბერ და ქბრბ საფრთხეების თანაკვეთა



ქბრბ და კიბერ საფრთხეები თანაკვეთა

ავტორი: **გიორგი გურგენიძე**

თბილისი

2024

პუბლიკაციის შესახებ

წინამდებარე პუბლიკაცია შეიქმნა აშშ-ის სახელმწიფო დეპარტამენტის მხარდაჭერით. დოკუმენტში გამოთქმული შეხედულებები და მოსაზრებები ეკუთვნის ავტორს და არ ასახავს ან წარმოადგენს სტრატეგიისა და განვითარების ცენტრის (CSD) ან შეერთებული შტატების სახელმწიფო დეპარტამენტის შეხედულებებსა და მოსაზრებებს.

შინაარსი

შესავალი

საერთაშორისო უსაფრთხოებისთვის მნიშვნელოვანი გამოწვევაა ქბრბ (ქიმიური, ბიოლოგიური, რადიაციული, ბირთვული) და კიბერსაფრთხეების ურთიერთკავშირი. ეს თანაკვეთა განსაკუთრებით თვალსაჩინოა რუსეთის აგრესიის კონტექსტში უკრაინის მიმართ. რუსეთის შესაძლებლობები როგორც ქბრბ, ასევე კიბერ მიმართულებით მნიშვნელოვან ზიანს აყენებს უკრაინის კრიტიკულ ინფრასტრუქტურასა და მოსახლეობის დიდ ნაწილს.

წინამდებარე კვლევაში განხილულია ქბრბ და კიბერ შესაძლებლობებს გამოყენების მნიშვნელობა და მათგან გამოწვეული ზიანი. არსებული ლიტერატურის, რეალურად მომხდარი შემთხვევების, სტრატეგიული მნიშვნელობის მოვლენების მიმოხილვის შედეგად, მოცემულია ის უსაფრთხოების პოტენციური საშუალებები და მიდგომები, რომელთა მეშვეობითაც შესაძლებელია აღნიშნული საფრთხეების განეიტრალება და შესაბამისი რისკების შემცირება.

მეთოდოლოგია

მონაცემთა შეგროვება

წინამდებარე კვლევაში გამოყენებულია ხარისხობრივი კვლევის მეთოდი, რომელიც გულისხმობს არსებული ლიტერატურის მიმოხილვასა და რეალური შემთხვევების ანალიზს. მონაცემები შეგროვდა აკადემიური ჟურნალებიდან, სახელმწიფო ორგანოებისა და სამართალდამცავი სტრუქტურების ანგარიშებიდან, კიბერუსაფრთხოებაზე მომუშავე ორგანიზაციების კვლევითი ანგარიშებიდან, საიწმუნო და მაღალი რეპუტაციის მქონე საინფორმაციო წყაროებიდან, საერთაშორისო ორგანიზაციებისა და კიბერუსაფრთხოებაზე მომუშავე ე.წ. Think Tank-ების ნამუშევრებიდან.

აღნიშნული მეთოდი უზრუნველყოფს ერთის მხრივ საკითხების განხილვას სხვადასხვა პერსპექტივიდან და მეორეს მხრივ უახლეს ინფორმაციაზე წვდომას საკითხის აქტუალურობიდან და თანამედროვეობიდან გამომდინარე. რეალური მაგალითები შერჩეულია მათი რელევანტურობის მიხედვით, კვლევის მიზნების შესაბამისად, რათა თვალსაჩინო გახდეს ძირითადი ასპექტები.

განსაკუთრებული აქცენტი კეთდება რუსეთის შესაძლებლობებზე და მის სტრატეგიაზე უკრაინაში მიმდინარე ომში.

საკითხის ანალიზი ფოკუსირებულია საკვანძო თემებისა და მახასიათებლების იდენტიფიცირებაზე ქბრბ და კიბერსაფრთხეების თანაკვეთის ჭრილში. ინფორმაცია კატეგორიზებულია **საფრთხის ტიპის, კიბერ-შეტევის მეთოდის** და კრიტიკულ ქბრბ **ინფრასტრუქტურაზე მისი გავლენის** (ზიანის) მიხედვით.

შეზღუდვები

წინამდებარე კვლევის შეზღუდვას წარმოადგენს, ერთის მხრივ, კიბერ შეტევების სწრაფად და მუდმივად ცვალებადი ბუნება და მეორეს მხრივ, დეტალური ინფორმაციის მოძიების სირთულე სახელმწიფო სპეცსამსახურების მიერ განხორციელებული კიბერშეტევების შესახებ.

ასევე ქბრბ საფრთხეების კომპლექსურობა და სხვადასხვა ტიპის კრიტიკული ინფრასტრუქტურის ურთიერთდამოკიდებულება გამოწვევაა საკითხის დეტალურად გასაანალიზებლად.

მიუხედავად აღნიშნული შეზღუდვების და გამოწვევებისა, კვლევის მიზანია წარმოადგინოს ქბრბ და კიბერსაფრთხეების თანაკვეთა და შესაბამისი რისკების შემცირების **სტრატეგიები**, რეალურად მომხდარი შემთხვევების გათვალისწინებით.

ქბრბ და კიბერ საფრთხეების განმარტება

ქბრბ საფრთხეები ათწლეულების განმავლობაში საერთაშორისო უსაფრთხოების არქიტექტურის განუყოფელი ნაწილია და მნიშვნელოვანი ყურადღება ექცევა მის თითოეულ კომპონენტს. ქიმიური საფრთხეები მოიცავს ტოქსიკური სამრეწველო ქიმიკატების ან საბრძოლო ქიმიური აგენტების გამოყენებას. ბიოლოგიური საფრთხეები შედგება პათოგენების და ბიოტოქსინებისაგან, რომელთაც სერიოზული დაავადებების გამოწვევა და, რიგ შემთხვევებში, ეპიდემიების გამოწვევაც კი შეუძლია. რადიოლოგიური საფრთხეების შემთხვევაში ძირითადი რეაგენტებია რადიოაქტიური მატერიალები, რაც შეეხება ბირთვულს კომპონენტს - საუბარია პირდაპირ ბირთვულ იარაღზე ან ბირთვული ობიექტების მიმართ არსებულ საფრთხეებზე.

ქბრბ საფრთხეები

ქიმიური საფრთხეები შეიძლება გაჩნდეს სამრეწველო შემთხვევებისგან დაბორატორიული შეცდომის გამო, ან საომარი მოქმედებების დროს განზრახ გამოყენებისას. დადასტურებული ინფორმაციით, რუსეთს მრავალჯერ გამოუყენებია ქიმიური შეტევა, მათ შორის პოლიტიკური ოპონენტების წინააღმდეგაც.

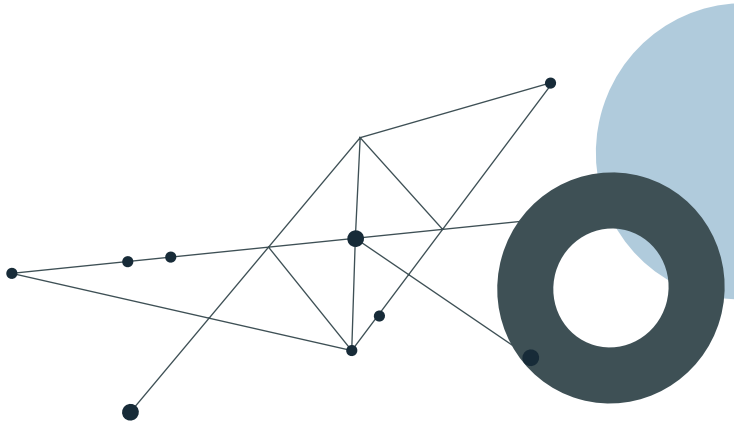
ბიოლოგიური საფრთხეები ფართომასშტაბიანი ზიანის მომტანია, ვინაიდან შეუძლია დაავადებების აფეთქებებისა და, ცალკეულ შემთხვევაში, ეპიდემიების გამოწვევაც კი.

ვარაუდობენ, რომ ბოლო ათწლეულის განმავლობაში რუსეთმა მრავალფეროვანი გახადა და დახვეწა მისი ბიოლოგიური იარაღის არსენალი. ამ ვარაუდს განაპირობებს მისი კვლევითი შესაძლებლობები/მნიშვნელოვანი კვლევითი რესურსი და ბიოიარაღის წარმოების პროგრამების ისტორია, რომელიც საფუძველს იღებს ჯერ კიდევ საბჭოთა პერიოდიდან.

რადიოლოგიურ საფრთხეებს მიეკუთვნება შესაბამისი მასალების მოხვედრა (გაბნევა, გაფრქვევა) კონტროლირებული გარემოს (დაბორატორიის) ფარგლებს გარეთ, რაც იწვევს რადიაციულ დასხივებას დაავადების სახით და ასევე გარემოს შესაბამის რადიოაქტიულ დაბინძურებას.

ბირთვული საფრთხეები დაკავშირებულია როგორც პირდაპირ ბირთვული იარაღის გამოყენებასთან, ასევე შესაბამისი ბირთვული ობიექტების დაზიანებასთან.

ზემოთ ჩამოთვლილი ქბრბ მიმართულებები, **ტექნოლოგიური პროგრესისა** და **გაციფრულების** გათვალისწინებით, სულ უფრო მეტად ხდება დამოკიდებული თანამედროვე ინფორმაციულ და საკომუნიკაციო ტექნოლოგიებზე (ICT). შესაბამისად ნებისმიერი კიბერსაფრთხე, რომელიც ეხება აღნიშნულ ტექნოლოგიებს, პოტენციურად გავრცელებადია ქბრბ მიმართულების სამართავ ტექნოლოგიურ გარემოზეც.



არსებობს კიბერსაფრთხეების მრავალი ტიპი, მათ შორის ბოლო ათწლეულის განმავლობაში განსაკუთრებით საყურადღებოა სახელმწიფო სპეცსამსახურებთან დაკავშირებული ჰაკერული დაჯგუფებების (APT groups - Advanced Persistent Threat) შეტევები კრიტიკულ ინფრასტრუქტურაზე.

ასეთი ჯგუფებისათვის ხელმისაწვდომია მნიშვნელოვანი ინტელექტუალური, ფინანსური და ტექნოლოგიური რესურსები. შესაბამისად, მათ მიერ განხორციელებული შეტევები და მომდინარე საფრთხე, პირველ რიგში უნდა განვიხილოთ ქბრბ მიმართულებით.

აღსანიშნავია, რომ გარდა ამ ჯგუფებისა, ხშირად საზიანო კიბერშეტევები მომდინარეობს კიბერკრიმინალებისგან, ჰაქტივისტებისგან და საზოგადოების/ორგანიზაციის წევრებისგან, თუმცა გასათვალისწინებელია, რომ როგორც წესი, ქბრბ მიმართულების კრიტიკული ინფრასტრუქტურა უამრავ ქვეყანაში კანონმდებლობით რეგულირდება და აუციელებელია უსაფრთხოებს მაღალი დონეზე დაცვა. რაც განაპირობებს მათ შედარებით დაცულობას და ტექნოლოგიურ გარემოში შელწევის სირთულეს. შესაბამისად, ასეთ ობიექტებზე განხორციელებული დადასტურებული და გამოძიებული შეტევების უმრავლესობა ზემოთ ნახსენებ სპეცსამსახურებთან დაკავშირებული ძლიერი ჰაკერული დაჯგუფებების (APT) მიერაა განხორციელებული.

რუსულ სპეცსამსახურებთან დაკავშირებული ძლიერი ჰაკერული დაჯგუფებები მრავალი წელია აქტიურად ოპერირებენ და რუსეთის ერთ-ერთ მნიშვნელოვან დასაყრდენს წარმოადგენენ სტრატეგიული მიზნების მისაღწევად.

ქბრბ და კიბერსაფრთხეების ურთიერთკავშირი

საერთაშორისო უსაფრთხოების კონტექსტში განსაკუთრებით საყურადღებოა ქბრბ და კიბერსაფრთხეებს შორის არსებული ურთიერთკავშირი. 2022 წელს გამოქვეყნებული NATO-ს ქბრბ თავდაცვის პოლიტიკაში (NATO, 2022. NATO's Chemical, Biological, Radiological and Nuclear (CBRN) Defence Policy.) ხაზგასმულია კიბერეცემენტის მნიშვნელობა ქბრბ საფრთხეების კონტექსტში. კერძოდ, ინტერნეტი და „დარქნეტი" (დაფარული ინტერნეტ წყაროები და გვერდები) მნიშვნელოვანი წყაროა WMD-შესაბამისი ტექნიკური ცოდნისა და ექსპერტიზის პროლიფერაციისათვის. დოკუმენტის მიხედვით, მავნე კიბერაქტორებმა შეიძლება სცადონ NATO-ს შესაძლებლობის - "თავიდან აიცილოს და ეფექტიანად უპასუხოს ქბრბ ინციდენტს" - შესუსტება. მათი სამიზნეა NATO-ს ან მისი მოკავშირეების საკომუნიკაციო-საინფორმაციო სისტემები.

კრიტიკული ინფრასტრუქტურის მიმართ განხორციელებული კიბერშეტევები მიუთითებს სამრეწველო ან სამეცნიერო ინფრასტრუქტურის განადგურებისთვის კიბერშესაძლებლობების შესაძლო გამოყენების რისკზე, ტოქსიკური სამრეწველო ქიმიკატების გავრცელების ან სხვა ქრბრ ინციდენტის გამოწვევის მიზნით.

ბოლოდროინდელმა ქიმიურმა და ბიოლოგიურმა კრიზისებმა გამოავლინა მავნე კიბერეცემენტები, მათ შორის OPCW-ის კომპიუტერულ სისტემაში უკანონო შეღწევის მცდელობები, ასევე კიბერშეტევები ჯანდაცვის სერვისების და სამედიცინო კვლევითი ორგანიზაციების წინააღმდეგ COVID-19-ის პანდემიის დროს.

საერთო ჯამში, შეგვიძლია განვსაზღვროთ ქბრბ და კიბერსაფრთხეების ურთიერთკავშირის შემდეგი მიმართულებები:

ინტერნეტი, როგორც WMD-შესაბამისი ცოდნის გავრცელების წყარო;

კიბერშეტევა ქბრბ პრევენციისა და რეაგირების მართვის საინფორმაციო სისტემებზე და ტექნოლოგიებზე;

ქბრბ დაქვემდებარებული კრიტიკული ინფრასტრუქტურის დაზიანება კიბერშეტევებით;

კიბერშეტევა ქბრბ მომუშავე ორგანიზაციებზე და თანამშრომლებზე.

კიბერშპიონაჟის ტაქტიკა

კრიტიკული ინფრასტრუქტურის ტექნოლოგიურ შემადგენელზე პირდაპირი შეტევები იწვევს მის პარალიზებასა და დაზიანებას, შესაბამისი ქბრბ ინციდენტებით, თუმცა, ხშირ შემთხვევაში, გამოიყენება შეუმჩნეველი და გრძელვადიანი კიბერშპიონაჟი. ამ შემთხვევაში, შემტევი მხარის მიზანია მგრძნობიარე ინფორმაციის მითვისება და არასანქცირებული წვდომის მოპოვება კლასიფიცირებულ მონაცემებზე ქბრბ ინფრასტრუქტურის შესახებ.

მოპოვებული სენსიტიური ინფორმაცია გამოიყენება სამომავლო დესტრუქციული კიბერშეტევებისთვის ან ვრცელდება დეზინფორმაციის სახით და მნიშვნელოვანი ინფორმაციის წყაროს წარმოადგენს ჰიბრიდული ოპერაციების განსახორციელებლად.

არსებული კვლევები

კვლევების უმრავლესობაში შეფასებულია კიბერშეტევების პოტენციალი ქბრბ ინციდენტების გამოწვევის კუთხით. მკვლევარები ძირითად აქცენტს აკეთებენ ე.წ. ICS-ის (Industrial Control Systems) ტექნოლოგიურ სისუსტეებზე. ასევე კიბერ ელემენტით გამოწვეული ბიოტერორიზმი ბოლო ათწლეულში განხორციელებული კვლევების ერთ-ერთი მნიშვნელოვანი თემაა. კიდევ ერთი განზომილებაა კიბერ-ბირთვული საფრთხეების სტრატეგიული მნიშვნელობა და მისი კვლევა.

მიუხედავად მრავალი მცდელობისა, ჯერ კიდევ არ არის სრულად გააზრებული და შეფასებული კიბერშეტევების მასშტაბურობა და შესაძლებლობები გლობალური ქბრბ ინციდენტების გამოწვევის კუთხით, ასევე მათ წინააღმდეგ არსებული და ეფექტიანი პოტენციური თავდაცვითი მექანიზმები.

ამის მიზეზია, ერთი მხრივ, სწრაფი ტექნოლოგიური პროგრესი, განსაკუთრებით ხელოვნური ინტელექტის განვითარება და გამოყენება შეტევითი ღონისძიებებისას, მეორე მხრივ კი კვანტური კომპიუტერული მეცნიერების კუთხით არსებული მიღწევები და მოლოდინები.

შესაბამისად, არსებული კვლევების ნაწილი შინაარსობრივად მოძველებულია და საჭიროებს გაანალიზებას, განახლებას, მუდმივად ცვალებადი და სწრაფად პროგრესირებადი ტექნოლოგიური რეალობის გათვალისწინებით.

რუსეთის შესაძლებლობები და განზრახვები

რუსეთმა მნიშვნელოვნად განავითარა მისი შესაძლებლობები როგორც ქბრბ, ასევე კიბერ მიმართულებით. ქბრბ კუთხით იგი ინარჩუნებს და აფართოებს ქიმიური და ბიოლოგიური იარაღის პროგრამებს, ასევე ჯერ კიდევ აქვს დიდი ბირთვული არსენალი. რაც შეეხება რუსეთის კიბერშესაძლებლობებს, ბოლო ათწლეულში განსაკუთრებულად აღსანიშნავია მის სპეცსამსახურთან დაკავშირებული რამდენიმე ძლიერი ჰაკერული დაჯგუფებების კიბეროპერაციები, მათ შორის კრიტიკული ინფრასტრუქტურის დაზიანება, კიბერშპიონაჟი და სხვ.

GRU, FSB, SVR-სთან კონკრეტული APT ჯგუფების კავშირი ხშირ შემთხვევაში დადასტურებულია და მათ მიერ განხორციელებული კიბერშეტევების ანალიზი აჩვენებს მკაფიო შეტევით შესაძლებლობებს, ხშირ შემთხვევაში უმაღლესი დონის კიბერსპეციალისტების, შეტევის მეთოდების, დაშიფრვის, ოპერაციული დაგეგმვის და ა.შ. არსებობას.

ქიმიური და ბიოლოგიური შესაძლებლობები

რუსეთს მდიდარი ისტორია აქვს ქიმიური და ბიოლოგიური იარაღის შექმნასა და გამოყენებასთან დაკავშირებით. ბოლო დროს მომხდარი შემთხვევები - 2018 წელს სერგეი და იულია სკრიპალების მკვლელობის მცდელობა და შემდგომში ალექსეი ნავალნის ნოვიჩოკით მოწამვლა ანათელი მაგალითებია იმისა, რომ რუსეთი მზადაა გამოიყენოს ქიმიური რეაგენტები და იარაღი მნიშვნელოვან ოპერაციებში. ასევე არსებობს დასაბუთებული ვარაუდი, რომ მის არსენალში შეიძლება იყოს დამატებით ახალი თაობის, ჯერ კიდევ უცნობი ქიმიური ნივთიერებები, რისი იდენტიფიცირებაც რთული იქნება შესაბამისი ინციდენტების დადგომისას. ამ ვარაუდს ამყარებს მისი კვლევითი შესაძლებლობები და ბიოიარაღის წარმოების წარმატებული პროგრამების არსებობა, რამდენიმე სერიოზული კვლევითი ინსტიტუტის ბაზაზე.

ბირთვული შესაძლებლობები

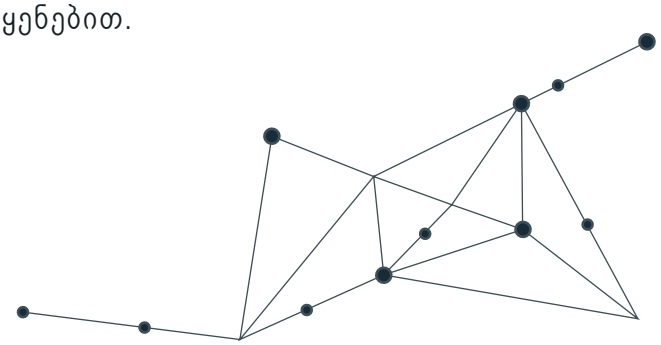
ცნობილია, რომ რუსეთს აქვს მსოფლიოში ერთ-ერთი უდიდესი ბირთვული არსენალი და შესაბამის ინვესტიციებს ახორციელებს მის განვითარებაში. რუსული სამხედრო დოქტრინა მოიცავს ბირთვული იარაღის პოტენციურ გამოყენებას კონფლიქტის დროს, რაც კიდევ ერთხელ ადასტურებს მის სტრატეგიულ მნიშვნელობას. შესაბამისად, გასაკვირი არ უნდა იყოს მისი მხრიდან კიბერშეტევები მოწინააღმდეგის ბირთვული ობიექტების წინააღმდეგ, მათ შორის ოპერაციების საბოტაჟი, სენსიტიური ინფორმაციის მოპარვა კიბერშპიონაჟით და ინფრასტრუქტურის დაზიანება. ეს ყველაფერი ცხადად აჩვენებს, რომ ბირთვულ საფრთხეს დამატებით ახალი განზომილება აქვს კიბერსაფრთხის სახით.

კიბერშესაძლებლობები

რუსული კიბერშესაძლებლობები კარგად დოკუმენტირებულია, აღწერილია და მუდმივი მონიტორინგის ქვეშაა როგორც ევროატლანტიკური, ასევე აზიის ქვეყნების შესაბამისი უსაფრთხოების სამსახურების მხრიდან. ასევე უსაფრთხოების თემაზე მომუშავე think tank-ები, ტექნოლოგიური კომპანიები და მკვლევარები განსაკუთრებულ ყურადღებას უთმობენ რუსული ჰაკერული დაჯგუფებების კიბეროპერაციებისა და მათ მიერ გამოყენებული მეთოდების შესწავლას.

სახელმწიფო სპეცსამსახურებთან დაკავშირებული APT28 (GRU), APT29 (SVR), Turla (FSB) და ა.შ. დაჯგუფებები ცნობილია კიბერშპიონაჟითა და კრიტიკული ინფრასტრუქტურის დაზიანების შესაძლებლობებით, კონკრეტული შემთხვევების შედეგების გათვალისწინებით. მათი ძირითადი სამიზნეებია: სამხედრო ობიექტები, სახელმწიფო სტრუქტურები, კვლევითი ორგანიზაციები და უმსხვილესი კერძო სამრეწველო კომპანიები.

რუსეთის კიბერსტრატეგია მოიცავს როგორც კიბერშპიონაჟს, ასევე საინფორმაციო ომის მეთოდებს, მათ შორის საზოგადოებრივ აზრზე გავლენის მოხდენასა და მოწინააღმდეგის დესტაბილიზაციას კიბერსივრცის გამოყენებით.

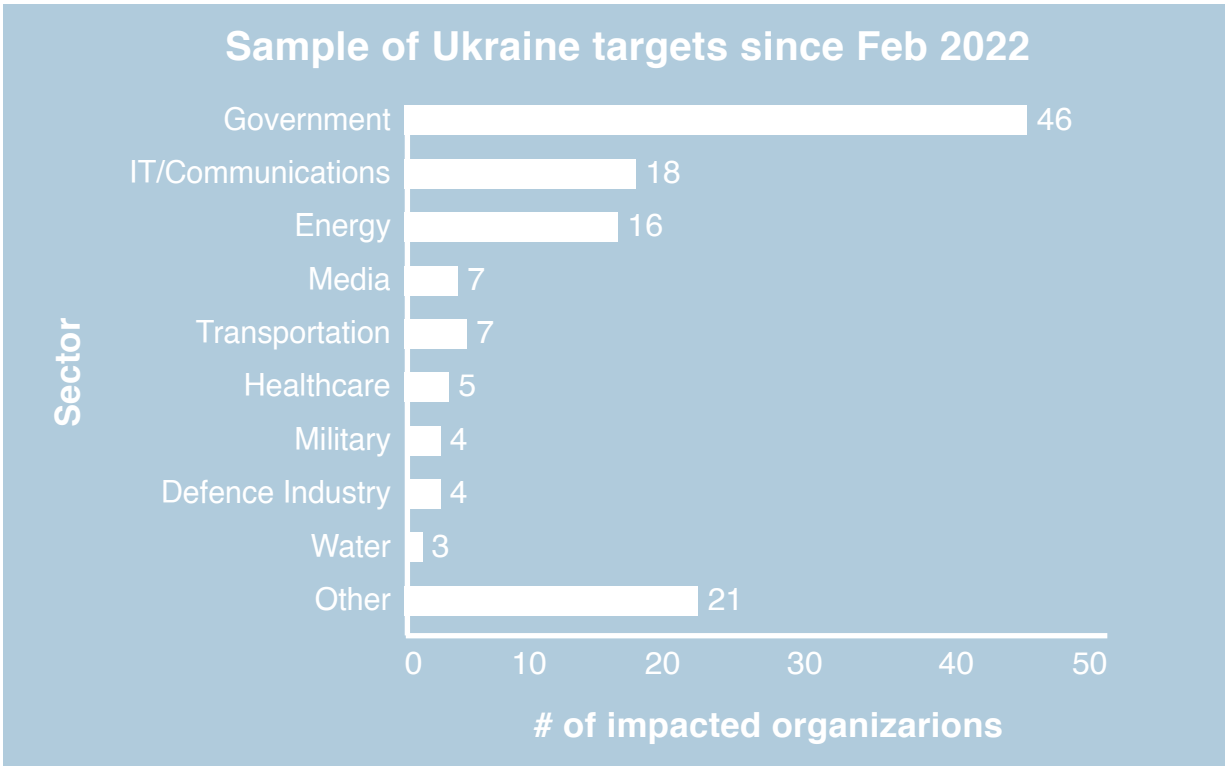


რეალური შემთხვევები/მაგალითები

2022-2024 წლების განმავლობაში რუსეთის ფართომასშტაბიან ომს უკრაინის წინააღმდეგ მნიშვნელოვანი კიბერ განზომილება აქვს. განსაკუთრებით აღსანიშნავია კიბერ შეტევები კრიტიკული ინფრასტრუქტურის მიმართ, რაც, ხშირ შემთხვევაში, იწვევს: ენერგო ობიექტების დაზიანებას და ენერგო მომარაგების შეწყვეტას ათიათასობით მოსახლისათვის, ასევე კომუნიკაციის შეზღუდვას და სრულად გათიშვას ცალკეულ რეგიონებში, სახელმწიფო და სამხედრო სამსახურების კომუნიკაციის მოშლას საინფორმაციო სისტემების დაზიანებით და ა.შ.

საომარი მოქმედებები უკრაინის წინააღმდეგ 2022–2024

გრაფიკზე მოყვანილია ამერიკული კომპანია Microsoft-ის ერთ-ერთი კვლევის (Microsoft Threat Intelligence, 2023) შედეგები. საინტერესოა რუსული კიბერშეტევების სამიზნე სექტორების განაწილება როგორც უკრაინის შიგნით, ასევე მისი პარტნიორი და მეგობარი ქვეყნების ტერიტორიებზე.



გრაფიკი 1: კიბერ შეტევების სამიზნე სექტორები უკრაინაში 2022 თებერვლის შემდგომ

გრაფიკზე მოცემულია ის სექტორები, რომელთაც შეეხო რუსული კიბერშეტევები ომის მიმდინარეობისას. საგულისხმოა, რომ პირდაპირ ნახსენებია ბირთვული ობიექტები და შესაბამისი ინფრასტრუქტურა უკრაინის პარტნიორ ქვეყნებში, ასევე თავდაცვის ინდუსტრია და ენერგოსექტორი.

გრაფიკი 2: კიბერ შეტევების სამიზნე სექტორები უკრაინის პარტნიორ ქვეყნებში 2022 თებერვლის შემდგომ

2022-2024 უკრაინის ომის განმავლობაში, რუსეთი ძირითადად უტევს უკრაინის კრიტიკული ინფრასტრუქტურის შემდეგ ობიექტებს: ელექტროგადამცემი ქსელი, საკომუნიკაციო ქსელები (მათ შორის GSM), სახელმწიფო სტრუქტურები. აღნიშული შეტევების მიზანი იყო ძირითადი სასიცოცხლო სერვისების შეფერხება, ქაოსის შექმნა და უკრაინის მთავრობის რეაგირების შეფერხება, შედეგად, მისი შესაძლებლობებისადმი უნდობლობისა და ეჭვის გაჩენა მოსახლეობაში. შესაბამისად, კიბეროპერაციები გამოიყენება სამხედრო ოპერაციების პარალელურად და მისი შემადგენელი ნაწილია, რაც განასახიერებს რუსეთის თანამედროვე სამხედრო სტრატეგიას.

ცნობილი ქბრბ ინციდენტები და კიბერშეტევები

ქვემოთ მოცემულ ცხრილში ნაჩვენებია ერთ-ერთი კვლევის (Adil Radoini and Muznah Siddiqui, 2016) შედეგები, სადაც მოყვანილია 1992 წლიდან 2016 წლის ჩათვლით მომხდარი კიბერინციდენტები კრიტიკული ინფრასტრუქტურის წინააღმდეგ ქბრბ საფრთხეების ირგვლივ.

#	MONTH/YEAR	NAME	COUNTRY	DESCRIPTION	CATEGORY
1	February 1992	Ignalina Nuclear Power Plant	Lithuania	Employee attempted sabotage	Intentional
2	June 1999	Bradwell Nuclear Power Plant	United Kingdom	Employee altered/destroyed data	Intentional
3	March, 2002	Davis-Besse Nuclear Power Station	United States	Worm	Intentional
4	June 2005	Japanese Nuclear Power Plants	Japan	Data release	Unknown
5	December 2006	Syrian Nuclear Program	Syria	Espionage	Intentional
6	March 2009	Energy Future Holdings	United States	Employee attempted sabotage	Intentional
7	June 2010	Natanz Nuclear Facility	Iran	Stuxnet virus used to destroy centrifuges	Intentional
8	June 2010	Oak Ridge National Laboratory	United States	Data theft via spear-phishing	Intentional
9	October 2011	Natanz Nuclear Facility	Iran	Duqu virus used to conduct espionage	Intentional
10	May 2012	Natanz Nuclear Facility	Iran	Flame virus used to conduct espionage	Intentional
11	January 2014	Monju Nuclear Power Plant	Japan	Data release	Unknown
12	December 2014	Korea Hydro and Nuclear Power Company	South Korea	Data theft and release	Intentional
13	February 2015	Japanese nuclear material control center	Japan	Nuclear facility used as relay point in cyberattack	Unknown
14	February 2016	Nuclear Regulatory Commission/U.S. Department of Energy	United States	An employee attempted to infect government computers with viruses distributed via spear-phishing emails	Intentional
15	April 2016	Gundremmingen Nuclear Power Plant	Germany	Two viruses entered the plant's fuel rod monitoring system	Unknown
16	June 2016	University of Toyama, Hydrogen Isotope Researc Center	Japan	Data theft via spear-phishing	Intentional

გრაფიკი 3: კიბერ შეტევები ქბრბ კრიტიკული ინფრასტრუქტურაზე

ფაქტია, რომ სხვადასხვა დროს სამიზნე გამხდარა ბირთვული ენერგეტიკის ობიექტები, ბირთვული სადგურები, ბირთვულ თემაზე მომუშავე ორგანიზაციები, ენერგოინფრასტრუქტურა, ლაბორატორიები, ჰიდროენერგეტიკული კომპანიები, მარეგულირებელი ორგანიზაციები, კვლევითი ლაბორატორიები და ა.შ.

როგორც ჩანს, შემტევები, მათი მიზანი, შეტევის ტიპები და მათ მიერ მიყენებული ზიანიც მრავალფეროვანია. შესაბამისად, ნათელია, რომ კიბერშეტევები გამოიყენება როგორც ქბრბ ინფრასტრუქტურის მართვის შესახებ სენსიტიური ინფორმაციის მითვისებისთვის, ასევე ამ ინფრასტრუქტურის პირდაპირი დაზიანებისათვის.

სტრატეგიული მნიშვნელობა

რუსული ქბრბ და კიბერშესაძლებლობების სტრატეგიული მნიშვნელობა დიდია. რუსეთის სამხედრო დოქტრინა გულისხმობს ასიმეტრიული ტაქტიკის გამოყენებას, მათ შორის ჰიბრიდული ომის ელემენტებს შესაბამისი სტრატეგიული მიზნების მისაღწევად. ქბრბ საფრთხეებში კიბერშესაძლებლობების ინტეგრაცია მნიშვნელოვნად აძლიერებს რუსეთის უნარს, რომ შეაფერხოს, დააზიანოს და სძლიოს მოწინააღმდეგეს. შესაბამისად საჭიროა ქბრბ და კიბერსაფრთხეების კავშირის განხილვა ეროვნული უსაფრთხოების არქიტექტურის ჩამოყალიბებისას.

ასიმეტრიული საბრძოლო მოქმედებები

რუსეთის მიერ ასიმეტრიული საბრძოლო მოქმედებები, მათ შორის კიბერ და საინფორმაციო ოპერაციები, შედეგის მიღწევის ეფექტიანი საშუალებაა, რომლის დროსაც, ერთი მხრივ, ხდება მოწინააღმდეგის სისუსტეების გამოყენება და, მეორე მხრივ, პირდაპირი კონფრონტაციის ალბათობის შემცირება.

მნიშვნელოვანია კიბერსივრცის თავისებურებების გათვალისწინება - შემტევს, ხშირ შემთხვევაში, შეუძლია განხორციელებული კიბერშეტევის უარყოფა და გაყალბებული მტკიცებულებების გავრცელება, შესაბამისი საინფორმაციო არხებით.

კიბერ ღონისძიებები მოიცავს: კრიტიკული ინფრასტრუქტურის დაზიანების საშუალებას, დეზინფორმაციის გავრცელებას, გაურკვევლობის შექმნას და ა.შ. ქბრბ საფრთხეების პოტენციურმა ინტეგრაციამ ამ სტრატეგიაში გამოიწვია შესაბამისი ოპერაციების ეფექტიანობის ზრდა.

გრაფიკი 4: ვიზუალიზაცია, სკრიპალების მოწამვლის ქეისთან დაკავშირებით, რუსული ე.წ. "Playbook", პოსტ-ინციდენტ აქტივობებისთვის

მაგალითად, ქვემოთ ჩამოთვლილი 3 ქბრბ ინციდენტის დროს რუსეთმა გამოიყენა კიბერსივრცე და შეტევის შესაძლებლობები ქბრბ შეტევის ეფექტისა და ზიანის გასაძლიერებლად:

- სერგეი სკრიპალის[1] მოწამვლის შემდეგ განხორციელებული კიბერ შეტევები OPCW ლაბორატორიაზე და ექსპერტებზე, ასევე ყალბი ნარატივების გავრცელება;
- ალექსეი ნავალნის მოწამვლის შემდეგ განხორციელებული დეზინფორმაციული კამპანია, ჟურნალისტების წინააღმდეგ შეტევები;
- სირიაში ქიმიური იარაღის გამოყენების შემდეგ განხორციელებული საინფორმაციო დეზინფორმაციული კამპანია, ყალბი პერსონები და რესურსები.

საინფორმაციო სივრცეზე კიბერშეტევები, დეზინფორმაციის გავრცელება და ჰიბრიდული ომის კომპონენტები (U.S. Deparment of State, Global Engagement Center, 2022.) გამოყენებულია უკრაინის წინააღმდეგ საომარი მოქმედებების დროსაც.

[1] https://ge.usembassy.gov/putins-poisons-2018-attack-on-sergei-skripal/

გრაფიკი 5: აშშ სახელმწიფო დეპარტამენტის განცხადება, რუსულ დეზინფორმაციასთან დაკავშირებით

შეკავების სტრატეგიები

ქბრბ და კიბერსაფრთხეების თანაკვეთის შედეგად წარმოშობილი რისკების შესამცირებლად გამოიყენება შემდეგი სტრატეგიები:

- კრიტიკული ინფრასტრუქტურის, განსაკუთრებით ქბრბ მიმართულების ობიექტების, კიბერმედეგობის გაძლიერება;
- რეაგირების გეგმების შემუშავება, რომლებიც მართავს კიბერინციდენტით გამოწვეულ ქბრბ ინციდენტებს;
- საერთაშორისო თანამშრომლობის გაძლიერება და საფრთხის შესახებ ინფორმაციის გაზიარება;
- კვლევისა და განვითარების მიმართულებით ინვესტირება თანამედროვე ტექნოლოგიების გათვალისწინებით.

კიბერმედეგობის გაძლიერება

კრიტიკული ინფრასტრუქტურის კიბერმედეგობის გაძლიერება ფუნდამენტური აქტივობაა კიბერშეტევით გამოწვეული ქბრბ რისკების შესამცირებლად. აღნიშული მოიცავს: კიბერუსაფრთხოების ძლიერ ორგანიზაციულ-ტექნიკურ კონტროლის სისტემის დანერგვას, უსაფრთხოების დამოუკიდებელი აუდიტის პერიოდულ ჩატარებას, საუკეთესო პრაქტიკისა და დარგობრივი სტანდარტების გათვალისწინებას და მათთან შესაბამისობის უზრუნველყოფა, კიბერშეტევების სიმულაციასა და ინციდენტების მართვის პროცესის ტესტირებას. მნიშვნელოვანია ტექნიკური პერსონალის კომპეტენციის ამაღლება მუდმივი ტრენინგითა და განვითარების ხელშეწყობით.

ინტეგრირებული რეაგირების გეგმები

ეფექტიანი კრიზისის მენეჯმენტისთვის მნიშვნელოვანია შემუშავდეს ინტეგრირებული რეაგირების გეგმები, რომლებიც მოიცავს კონკრეტული კიბერშეტევით გამოწვეული ქბრბ ინციდენტების მართვას. ეს გეგმები უნდა მოიცავდეს მათ შორის კოორდინაციის მექანიზმებს კიბერუსაფრთხოების გუნდებს, გადაუდებელი დახმარების სამსახურებსა და ჯანდაცვის მიმართულების ექსპერტებს შორის. რეგულარული სავარჯიშოები და სიმულაციები უზრუნველყოფენ აღნიშული ინტეგრირებული გეგმების სისუსტეების გამოვლენას, მათ გამოსწორებასა და მუდმივ გაუმჯობესებას. შესაძლებელია შემუშავდეს ქბრბ ინციდენტების სცენარები კონკრეტული ინფრასტრუქტურის ობიექტების ჭრილში.

საერთაშორისო კოოპერაცია

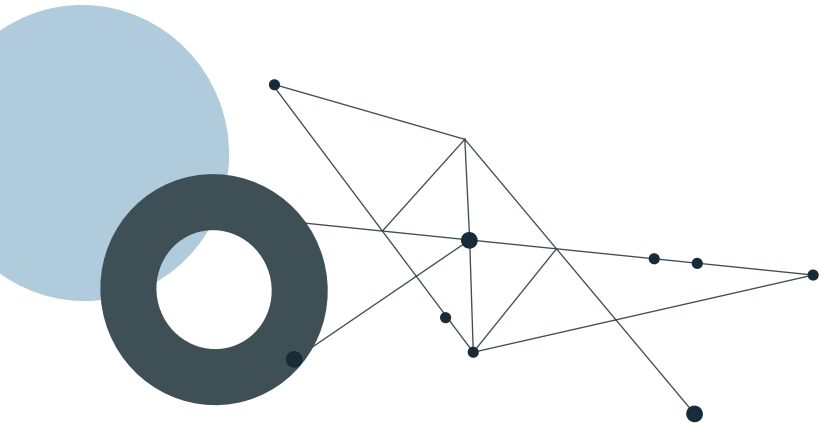
საერთაშორისო თანამშრომლობის ხელშეწყობა სასიცოცხლოდ მნიშვნელოვანია ნებისმიერი ქვეყნის შესაბამისი მიმართულების სამსახურებისათვის. კიბერუსაფრთხოების მართვა დიდ რესურსს მოითხოვს როგორც მატერიალური, ისე ადამიანური (მათ შორის ინტელექტუალური) კაპიტალის თვალსაზრისით. ერთი მხრივ, ძვირია ორგანიზაციის მატერიალურ-ტექნიკური ბაზით აღჭურვა, მეორე მხრივ კი - შესაბამისი კადრების მოზიდვა და შენარჩუნება. მრავალი ქვეყნის კრიტიკულ ინფრასტრუქტურულ ობიექტებში გამოწვევაა კიბერუსაფრთხოების სპეციალისტების დეფიციტი.

შესაბამისად, უმნიშვნელოვანესია პარტნიორ ქვეყნებსა და ორგანიზაციებს შორის საუკეთესო პრაქტიკის, გამოცდილებისა და საფრთხის შესახებ არსებული ინფორმაციის გაზიარება.

ინფორმაციის მუდმივი გაზიარება და კავშირის არსებობა ხელს შეუწყობს კიბერ-ქბრბ ინციდენტების დროს კოორდინირებული და ეფექტიანი რეაგირების პროცესს.

ინფორმაციის გაზიარების მნიშვნელობა და ეფექტიანობა კარგად ჩანს უკრაინის მაგალითზე. მრავალი კიბერშეტევის მოგერიება და მისი პოტენციური ზიანის შემცირება მოხერხდა დასავლელი პარტნიორებისა და ორგანიზაციების მიერ უკრაინისთვის მიწოდებული აღრეული-გაფრთხილების სისტემის მეშვეობით.

კერძოდ, ე.წ. TTP (Tactics, Techniques, Procedures) და IOC (Indicators of Compromise)-ების გაზიარების შედეგად, შესაბამისი უკრაინული სამსახურები მომზადებულნი და ხშირ შემთხვევაში, დაცული შეხვდნენ რუსეთიდან მომდინარე კიბერშეტევებს, მათი ქბრბ და კრიტიკული ინფრასტრუქტურის მიმართ.



თანამედროვე ტექნოლოგიების განვითარების გათვალისწინებით და ტექნოლოგიური პროგრესის ტემპიდან გამომდინარე, განსაკუთრებული მნიშვნელობა ენიჭება კვლევით საქმიანობას. ისეთი ტექნოლოგიები და მიმართულებები, როგორებიცაა: AI (ხელოვნური ინტელექტი), ე.წ. ბლოქჩეინი, 5/6G კომუნიკაციის სტანდარტი, კვანტური კომპიუტერული სისტემები და ა.შ. ახალ გამოწვევებს ქმნიან როგორც შეტევითი, ასევე თავდაცვითი თვალსაზრისით. შესაბამისად, აუცილებელია ამ ტექნოლოგიების სისუსტეებისა და შესაძლებლობების/დადებითი და უარყოფითი მხარეების შესწავლა და გათვალისწინება მათ გამოყენებამდე კრიტიკულ ინფრასტრუქტურაში, განსაკუთრებით ქბრბ მიმართულებებში.

შექმნილია და ტესტირებას გადის რამდენიმე GenAI მოდელი ქბრბ მიმართულებით, რისი საშუალებითაც შესაძლებელია შეტევითი და თავდაცვითი ქბრბ ოპერაციების მოდელირება და მათი შედეგების პროექცია (Barrett, Jackson, Murphy, Madkour, Newman, 2024.).

დასკვნა

ქბრბ და კიბერსაფრთხეების თანაკვეთა კომპლექსური და განვითარებადი გამოწვევაა გლობალური უსაფრთხოებისათვის. რუსეთის შესაძლებლობები და განზრახვები ორივე მიმართულებით თვალსაჩინოს ხდის ყოვლისმომცველი მიდგომისა და სტრატეგიის შემუშავების აუცილებლობას შესაბამისი რისკების შესამცირებლად. კიბერმედეგობის გაძლიერებით, ინტეგრირებული რეაგირების გეგმების შემუშავებით, საერთაშორისო კოოპერაციის გაძიერებით და კვლევითი საქმიანობის ხელშეწყობით შესაძლებელია აღნიშული რისკების შემცირება და კატასტროფული ქბრბ ინციდენტების პრევენცია. გასათვალისწინებელია, რომ თანამედროვე ტექნოლოგიების მეშვეობით შესაძლებელია ამ ტიპის საფრთხეების უფრო ძირეული კვლევა და ინოვაციური გადაწყვეტილებების შემუშავება.

ბიბლიოგრაფია

NATO, 2022. NATO's Chemical, Biological, Radiological and Nuclear (CBRN) Defence Policy.

https://www.nato.int/cps/en/natohq/official_texts_197768.htm

Microsof. 2023. "A year of Russian hybrid warfare in Ukraine. Microsoft Threat Intelligence".

https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf

Radoini, A., & Siddiqui, M. (2016). The Cyber0threat Agains Chemical, Biological, Radiological and Nuclear (CBRN) Facilities. (pp. 104–109). United nations interregional crime and Justice research institute (UNICRI).

https://unicri.it/sites/default/files/2021-12/16_cyber_threat.pdf

Putin's Poisons: 2018 Attack on Sergei Skripal.

https://ge.usembassy.gov/putins-poisons-2018-attack-on-sergei-skripal/

U.S. Department of State, Global Engagement Center, Special Report. 2022. "The Kremlin's Chemical Weapons Disinformation Campaigns"

Anthony Barrett et al. 2024. "A Framework for Assessing and Managing Dual-Use Hazards of AI Foundation Models"

https://vcresearch.berkeley.edu/news/framework-assessing-and-managing-dual-use-hazards-ai-foundation-models