საქართველოს თავდაცვის სამინისტრო

სსიპ - კიბერუსაფრთხოების ბიურო

კიბერ თავდაცვა

კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები

(ნაშრომების და სტატიების კრებული)

ვლადიმერ სვანაძე

სსიპ - კიბერუსაფრთხოების ბიუროს კონსულტანტი

ანდრია გოცირიძე

სსიპ - კიბერუსაფრთხოების ბიუროს დირექტორი

თბილისი

2015

ს ა რ ჩ ე ვ ი

წინასიტყვაობა

კიბერსივრცეში უსაფრთხოების უზრუნველყოფის სირთულეებს საზღვრები არ გააჩნია. თუმცა ყველა ქვეყანა ცდილობს ეს საკითხი გადაჭრას თავად დამოუკიდებლად, რის გამოც ყველა საჭირო ზომები და ღონისძიებები ხშირ შემთხვევაში არ არის საკმარისი. არსებობს უამრავი სირთულე როგორც კიბერუსაფრთხოების სირთულეების ჩვენეულ გაგებაში, ისე სახელმწიფო პოლიტიკაში და ტექნიკურ შესაძლებლობებში, რომლებიც აუცილებელია მოცემული საკითხების გადასაჭრელად.

წინამდებარე კრებულში მოცემულია ის ნაშრომები, რომლებიც გადმოცემს კიბერსივრცის უსაფრთხოების უზრუნველყოფისა და მისი მაქსიმალური დაცვის საკითხებს. კერძოდ, კრებულში გაეცნობით იმ საფრთხეებს, რომლებიც არსებობს კიბერსივრცეში, ამ საფრთხეების წარმოქნის წყაროებსა და მათ სახეობებს. ასევე საერთაშორისო და რეგიონალურ დონეზე განხორციელებულ იმ ღონისძიებებს, რომლებიც მიმართულია კიბერსივრცის დაცვაზე. გარდა ამისა კრებულში მოცემულია ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების პოლიტიკისა და სტრატეგიების მოკლე აღწერილობები, საერთო პრინციპები და რეკომენდაციები. ასევე ზოგიერთი ქვეყნის იმ ორგანიზაციულ - სტრუქტურული ერთეულების მოკლე აღწერილობა, რომლებიც ანხორციელებენ აუცილებელ ღონისძიებებს მიმართულს კიბერსივრცის დაცვასა და კიბერუსაფრთხოების უზრუნველყოფაზე. ყოველივეს ფონზე განხილულია საქართველოს კიბერუსაფრთხოების სტრატეგია, პოლიტიკა და სუბიექტები. ასევე გახილულია ქვეყანაში კიბერუსაფრთხოების ის გამოწვევები, რაც გათვალისწინებულია ქვეყნის ეროვნული უსაფრთხოების კონცეფციაში.

აგრეთვე კრებულში მოცემულია წამყვანი ქვეყნების კიბერშესაძლებლობების მიმოხილვა, მათი კიბერუსაფრთხოების პოლიტიკისა და სტრატეგიების მოკლე აღწერილობები, საერთო პრინციპები და რეკომენდაციები. კერძოდ, ნაშრომში განხილულია შეერთებული შტატების, დიდი ბრიტანეთის, ნიდერლანდების სამეფოს, რუსეთისა და ირანის კიბერშესაძლებლობები, მათი კიბერსივრცის დაცვის

ორგანიზაციული და სტრუქტურული მოწყობა, რაც შეიძლება მივიჩნიოთ საუკეთესო გამოცდილებად საქართველოს კიბერუსაფრთხოების მოწყობისთვის.

არსებობს ტერმინის „კიბერსივრცის“ განმარტების ბევრი ვარიანტი და ყველა მათგანი იძლევა თავისებურ განსაზღვრებას. თუმცა ყველა განმარტებაში აღნიშნულია, რომ „კიბერსივრცე“ წარმოადგენს ინფორმაციულ - ტექნოლოგიური ინფრასტრუქტურის ურთიერთკავშირის კომპლექსს, რომელიც თავისთან მოიცავს ინტერნეტის გლობალურ ქსელს, კომპიუტერულ სისტემებს, ტელესაკომუნიკაციო ქსელებსა და პროცესორებს.

ბოლო ორ ათწლეულში ჩვენ გავხდით ე. წ. „ინფორმაციული აფეთქების“ უნებლიე მოწმეები, როცა პრაქტიკულად არავის არ შეუძლია გვერდი აუაროს ინფორმაციულ ქსელებზე დაშვებასა და მის გამოყენებას, იქნება ეს პირადი საყოფაცხოვრებო თუ პროფესიულ დონეზე. ამის გარდა, გლობალური ქსელების მიმართ არსებულ მზარდ ინტერესს თან ახლავს მისი უსაფრთხოების უზრუნველყოფის ადეკვატური ზომები. ეს გამოწვეულია იმ ფაქტით, რომ თავდაპირველად ინტერნეტი იქმნებოდა სამეცნიერო მონაცემების გაცვლის მიზნით, თუმცა დღეს ეს სურათი კარდინალურად არის შეცვლილი და ამჟამად ინტერნეტის გლობალური ქსელი წარმოადგენს მსოფლიო ეკონომიკის მხარდამჭერ ერთერთ ძირითად საშუალებას. აღსანიშნავია ის გარემოება, რომ ინტერნეტის კონსტრუქციული თუ დესტრუქციული მიზნებით გამოყენებისა და მისი ფუნქციონირების საკმაოდ სწრაფად მზარდი პროცესი წინ უსწრებს ინფრასტრუქტურის რეფორმირებისა და უსაფრთხოების უზრუნველყოფის ძალისხმევას. თავის მხრივ კიბერუსაფრთხოება ანუ ინტერნეტის გლობალური ქსელის უსაფრთხოება მოიცავს საკითხის გადაჭრის გლობალურ მასშტაბს, თუმცა ამ მიმართულებით არსებული ღონისძიებების დიდი ნაწილი ხორციელდება ცალკეული ქვეყნებისა და მათი ეროვნული უსაფრთხოების პოლიტიკის დონეზე, რაც არ არის საკმარისი და საკითხი მოითხოვს საერთაშორისო თუ რეგიონალურ მიდგომას.

წიგნში ასევე განხილულია სოციალური ქსელები და ეროვნული უსაფრთხოება, არსებული სირთულეები მოცემული მიმართულებით. ბოლოს მკითხველს შეუძლია

გაეცნოს იმ რეკომენდირებულ ლიტერატურას, რომელიც აღიარებულია კიბერუსაფრთხოების სფეროში, და რომლებიც მომზადებულია დარგიას აღიარებული ექსპერტების მიერ.

ბოლოს შეიძლება აღინიშნოს, რომ წინამდებარე წიგნი არის ქართულად აკადემიურ დონეზე შედგენილი, პირველი სრულყოფილი გამოცემა კიბერ სივრცისა და მასთან დაკავშირებილი სირთულეებისა და გამოწვევების შესახებ.

კრებულში მოცემული ნაშრომები განკუთვნილია როგორც მოცემული დარგის სპეციალისტებისთვის და სამართალმცოდნეებისთვის, ისე იმ დაინტერესებული პირებისთვის, რომლებსაც სურთ ამ მიმართულებით შეიძინონ გარკვეული ცოდნა. აგრეთვე, კრებულში განხილული საკითხები, დასკვნები და რეკომენდაცვიები შეიძლება გამოიყენოს როგორც საკანონმდებლო და აღმასრულებელი ხელისუფლების, ისე კერძო და სამოქალაქო სექტორის წარმომადგენლებმა.

წიგნი, თავისი ინფორმაციული დატვირთულობიდან გამომდინარე, ასევე სასარგებლო და გამოყენებადი იქნება თავდაცვის სამინისტროს და შეიარაღებული ძალების სხვადასხვა სტრუქტურული ერთეულებისთვის.

ავტორებისგან

Foreword

Security challenges in cyberspace have no borders. However, every country strives to solve the issue on their own, which is the reason why all necessary measures and actions in many cases are not enough to deal with the problem. There are lot of difficulties in our way of understanding the complexity of cyber security field as well as in state policy and technical abilities that are essential for the solution of the above mentioned issues.

The present book is the collection of works that depicts the maximum security and protection of cyberspace. In particular, the collection will introduce the readers with the existing threats in cyberspace and various types of sources; also the events/activities on international and regional level aimed at the protection of cyberspace. Collection also includes: brief descriptions of cyber security policies, strategies, general principles and recommendations of EU member states; brief descriptions of some organizational - structural units, which are responsible for the implementing all necessary measures for the protection of cyberspace; cyber security strategy, policy and subjects of Georgia based on the above mentioned background; cyber security challenges within the country, which are envisaged in the National Security Concept of Georgia.

Collection includes the brief description of cyber capabilities, cyber security policies, strategies, general principals and recommendations of the leading countries. In particular, mentioned work describes cyber capabilities of the United States, Great Britain, the Netherlands, Russia and Iran, also their organizational and structural arrangements for the protection of cyber space, which can be considered as the best example for Georgia in order to achieve the same success.

The term "cyber space" has various definitions and each of them have specific description. However, all the definitions state that "cyberspace" is technological – infrastructural interconnection, which includes the Internet global network, telecommunication networks and processors.

During the last two decades we have become an involuntary witnesses of so-called "Information explosion", what means, that virtually no one can bypass the access and use of information networks on private or professional level. In addition, the growing interest on global networks is accompanied by adequate safety measures. This is due to the fact that the Internet was originally developed for the exchange of scientific data, but this picture has radically changed, and nowadays Internet global network is one of the main assets to support world economy.

It should be emphasized, that the use of the internet for constructive or destructive purposes and the fast-growing process of its functioning outstrips the infrastructure reforming process and security provision effort. One the other hand cyber security or security of the Internet global network includes its part in solving the problem on a global scale, though the greater part of the activities is carried out by individual countries on their national policy level, which is not enough, and requires international and regional approach.

The book also deals with social networks and national security and the difficulties in this direction. At the end reader can be familiarized with the recommended literature, which is recognized in the field of cyber security and prepared by professional experts.

Finally it may be noted that this book is completed on the academic level, on Georgian and represents the first complete edition on cyber space, related difficulties and challenges.

The works in the collection are designed for both professionals and the legal authorities, as well as for those interested parties who wish to acquire some knowledge in this direction. Also, the issues, findings and recommendations can be used by both legislative and executive authorities, as well as by the representatives of private and civil society.

Authors

საქართველოს ეროვნული უსაფრთხოების კონცეფცია და კიბერუსაფრთხოების გამოწვევები

შესავალი[1]

საქართველოსთვის მეტად მნიშვნელოვანია ინტერნეტ სივრცის უსაფრთხოებისა და ელექტრონული ინფორმაციის დაცულობის უზრუნველყოფა. ინფორმაციული ტექნოლოგიების სწრაფ განვითარებასთან ერთად იზრდება მათზე სახელმწიფოს კრიტიკული ინფრასტრუქტურის დამოკიდებულება. ამის გათვალისწინებით, დიდი მნიშვნელობა ენიჭება კიბერსივრცეში არასანქცირებული შეღწევის აღკვეთასა და თავდაცვითი ღონისძიებების გაძლიერებას.

ინფორმაციულ ტექნოლოგიებზე სახელმწიფოს კრიტიკული ინფრასტრუქტურის დამოკიდებულებასთან ერთად იზრდება ის გამოწვევები, რომლებიც საქართველოს ინფორმაციული სივრცის დაცვასთანაა დაკავშირებული. 2008 წლის რუსეთ - საქართველოს ომის დროს რუსეთის ფედერაციამ საქართველოს წინააღმდეგ, სახმელეთო, საჰაერო და საზღვაო შეტევების პარალელურად, მიზანმიმართული და მასობრივი კიბერთავდასხმები განახორციელა. ამ კიბერშეტევებმა აჩვენა, რომ კიბერსივრცის დაცვა ეროვნული უსაფრთხოებისთვის ისევე მნიშვნელოვანია, როგორც სახმელეთო, საჰაერო და საზღვაო სივრცეების დაცვა.

საქართველოს მიზანია, შექმნას ინფორმაციული უსაფრთხოების ისეთი სისტემა, რომლის დროსაც ნებისმიერი კიბერთავდასხმის საზიანო შედეგები მინიმუმამდე იქნება შემცირებული და ასეთი თავდასხმის შემდეგ უმოკლეს დროში გახდება შესაძლებელი ინფორმაციული ინფრასტრუქტურის ფუნქციონირების სრული აღდგენა.

საქართველო დიდ მნიშვნელობას ანიჭებს საიდუმლო ინფორმაციის უსაფრთხოების უზრუნველყოფას და სახელმწიფოს საინფორმაციო სისტემების დაცვას.

[1] საქართველოს ეროვნული უსაფრთხოების კონცეფცია

იგი ქმნის შესაბამის საკანონმდებლო ბაზას და ინფრასტრუქტურას, რომელიც აუცილებელია ინფორმაციული ტექნოლოგიების გასაუმჯობესებლად და ინფორმაციის დაცულობის უზრუნველსაყოფად.

კიბერუსაფრთხოების უზრუნველყოფისათვის დიდი მნიშვნელობა ენიჭება საქართველოს მეგობარ ქვეყნებთან თანამშრომლობას და მათი გამოცდილების გაზიარებას. ასევე მნიშვნელოვანია განისაზღვროს საქართველოსთვის სტრატეგიულად პარტნიორი და პოტენციურად მოწინააღმდეგე ქვეყნები.

კვლევის საგანს წარმოადგენს ეროვნული უსაფრთხოების კონცეფციის საფუძველზე, კიბერუსაფრთხოების სფეროში საქართველოსთვის პოტენციურად მოწინააღმდეგე და სტრატეგიულად პარტნიორი ქვეყნებისა და ორგანიზაციების განსაზღვრა.

კვლევაში განხილულია არსებული ვითარება; კიბერშეტევის ძირითადი სექტორები და მთავარი მოთამაშე ქვეყნები; პოტენციურად მოწინააღმდეგე და სტრატეგიულად მნიშვნელოვანი ქვეყნებისა და ორგანიზაციების მოკლე აღწერა მოცემული მიმართულებით; კვლევა მთავრდება რეზუმეთი, სადაც გაკეთდება კვლევის შეჯამება და მომზადდება კვლევიდან გამომდინარე შესაბამისი რეკომენდაციები.

არსებული ვითარება

კიბერსივრცეში დღეს არსებული მდგომარეობა სულ უფრო შემაშფოთებელია, რადგან უსაფრთხოების სფეროს ანალიტიკოსების მიერ ჩატარებული კვლევების მიხედვით, დიდი ქვეყნები თავიანთ პროგრამებს აგებენ კიბერ - ომის წარმოების შესაძლებლობებზე. დღეს უკვე არსებობს სერიოზული მოსაზრებები, რომ კიბერ - ომი და მასთან დაკავშირებული აქტიურობები ადრე თუ გვიან აუცილებლად მოხდება.

ჩვეულებრივი საბრძოლო მოქმედებებისგან განსხვავებით, სადაც გამოიყენება ფიზიკური ძალა და საბრძოლო ტექნიკა, კიბერ - ომი წარმოადგენს უფრო დახვეწილ საშუალებას, რომლის დროსაც სტრატეგიულ დონეზე შესრულებულმა ამოცანამ შეიძლება გამოიწვიოს გაცილებით დიდი ზარალი და მოწინააღმდეგეს მიაყენოს

კოლოსალური ზიანი. თანამედროვე ქსელების დიდი ნაწილი ეფუძნება ინტერნეტს და მასთან მიერთებულ კომპიუტერულ სისტემებს, სადაც ჩართულია საბანკო, ჯანდაცვის, ენერგეტიკული და სხვა სასიცოცხლოდ მნიშვნელოვანი სფეროები, და ამის გათვალისწინებით, მიზანმიმართული თავდასხმა კრიტიკული ინფრასტრუქტურის ობიექტებზე შეიძლება აღმოჩნდეს კატასტროფული. მიჩნეულია, რომ დღეს ყველაზე დაუცველი და მოწყვლადი სექტორებია:

- საბანკო სექტორი და სხვა საფინანსო ინსტიტუტები;
- საფონდო ბირჟები;
- ბირთვული ელექტროსადგურები;
- წყლის მომარაგებისა და გამწმენდი სისტემები.

კარგად შესრულებული კიბერშეტევა ნებისმიერ ზემოთ მოცემულ სექტორზე გამოიწვევს შიშს, სამოქალაქო პანიკასა და მასიურ არეულობებს. ასევე პარალიზებული იქნება სახელმწიფო სტრუქტურები ყველა დონეზე. ამიტომ, კიბერუსაფრთხოების დარგის ანალიტიკოსები რჩებიან იმ აზრზე, რომ კიბერ - ომმა, მინიმალური დანახარჯებითა და ძალისხმევით, ტრადიციული ომის მსგავსად შეიძლება გამოიწვიოს მასიურად ადამიანთა ფიზიკური განადგურება.

ძირითადი მოთამაშეები

2014 წლის კვლევების მიხედვით, მსოფლიოში კიბერშეტევებში ძირითად მოთამაშეებად, ისევე როგორც 2013 წელს, იყვნენ:

- შეერთებული შტატები;
- რუსეთი;
- ირანი;
- ჩინეთი;
- ჩრდილოეთ კორეა;
- ისრაელი.

ეს არის ქვეყნები, რომლებიც თავიანთ საქმიანობაში იყენებენ უფრო აგრესიულ მეთოდებს და მოქმედებენ გლობალურად, როცა სხვა უფრო ნაკლებად მნიშვნელოვანი მოთამაშეები შემოიფარგლებიან მხოლოდ მცირე მასშტაბის კიბერშეტევებით. ქვემოთ მოყვანილია მოკლე ინფორმაცია თითოეული ქვეყნის შესახებ, კერძოდ:

შეერთებული შტატები

ყოველი კიბერშეტევა შეერთებული შტატების კრიტიკულ ინფრასტრუქტურაზე შეიძლება განხილულ იქნას როგორც ომის აქტი[2]. იმის შეგნება, რომ კიბერ - ომი გარდაუვალი პროცესია, შეერთებული შტატების მთავრობამ გაზარდა ბიუჯეტი და 2015 წლისთვის შეადგინა 14 მილიარდი ამერიკული დოლარი[3]. ასევე, გაიზარდა სხვადასხვა სასწავლო კურსები და სპეციალური ტრენინგების რაოდენობა. გასულ წელს, შეერთებული შტატების კიბერუსაფრთხოების პოლიტიკა მიმართული იყო შემტევით სტრატეგიაზე, წარმოებდა კიბერშეტევების შესაძლებლობების განვითარება და დახვეწა. ქვეყანას ადანაშაულებენ ირანის ატომურ ელექტროსადგურსა და მის ქსელებზე განხორციელებულ კიბერშეტევებში, თუმცა ეს ფაქტი დამტკიცებული არ არის.

რუსეთი

რუსეთი ინიცირებას უკეთებს ზოგიერთ ყველაზე მოწინავე კიბერშეტევას, რისთვისაც იყენებს როგორც სახელმწიფო რესურსებს, ისე კიბერდამნაშავეთა სამყაროს. რუსეთის საქმიანი ქსელი არის ფართო და ძველი, რომელიც ორგანიზებული იყო ჯერ კიდევ საბჭოთა კავშირის პერიოდში და ის შედგება ყოფილი სუკ - ის კიბერ - შპიონებისგან. მათ მიერ გამოიყენება მაღალი დონის ისეთი ინსტრუმენტები, რომელთაც ანალოგი არ გააჩნიათ არსად მსოფლიოში. გარდა ამისა, კიბერშეტევის პროცესში ისინი იჩენენ დიდ მოთმინებასა და არიან მეტად „დაჟინებულნი“. ზოგიერთ შემთხვევაში, კიბერშეტევის განსახორციელებლად ემზადებიან მთელი წელი, და ამავდროულად კვალსაც არ ტოვებენ, რომ ეს შეტევა მოხდა. თუმცა უნდა ითქვას, რომ ძალზედ ფართოდ გამოიყენება კორპორატიული შპიონაჟი, რომლის დროსაც

[2] By head of Cyber Command and Army General Keith Alexander

[3] ეს არის ოფიციალური მონაცემები, თუმცა არსებობს ასევე დახურული ბიუჯეტი, რომლის რაოდენობა ცნობილი არ არის

კონკურენტებიდან ხდება ინფორმაციის მოპარვა, რათა შემდეგ ის სარფიანად და მომგებიანად გაყიდონ.

ირანი

ირანმა ცოტა ხნის წინ დაასრულა კიბერ თავდაცვითი სისტემების დაყენების პროცესი საბანკო, საკომუნიკაციო, ნავთობის, მრეწველობისა და ატომური ობიექტების საიტებზე. გარდა ამისა, ირანმა წლის დასაწყისში წარუდგინა საზოგადოებას თავისი ახალი შესაძლებლობები, რომლებიც მიმართულია სხვა ქვეყნების მხრიდან კიბერშეტევების წინააღმდეგ. ირანიდან წამოსული DDoS შეტევების უმრავლესობა მიმართულია შეერთებული შტატების საბანკო და საფინანსო სექტორზე[4], ასევე ისრაელისა და არაბული სამყაროს ენერგეტიკულ ობიექტებზე.

ჩინეთი

მიუხედავად იმისა, რომ ჩინეთი ითვლება კიბერშეტევების ერთერთ მთავარ წყაროდ, მათი მეთოდები მიჩნეულია ნაკლებ რთულად და ხშირ შემთხვევაში ჩინეთის მხრიდან წამოსული კიბერშეტევა ადვილად ამოსაცნობი და დასადგენია. თუმცა, ჩინეთის უპირატესობას წარმოადგენს ჰაკერთა ჯგუფების დიდი რაოდენობა და მათი მხრიდან განხორციელებული კიბერშეტევების მასიურობა. გარდა ამისა, მსგავსმა ტაქტიკამ ჩინეთს საშუალება მისცა მოეპოვებინა როგორც სახელმწიფო ისე კორპორატიული საიდუმლოებები, რომელთა გამოყენებაც მათ შეუძლიათ თავიანთი მიზნებისთვის.

ჩრდილოეთ კორეა

ჩრდილოეთ კორეა, რომელიც არ არის მაღალი ტექნოლოგიური შესაძლებლობების ქვეყანა, მაინც გახდა კიბერშეტევებში ერთერთი ლიდერი. ქვეყანა წარმოადგენს დიდ საფრთხეს თავისი ბირთვული და კიბერ არსენალის გამო. ჩრდილოეთ კორეის ე. წ. „კიბერ არმია“ შედგება დაახლოებით 3, 000 ჰაკერისგან,

[4] მათ შორისაა ისეთი მსხვილი ბანკები, როგორებიცაა Wells Fargo, Bank of America, PNC and Citigroup Citibank

რომლებსაც განათლება მიღებული აქვთ უცხოეთში და ყველა ისინი კიბერშეტავას ახორციელებენ ქვეყნის გარედან. შედეგად, მათი შესაძლებლობები არის არამარტო ძლიერი, არამედ რთულად ამოსაცნობიც, რაც ზრდის გაურკვევლობას და შესაბამისად რისკის ქვეშ აყენებს სხვა ქვეყნების ეროვნულ კრიტიკულ ინფრასტრუქტურას.

ისრაელი

ისრაელმა გასულ წელს უკვე დაასრულა კიბერთავდაცვითი მართვის ცენტრის შექმნა. გარდა ამისა, ირანის ბირთვული პროგრამის წინააღმდეგ საბრძოლველად ქვეყანამ ბიუჯეტში გამოყო რამდენიმე მილიარდი ამერიკული დოლარი. თუმცა ქვეყანას ირანის მხრიდან განხორციელებული კიბერშეტევებიდან რაიმე სახის სერიოზული დაზიანება არ მიუღია. ამ სფეროში ისრაელი აქტიურად თანამშრომლობს შეერთებულ შტატებთან.

რეგიონში მოთამაშე ქვეყნები და ორგანიზაციები

ქვეყნის კიბერუსაფრთხოების უზრუნველყოფისათვის დიდი მნიშვნელობა ენიჭება სწორად განისაზღვროს მოცემული მიმართულებით, საქართველოსთვის სტრატეგიულად პარტნიორი და პოტენციურად მოწინააღმდეგე ქვეყნები. ასევე ის ორგანიზაციები, რომლებიც წარმოადგენენ საფრთხეს ქვეყნის ეროვნული უსაფრთხოებისთვის, ან პირიქით, მათთან თანამშრომლობითა და პარტნიორობით შესაძლებელია მაქსიმალურად იქნას მიღწეული ქვეყნის უსაფრთხოება.

რუსეთი

საქართველოს ეროვნული უსაფრთხოების კონცეფციის[5] მიხედვით, ქვეყნისთვის დიდი საფრთხის შემცველია რუსეთი და მისი ქმედებები, ასევე ოკუპირებული ტერიტორიებიდან მომდინარე საფრთხეები, რომელიც ისევ რუსეთის ფაქტორს უკავშირდება.

[5] http://factcheck.ge/wp-content/uploads/2014/01/ebmeba-shalva-thadumadze-sazghvris-khazze-rati-Law-phaili-2-erovnuli-usaphrthkhoebis-kontsephtsia-2011.pdf

იმავე კონცეფციაში არაფერი არ წერია რუსეთიდან მომდინარე კიბერსაფრთხეებზე. 2008 წლის აგვისტოს ომის დროს რუსეთმა სახმელეთო, საზღვაო და საჰაერო თავდასხმის პარალელურად, მიიტანა მასირებული შეტევა საქართველოს კიბერ სივრცეზე, რის შედეგადაც დაზიანდა კრიტიკული ინფრასტრუქტურის დიდი ნაწილი[6]. ამის შემდეგ, 2008 – 2014 წლებში საქართველოს სახელმწიფო თუ კერძო საიტები არაერთხელ გახდა რუსეთის მხრიდან შეტევის ობიექტები. მსგავსი კიბერშეტევები ხორციელდებოდა როგორც უშუალოდ რუსეთის, ისე მის მიერ ოკუპირებული ტერიტორიებიდან, ძირითადად სოხუმიდან.

შეერთებული შტატების ნახევრად სამთავრობო ორგანიზაციის FireEye - ს[7] მიერ ჩატარებული კვლევის თანახმად, 2008 – 2014 წლებში რუსეთის მხრიდან სისტემატურად ხორციელდებოდა კიბერშეტევა[8] შინაგან და საგარეო საქმეთა სამინისტროების საიტებზე (იხილეთ *ცხრილი 1*).

[6] ეს განმარტება მიეცა მოგვიანებით, ომის შემდეგ, როცა საქართველოს ხელისუფლებამ დაიწყო კიბერუსაფრთხოების სტრატეგიასა და ინფორმაციული უსაფრთხოების საკითხებზე მუშაობა

[7] https://www.fireeye.com/

[8] ექსპერტთა აზრით, კიბერშეტევები ხორციელდებოდა რუსული ჰაკერული დაჯგუფება APT 28 - ის მიერ, რომელსაც არაოფიციალური მონაცემებით, კოორდინაციას უწევს რუსეთის ფედერალური უშიშროების სამსახური

ცხრილი 1

Malware	Targeting	Russian Attributes
Evolves and Maintains Tools for Continued, Long-Term Use • Uses malware with flexible and lasting platforms • Constantly evolves malware samples for continued use • Malware is tailored to specific victims' environments, and is designed to hamper reverse engineering efforts • Development in a formal code development environment **Various Data Theft Techniques** • Backdoors using HTTP protocol • Backdoors using victim mail server • Local copying to defeat closed/air gapped networks	**Georgia & the Caucasus** • Ministry of Internal Affairs • Ministry of Defense • Journalist writing on Caucasus issues • Kavkaz Center **Eastern European Governments & Militaries** • Polish Government • Hungarian Government • Ministry of Foreign Affairs in Eastern Europe • Baltic Host exercises **Security-related Organizations** • NATO • OSCE • Defense attaches • Defense events and exhibitions	**Russian Language Indicators** • Consistent use of Russian language in malware over a period of six years • Lure to journalist writing on Caucasus issues suggests APT28 understands both Russian and English **Malware Compile Times Correspond to Work Day in Moscow's Time Zone** • Consistent among APT28 samples with compile times from 2007 to 2014 • The compile times align with the standard workday in the UTC + 4 time zone, which includes major Russian cities such as Moscow and St. Petersburg

წყარო: Chart by FireEye

საინტერესოა ასევე, 2009 წლის 6 – 7 აგვისტოს რუსი ჰაკერების მიერ განხორციელებული კიბერშეტევა პოპულარულ ქართულ სოციალურ ქსელებზე, რომლის მიზეზი ქართველი ბლოგერის „სოხუმი“ - ს პოლიტიკური შეხედულებები გახდა. 7 აგვისტოს გააქტიურდა კიბერშეტევა და ცხადი გახდა, რომ მას რუსული სპეცსამსახურები ახორციელებდნენ, რომლებიც ბლოკავდნენ ინფორმაციას, რომელსაც ბლოგერი `სოხუმი` ავრცელებდა და აგვისტოს ომის წლისთავს უკავშირდებოდა. უკვე ყველა სპეციალისტი ადასტურებს, რომ შეტევა ვებგვერდებზე რუსეთიდან

განხორციელდა და იმდენად კარგად იყო ორგანიზებული, რომ ცალკეული ჰაკერების მოქმედებას გამორიცხავს.

რუსი ჰაკერების, მთავარი სამიზნე ის ვებგვერდები და პირებია, რომლებიც ინტერნეტის სივრცეში ქართულ სახელმწიფოებრიობასა და ინტერესებს იცავენ.

სამხრეთ კავკასია და თურქეთი

სამხრეთ კავკასიის ქვეყნები (აზერბაიჯანი, სომხეთი) და თურქეთი ეროვნული უსაფრთხოების კონცეფციის მიხედვით, მოიაზრებიან საქართველოს პარტნიორ ქვეყნებად, რომლებთანაც ურთიერთობა უნდა წარიმართოს სავაჭრო - ეკონომიური თანამშრომლობის მიმართულებით. ასევე, არ დაფიქსირებულა ნახსენები ქვეყნების მხრიდან კიბერშეტევები და ქართულ კიბერსივრცეში არასანქცირებული შეღწევის ფაქტები.

თუმცა თუ გავითვალისწინებთ იმ გარემოებას, რომ სომხეთი და რუსეთი მოიაზრებიან ერთმანეთის სტრატეგიულ პარტნიორებად, სომხეთში არსებულ რუსულ სამხედრო ბაზებს, რუსეთისა და თავად სომხეთის მუდმივ ინტერესებს რეგიონში, მაშინ შეიძლება ითქვას, რომ სომხეთი მომავალში, სამხრეთ კავკასიაში სიტუაციის ესკალაციის შემთხვევაში, შეიძლება გახდეს საქართველოს არაპირდაპირი პოტენციური მოწინააღმდეგე, რაც ამის პარალელურად, ასევე არ გამორიცხავს ქართულ კიბერსივრცეზე შეტევის განხორციელებას უკვე სომხეთის ტერიტორიიდან.

ირანი

ირანი, როგორც ზემოთ იყო ნახსენები, წარმოადგენს ერთერთ მთავარ მოთამაშეს კიბერსივრცესა და მასთან დაკავშირებულ საკითხებში. მისი მთავარი სამიზნე არის დასავლეთი, შეერთებული შტატები და ისრაელი. თუმცა ბოლო დროს განვითარებული მოვლენების ფონზე, შეიძლება ვივარაუდოთ, რომ ირანსა და დასავლეთს შორის შემცირდეს დაძაბულობა კიბერუსაფრთხოების სფეროშიც. ირანს ასევე გააჩნია თავისი მუდმივი ისტორიული ინტერესები კავკასიაში. საქართველოსა და ირანს შორის ამ

ეტაპზე არის ნორმალური ურთიერთობები, რომელიც სავაჭრო - ეკონომიურს არ სცილდება.

ორგანიზაციები

პარიზში, 2015 წლის 7 იანვარს მომხდარმა ტერაქტმა და მასთან დაკავშირებულმა ჰაკერულმა თავდასხმებმა ფრანგულ კიბერსივრცეზე[9], მსოფლიო საზოგადოებრიობა დააყენა კიბერუსაფრთხოების ახალი გამოწვევების წინაშე. ამ მოვლენებს გვერდი არ აუვლია საქართველოსთვისაც, კერძოდ 2015 წლის 10 იანვარს[10], „ახლო აღმოსავლეთის კიბერ არმიის“ (the Middle Eastern Cyber Army - MECA) მიერ განხორციელდა კიბერშეტევა ფრანგული ჰიპერმარკეტის Carrefour - ის ოფიციალურ ვებ - გვერდზე http://carrefour.com.ge/ და რისკის ქვეშ შეიძლება აღმოჩენილიყო ქვეყნის მთლიანი კრიტიკული ინფრასტრუქტურა. გამომდინარე, რომ ქვეყანაში ფუნქციონირებს ამერიკული და ევროპული კომპანიების, ასევე საერთაშორისო ორგანიზაციების წარმომადგენლობითი ოფისები, რომლებიც მოიხმარენ ქვეყანაში არსებულ ინტერნეტის ქსელს და მასთან მიერთებულ კომპიუტერულ სისტემებს, არ გამოირიცხება, რომ კომპანიების სათაო ოფისზე და მათ საიტებზე განხორციელებული კიბერშეტევები უარყოფითად აისახოს ქვეყნის ინტერნეტ სივრცეზე, რაც ქვეყნისთვის ასევე დიდი რისკის შემცველი იქნება.

საყურადღებოა, რომ ბოლო წლებში, განსაკუთრებით სირიაში საომარი მოქმედებებისა და ახლო აღმოსავლეთში ე. წ. „ისლამური სახელმწიფოს“ (ISIS) ასპარეზზე გამოსვლის შემდეგ, ერთი - ორად გაიზარდა კიბერშეტევების რიცხვი. ამ მიმართულებით, განსაკუთრებით აქტიურობენ ჰაკერული დაჯგუფებები „ახლო აღმოსავლეთის კიბერ არმია“ (the Middle Eastern Cyber Army - MECA), Fallaga Hackers Team და Cyber Caliphate, ასევე „სირიის ელექტრონული არმია“ (SEA), რომელსაც დიდ მხარდაჭერას უწევს „ირანის კიბერ არმია“ (ICA).

[9] 7 იანვრის შემდეგ ჰაკერული თავდასხმა განხორციელდა დაახლოებით 19, 000 ფრანგულ ვებ - გვერდზე
[10] http://www.zone-h.org/archive/notifier=Middle%20East%20Cyber%20Army/page=22

სტრატეგიულად პარტნიორი ქვეყნები და ორგანიზაციები

კიბერუსაფრთხოების სფეროში დიდი მნიშვნელობა აქვს საერთაშორისო ურთიერთობებს, განსაკუთრებით აუცილებელია მჭიდრო ფორმატში სტრატეგიულ პარტნიორებთან და ორგანიზაციებთან თანამშრომლობა.

საქართველოს ეროვნული უსაფრთხოების კონცეფციის მიხედვით, დიდი მნიშვნელობა ენიჭება შეერთებულ შტატებთან, უკრაინასთან და თურქეთთან პარტნიორობას. ასევე, ჩრდილო ატლანტიკურ ალიანსში ქვეყნის გაწევრიანებასა და ევროკავშირში ინტეგრაციის პროცესს.

შეერთებული შტატები

შეერთებული შტატები კიბერუსაფრთხოების სფეროში უდავო ლიდერია. მიუხედავად ამისა, ქვეყნის ხელისუფლება მუდმივად ზრუნავს დარგის განვითარებაზე, მუშაობს და ნერგავს ახალ ტექნოლოგიებს, აწარმოებს სამეცნიერო - კვლევით სამუშაოებს. 2015 წლის სახელმწიფო ბიუჯეტში კიბერუსაფრთხოების მიმართულებით გათვალისწინებულია 14 მილიარდი ამერიკული დოლარი. ქვეყანაში ამ მიმართულებით მუშაობენ როგორც კერძო, ისე ნახევრად სამთავრობო ორგანიზაციები, რომელთაგან აღსანიშნავია ISACA[11] და FireEye[12], რომელთა კომპეტენტურობა და სტანდარტები აღიარებულია მთელს მსოფლიოში. აქვე აღსანიშნავია, რომ თავდაცვის სექტორში დანერგილია C4ISR[13] სისტემა, რომლის ერთერთი კომპონენტი შეიცავს არმიაში კომპიუტერული სისტემების უსაფრთხოების ელემენტებს[14].

2011 წლის მაისში[15] შეერთებულმა შტატებმა გამოაქვეყნა თავისი სტრატეგია კიბერსივრცის დაცვაზე. სტრატეგიას საფუძვლად უდევს მთავრობას, საერთაშორისო პარტნიორებსა და კერძო სექტორს შორის თანამშრომლობის მოდელი, სადაც

[11] https://www.isaca.org/Pages/default.aspx
[12] https://www.fireeye.com/
[13] Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance (C4ISR) systems enable military forces to gather, analyze and quickly disseminate intelligence information. These systems help ensure effective protection of national borders, regional boundaries, temporary installations and assets.
[14] მოცემული სისტემით სარგებლობს ასევე NATO - ს წევრი ქვეყნები
[15] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

აღწერილია მთელი რიგი ღონისძიებები, რომლებიც აუცილებელია გატარდეს შემდეგი შვიდი მიმართულებით:

- ეკონომიკა - საერთაშორისო სტანდარტებისა და ინოვაციების მოზიდვა, ღია და ლიბერალური ბაზარი;
- ეროვნული ქსელის დაცვა - უსაფრთხოების ამაღლება, სანდოობა და მდგრადობა;
- სამართალებრივი მხარე - თანამშრომლობისა და სამართლებრივი ნორმების გაფართოება;
- სამხედრო სფერო - უსაფრთხოების თანამედროვე გამოწვევებზე მზადყოფნა;
- სამთავრობო ინტერნეტის ქსელი - სამთავრობო სტრუქტურების ეფექტურობისა და მრავალმომცველობის გაფართოება;
- საერთაშორისო განვითარება - უსაფრთხოების ორგანიზება, საერთაშორისო კომპეტენციების განვითარება და ეკონომიკური აყვავება;
- თავისუფლება ინტერნეტში - მოქალაქეთა კერძო ცხოვრების ხელშეუხებლობისა და თავისუფლების მხარდაჭერა.

ესტონეთი

კიბერუსაფრთხოების სტრატეგია ქვეყანამ მიიღო 2008 წელს[16], მას შემდეგ რაც 2007 წელს რუსეთის მხრიდან განხორციელდა მასირებული კიბერშეტევა ქვეყნის კიბერ სივრცეზე. ესტონეთი დიდ მნიშვნელობას ანიჭებს თავისი კიბერსივრცის დაცვას და ამახვილებს ყურადღებას ინფორმაციული სისტემების უსაფრთხოებაზე. სარეკომენდაციო ღონისძიებები ატარებს სამოქალაქო ხასიათს და ეფუძნება სამართლებრივ რეგულაციებს, სწავლებასა და თანამშრომლობას.

მოცემულ დოკუმენტში აღწერილია სახელმწიფოში კიბერუსაფრთხოების სფეროში არსებული ვითარება და განსაზღვრავს ეროვნულ პოლიტიკას მოცემული მიმართულებით. ქვეყანაში არ არსებობს ერთიანი სახელმწიფო ორგანო, რომელიც პასუხისმგებელი იქნებოდა კიბერსივრცის დაცვის უზრუნველყოფაზე. ამ პროცესში

[16] https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

უშუალოდ მონაწილეობს რამდენიმე სამინისტრო და მათი ქვედანაყოფი. ინფორმაციული უსაფრთხოების უზრუნველყოფაში მთავარი როლი ეკუთვნის ეკონომიკისა და კავშირგაბმულობის სამინისტროს (MEAC)[17]. სამინისტროს დაქვემდებარებაში არის ცენტრალური აღმასრულებელი ხელისუფლების ორი ორგანო, რომლებიც ახდენენ კიბერუსაფრთხოების სახელმწიფო პოლიტიკის რეალიზაციას. ეს ორგანოებია: ინფორმაციული სისტემების სახელმწიფო დეპარტამენტი (RISO)[18], რომელიც არის მთავარი მაკოორდინირებელი ორგანიზაცია ინფორმაციისა და საკომუნიკაციო ტექნოლოგიების სფეროში (ICT)[19], და ესტონეთის ინფორმატიკის ცენტრი (RIA)[20], რომელიც პასუხისმგებელია მთლიანი ქსელის უსაფრთხოების უზრუნველყოფაზე, კრიტიკული ინფორმაციული ინფრასტრუქტურის სახელმწიფო სუბიექტების ტექნიკურ უსაფრთხოებაზე, ასევე სახელმწიფო ორგანიზაციების ინტერესებიდან გამომდინარე მონაცემთა გადაცემის სისტემის დამუშავება და მართვა. მოცემული ცენტრის შემადგენლობაში ფუნქციონირებს ესტონეთის საგანგებო სიტუაციებზე რეაგირების ოპერატიული ჯგუფი (CERT)[21]. უშუალოდ კრიტიკული ინფრასტრუქტურის დაცვასა (CIIP) და კიბერუსაფრთხოებას უზრუნველყოფს შინაგან საქმეთა და თავდაცვის სამინისტროების სპეციალური სტრუქტურული ერთეულები. ორივე სამინისტრო პასუხისმგებელია ქვეყნის შიდა უსაფრთხოებასა და კრიზისების მართვაზე. საფოსტო და საბაზრო ელექტრონული კავშირის მომსახურების სფეროს კოორდინირებას უწევს კავშირგაბმულობის ეროვნული საბჭო. სახელმწიფოსა და კერძო სექტორს შორის პარტნიორობისთვის შეიქმნა პროექტი „კომპიუტერული უსაფრთხოება 2009“, რომელიც მიმართულია ინფორმაციული უსაფრთხოების გაძლიერებისკენ.

ესტონეთმა მოკლე ხანში შეძლო მაქსიმალურად განევითარებინა კიბერუსაფრთხოების სფერო, შეიძინა დიდი გამოცდილება და ევროკავშირის წევრ - ქვეყნებს შორის გახდა ერთერთი წამყვანი ქვეყანა მოცემულ დარგში. NATO - ს მიერ

[17] https://www.mkm.ee/en
[18] http://www.riso.ee/en/
[19] Information and Communication Technology
[20] https://www.ria.ee/en/
[21] https://www.ria.ee/cert-estonia

ტალინში შეიქმნა ალიანსის კომპიუტერული თავდაცვის სფეროში მოწინავე გამოცდილების გაცვლის ცენტრი (CCDCOE)[22].

უნდა ითქვას, რომ ესტონეთი მოცემული დარგის მიმართულებით არის დიდი კონტრიბუტორი როგორც NATO – ში, ისე EU - ში.

დიდი ბრიტანეთი

2009 წელს[23] მიღებული კიბერუსაფრთხოების სტრატეგია ხაზს უსვამს კიბერუსაფრთხოების უზრუნველყოფის საკითხთან კომპლექსური მიდგომის აუცილებლობას, რომლის რეალიზაციაში უნდა მონაწილეობდნენ სახელმწიფო სუბიექტები, მრეწველობის ყველა დარგის წარმომადგენლები, სამოქალაქო საზოგადოებრივი ორგანიზაციები და საერთაშორისო პარტნიორები.

სტრატეგიის მთავარი მიზანია გაიყვანოს დიდი ბრიტანეთი მოწინავე პოზიციებზე ინფორმაციული და სატელეკომუნიკაციო ტექნოლოგიების სფეროში ინოვაციების, ინვესტიციებისა და ხარისხიანი მომსახურების მიხედვით. ასევე მთლიანად ისარგებლოს კიბერსივრცის ყველა უპირატესობებითა და მიღწევებით. 2011 წელს შემოღებული სტრატეგია ასახავს მაქსიმალური რისკების შემცირებას დამნაშავეთა (მათ შორის ტერორისტების) და სხვა სახელმწიფოთა მხრიდან კიბერშეტევების მიმართ, რაც მიმართულია კიბერსივრცეში თითოეული მოქალაქის, საზოგადოებისა და ეკონომიკის უსაფრთხოებისკენ.

სტრატეგია ითვალისწინებს ორი ახალი ორგანიზაციის შექმნას[24]. პირველ რიგში ეს არის მინისტრთა კაბინეტის სტრუქტურაში შემავალი კიბერუსაფრთხოების სამმართველო (OCS)[25], რომელიც უზრუნველყოფს სტრატეგიულ ხელმძღვანელობასა და უწყებათაშორის დონეზე შეთანხმებულ მოქმედებას. არსებობს ასევე კიბერუსაფრთხოების ოპერატიული ცენტრი (CSOC), რომელიც ფუნქციონირებს

[22] Cooperative Cyber Defense Centre of Exelllence https://ccdcoe.org/tallinn-manual.html
[23] 2011 წელს მოხდა სტრატეგიის განახლება https://www.cpni.gov.uk/advice/cyber/cir/
[24] ორივე ორგანიზაციამ დაიწყო ფუნქციონირება 2010 წელს
[25] https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance

სახელმწიფო კავშირების მთავარი ოფისის (GCHQ)[26] ბაზაზე ქ. ჩელტენჰემში. ეს არის ახალი ცენტრი, სადაც თავმოყრილია სხვადასხვა უწყებების არსებული ფუნქციები კიბერსივრცის მდგომარეობის მონიტორინგისა და ღონისძიებების კოორდინაცია ექსტრემალურ რეაგირებაზე. ცენტრი ასევე გააკეთებს ანალიზს იმ საფრთხეებზე, რომელიც ემუქრება დიდი ბრიტანეთის კომპიუტერულ ქსელებსა და მათ მომხმარებლებს, გამოიმუშავებს შესაბამის რეკომენდაციებსა და საინფორმაციო სახელმძღვანელოებს. ეროვნული ინფრასტრუქტურის დაცვის ცენტრის (CPNI)[27] შემადგენლობაშია კომპიუტერების დახმარების სასწრაფო სამსახური (CERT Service)[28].

დიდ ბრიტანეთს გააჩნია საინტერესო სტრუქტურა დარგის აკადემიურ დონეზე განვითარების შესახებ. კერძოდ, ამ პროცესს კურირებს სახელმწიფო კავშირების მთავარი ოფისი (GCHQ), რომლის ეგიდით შეირჩა ქვეყნის რვა უმაღლესი სასწავლებელი და მათ ბაზაზე გაიხსნა სამეცნიერო - კვლევითი ცენტრები კიბერუსაფრთხოების სხვადასხვა მიმართულებებითა და პროფილით.

აღსანიშნავია ის გარემოება, რომ დიდი ბრიტანეთი კიბერუსაფრთხოების საკითხებში არ არის დიდი კონტრიბუტორი NATO – სა და EU - ში, თუმცა ქვეყანამ შეძლო შეექმნა კიბერუსაფრთხოების განვითარების დახვეწილი სისტემა.

ჩრდილო ატლანტიკური ხელშეკრულების ორგანიზაცია (NATO)[29]

საქართველო მიისწრაფვის გახდეს NATO - ს სრულუფლებიანი წევრი. ამიტომ ალიანსთან თანამშრომლობა ყველა მიმართულებით, მათ შორის კიბერუსაფრთხოების საკითხებში აუცილებელი პირობაა.

2002 წელს, მას შემდეგ რაც 1990 წლების ბოლოს ბალკანებზე სამხედრო ოპერაციის დროს განხორციელდა ქსელური შეტევები, ალიანსმა შეიმუშავა და გაუშვა კიბერ - დაცვის საკუთარი პროგრამა. ალიანსის ხელმძღვანელობამ გაითვალისწინა

[26] http://www.gchq.gov.uk/Pages/homepage.aspx
[27] http://www.cpni.gov.uk/Templates/CPNI/pages/Default.aspx
[28] https://www.cpni.gov.uk/advice/cyber/cir/
[29] http://www.nato.int/

„ბალკანეთის გაკვეთილები“, და 2002 წელს პრაღის სამიტზე[30] ნატო - ს წევრი ქვეყნების ლიდერები შეთანხმდნენ კიბერნეტიკული თავდაცვის პროგრამის შემუშავებასა და ინფორმაციულ ქსელებში ინციდენტებზე რეაგირების საკუთარი ჯგუფის (NCIRC)[31] შექმნაზე. ჯგუფის საკოორდინაციო ცენტრი განთავსებულია ბრუსელში, ნატო - ს შტაბ ბინაში, ხოლო ალიანსის სამეთაურო ოპერაციების მართვის შტაბში[32] ორგანიზებულ იქნა NCIRC - ს ტექნიკური ცენტრი. მოცემული სტრუქტურის შექმნით, ალიანსმა გადაწყვიტა მთელი რიგი სირთულეები დაკავშირებული კიბერუსაფრთხოების საკითხებთან. კერძოდ, ნატო - ს კომპიუტერულ ქსელებში არასანქცირებული შეღწევისა და სხვა მავნებლობების აღმოჩენა და განეიტრალება, ასევე ქსელების კრიპტოგრაფიული დაცვის ეფექტური მართვის უზრუნველყოფა.

გარდა ამისა, ალიანსის ექსპერტები უზრუნველყოფენ კომპიუტერულ ქსელებში საფრთხის წარმოქმნის საწინააღმდეგო ტექნიკურ ღონისძიებების, ასევე შეიმუშავებენ უსაფრთხოების უზრუნველყოფის რეჟიმსა და კომპიუტერული დანაშაულებების გამოძიების მეთოდოლოგიას. ამის პარალელურად, ტალინში შეიქმნა ალიანსის კომპიუტერული თავდაცვის სფეროში მოწინავე გამოცდილების გაცვლის ცენტრი (CCDCOE)[33], ნატო - მ ასევე დააფუძნა კიბერ - თავდაცვის ღონისძიებების მართვის სპეციალური ორგანო (CDMA)[34], რომელმაც ფუნქციონირება დაიწყო 2008 წელს. ამ უკანასკნელის ფუნქციებში შედის ალიანსის კომპიუტერულ ქსელზე შეტევის შემთხვევაში „კიბერ - თავდაცვის ოპერატიული და ეფექტური ღონისძიებების“ ორგანიზება და კოორდინაცია. 2009 წელს სტრასბურგის სამიტზე[35] ნატო - ს წევრმა ქვეყნებმა ვალდებულება აიღეს დააჩქარონ კიბერ - თავდაცის თანამედროვე

[30] http://www.nato.int/docu/comm/2002/0211-prague/

[31] Computer Incident Response Capability https://www.terena.org/activities/tf-csirt/meeting11/NCIRC-Anil.pdf

[32] ქ. მონსი, ბელგია

[33] Cooperative Cyber Defense Centre of Excellence https://ccdcoe.org/tallinn-manual.html

[34] The Cyber Defense Management Authority (CDMA): The Authority was called upon to initiate and coordinate response to cyber-attacks against allied member states, and NATO itself. CDMA was created and was operational in mid-2008. It was a big step in NATO Cyber Defense because it helps member states improve their own cyber security. Rapid-Reaction Teams (RRT's) are also being created and will be available to member states in order to help them counter cyber-attacks and will be available for immediate deployment http://csis.org/blog/nato-and-cyber-defense-brief-overview-and-recent-events

[35] http://www.nato.int/cps/en/natolive/news_52837.htm

საშუალებების შეძენა, გახადონ კიბერდაცვა ალიანსის განუყოფელ ნაწილად, განავითარონ საერთაშორისო თანამშრომლობა არამარტო ნატო - ს წევრ - ქვეყნებს შორის, არამედ ასევე პარტნიორ ქვეყნებთან. ალიანსი ასევე ახორციელებს მხარდამჭერ პროგრამებს მიმართულს წევრი და პარტნიორი ქვეყნების კიბერუსაფრთხოების ეროვნული პოლიტიკის განვითარებისა და კიბერ - საფრთხეებზე ექსტრემალური რეაგირების ჯგუფის შექმნისკენ.

კრიტიკული ინფრასტრუქტურის დაცვა არის ალიანსის ძირითადი მიმართულება ასევე სამოქალაქო თავდაცვის დაგეგმვის სფეროში. ამ სფეროში ღონისძიებების გატარების აუცილებლობაზე ნატო - ს ფარგლებში არაერთი დოკუმენტია მიღებული, სადაც ასახულია სამოქალაქო თავდაცვის დაგეგმვის პრინციპები, რომლებიც შემუშავდა წევრი ქვეყნების შესაბამისი უწყებებისთვის. გარდა ამისა, გეგმის ახალ რედაქციაში კიბერ - საფრთხეების ჭრილში, მოცემულია სამოქალაქო თავდაცვის საგანგებო სიტუაციების ისეთი მიმართულებები როგორიცაა ქიმიური, ბიოლოგიური და ატომური იარაღის გამოყენების წინააღმდეგ. ნატო - ს სამოქალაქო თავდაცვის დაგეგმვის მთავარი კომიტეტი და მისი რვა განყოფილება და კომიტეტი აგრძელებს კრიტიკული ინფრასტრუქტურის დაცვის ფუნქციონალური ასპექტების შესწავლას. ამის შედეგად, მუშავდება შესაბამისი რეკომენდაციები დაგეგმვის ყველა სახეობის მიმართულებით, რასაც ახორციელებს სათანადო განყოფილებები და კომიტეტები.

2007 წლის ნატო - ს საპარლამენტო ასამბლეაზე წარმოდგენილ სპეციალურ მოხსენებაში, ასევე ალიანსის კრიტიკული ინფრასტრუქტურის დაცვის საკითხებზე მომზადებულ სხვა ანგარიშებში (173 DSCFC 09 E bis)[36] განსაზღვრულია ნატო - ს წევრი ქვეყნებისა და მთლიანად ალიანსის კრიტიკული ინფრასტრუქტურის დაცვის საერთო პრინციპები. ისინი განსაზღვრავენ სხვადასხვა ნორმებს, მათ მსგავსებასა და სხვაობას, ასევე კრიტიკული ინფრასტრუქტურის დაცვის დარგობრივი სტრატეგიების განვითარებისა და რეალიზაციის სფეროში განსაზღვრავენ სუბიექტებს თავისი

[36] http://www.nato-pa.int/default.asp?SHORTCUT=1782

ფუნქციებით, სადაც აგრეთვე შედის ენერგეტიკა, სამოქალაქო ავიაცია და საზღვაო პორტების უსაფრთხოება.

ევროპული კავშირი (EU)[37]

ევროკავშირი წარმოადგენს ინფორმაციული უსაფრთხოების სფეროში საერთაშორისო დონეზე არსებულ მთავარ სუბიექტს. ამავდროულად, ევროკავშირი დიდ ყურადღებას უთმობს ისეთ საკითხებს, როგორიც არის კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვა, ინფორმაციული საზოგადოების ფორმირება და ინფორმაციული დაცვა. ევროკავშირმა დაიწყო სამეცნიერო - კვლევითი და სხვა სახის პროგრამების რეალიზება, რომელიც უკავშირდება ინფორმაციული რევოლუციის ასპექტებსა და განათლებაზე, ბიზნესზე, ჯანდაცვასა და კავშირგაბმულობაზე მათ გავლენას.

2004 წლის 20 ოქტომბერს[38] ევროკავშირის კომისიის მიერ მიღებული კომუნიკე კრიტიკული ინფრასტრუქტურის დაცვაზე იძლევა კრიტიკული ინფრასტრუქტურისა და მისი ობიექტების განსაზღვრებას, ასევე ადგენს კრიტერიუმებს იმ ობიექტების მიმართ, რომლებიც შეიძლება წარმოიშვას მომავალში. 2005 წლის ნოემბერში[39] ევროკავშირის კომისიის მიერ მიღებულია კრიტიკული ინფრასტრუქტურის დაცვის ევროპული პროგრამა „მწვანე წიგნი“, სადაც განსაზღვრულია ევროკავშირის მოქმედების მიმართულებები მოცემულ სფეროში. 2008 წელს ევროკავშირის კომისია შეუდგა პროექტის რეალიზებას, რომელიც მიმართულია კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის საერთო სტრატეგიის გამომუშავებაზე.

ქვემოთ მოცემულია ევროკავშირის კომისიის სხვა პროექტები და სტრატეგიები:

[37] http://europa.eu/index_en.htm
[38] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm
[39] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm

- ევროკავშირის კომისიის დაკვეთით, ელექტრონული კავშირის ინფრასტრუქტურის შეღწევადობისა და საიმედოობის პრობლემების კვლევების ჩატარება (ARECI)[40];
- პროექტი „კრიტიკული ინფრასტრუქტურის საფრთხეების შეტყობინების ინფორმაციული ქსელი“ (CIWIN)[41];
- 2004 წლის მარტში შეიქმნა და 2005 წლის სექტემბერში, კუნძულ კრეტაზე დაიწყო ფუნქციონირება ქსელური და ინფორმაციული უსაფრთხოების ევროპულმა სააგენტომ (ENISA)[42]. სააგენტოს მიზანია ევროკავშირის ფარგლებში ელექტრონული ქსელების უსაფრთხოების მაღალი დონის მიღწევა;
- ტელემეტრიის ტრანსევროპული სამთავრობოთაშორისო სამსახური (TESTA)[43]. ეს არის სამთავრობოთაშორისო კავშირის ქსელი, რომელიც მოქმედებს მხოლოდ ევროკავშირის ფარგლებში. ის არ არის ჩართული ინტერნეტ - სივრცეში და სხვადასხვა უწყების თანამდებობის პირებს ერთმანეთთან ურთიერთობისას, ინფორმაციის დაზიანებისა და გადინების თავიდან აცილების საშუალებას აძლევს;

ინფორმაციული უსაფრთხოების სფეროში ევროკავშირის სამეცნიერო - კვლევითი პროექტები:

- ინფორმაციული საზოგადოების ტექნოლოგიები (პროექტები FP6[44] და FP7[45]);
- უსაფრთხოების პრობლემების ევროპული სამეცნიერო - კვლევითი პროგრამა (ESRP)[46];

[40] The Availability and Robustness of Electronic Communications Infrastructures file:///C:/Users/Admin/Downloads/StudyFinalReport.pdf
[41] The Critical Infrastructure Warning Information Network https://ciwin.europa.eu/Pages/Home.aspx
[42] The European Union Agency for Network and Information Security https://www.enisa.europa.eu/
[43] The European Software Testing Awards http://www.softwaretestingawards.com/
[44] http://ec.europa.eu/research/fp6/index_en.cfm
[45] http://ec.europa.eu/research/fp7/index_en.cfm
[46] http://www.statewatch.org/Targeted-issues/ESRP/security-research.html

- კრიტიკული ინფორმაციული ინფრასტრუქტურის პრობლემების სამეცნიერო - კვლევითი საკოორდინაციო პროექტი (CI2RCO)[47];
- ინფრასტრუქტურისა და პროექტირების არქიტექტურა[48].

ინფორმაციული უსაფრთხოების საკითხებში ევროკავშირის სამართლებრივ - ნორმატიული ბაზა:

- მონაცემთა დაცვის დირექტივა (1995 წელი)[49];
- ელექტრონული ხელმოწერის დირექტივა (1999 წელი)[50];
- ელექტრონული კავშირების სფეროში კონფიდენციალობის დაცვის დირექტივა (2002 წელი)[51];
- ჩარჩო დირექტივა (2002 წელი)[52];
- ინფორმაციულ სისტემებზე შეტევის საბჭოს ჩარჩო გადაწყვეტილება (2005 წელი)[53];
- მონაცემთა შენახვის დირექტივა (2006 წელი).

უსაფრთხოებისა და ექსტრემალური რეაგირების ფორუმი (FIRST)[54]

ფორუმი დაფუძნდა 1990 წელს და წარმოადგენს ინფორმაციული უსაფრთხოების სფეროში ინციდენტებზე ექსტრემალური რეაგირების სპეციალისტების მსოფლიოში არსებულ ერთადერთ საერთაშორისო ფორუმს. ეს ორგანიზაცია წარმოადგენს ქსელებში ექსტრემალური რეაგირების სფეროში მსოფლიოში აღიარებულ ლიდერს და აერთიანებს ოპერატიული რეაგირების ჯგუფებს, რომლებიც მუშაობენ სხვადასხვა უწყებრივ დონეებზე, როგორც სახელმწიფო ისე კერძო სექტორში, მათ შორის საგანმანათლებლო დაწესებულებებში. ფორუმის საქმიანობა მიმართულია ინციდენტების აღკვეთის

[47] ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/security/ci2rco-executive-summary_en.pdf
[48] http://www.service-architecture.com/articles/cloud-computing/infrastructure_as_a_service_iaas.html
[49] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 24 October 1995 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
[50] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 13 December 1999 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:en:HTML
[51] http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_en.htm
[52] http://europa.eu/legislation_summaries/information_society/legislative_framework/l24216a_en.htm
[53] http://europa.eu/legislation_summaries/information_society/internet/l33193_en.htm
[54] The Forum of Incident Response and Security Teams http://www.first.org/

გაძლიერებასა და კოორდინირებულ თანამშრომლობაზე, ასევე სწრაფი რეაგირების სფეროში შესაძლებლობების გაძლიერებაზე. ფორუმი მის წევრებსა და ზოგადად საზოგადოებას შორის ინფორმაციისა და გამოცდილების გაცვლის საშუალებას იძლევა.

რეზუმე

წინამდებარე კვლევაში განხილული იყო საქართველოსთვის პოტენციურად და სტრატეგიულად პარტნიორი ქვეყნებისა და ორგანიზაციების ზოგადი მიმოხილვა.

საქართველოს ეროვნული უსაფრთხოების კონცეფციის მიხედვით, რუსეთი და მისი ქმედებები ისევ წარმოადგენს საფრთხეს ქვეყნის ეროვნული უსაფრთხოებისთვის, მათ შორის კიბერსივრცის დაცულობის მიმართულებითაც. ასევე შეიძლება მომავალში საფრთხის შემცველი გახდეს სომხეთი და ირანი, რომლებიც მოიაზრებიან რუსეთის სტრატეგიულ მოკავშირეებად და გააჩნიათ თავისი მუდმივი ინტერესები სამხრეთ კავკასიაში. შესაბამისად, მოცემული ქვეყნები შეიძლება განხილულ იქნას როგორც პოტენციური მოწინააღმდეგეები კიბერ სივრცის დაცულობის მიმართულებითაც[55]. ასევე საფრთხედ შეიძლება შეფასდეს კვლევაში მოყვანილი ჰაკერული დაჯგუფებები და ორგანიზაციები „ახლო აღმოსავლეთის კიბერ არმია“ (the Middle Eastern Cyber Army - MECA), Fallaga Hackers Team და Cyber Caliphate, „სირიის ელექტრონული არმია“ (SEA).

იგივე კონცეფციიდან და ქვეყნის საგარეო პოლიტიკიდან გამომდინარე, საქართველოს სტრატეგიულ პარტნიორებად ითვლებიან შეერთებული შტატები, უკრაინა და თურქეთი[56]. ასევე ევროკავშირი და მისი ზოგიერთი წევრი ქვეყანა, და ჩრდილოეთ ატლანტიკური ხელშეკრელუბის ორგანიზაცია, რომლის სრულუფლებიანი წევრობისკენ მიისწრაფვის ქვეყანა.

[55] სომხეთი კიბერუსაფრთხოების თვალსაზრისით წარმოადგენს ნაკლებად საინტერესო ქვეყანას, ვინაიდან მისი კიბერსივრცის დაცულობა და ამ მიმართულებით აქტიურობა დიდად არის დამოკიდებული რუსეთზე

[56] კიბერუსაფრთხოების მიმართულებით, თურქეთი და უკრაინა ნაკლებად შეიძლება მოვიაზროთ სტრატეგიული პარტნიორობის ფარგლებში

კიბერუსაფრთხოების სფეროში სტრატეგიული თანამშრომლობა შესაძლებელია განხორციელდეს შეერთებულ შტატებთან, ესტონეთთან და დიდ ბრიტანეთთან. ამ უკანასკნელთან მსგავსი სახის თანამშრომლობა მიზანშეწონილია წარიმართოს სამეცნიერო - კვლევითი ცენტრებისა და საგანმანათლებლო პროგრამების ფარგლებში, ასევე ამ მიმართულებით გადმოღებული იქნას დიდი ბრიტანეთის კიბერუსაფრთხოების განვითარების როგორც ერთერთი საუკეთესო გამოცდილების მქონე ქვეყნის მოდელი, რომელიც ერთერთ დახვეწილ და სრულყოფილ მოდელად არის მიჩნეული.

მნიშვნელოვანია ესტონეთთან თანამშრომლობა, ვინაიდან ქვეყანამ მოკლე დროში შეძლო განევითარებინა კიბერუსაფრთხოების სფერო და გახდა ერთერთი მოწინავე ევროკავშირისა და ალიანსის წევრ ქვეყნებს შორის, და მათი გამოცდილება იქნება მნიშვნელოვანი საქართველოს თავდაცვაში კიბერუსაფრთხოების განვითარების მიმართულებით. კიბერუსაფრთხოების სფეროში ესტონეთი არის ერთერთი ძირითადი კონტრიბუტორი როგორც ალიანსში, ისე ევროკავშირში.

შეერთებულ შტატებსა და საქართველოს შორის 2009 წლის 9 იანვარს ხელი მოეწერა ქარტიას სტრატეგიული პარტნიორობის შესახებ[57], სადაც შედის ასევე თანამშრომლობა თავდაცვისა და უსაფრთხოების სფეროებში[58]. ქარტიის ფარგლებში და მის საფუძველზე შეერთებულ შტატებთან სტრატეგიული თანამშრომლობა მიზანშეწონილია განვითარდეს ნატოსთან თავსებადი კიბერუსაფრთხოების განვითარების გზით. კერძოდ, დარგში არსებული სისტემებისა და ტექნოლოგიების[59] მოწოდება/დანერგვის მიმართულებით, აუცილებელი სასწავლო პროგრამებითა[60] და კონსულტაციებით.

[57] http://www.civil.ge/geo/article.php?id=20340

[58] საქართველოსა და შეერთებულ შტატებს შორის მოქმედებს ბევრი სხვა სამართლებრივი დოკუმენტი თავდაცვის სფეროში თანამშრომლობის თაობაზე

[59] მაგალითისთვის, FireEye და C4ISR სისტემები, რომლითაც ასევე NATO - ს ბევრი წევრი ქვეყანა სარგებლობს

[60] ISACA - ს სერტიფიცირებული კურსები

კვლევაში მოცემულია სამი ქვეყანა, რომლებთანაც სტრატეგიულ დონეზე თანამშრომლობა დადებითი შედეგების მომტანი იქნება კიბერთავდაცვის სფეროს განვითარებისთვის, თუმცა ასევე შესაძლებელი და აუცილებელია თანამშრომლობა ევროკავშირისა და ალიანსის სხვა წევრ - ქვეყნებთანაც.

საერთაშორისო დონეზე თანამშრომლობა არის ერთერთი ძირითადი პირობა და საწინდარი კიბერუსაფრთხოების დარგის განვითარებისთვის. ამიტომ აუცილებელია პარტნიორული ურთიერთობები ევროკავშირის ფარგლებში მოქმედ ორგანიზაციებთან[61], ასევე სხვადასხვა პროექტებში ჩართულობა[62].

[61] მაგალითად, ENISA; FIRST
[62] მაგალითად, ESRP; CIWIN; CI2RCO და სხვა

ირანის კიბერუსაფრთხოების შესაძლებლობები. ორგანიზაციები

შესავალი

ირანი წარმოადგენს ერთერთ მთავარ მოთამაშეს კიბერსივრცესა და მასთან დაკავშირებულ საკითხებში. საქართველოსა და ირანს შორის ამ ეტაპზე არის ნორმალური ურთიერთობები, რომელიც სავაჭრო - ეკონომიურს არ სცილდება და ქვეყანა არ შეიძლება მივიჩნიოთ პირდაპირ საფრთხედ.

ირანის კიბერშესაძლებლობები არსებული მდგომარეობით არის ერთერთი ძლიერი მთელს მსოფლიოში. ირანელმა ჰაკერებმა შეძლეს განეხორციელებინათ მთელი რიგი კიბერ შეტევები დასავლეთის საბანკო და საფინანსო ინსტიტუტებზე, ასევე ისრაელისა და საუდის არაბეთის ენერგეტიკულ სექტორზე. მსგავსი შეტევების უმეტესობამ შეძლო გარკვეული ზიანის მიყენება და მათი აღმოჩენა გახდა შეუძლებელი ჰაკერთა სხვა ჯგუფების მხრიდან.

ირანის კიბერ დოქტრინა, სტრატეგია და მიზნები

ირანის კიბერ ოპერაციები ხორციელდება იმ რწმენით, რომ „კიბერ სივრცე არის the Hidden Imam - ის (შიიტების დოქტრინის ცენტრალური სწავლება) ფაქტიური არენა“. ირანის კიბერ დოქტრინა ძირითადად ეყრდნობა ასიმეტრიული ომის ტაქტიკას, რომელიც განისაზღვრება როგორც კონფლიქტი, სადაც ორი მოწინააღმდეგე მხარის რესურსები, ტაქტიკა და ბრძოლის არსი თვისობრივად და არსებითად განსხვავდება ერთმანეთისგან. ამავდროულად, ცდილობენ გამოიყენონ მოწინააღმდეგე მხარისთვის დამახასიათებელი სუსტი და ადვილად მოწყვლადი ადგილები.

ასეთი მიდგომა მოიცავს არასტანდარტული ომის წარმოების ტაქტიკასა და სტრატეგიას, ანუ გამოიყენონ ისეთი სტრატეგია, რომელიც გაუკეთებს კომპენსირებას როგორც არსებულ რაოდენობრივ, ისე ხარისხობრივ დეფიციტს. ჰაკერული ჯგუფების აქტიური გამოყენებითა და მათი წახალისებით ხდება არასაკმარისი სამხედრო ძალის

გარკვეული ბალანსი, რაც ირანის სტრატეგიის ასიმეტრიულობის მთავარი განმსაზღვრელი ფაქტორია.

გარდა ამისა, კიბერ ოპერაციებში ფსიქოლოგიური ასპექტების გამოყენება წარმოადგენს ასევე ასიმეტრიული ბრძოლის ტაქტიკას, რასაც ხელს უწყობს ირანის ხელისუფლება. ბოლო პერიოდში საგრძნობლად მოიმატა რეჟიმის მხარდამჭერი ჰაკერული ჯგუფების აქტიურობამ, რაც უკავშირდება საერთაშორისო დაძაბულობის შესუსტების მიზნით ქვეყნის ხელისუფლების განცხადებას, ინტერნეტ სივრცეზე კონტროლის შესუსტების თაობაზე.

ეს არის ირანის კიბერ დოქტრინისა და სტრატეგიის მთავარი არსი. დოქტრინა ასევე შეიცავს შემდეგ ძირითად ასპექტებს:

- ირანის ინფრასტრუქტურის დაცვა და თავდაცვითი შესაძლებლობების განვითარება;
- შიდა ოპოზიციის შეზღუდვა/ჩახშობა და ოპერატიული შესაძლებლობების განვითარება;
- დასავლეთის კიბერ აქტივებისა და შესაძლებლობების წინააღმდეგ თავდასხმითი შესაძლებლობების განვითარება;
- დასავლეთის გავლენის აღმოფხვრა.

ირანის კიბერ სტრუქტურა

ირანის კიბერ ძალების სტრუქტურა არის დახვეწილი და რთულად აღსაქმელი. სტრუქტურაში შემავალ წევრებსა და რგოლებს შორის კავშირსა და კომუნიკაციაზე არსებული კონტროლის დონე და უსაფრთხოების ზომები იმდენად მაღალია, რომ ჰაკერთა უმრავლესობამ არც კი იცის, რომ ისინი მუშაობენ ირანის ხელისუფლებაზე. ირანელი ჰაკერების შემოქმედებითობა, ნიჭი და უნარ - ჩვევები იმდენად მაღალია, რომ ექსპერტებმა ისინი შეადარეს მათ კოლეგებს შეერთებული შტატებიდან, რუსეთიდან და ისრაელიდან.

უმაღლესი სახელმწიფო ორგანო, რომელიც დაკავებულია კიბერსივრცის საკითხებით, არის ახლად შექმნილი „კიბერსივრცის უმაღლესი საბჭო (High Council of Cyberspace)“. საბჭოში შედიან ირანის უმაღლესი ხელისუფლების წარმომადგენლები:

- პარლამენტი;
- ქვეყნის პრეზიდენტი;
- სასამართლო ხელისუფლების ხელმძღვანელი;
- სახელმწიფო მედია საშუალებების ხელმძღვანელი;
- დაზვერვის მინისტრი;
- მეცნიერების მინისტრი;
- კულტურის მინისტრი;
- ინფორმაციული და კომუნიკაციების ტექნოლოგიების მინისტრი;
- Hamid Shahriari - ირანის კომპიუტერული კვლევების ცენტრის პრეზიდენტი (სპეციალური სტატუსი, ექვემდებარება უშუალოდ აიათოლას ინსტიტუტს).

აიათოლა ალი ჰომეინის პირადი ბრძანებით, საბჭო შეიქმნა 2012 წელს და მისი მიზანია ქვეყანაში კიბერსივრცის განვითარება და ამ მიმართულებით აქტიური პოლიტიკის წარმოება. ყველა ირანული ორგანიზაცია, რომლებიც ახორციელებენ კიბერ ოპერაციებს, ექვემდებარებიან საბჭოს და მუშაობენ მის ფარგლებში.

ინფორმაციული და კომუნიკაციების ტექნოლოგიების სამინისტროში შედის ინფორმაციული უსაფრთხოების ცენტრი (Center for Information Security - MAHER), რომელსაც ასევე ეძახიან ირანის CERT - ს (დანართი 1).

საინტერესო და მნიშვნელოვანია ირანის შეიარაღებული ძალების გენერალური შტაბი, სადაც სტრუქტურულად გაერთიანებულია ის ორგანიზაციები, რომლებიც პასუხისმგებელნი არიან კიბერსივრცის დაცვაზე და ასევე თავადაც ახორციელებენ კიბერ შეტევებს (დანართი 2).

შეიარაღებული ძალების გენერალურ შტაბში შედის სამოქალაქო თავდაცვის ორგანიზაციისა (the Passive Civil Defense Organization) და ისლამური რევოლუციის მცველები (the Pasdaran) კიბერ ერთეულები. სამოქალაქო თავდაცვის ორგანიზაცია (the Passive Civil Defense Organization) ასრულებს თავდაცვით როლს ირანის ქსელის დაცვაში და ის თავის მხრივ შეიცავს the Cyber Defense Command - ს და the Gerdab, რომელიც პასუხისმგებელი იყო 2009 წელს ირანში პოლიტიკური არეულობის მხარდამჭერთა გამოვლენასა და დაშინებაზე.

ისლამური რევოლუციის მცველები (the Pasdaran) არის ირანში არსებული რეჟიმის ძირითადი დასაყრდენი ძალა და ის არაოფიციალურად ექვემდებარება აიათოლას ინსტიტუტს. The Pasdaran - ის კიბერშესაძლებლობა არის საკმაოდ ძლიერი, კერძოდ ის შეიცავს შემდეგ კიბერ ერთეულებს:

- ირანის კიბერ არმია (Iran's Cyber Army - ICA), რომელიც ცნობილია როგორც ჰაკერთა ჯგუფი;
- The Karbala Mazandaran Cyber Culture Forces, რომელიც ასევე წარმოადგენს ჰაკერთა ჯგუფს;
- სირიელ სამხედროებთან ოპერირების ჯგუფი Iranian - Syrian joint Signals Intelligence (SIGINT);
- The Basij Paramilitary Force:
    - Cyber Police (FETA/FATA);
    - Basij Cyber Council;
    - Dr. Hassan Abbasi – Director of Basij Cyber Council.

გარდა ამისა, ირანში ასევე ფუნქციონირებს ე. წ. დამოუკიდებელ ჰაკერთა ჯგუფები, რომლებიც ასევე ისლამური რევოლუციის მცველების (the Pasdaran) არაპირდაპირი ხელმძღვანელობის ქვეშ საქმიანობენ, კერძოდ:

- Ashiyane;
- Shabgard;
- Parastoo;

- Izz ad Din al – Qassam;
- Islamic Cyber Resistance Group - ICR.

ირანის სამხედრო ჩინოვნიკები და უმაღლესი ხელისუფლების წარმომადგენლები ღიად აცხადებენ, რომ ყველა ეს ორგანიზაცია აქტიურად არის ჩართული კიბერ შეტევების ოპერაციებში.

The Karbala Mazandaran Cyberculture Forces

ეს არის ოფიციალური სტრუქტურული ორგანო, რომელიც აკონტროლებს კულტურულ და რელიგიურ საკითხებს კიბერსივრცეში. ამავდროულად, ორგანიზაცია თავადაც ეწევა შემტევით და ჰაკერულ საქმიანობას.

ირანის კიბერ არმია (Iran's Cyber Army - ICA)

ეს არის ჰაკერთა ჯგუფი, რომელიც შედგება ინფორმაციული ტექნოლოგიების მაღალი დონის სპეციალისტებისგან და პროფესიონალი ჰაკერებისგან, რომელთა ვინაობა უცნობია. ჯგუფი ოფიციალურად არსად არ არის რეგისტრირებული და ფაქტიურად, მის საქმიანობაზე არავინ არ იღებს პასუხისმგებლობას. მიუხედავად ამისა, არსებობს დამტკიცებული ფაქტები, რომ ICA შეიქმნა ისლამური რევოლუციის მცველების (the Pasdaran) მიერ 2005 წელს და კავშირშია ქვეყნის შეიარაღებულ ძალებთან.

ეს თავდასხმები ძირითადად ხორციელდება ირანის საზღვრებს გარედან, კერძოდ, დიდი ბრიტანეთიდან, ჩინეთიდან, პაკისტანიდან და საუდის არაბეთიდან.

The Basij Paramilitary Force

ორგანიზაცია არის გასამხედროებული და იმყოფება ისლამური რევოლუციის მცველების (the Pasdaran) მეთაურობის ქვეშ. ის თავისთან აერთიანებს Cyber Police - ს (FETA/FATA) და Basij Cyber Council - ს. FETA/FATA ეხმარება არსებულ რეჟიმს კიბერ კანონების დაცვასა და დასავლური გავლენის განდევნისგან. ის ასევე სუსტი და მოწყვლადი მხარეების გამოსავლენად, აკეთებს სამთავრობო საიტების სკანირებასა და

იდენტიფიცირებას, ფილტრავს ელ. ფოსტას „არასასურველი“ წერილებისგან და შეტყობინებებისგან.

Basij - ის კიბერ შესაძლებლობები შეიცავს:

- სატელიტური ჩახშობა;
- სოციალური ქსელებისა და ზოგადად ინტერნეტის ცენზურა;
- კიბერ პოლიციის ერთეული;
- პროპაგანდა და დეზინფორმაცია;
- სოციალური მედიისა და სხვა საიტების ფილტრაცია.

The Basij Cyber Council - ი ოპერირებს Dr. Hassan Abbasi - ს ხელმძღვანელობით და ის ეწევა უნივერსიტეტებიდან ახალგაზრდა, ნიჭიერი და პროფესიონალი კადრების მოზიდვასა და რეკრუიტს. ირანის ხელისუფლება დიდ ყურადღებას უთმობს პროფესიულ განვითარებას და პერსპექტიულ ახალგაზრდებს უქმნიან ყველა საჭირო პირობას მუშაობისთვის და სწავლისთვის.

The Cyber Defense Command

გაერთიანებულია შეიარაღებული ძალების სამოქალაქო თავდაცვის ორგანიზაციაში (the Passive Civil Defense Organization). ის პასუხისმგებელია ქვეყნის ქსელების, მასთან დაკავშირებული ინფრასტრუქტურისა და კომპიუტერული სისტემების უსაფრთხოებაზე, ასევე იცავს მონაცემთა ბაზებს არასანქცირებული შეღწევისგან.

Ashiyane

ონლაინ სივრცეში პირველად გამოჩნდა 2003 წელს. ჯგუფს აქვს თავისი კომპანია Ashiyane Security Center, თავისი ვებ - გვერდი ashiyanehost.com და ტრენინგ პორტალი. მის სამიზნეს წარმოადგენს როგორც კერძო, ისე სახელმწიფო სექტორი. ჯგუფის ლიდერია Behrouz Kamalian.

Elecomp Expo – ზე ჯგუფმა მოიპოვა აღიარება და მიიღო ჯილდოები. Elecomp Expo კომპიუტერებისა და ელექტრონული სისტემების გამოფენა ირანში.

Islamic Cyber Resistance Group (ICR)

ეს ჯგუფი ახალია, ის მხოლოდ გასულ წელს გამოჩნდა. ჯგუფი თავის საქმიანობას ახორციელებს ალჟირიდან, საუდის არაბეთიდან და ირანიდან. მისი მოტივაცია ეფუძნება ისლამურ იდეოლოგიას. სამიზნეს წარმოადგენს დასავლეთისა და ისრაელის კომპანიები. ჯგუფი აქტიურად თანამშრომლობს სირიის ელექტრონულ არმიასთან, რომელთანაც ერთად აქტიურად იყენებს ფსიქოლოგიური ოპერაციების ტაქტიკას.

Parastoo

ჯგუფის სახელი სპარსულად ნიშნავს „პატარა ჩიტს“. ჯგუფს აქვს კავშირები ისლამური რევოლუციის მცველებთან (the Pasdaran) და Hezbollah - სთან. ის ასევე შემჩნეულია ირანის ელიტარულ სპეციალური დანიშნულების ძალებთან Quds Force - თან (ექვემდებარება აითოლას ინსტიტუტს) კავშირებში.

კიბერ შეტევების ანალიზი აჩვენებს, რომ ჯგუფი თავის შეტევებს გეგმავს და ახორციელებს Iranian Cyber Army - თან ერთად.

ჯგუფის საიტი parastoo.ir, რომელიც ამჟამად მიუწვდომელია, რეგისტრირებულია Zohre Sajadian - ის მიერ, რომელიც ასევე ფლობს საიტს hackers4hire.ir და უსაფრთხოების ფორუმს rce.ir.

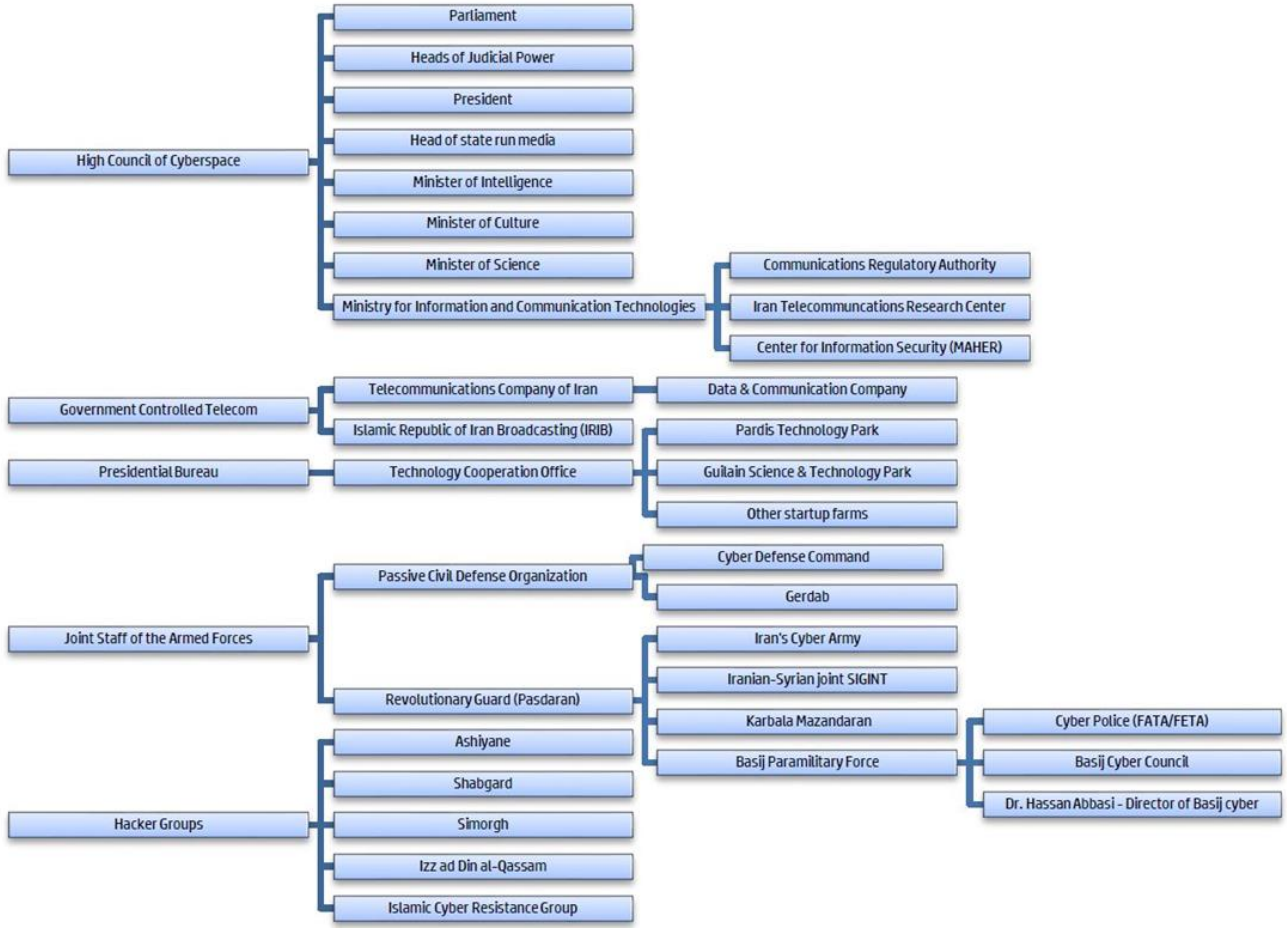
Shabgard

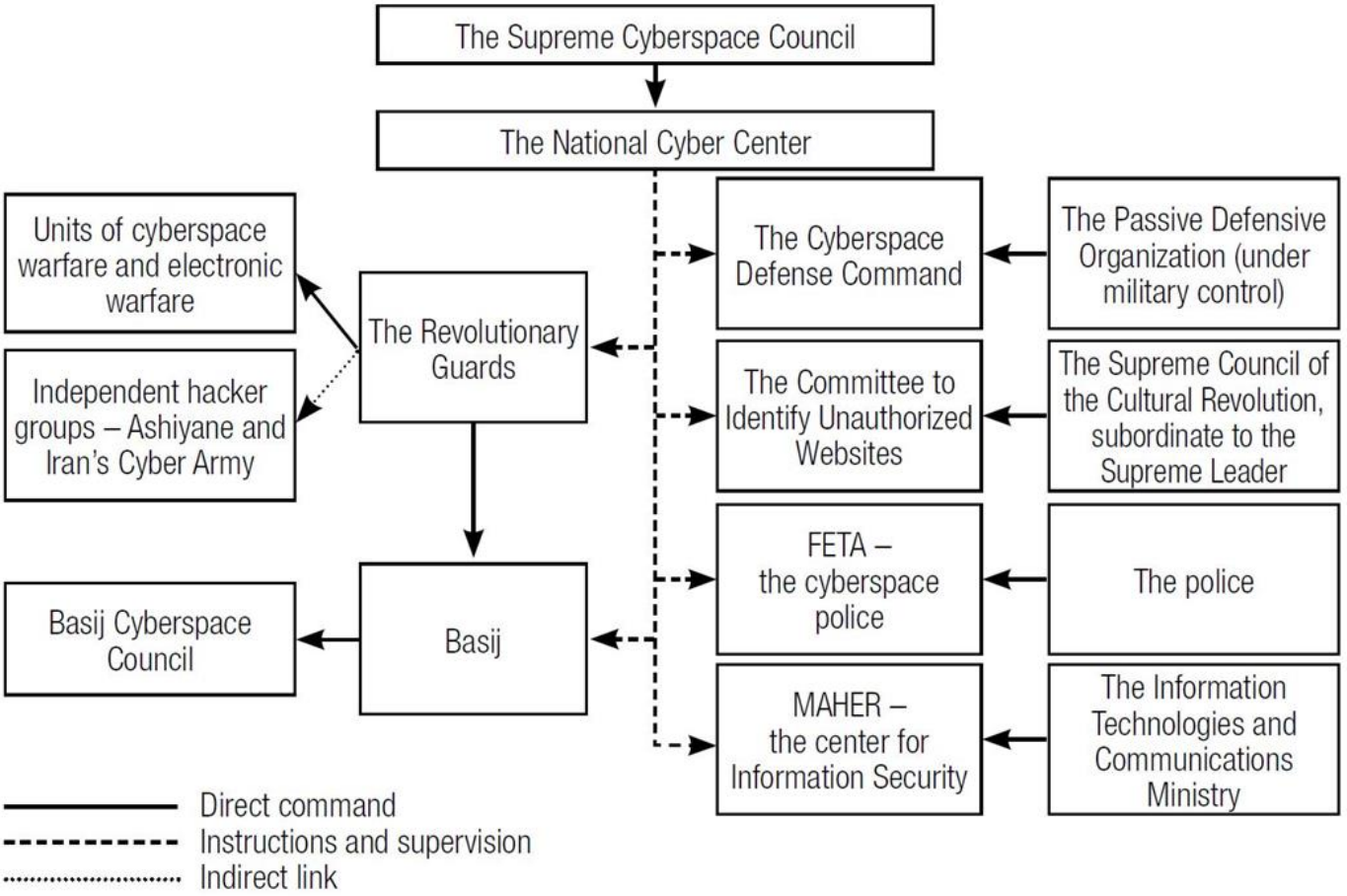
ჯგუფის სახელი სპარსულად ნიშნავს „შავ მცველს“. მისი საიტი შეიქმნა 2003 წელს, თუმცა ჯგუფის საქმიანობა, ტაქტიკა, მეთოდები და პროცედურები, ისევე როგორც თვდასხმის სამიზნეები ცნობილი არ არის. არსებობს ვარაუდი, რომ ჯგუფი აწარმოებს ჰაკერთა ტრენინგებს საიტის Webamooz.ir პორტალის საშუალებით. ტრენინგები მოიცავს penetration testing, application security, Android programming,

networking, Debian Linux administration, PHP, Perl for penetration testers, and Python. საიტი სთავაზობს ასევე შეუერთდნენ ირანის ერთერთ პრესტიჟულ უნივერისტეტს Shahid Beheshti University, სადაც ისწავლება კომპიუტერული მეცნიერებები და ინჟინერია. 2011 წელს facebook - ზე გაჩნდა ინფორმაცია, რომ ჯგუფი მონაწილეობას მიიღებდა Elekomp Expo - ში.

დანართი 1

Iranian cyber organizational chart




The Supreme Cyberspace Council
The National Cyber Center
Units of cyberspace warfare and electronic warfare
Independent hacker groups – Ashiyane and Iran's Cyber Army
The Revolutionary Guards
Basij
Basij Cyberspace Council
The Cyberspace Defense Command
The Passive Defensive Organization (under military control)
The Committee to Identify Unauthorized Websites
The Supreme Council of the Cultural Revolution, subordinate to the Supreme Leader
FETA – the cyberspace police
The police
MAHER – the center for Information Security
The Information Technologies and Communications Ministry
Direct command
Instructions and supervision
Indirect link

ორგანიზაციები

ბოლო დროს კიბერსივრცეში განვითარებული მოვლენები ნათლად აჩვენებს, რომ სულ უფრო აქტიურად ხდება ჰაკერული დაჯგუფებების გამოყენება ტერორისტული ორგანიზაციებისა და მათთან ასოცირებული კერძო პირების მიერ, წარმოებს მათი არასანქცირებული შეღწევა და ჰაკერული თავდასხმები სახელმწიფო თუ კერძო სექტორის ვებ - გვერდებზე, რაც პირდაპირ საფრთხეს უქმნის როგორც ცალკეულ ორგანიზაციებსა და მომხმარებლებს, ისე მთლიანად საერთაშორისო, რეგიონალურ თუ ეროვნულ უსაფრთხოებას. ვითარებას კიდევ უფრო ართულებს ის გარემოება, რომ დანაშაულებრივ ქმედებებში გამოიყენება უახლესი კომპიუტერული და პროგრამული ტექნოლოგიების მიღწევები.

სირიის ელექტრონული არმია Syrian Electronic Army (SEA)

სირიის ელექტრონული არმია (SEA), რომელსაც ასევე უწოდებენ სირიის კიბერ არმიას (the Syrian Cyber Army), შეიქმნა 2011 წელს. ეს არის არაბულ სამყაროში პირველი ვირტუალური საჯარო არმია (http://sea.sy/index/en), რომლის სამიზნეებია ქვეყნის პოლიტიკური ოპოზიციის წარმომადგენლებისა და დასავლური ვებ - გვერდები. მისი მიზანია ასადის რეჟიმის მხარდაჭერა და სახელისუფლებო პროპაგანდის გავრცელება როგორც ქვეყნის შიგნით, ისე ქვეყნის გარეთ, რისთვისაც აქტიურად გამოიყენება სოციალური ქსელები, სხვადასხვა ბლოგები, კორპორატიული და სახელმწიფო აქაუნტები. SEA ბაზირებს სირიაში, საიდანაც ძირითადად აწარმოებს თავის საქმიანობას. თუმცა, ზოგიერთი კიბერ შეტევა არმიის სახელით, განხორციელდა სირიის საზღვრის გარედანაც.

აღსანიშნავია, რომ SEA - ს საშუალებით, ონლაინ რეჟიმში სოციალური ქსელების გამოყენებით, წარმოებს „მოხალისეთა“ დაქირავებისა და მათი გადაბირებითი სამუშაოები.

SEA აქტიურად თანამშრომლობს ირანის შეიარაღებულ ძალებთან, ისლამის რევოლუციის მცველებთან და ჰაკერულ დაჯგუფებებთან. ამის ერთერთი მაგალითია the Iran-Syria joint Signal Intelligence (SIGINT) პროგრამა, სადაც ასევე ჩართულია

Hezbollah. არმიის სისტემის სარეზერვო ფაილი შეიცავს კოდს cker.ir, რომლის მფლობელია ირანელი ჰაკერი Mormoroth - ი.

სირიის ელექტრონული არმია (SEA) ამ ეტაპზეც აგრძელებს თავის აქტიურ ჰაკერულ საქმიანობას.

The Cyber Caliphate

The Cyber Caliphate უკავშირდება ე. წ. „ისლამურ სახელმწიფოს“(ISIS). თუმცა მის შესახებ ბევრი რამ ცნობილი არ არის. მაგრამ ზოგიერთის ვარაუდით, მოცემული ჰაკერული დაჯგუფების ერთერთი ლიდერი არის არაბული წარმოშობის, დიდი ბრიტანეთის მოქალაქე Junaid Hussain, რომელიც ერთხელ იყო უკვე დაპატიმრებული გაერთიანებული სამეფოს ყოფილი პრემიერ - მინისტრის ტონი ბლერის Gmail - ის ანგარიშის დაჰაკერების გამო. ის ასევე დაკავშირებული იყო ჰაკერთა ჯგუფთან Team Poison, რომელთა მტკიცებით, მათ აქვთ არასანქცირებული წვდომა Blackberry - სა და NATO - ს ქსელებთან, ასევე გაერთიანებული არიან “Anonymous” - თან, საბანკო ანგარიშებზე შეღწევის მიზნით.

სხვა წყაროების მიხედვით, Junaid Hussain ახორციელებს ციფრული სფეროს ექსპერტების გადაბირებას სირიისა და ე. წ. „ისლამური სახელმწიფოსთვის“ (ISIS). მოცემული მიმართულების ანალიზი ნათლად აჩვენებს, რომ Cyber Caliphate არის სწრაფად მზარდი ჰაკერული ორგანიზაცია და ექპერტებს მიაჩნიათ, რომ მისი შესაძლებლობები უახლოეს მომავალში გაცილებით დიდი იქნება. ბოლო ერთ თვეში Cyber Caliphate - მა ორჯერ დააჰაკერა Albuquerque Journal - ის, New Mexico’s Mountain View Telegraph - ისა და მერილანდის WBOC 16 TV - ს ვებ - გვერდები, ასევე Twitter. Cyber Caliphate - მა ამა წლის 12 იანვარს ერთმანეთის მიყოლებით განახორციელა რამოდენიმე კიბერშეტევა შეერთებული შტატების ცენტრალური სარდლობის Twitter - ისა და YouTube - ს ანგარიშებზე.

ახლო აღმოსავლეთის კიბერ არმია (the Middle Eastern Cyber Army - MECA)

ახლო აღმოსავლეთის კიბერ არმია (the Middle Eastern Cyber Army - MECA) წარმოადგენს სრულიად უცნობ ჰაკერულ დაჯგუფებას, რომელიც ასპარეზზე გამოჩნდა გასული 2014 წლის 23 სექტემბერს, როცა მან განახორციელა ჰაკერული თავდასხმები აშშ - ს კიბერსივრცეზე. არ არსებობს არავითარი ინფორმაცია იმის შესახებ, თუ ვინ შეიძლება იდგეს MECA - ს უკან. თუმცა შეიძლება ითქვას, რომ ეს შეიძლება იყოს როგორც რომელიმე ტერორისტული დაჯგუფება ან სახელმწიფო, ისე კერძო პირი. თუმცა ზოგიერთი ანალიტიკოსის ონფორმაციით MECA შეიძლება ბაზირებდეს ან სირიაში, ან მავრიტანიაში. ორგანიზაციის საქმიანობის მიზნებიდან და ტაქტიკიდან გამომდინარე, ის უნდა იყოს დაკავშირებული სირიის ელექტრონულ არმიასთან (SEA) და ირანის ჰაკერულ ჯგუფებთან, საიდანაც უნდა წარმოებდეს MECA - ს კიბერ ოპერატორების მართვა, დავალებების მიცემა, კოორდინაცია და წვრთნა.

ბიბლიოგრაფია

1) Threat Intelligence Briefing Episode, by HP Security Research, February 2014;
2) Iran and Cyberspace Warfare, by Gabi Siboni and Sami Kronenfeld, Military and Strategic Affairs, Volume 4, No. 3, December, 2012;
3) Iran's Emergence as a Cyber Power, by Fareed Zakariaa, August 20, 2014;
4) Cybersecurity and Stability in the Gulf, by James Andrew Lewis, CSIS, January 2014;
5) პარიზის ტერაქტი და ახალი გამოწვევები კიბერსივრცეში, ვლადიმერ სვანაძე, http://zeti.ge/menu_id/27/id/778/, 21 იანვარი, 2015;
6) http://www.zone-h.org/;
7) https://www.fireeye.com/.

რუსეთის კიბერუსაფრთხოების შესაძლებლობები

შესავალი

საქართველოს ეროვნული უსაფრთხოების კონცეფციის მიხედვით, ქვეყნისთვის დიდი საფრთხის შემცველია რუსეთი და მისი ქმედებები. 2014 წლის კვლევების მიხედვით, მსოფლიოში კიბერშეტევებში ერთერთ მთავარ მოთამაშედ, ისევე როგორც 2013 წელს, დასახელებული არის რუსეთი.

რუსეთში ინფორმაციული უსაფრთხოების სფეროში მთავარ ორგანიზაციებად ითვლება უშიშროების საბჭო, უშიშროების ფედერალური სამსახური (ФСБ), დაცვის ფედერალური სამსახური, ტექნიკისა და ექსპერტის კონტროლის ფედერალური სამსახური, თავდაცვისა და ინფორმაციული ტექნოლოგიებისა და კავშირგაბმულობის სამინისტროები.

თითოეულ დასახელებულ ორგანიზაციულ უწყებას გააჩნია თავისი კომპეტენციის ფარგლები და დაკისრებული პასუხისმგებლობა. კერძოდ, უშიშროების საბჭო განსაზღვრავს ინფორმაციულ სფეროში რუსეთის ეროვნულ ინტერესებს, ობიექტებს, სუბიექტებსა და სხვა რესურსებს, რომლებიც უნდა იყოს დაცული, ასევე კოორდინირებას უწევს ინფორმაციული უსაფრთხოების სტრატეგიის დამუშავებას. უშიშროების ფედერალური სამსახური (ФСБ) პასუხისმგებელია რუსეთის ფედერაციის უსაფრთხოებასა და კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის უზრუნველყოფაზე. კონტრდაზვერვის სამსახურში ფუნქციონირებს კომპიუტერული და ინფორმაციული უსაფრთხოების სამმართველო, რომელიც ასევე კურირებს ჰაკერთა დაჯგუფებებს.

იგივე უშიშროების ფედერალური სამსახური (ФСБ) აწარმოებს ინფორმაციული უსაფრთხოების სფეროში სახელმწიფოს სამეცნიერო - ტექნიკური პოლიტიკის დაგეგმვასა და რეალიზებას, უზრუნველყოფს კომპიუტერული ქსელების კრიპტოგრაფიულ და საინჟინრო - ტექნიკურ დაცვას, იცავს სახელმწიფო

საიდუმლოებასა და კავშირგაბმულობის ყველა სახეობას. დაცვის ფედერალური სამსახურის შემადგენლობაშია ინფორმაციისა და სპეციალური კავშირების სამსახური, რომელმაც 2003 წლის შემდეგ აიღო იმ ფუნქციების დიდი ნაწილი, რომელიც ადრე შედიოდა ინფორმაციისა და სამთავრობო კავშირების ფედერალური სააგენტოს (ФАПСИ) კომპეტენციაში.

ФАПСИ - ს დანარჩენი ფუნქციები გადანაწილდა თავდაცვის სამინისტროს შეიარაღებული ძალების გენერალური შტაბის, უშიშროებისა (ФСБ) და დაცვის ფედერალურ სამსახურებს შორის. ტექნიკისა და ექსპერტის კონტროლის ფედერალური სამსახური იმყოფება თავდაცვის სამინისტროს დაქვემდებარებაში. მოცემული სამსახურის კომპეტენციის ფარგლებში შედის უცხოეთის სახელმწიფოების ტექნიკურ ჯაშუშობასთან ბრძოლა, საიდუმლო ინფორმაციის დაცვა და კომპიუტერული ქსელებისა და სისტემების უსაფრთხოების უზრუნველყოფა. ინფორმაციული ტექნოლოგიებისა და კავშირგაბმულობის სამინისტრო რეალიზებას უკეთებს სახელმწიფო პოლიტიკასა და ახორციელებს ზედამხედველობას კავშირგაბმულობის სექტორში.

რუსეთის ინფორმაციული უსაფრთხოების სტრატეგია

გასული 2014 წლის იანვარში, რუსეთის ფედერალურმა საბჭომ ფართო განხილვისათვის წარმოადგინა „რუსეთის ფედერაციის კიბერუსაფრთხოების სტრატეგიის კონცეფცია“, რომელიც მიმართულია თანამედროვე ინფორმაციულ სამყაროში ახალი საფრთხეების განსაზღვრაზე. კონცეფციამ დარგის ექსპერტთა შორის გამოიწვია აზრთა სხვადასხვაობა, თუმცა მათ მიერ ჩამოყალიბებულ იქნა საერთო რეკომენდაციები, კერძოდ:

1) ინფორმაციული უსაფრთხოების არსებულ ტერმინოლოგიასთან კიბერუსაფრთხოებისა და კიბერსივრცის თანხვედრი ტერმინოლოგიის შემუშავება;
2) კიბერსივრცის დაცვის კომპლექსური სისტემების შემუშავება;

3) კიბერსივრცის მოდელისა და იმ ძირითადი ფაქტორების შემუშავება, რაც გავლენას ახდენს მის ფუნქციონირებაზე. ასევე სავარაუდო საფრთხეების მათემატიკური მოდელების შექმნა;
4) კიბერსივრცის მდგრადობის უზრუნველყოფის სპეციალური მეთოდების შექმნა:
   - კრიპტოგრაფიული დაცვის ახალი მეთოდების რეალიზება;
   - ტოპოლოგიური სტრუქტურის ანალიზი და შესაბამისი რეკომენდაციების შემუშავება;
   - სპეციალური პროცედურების გამოყენებით ინფორმაციული უსაფრთხოების მეთოდების შემუშავება;
5) კიბერუსაფრთხოების უზრუნველყოფის ინტელექტუალური მეთოდები, კერძოდ:
   - მომხმარებლის ინტელექტუალური იდენტიფიკაცია;
   - ინტელექტუალური მეთოდებით ვირუსებისა და სხვა შეტევების გაუვნებელყოფა;
   - არასანქცირებული შეღწევისა და შეტევის გამოვლენის ინტელექტუალური მეთოდები;
   - ინფორმაციული უსაფრთხოების მდგომარეობის ანალიზი;
   - ნეიროქსელურ ტექნოლოგიებზე დაფუძნებული კრიპტოგრაფიული დაცვის ახალი მეთოდები.

თავად სტრატეგიის მიზანს წარმოადგენს საგარეო და საშინაო პოლიტიკაში პრიორიტეტების, პრინციპებისა და ღონისძიებების სისტემების განსაზღვრის საფუძველზე პიროვნების, ორგანიზაციებისა და სახელმწიფოს კიბერუსაფრთხოების უზრუნველყოფა.

სტრატეგიის <u>პრიორიტეტებია</u>:

1) ეროვნული სისტემებისა და ქსელების დაცვის განვითარება;
2) კრიტიკული ინფორმაციული ინფრასტრუქტურის სანდოობის განვითარება და მუდმივი განახლება;

3) კიბერსივრცეში სახელმწიფო რესურსების უსაფრთხოების უზრუნველყოფის სრულყოფის ღონისძიებების გატარება;
4) კიბერუსაფრთხოების სფეროში სახელმწიფო, კერძო სექტორისა და სამოქალაქო საზოგადოების საპარტნიორო მექანიზმების შემუშავება;
5) კიბერსივრცეში უსაფრთხო ქცევის კულტურის შემუშავება და მოქალაქეთა ცნობიერების ამაღლება;
6) გლობალურ დონეზე კიბერუსაფრთხოების ამაღლების მიზნით საერთაშორისო თანამშრომლობის განვითარება.

კიბერუსაფრთხოების სტრატეგიას საფუძვლად უდევს შემდეგი ძირითადი პრინციპები:

1) ინფორმაციის მიღებისა და გამოყენების სფეროში ადამიანისა და მოქალაქის კონსტიტუციური უფლებებისა და თავისუფლების გარანტიის პრინციპი;
2) კიბერსივრცეში პიროვნებისა და ორგანიზაციების მაქსიმალური დაცულობის პრინციპი;
3) კიბერუსაფრთხოების უზრუნველყოფის ფარგლებში, ინფორმაციული საზოგადოების ყველა სუბიექტის (პიროვნება, კერძო და სახელმწიფო სექტორი) კონსტრუქციული თანამშრომლობის პრინციპი;
4) კიბერუსაფრთხოების მოთხოვნების დაცვაზე დადგენილი პასუხისმგებლობის ბალანსის შენარჩუნების პრინციპი;
5) საფრთხეების პრიორიტეტების განსაზღვრის პრინციპი;
6) კიბერუსაფრთხოების უზრუნველყოფის საშუალებებისა და მეთოდების სისტემური აქტუალიზაციის პრინციპი.

კონცეფციის მიხედვით, რუსეთის კიბერუსაფრთხოებითი უზრუნველყოფა უნდა განხორციელდეს შემდეგი მიმართულებებით:

1) კიბერუსაფრთხოების უზრუნველყოფაზე საერთო სისტემური ზომების მიღება;
2) კიბერუსაფრთხოების უზრუნველყოფაზე სამართლებრივ - ნორმატიული ბაზისა და სამართლებრივი ღონისძიებების სრულყოფა;

3) კიბერუსაფრთხოების სფეროში სამეცნიერო - კვლევითი სამუშაოების წარმოება;
4) კიბერუსაფრთხოების უზრუნველყოფის საშუალებების შემუშავებისთვის, წარმოებისა და გამოყენებისთვის პირობების შექმნა;
5) საკადრო და საორგანიზაციო ღონისძიებების სრულყოფა;
6) ადგილობრივი და საერთაშორისო თანამშრომლობის ორგანიზება;
7) კიბერსივრცეში უსაფრთხო ქცევის კულტურის ფორმირება და განვითარება.

ექსპერტთა აზრით, 2014 და 2015 წელი კიბერუსაფრთხოების სფეროში, რუსეთისთვის იქნება გადამწყვეტი პერიოდი, რომლის დროსაც გამოიკვეთება სახელწიფო პოლიტიკის ახალი დოქტრინალური საფუძვლები და საგარეო კონტურები, ასევე სტარტს აიღებს ახალი გრძელვადიანი პროგრამები და პროექტები. იგივე ექსპერტები ვარაუდობენ, რომ ამ პერიოდში ძალზედ მოწყვლადი იქნება რუსეთის კიბერსივრცე, რომელიც გარკვეული რისკების შემცველია ქვეყნის ეროვნული უსაფრთხოებისთვის. შეიძლება ითქვას, რომ კიბერუსაფრთხოების პოლიტიკა რუსეთში კრიზისულ ფაზაში შედის, თუმცა მიიჩნევენ, რომ ეს იქნება პოზიტიური პროცესის დასაწყისი.

კონცეპტუალური შეხედულებები რუსეთის შეიარაღებული ძალების ინფორმაციულ სივრცეში მოქმედებებზე

რუსეთის შეიარაღებული ძალების მოღვაწეობას ინფორმაციულ სივრცეში საფუძვლად უდევს შემდეგ <u>პრინციპთა ერთობლიობა:</u>

1) <u>კანონიერება</u> - მოითხოვს რუსეთის კანონმდებლობის, აგრეთვე აღიარებული და არსებული საერთაშორისო სამართლის ნორმების დაცვას. ყველა გადაწყვეტილებას დაკავშირებულს აქტიურ მოქმედებებთან ქვეყნის შიგნით თუ მის ფარგლებს გარეთ იღებს რუსეთის პრეზიდენტი. საერთაშორისო სამართლის თანახმად, რუსეთის შეიარაღებული ძალები გლობალურ ინფორმაციულ სივრცეში აღიარებს შემდეგ ნორმებსა და პრინციპებს:
   - სახელმწიფო სუვერენიტეტის პატივისცემა;
   - სხვა სახელმწიფოების საშინაო საქმეებში ჩაურევლობა;

- ძალისა და შეტევითი ღონისძიებების გამოუყენებლობა;
- ინდივიდუალურ და კოლექტიურ თავდაცვაზე უფლება.

2) პრიორიტეტულობა - წარმოებს საფრთხეების შესახებ აქტუალური და სანდო ინფორმაციის შეგროვება, მისი ოპერატიულ დონეზე დამუშავება, ღრმა ანალიზი, რეალიზაცია და დაცვითი ღონისძიებების დროული განხორციელება. მოცემული პროცესის ერთობლიობა ქმნის არმიის ეფექტური მართვის ხელსაყრელ გარემო პირობებს.
3) კომპლექსურობა - ინფორმაციულ სივრცეში მოიცავს შტაბებისა და შენაერთების ისეთი ღონისძიებების ერთობლიობას, როგორებიცაა სამხედრო დაზვერვა, ოპერატიული შენიღბვა, რადიოელექტრონული ბრძოლა, კავშირგაბმულობა, ავტომატიზირებული მართვა, შტაბების ინფორმაციული მუშაობა, აგრეთვე საკუთარი ინფორმაციული სისტემების დაცვა.
4) ურთიერთქმედება - ინფორმაციულ სივრცეში თავისი ქმედებები თავდაცვის სამინისტრომ უნდა შეუთანხმოს აღმასრულებელი ხელისუფლების სხვა ფედერალურ სამსახურებსა და ორგანოებს.
5) თანამშრომლობა - მოითხოვს მეგობარ ქვეყნებთან და საერთაშორისო ორგანიზაციებთან თანამშრომლობას.
6) ინოვაცია - რუსეთის შეიარაღებული ძალებისგან მოითხოვს ინფორმაციულ სივრცეში გამოიყენოს მოწინავე ტექნოლოგიები, საშუალებები და მეთოდები. ასევე ინფორმაციული უსაფრთხოების ამოცანების გადაწყვეტის პროცესში მოიზიდოს მაღალკვალიფიციური პირადი შემადგელობა.

შეიარაღებული ძალები ინფორმაციულ სივრცეში თავისი ამოცანების გადაჭრისას ხელმძღვანელობს კიბერ კონფლიქტების შეკავების, აღკვეთისა და გადაჭრის უფლებათა ერთობლიობით. კერძოდ, შეკავებისა და აღკვეთის უფლებები მოიცავს:

- შეიარაღებულ ძალებში ინფორმაციული უსაფრთხოების სისტემების განვითარება;

- ინფორმაციული უსაფრთხოების ძალებისა და საშუალებების მუდმივი მზადყოფნა;
- პრიორიტეტულ საფუძვლებზე თანამშრომლობის განვითარება კოლექტიური უსაფრთხოებისა და შანხაის ორგანიზაციების ქვეყნებთან, ასევე დსთ - ს წევრ - ქვეყნებთან. აგრეთვე, პარტნიორი ქვეყნების წრის გაფართოება და თანამშრომლობის განვითარება;
- ინფორმაციულ სივრცეში არსებული და აღიარებული საერთაშორისო ნორმების საფუძველზე გლობალური ინფორმაციული უსაფრთხოების უზრუნველყოფა;
- კიბერ კონფლიქტების აღმოცენებისა და ესკალაციის ფაქტორების დადგენა და მათზე კონტროლის დაწესება;
- კიბერ კონფლიქტის საერთაშორისო დონეზე გავრცელების აღკვეთა;
- კიბერ კონფლიქტების ფაქტორების ნეიტრალიზაცია და მათი კონსტრუქციული თანამშრომლობის პირობებში გადაყვანა;
- საჯაროდ, ობიექტურად და დროულად მსოფლიო საზოგადოების ინფორმირება და მიზეზების განმარტება.

ინფორმაციულ სივრცეში კონფლიქტების გადაჭრა:

- მშვიდობიანი საშუალებები;
- კონფლიქტის ესკალაციისა და მისი კრიზისულ ფაზაში გადასვლის შემთხვევაში, ინდივიდუალური და კოლექტიური თავდაცვითი ძალების გამოყენება;
- ინდივიდუალური და კოლექტიური თავდაცვის ფარგლებში საპასუხო დარტყმის პოტენციალის განსაზღვრა;
- ინდივიდუალური და კოლექტიური თავდაცვის ინტერესებიდან გამომდინარე ინფორმაციული უსაფრთხოების უზრუნველყოფის მიზნით, საკუთარი ძალებისა და საშუალებების განლაგება უცხო ქვეყნის ტერიტორიაზე, ამ უკანასკნელთან შესაბამისი შეთანხმების საფუძველზე;

- კონფლიქტის მსვლელობისას ქვეყნისა და საერთაშორისო მასობრივი საინფორმაციო საშუალებების მუდმივი ინფორმირება.

ინფორმაციულ სივრცეში რუსეთის შეიარაღებული ძალები მუდმივად ცდილობენ ნდობითი ღონისძიებების გამყარებას. კერძოდ:

- ინფორმაციულ სივრცეში უსაფრთხოების უზრუნველსაყოფად ეროვნული კონცეფციების გაცვლა;
- ინფორმაციულ სივრცეში კრიზისული მოვლენებისა და საფრთხეების, და მათი ნეიტრალიზაციის შესახებ ოპერატიული ინფორმაციის გაცვლა;
- ინფორმაციულ სივრცეში მოღვაწეობის შესახებ კონსულტაციები, და თანამშრომლობა კონფლიქტების მოგვარების სფეროში.

თანამედროვე პირობებში რუსეთის შეიარაღებული ძალების თავდაცვისუნარიანობა ბევრად არის დამოკიდებული ინფორმაციულ სივრცეში მათ ეფექტურ მოქმედებაზე. შეიარაღებული ძალები გეგმავენ გადაჭრან მათ წინაშე არსებული ამოცანები თავდაცვისა და უსაფრთხოების უზრუნველყოფაზე, ინფორმაციულ სივრცეში შეიარაღებული ძალების მოქმედების ძირითადი პრინციპებისა და უფლებების გამოყენებით.

მოცემული კონცეპტუალური შეხედულებების რეალიზებისას, რუსეთის შეიარაღებული ძალები მაქსიმალურად გამოიყენებს ინფორმაციულ სივრცეს შემდეგი მიმართულებებით:

- ქვეყნის თავდაცვისუნარიანობის გასაძლიერებლად;
- სამხედრო კონფლიქტების შეკავებისა და აღკვეთისათვის;
- სამხედრო თანამშრომლობის განვითარებისათვის;
- საერთაშორისო საზოგადოების ინტერესებიდან გამომდინარე, გლობალური ინფორმაციული უსაფრთხოების სისტემის ფორმირებისათვის.

შეიარაღებული ძალები, სპეციალური სამსახურები და ინფორმაციული უსაფრთხოება

2010 წლის თებერვალში, რუსეთის ფედერაციამ გამოუშვა თავისი ახალი სამხედრო დოქტრინა, სადაც განხილულია პოლიტიკური და საინფორმაციო საშუალებების გამოყენება მიმართული რუსეთისა და მისი მოკავშირეების ეროვნული ინტერესების დაცვაზე. დოქტრინა განსაზღვრავს თანამედროვე სამხედრო კონფლიქტისთვის დამახასიათებელ თავისებურებებს, რაც მოიცავს სამხედრო ძალებისა და საინფორმაციო ომის წარმოების კომპლექსურ ერთობლიობას. ფაქტიურად, დოქტრინა შეიცავს კიბერუსაფრთხოების გააქტიურების საშუალებებს.

2012 წლის მარტის თვეში, დიმიტრი როგოზინმა გააკეთა განცხადება შეიარაღებულ ძალებში შეერთებული შტატების მსგავსი (U.S.CYBERCOM) „კიბერ სარდლობის“ შექმნაზე, რაც პრაქტიკულად ნიშნავს ინფორმაციული უსაფრთხოების საკითხებში სპეციალურ სამსახურებზე სრულ დომინირებას. აქვე უნდა ითქვას, რომ ადრე თავდაცვის სამინისტროს პრიორიტეტულ ამოცანებში ეს საკითხები არ შედიოდა. იმავე წლის ბოლოსთვის დასრულდა არაკომერციული სტრუქტურის პერსპექტიული კვლევების ფონდის შექმნა, რომლის ბიუჯეტი განისაზღვრა 3 მილიარდი რუბლით. ფაქტიურად, ფონდის შექმნა განხორციელდა დაჩქარებული წესით.

საინტერესოა, რომ 2012 წლის ოქტომბერში, თავდაცვის სამინისტრომ სტრატეგიული ინიციატივების სააგენტოსთან, რუსეთის განათლებისა და მეცნიერების სამინისტროსთან და პროგრამირებისა და კომპიუტერული ტექნოლოგიების სფეროში წამყვან უმაღლეს სასწავლებელთან (МГТУ им. Баумана) ერთად საფუძველი ჩაუყარა ყოველწლიურ კონკურსს (უკვე გამოცხადებულია 2015 – 2016 წლებზე), რომლის მთავარი თემა იყო ანტივირუსული სისტემების გვერდის ავლის საშუალებები და მეთოდები, ასევე ქსელის დაცვა. არსებობს მოსაზრება, რომ ამ კონკურსის ფარგლებში წარმოებს საბრძოლო შემტევი ვირუსების შემუშავება. ეს კარდინალურად ცვლის სურათს დაკავშირებულს კიბერ დაპირისპირების სფეროში თავდაცვითი სტრატეგიის შესახებ, რაც სამხედრო დოქტრინით არის გაწერილი.

საყურადღებოა ის ფაქტი, რომ 2013 წლის 13 თებერვალს რუსეთის შეიარაღებული ძალების გენერალურ შტაბში შეიქმნა რამოდენიმე ახალი ნახევრად საიდუმლო სტრუქტურა, რომლებიც პასუხისმგებელნი არიან ინფორმაციულ უსაფრთხოებაზე, რაც მიანიშნებს შეიარაღებული ძალების გააქტიურებას დაკავშირებულს კიბერსივრცესთან და მის დაცულობასთან. არსებული ინფორმაციით, ახლადშექმნილი სტრუქტურები ამუშავებენ ასევე შემტევ ვირუსებს და მათი თანამშრომლების ნაწილს შეადგენს ზემოთნახსენები კონკურსის მონაწილეები.

მიუხედავად თავდაცვის სამინისტროს მზარდი ინტერესისა სამხედრო - სტრატეგიული ხასიათის კიბერსაფრთხეებზე, რუსეთის სპეციალური სამსახურები (ФСБ, ФСО და ФСТЭК) მაინც ინარჩუნებენ წამყვან როლს ქვეყნის კიბერუსაფრთხოების უზრუნველყოფის საკითხებში. 2013 წლის 15 იანვარს, კასპერსკის ლაბორატორიის მიერ კიბერჯაშუშური ქსელის Red October - ის (არსებობს მოსაზრება, რომ ეს ქსელი მუშაობდა რუსეთის სპეციალური სამსახურების დავალებებზე) გახსნის შემდეგ რამოდენიმე დღეში, ვლადიმერ პუტინმა ხელი მოაწერა ბრძანებას, რომლის თანახმად რუსეთის ფედერალური უშიშროების სამსახურს (ФСБ) ავალდებულებს შექმნას სახელმწიფო სისტემები მიმართული ქვეყნის კრიტიკული ინფრასტრუქტურისა და მთლიანად კომპიუტერული ქსელის კიბერშეტევებისგან დაცვის უზრუნველყოფაზე. დარგის ექსპერტები მიიჩნევენ, რომ პუტინის ეს ბრძანება რუსეთის ინფორმაციული უსაფრთხოების პოლიტიკის განვითარებაში არის გადამწყვეტი მნიშვნელობის მქონე.

ამავდროულად, 2012 წლის ბოლოს, სენატორ რუსლან გატაროვის მიერ ინიცირებული წინადადება რუსეთის კიბერუსაფრთხოების სტრატეგიის კომპლექსური მიდგომის საკითხების შემუშავების შესახებ, არ წარმოადგენს პრიორიტეტულს, ვინაიდან რუსეთის ფედერაციის საბჭოს არ გააჩნია საჭირო კომპეტენცია მოცემული მიმართულებით.

საინტერესოა, რომ კიბერუსაფრთხოების საკითხის პარალელურ რეჟიმში განვითარება, მომავალში გამოიწვევს გარკვეულ დაპირისპირებას სამხედროებსა და სპეციალურ სამსახურებს შორის უფლებამოსილებების შესახებ. ეს პროცესი დიდ

გავლენას იქონიებს რუსეთის კიბერ სარდლობის ჩამოყალიბების საბოლოო შედეგზე, ვინაიდან ჯერ ბოლომდე არ არის გარკვეული მსგავსი სტრუქტურის შექმნით როგორ გადანაწილდება უფლებამოსილებები და პროცესში ჩართულობა, არ არსებობს ასევე სტრუქტურულ - ორგანიზაციული სქემა.

ქვეყნის ინფორმაციული უსაფრთხოების უზრუნველყოფაში ყველა სპეციალურ სამსახურს (ФСБ, ФСО და ФСТЭК) თავისი ინტერესი და ფუნქცია გააჩნია, რაც გარკვეულწილად ეწინააღმდეგება შეერთებული შტატების მსგავსი „კიბერ სარდლობის“ (U.S.CYBERCOM) შექმნის იდეასა და ინიციატივას, რომელიც თავის დროზე როგოზინმა წამოაყენა და მხარდაჭერილ იქნა როგორც ყოფილი მინისტრის სერდუკოვის, ისე ამჟამინდელი მინისტრის შოიგუს მიერ. ვერ ხერხდება ერთმანეთისგან სამხედროებისა და სპეციალური სამსახურების ფუნქციონალურ - სტრუქტურული გამიჯვნა. ფაქტიურად, რუსეთი კიბერუსაფრთხოების საერთო სტრატეგიის საკითხებში მიდის სამხედროებისა და სპეციალური სამსახურების სინქრონიზაციის პროცესისკენ, რაც გარკვეული რისკების შემცველი იქნება თავად ქვეყნისთვის, ვინაიდან დარგი დაუბრუნდება ძველ ჩარჩოებს, სადაც კიბერუსაფრთხოების თემას ექნება მეორეხარისხოვანი როლი საგარეო სტრატეგიული საფრთხეების შეფასებისას და ზოგადად, ეროვნული უსაფრთხოების საკითხებში.

მიუხედავად ზემოაღნიშნულისა, რუსეთის უშიშროების ფედერალური სამსახური (ФСБ) უკვე აქტიურად მუშაობს ქვეყნის ერთიანი სისტემის შექმნაზე, რომელიც მიმართული იქნება კიბერ შეტევების აღმოჩენასა და გაფრთხილებაზე. ასევე არაოფიციალური ინფორმაციით, ФСБ - ს 16 - ე დირექტორატის კონტროლის ქვეშ იმყოფება რუსეთის ჰაკერთა მთელი რესურსები. სამსახური აგრეთვე მუდმივად მუშაობს ჰაკერთა ახალი რესურსების მოძიებასა და თავის სასარგებლოდ პროცესში ჩართვაზე არა მარტო ქვეყნის შიგნით, არამედ უცხოეთშიც, რაშიც ასევე აქტიურად მონაწილეობს რუსეთის საგარეო დაზვერვის სამსახური (СВР).

განხორციელებული ცნობილი კიბერშეტევები

რუსეთის მიერ განხორციელებულ ცნობილ კიბერშეტევებს შეიძლება მივაკუთვნოთ:

1) 2007 წლის აპრილ - მაისში, რუსეთსა და ესტონეთს შორის არსებული დაპირისპირება გადაიზარდა სერიოზულ კიბერშეტევაში, რომლის დროსაც გარკვეული დროის განმავლობაში მიუწვდომელი იყო ესტონური ინტერნეტ რესურსები.
2) 2008 წლის აპრილში რუსეთის მხრიდან განხორციელდა მასირებული კიბერ შეტევა რადიო თავისუფალ ევროპასა და რადიო თავისუფლებაზე.
3) 2008 წლის ივნისსა და ივლისში ლიტვის კიბერსივრცეზე განხორციელებული კიბერშეტევები.
4) 2008 წლის ივლის - აგვისტოში რუსეთის მხრიდან მოხდა კიბერ შეტევა საქართველოს კიბერსივრცეზე, რაც ზოგიერთი ექსპერტების მიერ შეფასდა ასევე როგორც მასშტაბური ხასიათის „საინფორმაციო ომი“ მიმართული საქართველოს წინააღმდეგ.
5) 2008 – 2014 წლებში რუსეთის მხრიდან სისტემატურად ხორციელდებოდა კიბერშეტევა საქართველოს შინაგან და საგარეო საქმეთა სამინისტროების, აღმოსავლეთ ევროპის ქვეყნების სახელისუფლებო, სამხედრო წარმომადგენლობების, NATO - სა და OSCE - ს საიტებზე, რაც წარმოდგენილია ქვემოთ მოცემულ ცხრილში 1. ეს კიბერშეტევები ხორციელდებოდა რუსული ჰაკერული დაჯგუფება APT 28 - ის მიერ, რომელსაც არაოფიციალური ინფორმაციით, კოორდინაციას უწევს რუსეთის ფედერალური უშიშროების სამსახური (ФСБ). დაჯგუფებისთვის დამახასიათებელია ორშაბათიდან პარასკევის ჩათვლით, დილის 8 საათიდან საღამოს 6 საათამდე მუშაობა. პირველად APT 28 ეგონათ ჩინური წარმოშობის, მაგრამ შემდეგ ექსპეტთა უმრავლესობა დარწმუნდა, რომ APT 28 არის რუსული ჰაკერული დაჯგუფება, რომლის სავარაუდო ადგილმდებარეობაა სანქტ - პეტერბურგი;

6) 2011 – 2014 წლებში რუსეთის მხრიდან განხორციელდა პერმანენტული კიბერშეტევები შეერთებული შტატების თავდაცვისა და უსაფრთხოების სტრუქტურულ ქვედანაყოფებზე. მათ შორის იყო პენტაგონისა და ეროვნული უსაფრთხოების სააგენტოს (NSA) დეპარტამენტები მოცემული კიბერშეტევების დროს გამოყენებული იქნა მავნებლური პროგრამა (malware) "Uroburos", რომლის შესახებ პირველი განცხადება გააკეთა გერმანულმა უსაფრთხოების კომპანიამ G Data Security - მ;

7) შეერთებული შტატების ფედერალური საგამოძიებო ბიუროს (FBI) განცხადებით, 2014 წლის აგვისტოს შუა რიცხვებში განხორციელდა მასირებული შეტევა უმსხვილეს ბანკზე JPMorgan Chase & Co. - ზე. კიბერ შეტევის წყარო მოდიოდა რუსეთიდან.

დასკვნა

რუსეთი მსოფლიოს ინფორმაციულ სივრცეში წარმოადგენს ერთერთ მთავარ მოთამაშეს, რომელიც მუდმივად ანვითარებს თავის შესაძლებლობებს. ქვეყანას გააჩნია მუდმივი ინტერესები და მიზნები, რომელთა მიღწევისთვის ის სამხედრო და პოლიტიკური შესაძლებლობების პარალელურად სულ უფრო აქტიურად იყენებს ინფორმაციულ სივრცეს.

რუსეთში ინფორმაციული უსაფრთხოების მიმართულება ამ ეტაპზე იმყოფება ახლის ჩამოყალიბებისა და არსებულის რეფორმირების სტადიაში. ქვეყანაში ეს სფერო ისევ რჩება სპეციალური სამსახურების კონტროლის ქვეშ, რის პარალელურად იწყება დარგის განვითარება შეიარაღებულ ძალებში, სადაც უკვე არსებობს ნახევრად საიდუმლო ქვედანაყოფები, რომლებიც მუშაობენ არამარტო კიბერ შეტევის შეკავებასა და აღკვეთაზე, არამედ თავადაც ახორციელებენ კიბერ შეტევებს. რუსეთმა დაიწყო საკითხის მიმართ კომპლექსური მიდგომა, რაც ნიშნავს ნებისმიერი სამხედრო თუ სხვა სახის გააქტიურება (პოლიტიკური, ეკონომიკური, სოციალური) მიმდინარეობს

ინფორმაციულ სივრცეში შესაბამისი ღონისძიებების გატარებით, კიბერშეტევითი ოპერაციების ჩათვლით.

ზემოაღნიშნულიდან გამომდინარე, შეიძლება ზოგადად ჩამოვაყალიბოთ რუსეთის ინფორმაციული უსაფრთხოების პოლიტიკის შემდეგი <u>ძირითადი მიმართულებები:</u>

- ქვეყნის საერთო ქსელის, კრიტიკული ინფორმაციული ინფრასტრუქტურის, კომპიუტერული სისტემებისა და მომხმარებელთა დაცვა;
- სამართლებრივ - ნორმატიული ბაზისა და სამართლებრივი ღონისძიებების სრულყოფა;
- სამეცნიერო - კვლევითი სამუშაოების წარმოება, რაც ასევე მოიცავს სემინარების, კონფერენციებისა და კონკურსების ჩატარებას;
- კიბერუსაფრთხოების უზრუნველყოფის ტექნოლოგიური საშუალებების შემუშავებისთვის, წარმოება/დანერგვისა და გამოყენებისთვის საჭირო პირობების შექმნა;
- საკადრო პოლიტიკის განვითარებისა და საორგანიზაციო ღონისძიებების სრულყოფა;
- ადგილობრივი კერძო სექტორის წარმომადგენლებთან და საერთაშორისო დონეზე თანამშრომლობის ორგანიზება და გაფართოება;
- ინფორმაციულ სივრცეში მომხმარებელთა უსაფრთხო ქცევის კულტურის ფორმირება და განვითარება;
- შეიარაღებულ ძალებში ინფორმაციული უსაფრთხოების სისტემების განვითარება;
- ინფორმაციული უსაფრთხოების ძალებისა და საშუალებების მუდმივი მზადყოფნა.

საქართველოს ეროვნული უსაფრთხოების კონცეფციის თანახმად, რუსეთი ისევ წარმოადგენს საფრთხეს საქართველოს სუვერენიტეტისთვის და მისი ეროვნული

უსაფრთხოებისთვის. ასევე რუსეთის შემტევითი აქტიურობა ინფორმაციულ სივრცეში გარკვეული საფრთხის შემცველია საქართველოს კიბერსივრცისთვის. სტატისტიკა აჩვენებს, რომ საქართველოს კიბერსივრცე არის ერთერთი პრიორიტეტული რუსი ჰაკერული დაჯგუფებებისთვის, რომელთა ძირითად ობიექტებს წარმოადგენს არამარტო სამთავრობო, არამედ ასევე კერძო თუ სამოქალაქო სექტორის საიტები. მსგავსი კიბერ შეტევების ძირითადი მოტივი არის სამუშაო პროცესის პარალიზება და ინფორმაციის შეგროვება.

ცხრილი 1

Malware	Targeting	Russian Attributes
Evolves and Maintains Tools for Continued, Long-Term Use • Uses malware with flexible and lasting platforms • Constantly evolves malware samples for continued use • Malware is tailored to specific victims' environments, and is designed to hamper reverse engineering efforts • Development in a formal code development environment **Various Data Theft Techniques** • Backdoors using HTTP protocol • Backdoors using victim mail server • Local copying to defeat closed/air gapped networks	**Georgia & the Caucasus** • Ministry of Internal Affairs • Ministry of Defense • Journalist writing on Caucasus issues • Kavkaz Center **Eastern European Governments & Militaries** • Polish Government • Hungarian Government • Ministry of Foreign Affairs in Eastern Europe • Baltic Host exercises **Security-related Organizations** • NATO • OSCE • Defense attaches • Defense events and exhibitions	**Russian Language Indicators** • Consistent use of Russian language in malware over a period of six years • Lure to journalist writing on Caucasus issues suggests APT28 understands both Russian and English **Malware Compile Times Correspond to Work Day in Moscow's Time Zone** • Consistent among APT28 samples with compile times from 2007 to 2014 • The compile times align with the standard workday in the UTC + 4 time zone, which includes major Russian cities such as Moscow and St. Petersburg

წყარო: Chart by FireEye

ბიბლიოგრაფია

1) Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space, by NATO Research Center, February, 2014;
2) "Information Troops" – a Russian Cyber Command?, by Keir Giles, Conflict Studies Research Centre Oxford, UK, 2013;
3) "The Battlefield On Your Laptop", K. Mshvidobadze, Radio Free Europe/Radio Liberty 21 March 2011;
4) "Russian Views on Information-based Warfare", by T.L. Thomas, Foreign Military Studies Office (FMSO), July 1996;
5) "Electronic Warfare", US Joint Publication 3-13.1;
6) http://www.dia.mil/News/SpeechesandTestimonies/ArticleView/tabid/11449/Article/570863/statement-for-the-record-worldwide-threat-assessment.aspx
7) КОНЦЕПЦИЯ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ, Проект, 2014;
8) Киберпространство. Американская и российская концепции, Фатех Вергасов, 2013;
9) INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS, by Eneken Tikk, Kadri, Kaska, Liis Vihul, 2010;
10) https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf.

დიდი ბრიტანეთის კიბერშესაძლებლობები

2009 წელს[63] მიღებული კიბერუსაფრთხოების სტრატეგია ხაზს უსვამს კიბერუსაფრთხოების უზრუნველყოფის საკითხთან კომპლექსური მიდგომის აუცილებლობას, რომლის რეალიზაციაში უნდა მონაწილეობდნენ სახელმწიფო სუბიექტები, მრეწველობის ყველა დარგის წარმომადგენლები, სამოქალაქო საზოგადოებრივი ორგანიზაციები და საერთაშორისო პარტნიორები.

სტრატეგია ითვალისწინებს ორი ახალი ორგანიზაციის შექმნას[64]. პირველ რიგში ეს არის მინისტრთა კაბინეტის სტრუქტურაში შემავალი კიბერუსაფრთხოების სამმართველო (OCS)[65], რომელიც უზრუნველყოფს სტრატეგიულ ხელმძღვანელობასა და უწყებათაშორის დონეზე შეთანხმებულ მოქმედებას. ის იქნება ასევე დაკავებული კიბერდანაშაულის შესახებ საკოორდინაციო საქმიანობით. ამასთან ერთად გამოყენებული იქნება არსებული შესაძლებლობები, რომელიც გააჩნია თავდაცვის სამინისტროს, სადაზვერვო სამსახურებს და პოლიციას (ლონდონის პოლიციის ელექტრონულ დანაშაულებებთან ბრძოლის განყოფილება, ინტერნეტის ქსელის დაცვისა და ბავშვთა ექსპლუატაციის წინააღმდეგ ქმედებების ცენტრი, ასევე განსაკუთრებით საშიში და ორგანიზებული დანაშაულის სააგენტო). მეორე, ეს არის კიბერუსაფრთხოების ოპერატიული ცენტრი (CSOC), რომელიც ფუნქციონირებს სახელმწიფო კავშირგაბმულობის შტაბის[66] ბაზაზე ქ. ჩელტენჰემში. ეს არის ახალი ცენტრი, სადაც თავმოყრილია სხვადასხვა უწყებების არსებული ფუნქციები კიბერსივრცის მდგომარეობის მონიტორინგისა და ღონისძიებების კოორდინაცია ექსტრემალურ რეაგირებაზე. ცენტრი ასევე გააკეთებს ანალიზს იმ საფრთხეებზე, რომელიც ემუქრება დიდი ბრიტანეთის კომპიუტერულ ქსელებსა და მათ

[63] 2011 წელს მოხდა სტრატეგიის განახლება https://www.cpni.gov.uk/advice/cyber/cir/
[64] ორივე ორგანიზაციამ დაიწყო ფუნქციონირება 2010 წელს;
[65] https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance
[66] http://www.gchq.gov.uk/Pages/homepage.aspx

მომხმარებლებს, გამოიმუშავებს შესაბამის რეკომენდაციებსა და საინფორმაციო სახელმძღვანელოებს.

ეროვნული ინფრასტრუქტურის დაცვის ცენტრის (CPNI)[67] შემადგენლობაშია კომპიუტერების დახმარების სასწრაფო სამსახური (CERT Service)[68].

გაერთიანებული სამეფოს მიდგომა ასევე მიმართულია კიბერუსაფრთხოების განვითარებაზე. სტრატეგიის მთავარი მიზანია გაიყვანოს დიდი ბრიტანეთი მოწინავე პოზიციებზე ინფორმაციული და სატელეკომუნიკაციო ტექნოლოგიების სფეროში ინოვაციების, ინვესტიციებისა და ხარისხიანი მომსახურების მიხედვით. ასევე მთლიანად ისარგებლოს კიბერსივრცის ყველა უპირატესობებითა და მიღწევებით. 2011 წელს შემოღებული სტრატეგია ასახავს მაქსიმალური რისკების შემცირებას დამნაშავეთა (მათ შორის ტერორისტების) და სხვა სახელმწიფოთა მხრიდან კიბერშეტევების მიმართ, რაც მიმართულია კიბერსივრცეში თითოეული მოქალაქის, საზოგადოებისა და ეკონომიკის უსაფრთხოებისკენ.

2014 წლის დეკემბერში[69] პრემიერ - მინისტრის ოფისმა გამოაქვეყნა მოხსენება კიბერუსაფრთხოების სფეროში მიმდინარე სამუშაოებისა და მომავალი გეგმების შესახებ. ეს წარმოადგენს 2011 წლის სტრატეგიის მხარდამჭერ დოკუმენტს, სადაც ასახულია სტრატეგიის მიზნების განხორციელების გზები და საშუალებები, კერძოდ:

- დიდი ბრიტანეთი გახდეს მსოფლიოში ერთერთი უსაფრთხო ადგილი კიბერსივრცეში ბიზნესის საწარმოებლად;
- დიდი ბრიტანეთი გახდეს უფრო სტაბილური კიბერშეტევების მიმართ და უკეთ დაიცვას ქვეყნების ინტერესები კიბერსივრცეში;
- ღია, გამჭვირვალე და სტაბილური კიბერსივრცის ფორმირება, რომელიც მხარს უჭერს ღია საზოგადოებას;

[67] http://www.cpni.gov.uk/Templates/CPNI/pages/Default.aspx
[68] https://www.cpni.gov.uk/advice/cyber/cir/
[69] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf

- დიდ ბრიტანეთში კიბერუსაფრთხოების ცოდნის, უნარებისა და შესაძლებლობების გაზრდა.

მოცემული მიზნების მისაღწევად დიდი ბრიტანეთის მთავრობა მუშაობს კიბერუსაფრთხოების ეროვნული პროგრამის[70] ფარგლებში, კერძოდ:

- უმაღლესი კლასის კიბერ საფრთხეების აღმოჩენისა და აღმოფხვრის მიზნით, ეროვნული შესაძლებლობების შემდგომი განმტკიცება;
- კიბერდანაშაულის დაძლევისა და ინტერნეტში ბიზნესის საწარმოებლად აუცილებელი ნდობის შენარჩუნების მიზნით, სამართალდამცავი ორგანოების უნარებისა და შესაძლებლობების გაზრდა;
- დიდი ბრიტანეთის კრიტიკული სისტემებისა და ქსელების უზრუნველყოფა სანდოობითა და სტაბილურობით;
- კიბერ ცნობიერებისა და ბრიტანული ბიზნესის რისკების მართვის გაუმჯობესება;
- საზოგადოების წევრების თავის დაცვასა და მათ მიერ მოხმარებული სერვისების კიბერუსაფრთხოების შესახებ ცნობიერების ამაღლების უზრუნველყოფა;
- კიბერუსაფრთხოების მიმართულებით სამეცნიერო კვლევებისა და განათლების გაძლიერება, მაღალკვალიფიცირებული კადრების ყოლა და ახალ ტექნოლოგიებზე მუშაობის მუდმივი პროცესის უზრუნველყოფა;
- საერთაშორისო პარტნიორებთან მუდმივი მუშაობა და მათთან საერთაშორისო დიალოგის წარმოება, რაც ხელს შეუწყობს ღია, დინამიური და უსაფრთხო კიბერსივრცის ჩამოყალიბებას.

მოცემული სამუშაოები ტარდება კიბერუსაფრთხოების ეროვნული პროგრამის (the National Cyber Security Programme (NCSP)) მხარდაჭერით. პროგრამის მიზნობრივი დაფინანსება მომავალი ორი წლის განმავლობაში შეადგენს 860 მილიონ ფუნტ სტერლინგს. პროგრამის მიზანია ხელი შეუწყოს ისეთ პროექტებს, რომლებიც განავითარებენ კიბერუსაფრთხოების შესაძლებლობებს და სტიმულს მისცემენ დიდი ბრიტანეთის კიბერუსაფრთხოების ბაზარს.

[70] the National Cyber Security Programme (NCSP)

მინისტრთა კაბინეტის ოფისსა და ეროვნული უსაფრთხოების საბჭოს მხარდამჭერია კიბერუსაფრთხოებისა და ინფორმაციული უზრუნველყოფის ოფისი[71], რომელიც მთავრობისთვის უზრუნველყოფს კიბერუსაფრთხოების სტრატეგიულ მიმართულებასა და კოორდინაციას უწევს პროგრამებს. ოფისის ხელმძღვანელია James Quinault და ის მუშაობს სხვა სახელმწიფო დეპარტამენტებთან და სააგენტოებთან, კერძოდ:

- მთავარი ოფისი[72];
- თავდაცვის სამინისტრო[73];
- სამთავრობო კავშირის მთავარი ოფისი[74];
- კომუნიკაციებისა და ელექტრონული უსაფრთხოების დეპარტამენტი[75];
- ეროვნული ინფრასტრუქტურის დაცვის ცენტრი[76];
- საგარეო და ბრიტანეთის თანამეგობრობის ოფისი[77];
- ბიზნესის, ინოვაციებისა და უნარების დეპარტამენტი[78].

საერთაშორისო ურთიერთობების ფარგლებში დიდი ბრიტანეთი აგრძელებს ორმხრივ და მრავალმხრივ თანამშრომლობას ევროკავშირთან, NATO - სთან, ბრიტანეთის თანამეგობრობისა და სხვა ქვეყნებთან. ორმხრივი თანამშრომლობა გაძლიერდა კორეის რესპუბლიკასთან, ისრაელთან, სინგაპურთან და იაპონიასთან. კერძოდ, ხელი მოეწერა ურთიერთგაგების მემორანდუმებს კორეის რესპუბლიკასთან და ისრაელთან; ხოლო სინგაპურთან და იაპონიასთან დაწყებულია მოლაპარაკებები კიბერუსაფრთხოების სფეროში მრავალმხრივი თანამშრომლობის შესახებ, რომელიც ამა

[71] The Office of Cyber Security & Information Assurance (OCSIA) https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance
[72] https://www.gov.uk/government/organisations/home-office
[73] https://www.gov.uk/government/organisations/ministry-of-defence
[74] Government Communications Headquarters (GCHQ) http://www.gchq.gov.uk/Pages/homepage.aspx
[75] the Communications-Electronics Security Department (CESG) http://www.cesg.gov.uk/Pages/homepage.aspx
[76] the Centre for the Protection of National Infrastructure (CPNI) http://www.cpni.gov.uk/
[77] the Foreign & Commonwealth Office (FCO) https://www.gov.uk/government/organisations/foreign-commonwealth-office
[78] the Department for Business, Innovation & Skills (BIS) https://www.gov.uk/government/organisations/department-for-business-innovation-skills

წლის მარტის თვეში დასრულდება; 2015 წელს ასევე იგეგმება დიალოგის დაწყება ინდოეთთან და ჩინეთთან.

დიდი ბრიტანეთი წარმატებით ეხმარება ევროკავშირს კიბერუსაფრთხოების სტრატეგიის ფორმირებაში, სადაც ასევე განსაზღვრულია ევროკავშირის ცალკეულ წევრ ქვეყნებთან მჭიდრო თანამშრომლობა. ასევე ქვეყანა არის აქტიური მონაწილე ევროპაში უსაფრთხოებისა და თანამშრომლობის ორგანიზაციის (ეუთო)[79] კიბერსივრცეში ნდობის აღდგენის ღონისძიებების[80] მიმართულებით.

2014 წლის ივნისში დიდი ბრიტანეთი გახდა NATO - ს კიბერ თავდაცვის ცენტრის[81] სრულუფლებიანი წევრი. ქვეყანა ცენტრის მუშაობაში შეიტანს მნიშვნელოვანს წვლილს და წარმოდგენილი იქნება განათლების, სასწავლო პროგრამების, კონსულტაციების, კვლევებისა და განვითარების (R&D) მიმართულებით. ასევე დიდი ბრიტანეთის ინიციატივა სამრეწველო კიბერ პარტნიორობის[82] შესახებ მოწონებული იქნა ალიანსის წევრი ქვეყნების მიერ და აღინიშნა უელსის სამიტის დეკლარაციაში, კერძოდ „technological innovations and expertise from the private sector are crucial to enable NATO and Allies to achieve the Enhanced Cyber Defence Policy"s objectives".

კიბერუსაფრთხოების ეროვნული პროგრამის (the National Cyber Security Programme (NCSP)) ფარგლებში ასევე ფინანსდება დიდი ბრიტანეთის თანამეგობრობის ქვეყნების სატელეკომუნიკაციო ორგანიზაციები, რათა მათ შეძლონ განვითარება და ეროვნული კიბერუსაფრთხოების მოდელის იმპლიმენტაცია.

მთავრობა აგრძელებს კიბერუსაფრთხოების გაძლიერებას შეიარაღებულ ძალებში, სადაც სამხედრო ოპერაციების დაგეგმვასა და განხორციელებაში სულ უფრო აქტიურად გამოიყენება კიბერშესაძლებლობები. შეიარაღებულ ძალებში ჩამოყალიბდა კიბერ თავდაცვის პარტნიორობა[83], რომლის მიზანია ინფორმაციული უსაფრთხოების

[79] the Organisation for Security and Cooperation in Europe (OSCE)
[80] Confidence Building Measures (CBMs) for cyberspace at the OSCE
[81] the NATO Cooperative Cyber Defence Centre of Excellence
[82] NATO Industry Cyber Partnership (NICP)
[83] the Defence Cyber Protection Partnership (DCPP)

უზრუნველყოფა, საუკეთესო პრაქტიკის გაზიარება, ცნობიერების ამაღლება და სტანდარტების დანერგვა. პარტნიორობა თავისთან მოიცავს კერძო ბიზნესის ცამეტ წარმომადგენელს, რომელთა შორის ყველაზე მსხვილი არის ADS[84] და techUK[85]. თავდაცვის კიბერუსაფრთხოების მოდელი ოფიციალურად იმპლიმენტირებული იქნება 2015 წელს. თუმცა უნდა ითქვას, რომ დიდ ბრიტანეთში ისევე როგორც ბევრ წამყვან ქვეყანაში კიბერუსაფრთხოების სფეროში სამოქალაქო და სამხედრო მიმართულებები მკაცრად არის ერთმანეთისგან გამიჯნული. თავდაცვის სამინისტროში კიბერუსაფრთხოების უზრუნველყოფასა და ოპერაციებზე პასუხისმგებელია სამინისტროს გაერთიანებული ძალების სარდლობა[86]. აღსანიშნავია, რომ 2015 წელს დაგეგმილია 200 - მდე ინფორმაციული ტექნოლოგიების სპეციალისტისა და პროგრამისტის გაწვევა. ასევე ყოფილი სამხედროებისგან იქმნება რეზერვისტთა ჯგუფი კიბერუსაფრთხოების მიმართულებით.

2014 წლის მარტში შეიქმნა ახალი ორგანიზაცია CERT - UK[87], რომლის მიზანია კიბერ ინციდენტებზე რეაგირება და ინფორმაციის გაზიარება NATO - ს წევრ ქვეყნებთან, ასევე თავად ალიანსთან.

დიდ ბრიტანეთში დიდი ყურადღება ეთმობა კიბერ სფეროში საჭირო უნარების, განათლების მიღებისა და პროფესიული განვითარების პროცესს. ასევე დარგის სამეცნიერო და კვლევით საქმიანობას. შეიძლება ითქვას, რომ ამ მიმართულებით დიდი ბრიტანეთი არის ერთერთი წამყვანი ქვეყანა, რომელსაც საკმაოდ მოქნილი და ეფექტური საგანმანათლებლო სისტემა აქვს შექმნილი[88] მთავრობა ეძებს ახალ ტალანტებს და უქმნის მათ ყველა საჭირო პირობას, რათა ისინი ჩამოყალიბდნენ მაღალი კვალიფიკაციის სპეციალისტებად. ქვეყნის ხელისუფლებამ შემოიღო საინტერესო ინიციატივა, კერძოდ კიბერუსაფრთხოება სხვადასხვა დონეზე ისწავლება ყველა

[84] https://www.adsgroup.org.uk/
[85] http://www.techuk.org/
[86] Joint Forces Command at MOD of UK https://www.gov.uk/government/organisations/joint-forces-command/about
[87] https://www.cert.gov.uk/
[88] ამ მიმართულებით ბიუროსთვის კარგი იქნება ბრიტანელ კოლეგებთან თანამშრომლობა

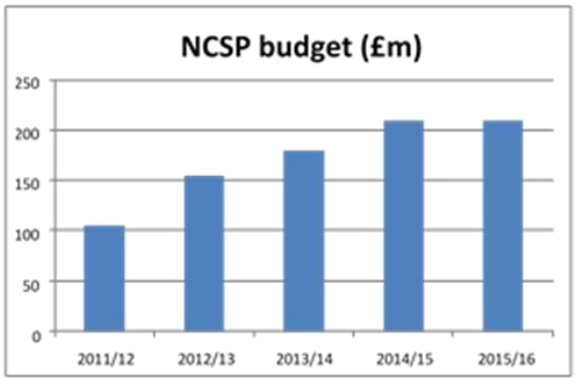
სასწავლებელში დაწყებული 11 წლის ასაკიდან[89]. ეს ინიციატივა იძლევა იმის საშუალებას, რომ ქვეყნის მოქალაქეს ადრეული ასაკიდან აქვს გარკვეული ზოგადი წარმოდგენა კიბერუსაფრთხოებაზე და კიბერსივრცეში არსებულ საფრთხებზე[90]. სკოლებში მოქმედებს პროგრამა Make IT Happy[91] და არსებობს სპეციალური სასწავლო მასალა Behind the screen[92]. კიბერუსაფრთხოების მიმართულებით საგანმანათლებლო პროგრამები ხორციელდება უშუალოდ მთავრობის, კერძოდ სამთავრობო კავშირის მთავარი ოფისის (GCHQ) მიერ, რომელიც პროფესიული განვითარების კუთხით თანამშრომლობს Tech Partnership - თან[93], ხოლო დარგის აკადემიურ დონეზე შესწავლისა და კვლევების მიმართულებით ოფისი პარტნიორობს 11 უმაღლეს სასწავლებელთან[94]. ცალკე არის გამოყოფილი სამაგისტრო პროგრამები[95], სადაც შერჩეულია ხუთი უმაღლესი სასწავლებელი და ისევ ოფისის პატრონაჟით ხორციელდება სასწავლო პროგრამები.

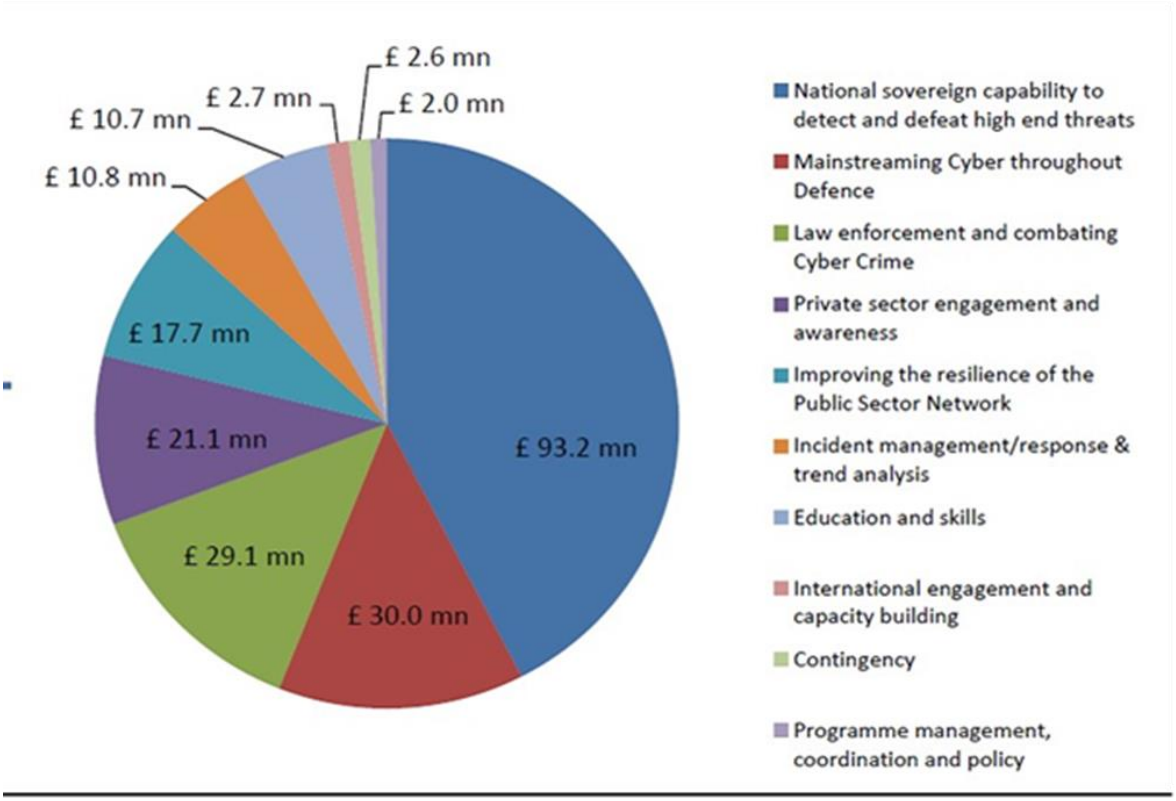
ექსპერტთა აზრით, მსგავსი საგანმანათლებლო სისტემა, რომელიც მთავრობის მკაცრი კონტროლის ქვეშ იმყოფება, სხვა წამყვან ქვეყნებთან მიმართებაში დიდ ბრიტანეთს უახლოეს მომავალში საშუალებას მისცემს იყოლიოს მაღალი კვალიფიკაციისა და პროფესიონალი ადამიანური რესურსი, და გახდეს დარგის ერთერთი ლიდერი ქვეყანა.

[89] ჩვენი ქვეყნისთვისაც საინტერესო ინიციატივა იქნებოდა
[90] ამით იზრდება ქვეყნის კიბერსივრცის დაცულობა და მცირდება რისკები
[91] http://makeithappy.cc4g.net/
[92] http://www.techfutureclassroom.com/
[93] http://www.thetechpartnership.com/
[94] https://www.cesg.gov.uk/awarenesstraining/academia/Pages/Academic-Centres.aspx
[95] http://www.gchq.gov.uk/press_and_media/press_releases/Pages/GCHQ-certifies-Masters-Degrees-in-Cyber-Security.aspx

NATIONAL CYBER SECURITY FUNDING

The allocation of NCSP funding for 2014/15 is set out below. These figures do not include spending in support of cyber objectives funded outside the NCSP. The chart demonstrates the spread of spend across the full range of cyber security activity. The sp end on „sovereign capabilities", not broken down here, supports activity across the Programme.





ეროვნული კიბერუსაფრთხოების დაფინანსება

დიაგრამებზე ნაჩვენებია NCSP - ის 2014/15/16 წლების ბიუჯეტი, სადაც კიბერ თავდაცვითი ღონისძიებებისთვის გამოყოფილია 30 მილიონი ფუნტი სტერლინგი. სქემა არ აჩვენებს სხვა დაფინანსების ოდენობას, რომელიც ხორციელდება არა NCSP - ის ფარგლებში.

ნიდერლანდების სამეფოს კიბერშესაძლებლობები

ნიდერლანდების სამეფომ კიბერუსაფრთხოების სტრატეგია მიიღო 2013 წელს[96] და სფეროს მთავარი მაკოორდინირებელი ორგანო არის კიბერუსაფრთხოების ეროვნული ცენტრი[97], რომელიც შედის ქვეყნის უსაფრთხოებისა და იუსტიციის სამინისტროში[98]. ცენტრის საქმიანობა ნახევრად გასაიდუმლოებულია, რაზეც პასუხისმგებელია დაზვერვისა და უსაფრთხოების გენერალური სამსახური[99].

ცენტრის სერვისებში შედის: - ექსპერტიზა და რეკომენდაციები[100]; - საფრთხეებსა და ინციდენტებზე რეაგირება[101] და - კრიზისების მართვის გაძლიერება[102].

საერთაშორისო დონეზე ცენტრი არის the Computer Security and Incident Response Teams (CSIRTs) – ის წევრი. ის ასევე აქტიურად თანამშრომლობს:

- FIRST (Forum of Incident Response and Security Teams)[103];
- EGC (European Government CERTs):
  - Germany - CERT-Bund[104];
  - Denmark – GovCertDK[105];
  - Finland - CERT-FI[106];
  - France – CERTA[107];
  - Great Britain- CPNI en GovCertUK[108];

[96] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf
[97] the National Cyber Security Centre https://www.ncsc.nl/english
[98] the Ministry of Security and Justice
[99] the General Intelligence and Security Service (AIVD)
[100] https://www.ncsc.nl/english/services/expertise-advice
[101] https://www.ncsc.nl/english/services/incident-response.html
[102] https://www.ncsc.nl/english/services/crisis-management-reinforcement.html
[103] http://www.first.org/
[104] https://www.cert-bund.de/
[105] https://www.govcert.dk/
[106] http://www.cert.fi/
[107] http://www.certa.ssi.gouv.fr/

- Hungary - CERT-Hungary[109];
- Norway – NorCERT[110];
- Austria - GovCERT.AT[111];
- Spain - CCN-CERT[112];
- Sweden - CERT-SE[113];
- Switzerland - GovCERT.ch[114];

- Terena (Trans-European Research and Education Networks Association)[115];
- ISF (Information Security Forum)[116];
- ENISA (European Network and Information Security Agency)[117];
- The following are other international CSIRTs with which we cooperate intensively:
  - Poland NASK[118] and CertPolska[119];
  - Australia AusCERT[120] and CERT.au[121];
  - United States of America CertCC[122] and US-CERT[123];
  - Japan JPCert[124];
- I4 (International Information Integrity Institute)[125].

[108] http://www.govcertuk.gov.uk/
[109] http://www.cert-hungary.hu/
[110] http://www.cert.no/
[111] http://www.govcert.at/
[112] https://www.ccn-cert.cni.es/
[113] http://www.cert.se/
[114] http://www.melani.admin.ch/
[115] http://www.terena.org/
[116] http://www.securityforum.org/
[117] http://www.enisa.europa.eu/
[118] http://www.nask.pl/nask_en/
[119] http://www.cert.pl/
[120] http://www.auscert.org.au/
[121] http://www.cert.gov.au/
[122] http://www.cert.org/
[123] http://www.us-cert.gov/
[124] http://www.jpcert.or.jp/english/
[125] https://i4online.com/

ციფრული სისტემები სულ უფრო დიდ როლს თამაშობს ნიდერლანდების სამეფოს დაზვერვისა და უსაფრთხოების საკითხში. ამის გამო, ქვეყნის შეიარაღებული ძალების მიზანია დაძლიონ ყველა ის საფრთხე, რომელიც დაკავშირებულია ციფრულ სფეროსთან და ზოგადად კიბერსივრცესთან. ამიტომ ნიდერლანდების შეიარაღებული ძალების საზღვაო, სახმელეთო, საჰაერო და კოსმოსური შენაერთების გვერდით, შეიქმნა მეხუთე ოპერატიული დომეინი.

ნიდერლანდების თავდაცვის სამინისტრო თავის კიბერ თავდაცვის სტრატეგიაში, რომელიც 2012 წლის 27 ივნისს[126] იქნა მიღებული, პრიორიტეტს ანიჭებს შემდეგ ექვს მიმართულებას:

1) ციფრული უსაფრთხოება უნდა იყოს მიმართული ყველა ფრონტზე

შეიარაღებული ძალები იყენებს ციფრულ სისტემებს პრაქტიკულად ყველა თავის ოპერაციაში. ისინი გამოიყენება ლოგისტიკაში, მართვასა და კონტროლში, დაზვერვაში, ჯარების დაცვაში, მანევრირებაში, ცეცხლის კორექტირებასა და წარმოებაში. თავდაცვის კიბერ სარდლობა[127] შედგება ყველა სამხედრო შენაერთის მოსამსახურისგან;

2) თავდაცვის სამინისტროსი და შეიარაღებული ძალების ციფრული მდგრადობის გაძლიერება

თავდაცვის ორგანიზაცია პასუხისმგებელია საკუთარი ქსელისა და სისტემების დაცვაზე. Joint Information Technology Command (JITC) უზრუნველყოფს ციფრული მდგრადობის გაძლიერებას.

JITC - ის დაქვემდებარებაშია თავდაცვის კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი[128], რომელიც უზრუნველყოფს თავდაცვის ციფრული ინფრასტრუქტურის დაცვას. 24/7 - ის რეჟიმში, ჯგუფი აფასებს რისკებს, თავდაცვის ქსელის სუსტ და მოწყვლად ადგილებს, იძლევა რჩევებს უსაფრთხოების ზომებზე;

3) სამხედრო კიბერ ოპერაციების შესაძლებლობები

[126] https://ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf
[127] Defence Cyber Command (DCC)
[128] the Defence Computer Emergency Response Team (DefCERT)

ნიდერლანდების შეიარაღებული ძალები არ უნდა იყოს კიბერშეტევებისგან მხოლოდ თავდაცვის მდგომარეობაში, არამედ მას უნდა შეეძლოს განახორციელოს საპასუხო კიბერშეტევა, რათა დაიცვას მთლიანი თავდაცვითი ინფრასტრუქტურა. ამ კუთხით, აქტიურად თანამშრომლობს სამხედრო დაზვერვისა და უსაფრთხოების სამსახურთან[129];

4) <u>ციფრულ სამყაროში დაზვერვის პოზიციების გაძლიერება</u>

ნიდერლანდების შეიარაღებულ ძალებს უნდა ჰქონდეთ წარმოდგენა იმ საფრთხეების შესახებ, რომელიც არსებობს კიბერსივრცეში, რათა მიიღონ შესაბამისი ზომები. ეს არის პოტენციური ან რეალური მოწინააღმდეგეებისა და თავდამსხმელების ტექნოლოგიური შესაძლებლობები, საიდანაც მოდის საფრთხეები.

- მომავალ წლებში სამხედრო დაზვერვისა და უსაფრთხოების სამსახურს (DISS)[130] მიეცემა მეტი უფლებები და ექნება უფრო მეტი შესაძლებლობები საიდუმლოდ შეაგროვოს ინფორმაციები კიბერუსაფრთხოებისა და კიბერსივრცის შესახებ. შედეგად, ინფორმაციის მიღების მიზნით, სამსახური შეძლებს რეგულარულად შეაღწიოს ქსელებსა და კომპიუტერულ სისტემებში. გარდა ამისა, სამსახური შეძლებს უკეთესად აკონტროლოს ქსელები და გამოიკვლიოს კიბერ შეტევების შესაძლებლობები;
- სამხედრო დაზვერვისა და უსაფრთხოების სამსახურსა (DISS) და მთავარ სადაზვერვო და უსაფრთხოების სამსახურს ექნებათ საერთო ბლოკი, რომელიც აწარმოებს რადიო და კიბერ სადაზვერვო საქმიანობას - the SIGINT Cyber Unit (cyber and signals intelligence);
- DISS მჭიდროდ თანამშრომლობს გაერთიანებული მართვის საინფორმაციო ცენტრთან[131], ნიდერლანდების სასამართლო მედიცინის ინსტიტუტთან[132],

[129] the Defence Intelligence and Security Service (DISS)
[130] the General Intelligence and Security Service (GISS)
[131] the Joint Information Management Command
[132] the Netherlands Forensic Institute

პოლიციის მომსახურების ეროვნულ სააგენტოსთან[133] და ნიდერლანდების სამეფო ჟანდარმერიასთან[134];

5) <u>ცოდნის მყარი ბაზის მიღება და კიბერსივრცეში ინოვაციური შესაძლებლობების გაზრდა</u>

თავდაცვის სამინისტრო მუდმივად მუშაობს კიბერსივრცის შესახებ ცოდნის, ახალი ტექნოლოგიებისა და უნარების განახლებაზე.

- თავდაცვის კიბერსივრცის ცენტრის ექსპერტები[135] განავითარებენ ცოდნას კიბერ ოპერაციების შესახებ. ცენტრი მჭიდროდ თანამშრომლობს სამეცნიერო - კვლევით ცენტრებთან[136];
- თავდაცვაში შექმნილია ვირტუალური ლაბორატორია, სადაც ტესტურ გარემოში ტარდება სამეცნიერო კვლევები;
- თავდაცვის საკადრო პოლიტიკაა კიბერ სფეროს მაღალკვალიფიციური სპეციალისტების მოზიდვა და მათი შენარჩუნება;
- 2012 წელს ნიდერლანდების თავდაცვის აკადემიაში დაინიშნა კიბერ ოპერაციების უფროსი ლექტორი;

6) <u>თავდაცვის უწყება ეროვნულ და საერთაშორისო დონეებზე თანამშრომლობს სხვადასხვა მიმართულებით</u>

- თავდაცვის უწყება წარმოდგენილია კიბერუსაფრთხოების ეროვნულ ცენტრში[137];
- თავდაცვის სამინისტრო წარმოდგენილია კიბერუსაფრთხოების საბჭოში, სადაც ასევე შედიან წარმომადგენლები სახელმწიფო და კერძო სექტორიდან, და სამეცნიერო წრეებიდან;
- თავდაცვის უწყება მჭიდროდ თანამშრომლობს IT ინოვაციების პლატფორმასთან 'Veilig Verbonden' [Safe Connection];

[133] the National Police Services Agency
[134] the Royal Netherlands Marechaussee
[135] the Defence Cyberspace Centre of Expertise (DCEC)
[136] ერთერთი ასეთი ინსტიტუტია the Netherlands Organisation for Applied Scientific Research https://www.tno.nl/en/
[137] the National Cyber Security Centre (NCSC) https://www.ncsc.nl/english

- თავდაცვის სამინისტრო ატარებს ერთობლივ ოპერაციებსა და ღონისძიებებს ალიანსთან და მის წევრებთან.

ნიდერლანდების ციფრული გარემოს დაცვის გასაძლიერებლად შეიარაღებული ძალების შემადგენლობაში შეიქმნა კიბერ სარდლობა[138], რომელიც არის ნიდერლანდების სამეფოს არმიის ნაწილი და პასუხისმგებელია კიბერუსაფრთხოების უზრუნველყოფაზე თავდაცვის უწყებასა და მის პარტნიორ ორგანიზაციებში.

კიბერ სარდლობა კონცენტრირდება კიბერუსაფრთხოების შემდეგ სამ მიმართულებაზე:

- თავდაცვა - ყველა ციფრული სისტემა უნდა იყოს დაცული კიბერ შეტევებისგან და ჯაშუშობისგან;
- დაზვერვა - შეიარაღებული ძალები უნდა იყვნენ წინასწარ ინფორმირებულნი ციფრულ სფეროში არსებული საფრთხეების შესახებ. ეს საფრთხეები შეიძლება მოდიოდეს როგორც გარედან, ისე საკუთარი სისტემებიდან;
- შეტევა - შეიარაღებულ ძალებს შეუძლია თავად განახორციელოს შეტევა, მოახდინოს მანიპულირება და მწყობრიდან გამოიყვანოს მოწინააღმდეგის სისტემები. პოტენციური მოწინააღმდეგეები არის სხვა სახელმწიფოები, ტერორისტული ორგანიზაციები და ჰაკერები.

ციფრული სისტემები ასრულებს დიდ და მნიშვნელოვან როლს ქვეყნის შეიარაღებულ ძალებში. საკომუნიკაციო, სანავიგაციო, სენსორული და სამხედრო ციფრული სისტემები მუდმივად არის კიბერ შეტევის რისკის ქვეშ. საფრთხეები შეიძლება მოდიოდეს სხვა სახელმწიფოებიდან, ასევე ტერორისტული, რელიგიური თუ კომერციული სუბიექტებისგან. საფრთხეებს შეიძლება მოჰყვეს:

- სისტემებზე ლოკალური და მასირებული შეტევა;
- ჯაშუშობა.

[138] the Dfence Cyber Command (DCC)

ამა წლის 2 თებერვალს შეიარაღებული ძალების კიბერ ოპერაციების ხელმძღვანელად დაინიშნა პოლკოვნიკი, დოქტორი Paul Ducheine, რომელიც აწარმოებს კვლევებს კიბერუსაფრთხოების სამხედრო და სამართლებრივი ასპექტების შესახებ. ახალი ხელმძღვანელი არის უფროსი ლექტორი ნიდერლანდების თავდაცვის აკადემიის სამხედრო მეცნიერების ფაკულტეტზე, სადაც კითხულობს კიბერ ოპერაციებსა და კიბერუსაფრთხოებას. შეიძლება ის მალე გახდეს ბრიგადის გენერალი.

შეერთებული შტატების კიბერშესაძლებლობები

შეერთებული შტატები არის მოწინავე ქვეყანა კიბერუსაფრთხოების საკითხებში და ის წარმოადგენს ერთერთ ძირითად მოთამაშეს მსოფლიოში. ყველაზე დიდი კიბერშეტევების პროცენტული მაჩვენებელი მოდის შეერთებული შტატების კიბერსივრცესა და მის ინფრასტრუქტურაზე.

ობამას ადმინისტრაციამ ქვეყნის 2015 წლის საფინანსო ბიუჯეტში კიბერუსაფრთხოების სფეროსთვის გამოყო 14 მილიარდი ამერიკული დოლარი[139]. არსებული ინფორმაციით ეს არის ბიუჯეტის ოფიციალური ნაწილი, თუმცა ექსპერტები ვარაუდობენ, რომ შეერთებული შტატები კიბერუსაფრთხოების უზრუნველყოფისთვის აპირებს დახარჯოს უფრო მეტი[140].

თავდაპირველად შეერთებულმა შტატებმა კიბერუსაფრთხოების თემაზე მუშაობა დაიწყო 2001 წლის 11 სექტემბრის ტერორისტული აქტის შემდეგ. თუმცა მანამდე, 1991 წელს ერაყში „უდაბნოს ქარიშხალში“ სამხედრო - საჰაერო ძალების მიერ აქტიურად გამოიყენებოდა უახლესი ინფორმაციული ტექნოლოგიები, ხოლო მის დაცვას უზრუნველყოფდა სპეციალურად შექმნილი ქვედანაყოფი.

უკვე 2011 წლის მაისში[141] შეერთებულმა შტატებმა გამოაქვეყნა თავისი სტრატეგია კიბერსივრცის დაცვაზე. სტრატეგიას საფუძვლად უდევს მთავრობას, საერთაშორისო პარტნიორებსა და კერძო სექტორს შორის თანამშრომლობის მოდელი, სადაც აღწერილია მთელი რიგი ღონისძიებები, რომლებიც აუცილებელია გატარდეს შემდეგი შვიდი მიმართულებით:

[139] გასულ წელს ეს მაჩვენებელი შეადგენდა 12,8 ამერიკულ დოლარს

[140] არაოფიციალური ხარჯვითი ნაწილი არის ეროვნული უსაფრთხოების სააგენტოს, ცენტრალური სადაზვერვო სააგენტოსა და იუსტიციის სამინისტროს უფლებამოსილებაში

[141] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

- ეკონომიკა - საერთაშორისო სტანდარტებისა და ინოვაციების მოზიდვა, ღია და ლიბერალური ბაზარი;
- ეროვნული ქსელის დაცვა - უსაფრთხოების ამაღლება, სანდოობა და მდგრადობა;
- სამართალებრივი მხარე - თანამშრომლობისა და სამართლებრივი ნორმების გაფართოება;
- სამხედრო სფერო - უსაფრთხოების თანამედროვე გამოწვევებზე მზადყოფნა;
- სამთავრობო ინტერნეტის ქსელი - სამთავრობო სტრუქტურების ეფექტურობისა და მრავალმომცველობის გაფართოება;
- საერთაშორისო განვითარება - უსაფრთხოების ორგანიზება, საერთაშორისო კომპეტენციების განვითარება და ეკონომიკური აყვავება;
- თავისუფლება ინტერნეტში - მოქალაქეთა კერძო ცხოვრების ხელშეუხებლობისა და თავისუფლების მხარდაჭერა.

შეერთებული შტატების კიბერუსაფრთხოების სფეროში 2015 წელი არის მნიშვნელოვანი ცვლილებების წელი. კერძოდ, პირველი 2015 წლის თებერვალში აშშ-ის პრეზიდენტის ადმინისტრაციაში მიიღეს გადაწყვეტილება, რომ ეროვნული დაზვერვის დირექტორის (Director of National Intelligence, DNI)[142] უშუალო დაქვემდებარებაში შეიქმნას ახალი სპეციალური სამსახური - კიბერსაფრთხეებზე სადაზვერვო მონაცემების ინტეგრაციის ცენტრი (Cyber Threat Intelligence Integration Center, CTIIC)[143]. უწყების ფუნქციებში შედის სახელმწიფო უწყებებიდან და კერძო სექტორიდან მიღებული სადაზვერვო მონაცემების შეგროვება, ანალიზი და რეკომენდაციების გაცემა. ასევე უწყებათაშორისო კოორდინაცია; მეორე, ცენტრალურმა სადაზვერვო სააგენტომ (the Central Intelligence Agency, CIA) ერთერთ პრიორიტეტულ მიმართულებად გამოაცხადა კიბერსაფრთხეების შეკავება, პრევენცია და შეტევითი ღონისძიებების განხორციელება, რისთვისაც სააგენტოში სპეციალურად შეიქმნა კიბერ -

[142] http://www.dni.gov/index.php
[143] https://www.cia.gov/index.html

ოპერაციების დირექტორატი, რომლის მიზანია კიბერ ოპერაციებისთვის უპირველესი პრიორიტეტის მინიჭება და სადაზვერვო ინფორმაციის შეგროვებისას ციფრული ინოვაციების გამოყენება; და მესამე, ამ წელს დაგეგმილია 30 ათასი პროგრამისტის/ჰაკერის დასაქმება სახელმწიფო სექტორში. ასევე პენტაგონი აპირებს აწარმოოს უფრო აგრესიული პოლიტიკა კიბერუსაფრთხოების მიმართულებით, რაც მოიცავს არამარტო არმიის კრიტიკული ინფრასტრუქტურის დაცვით ღონისძიებებს, არამედ ასევე კიბერ თავდასხმების და სპეციალური კიბერ შეტევითი ოპერაციების განხორციელებას პოტენციურ მოწინააღმდეგეზე.

ზოგადად, შეერთებული შტატების კიბერუსაფრთხოების სისტემა არის სამდონიანი. კერძოდ:

<u>პირველი დონე</u> არის ფედერალური უწყებები

- *თავდაცვის სამინისტრო;*
- *შიდა უსაფრთხოების სამინისტრო* (Department of Homeland Security, DHS)[144]
    - კიბერუსაფრთხოების და კომუნიკაციების ოფისი (Office of Cyber Security and Communications);
- *იუსტიციის დეპარტამენტი* (United States Department of Justice, DOJ)[145]
    - გამოძიების ფედერალური ბიუროს (Federal Bureau of Investigation, FBI)[146] კიბერგამოძიების ეროვნული გაერთიანებული ძალები (National Cyber Investigative Joint Task Force, NCIJTF);

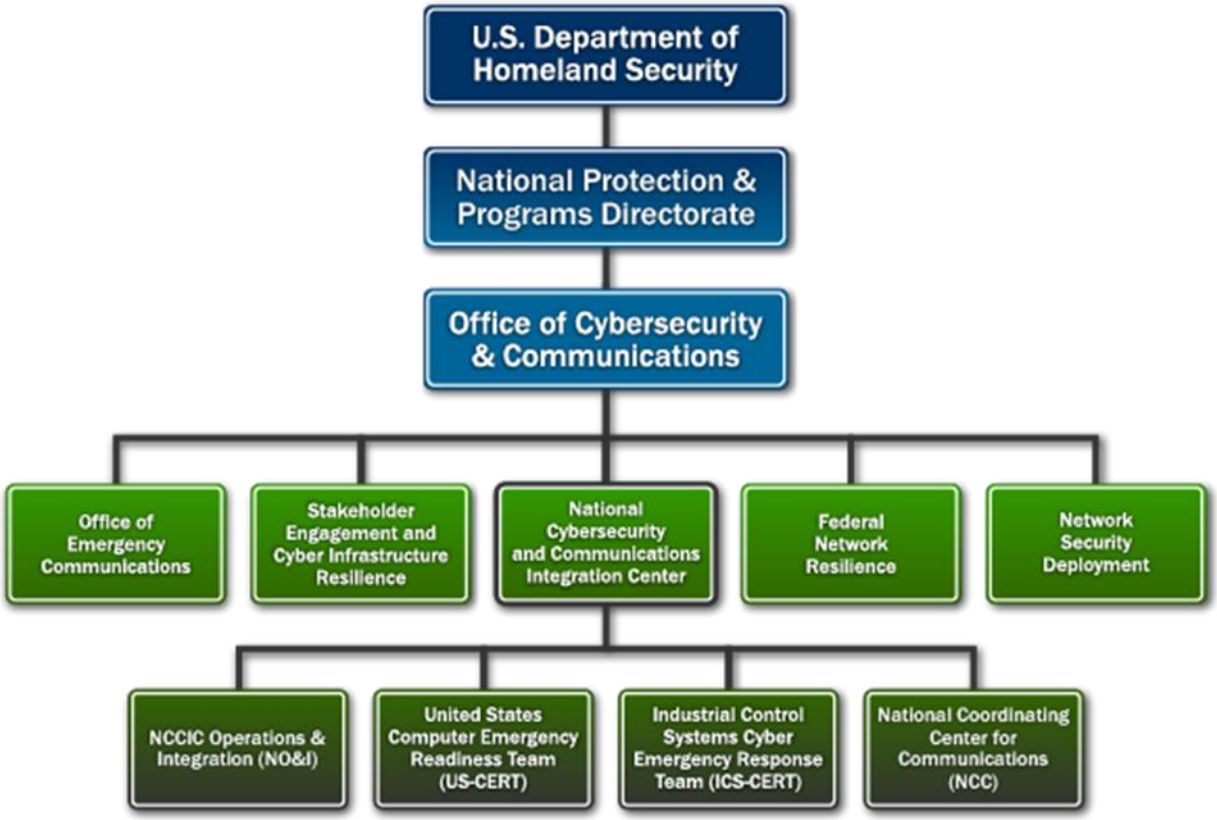
<u>მეორე დონე</u> - პირველ დონის რომელიმე სტრუქტურაში შემავალი

- კომპიუტერული უსაფრთხოების ინციდენტებზე რეაგირების ჯგუფი (United States Computer Emergency response Team, US-CERT)[147];
- კიბერუსაფრთხოების ეროვნული ცენტრი (National Cyber Security Division, NCSD);

[144] http://www.dhs.gov/
[145] http://www.justice.gov/
[146] http://www.fbi.gov/
[147] https://www.us-cert.gov/

- კიბერდანაშაულთან ბრძოლის ცენტრი (Cyber Crimes Center);
- კიბერსაფრთხეების საოპერაციო ცენტრი (NSA/CSS Threat Operations Center, NTOC);
- შეიარაღებული ძალების კიბერსარდლობა (United States Cyber Command, USCYBERCOM)[148].

<u>მესამე დონე</u> - ლოკალური და რეგიონალური სტრუქტურული ქვედანაყოფები. მათ საქმიანობაზე ზედამხედველობასა და კონტროლს ახორციელებენ ზემოთ ნახსენები ორგანიზაციები.



შეერთებული შტატების კიბერუსაფრთხოების ორგანიზაციულ - სტრუქტურული სქემა

კიბერუსაფრთხოების სამხედრო ასპექტების გამოყოფა პენტაგონის პრიორიტეტებში დაიწყო ჯერ კიდევ ჯორჯ ბუში - უმცროსის პრეზიდენტობის დროს. იმავდროულად, დაიწყო მკაცრი კონკურენცია შეერთებული შტატების სპეციალურ

[148] http://www.stratcom.mil/factsheets/2/Cyber_Command/

სამსახურებს შორის მოცემულ სფეროში უფლებამოსილების თაობაზე. მაშინ დადგა საკითხი ერთიანი გაერთიანებული კიბერსარდლობის (USCYBERCOM) შექმნის შესახებ, რომელიც ხელს შეუწყობდა კიბერსივრცეში სამხედროების მოქმედებას, თუმცა იმ დროს პენტაგონი ამისთვის მზად არ აღმოჩნდა და საკითხი ისევ ღიად დარჩა. ამიტომ საერთო პასუხისმგებლობა კიბეროომის პრობლემატიკასთან დაევალა შეიარაღებული ძალების სტრატეგიულ სარდლობას, ხოლო კიბერსივრცეში საბრძოლო ოპერაციების ფაქტიური განხორციელება დაევალა სამხედრო - საჰაერო ძალებს. შემდგომში ეს პროცესი უფრო განვითარდა და 2007 წელს შეერთებული შტატების სამხედრო - საჰაერო ძალებში შეიქმნა კიბერსარდლობა, რომელმაც ამ სტატუსით იარსება 2008 წლის ბოლომდე, რის შემდეგაც ეს ფუნქციები გადაეცა სამხედრო - საჰაერო ძალების კოსმოსურ (სტრატეგიულ) სარდლობას[149], სადაც 2009 წლის ივნისში შეიქმნა კიბერსარდლობის განახლებული სტრუქტურული ერთეული. ფაქტიურად,

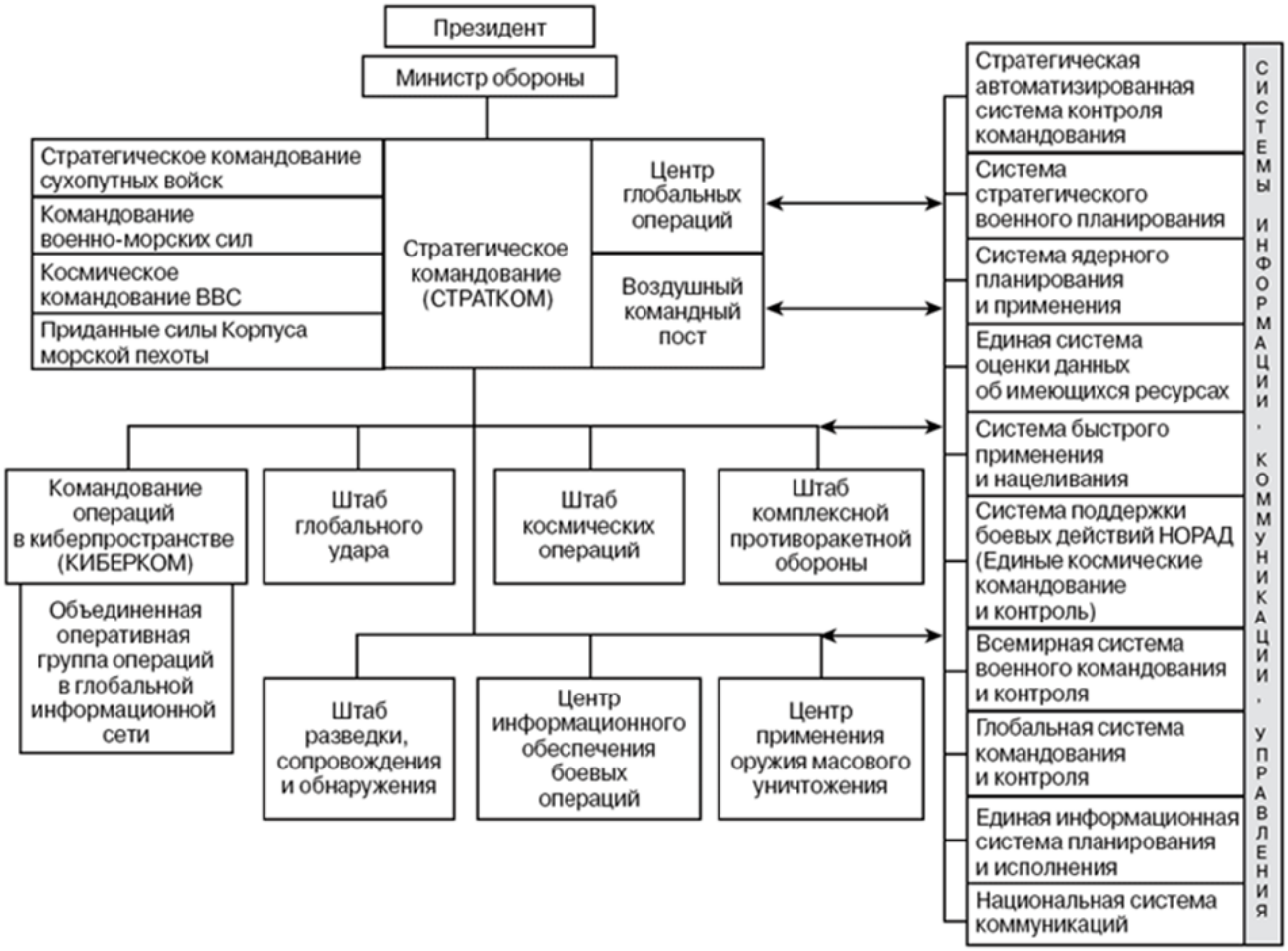
შეერთებული შტატების შეიარაღებული ძალების ხელმძღვანელობამ კიბერუსაფრთხოების უზრუნველყოფა მოაქცია ერთი სტრუქტურული ერთეულის ქვეშ, წინააღმდეგ შემთხვევაში კოორდინაციისა და ოპერატიულობის ხარისხი იქნებოდა ძალზედ დაბალი[150].

შეერთებული შტატების გამოცდილება აჩვენებს, რომ ორგანიზაციულ - სტრუქტურული თვალსზრისით, აუცილებელია შეიარაღებული ძალებისა და სამოქალაქო სექტორის (მათ შორის სპეციალური სამსახურების) ფუნქციების ერთმანეთისგან გამიჯვნა. კიბერსარდლობა თავის ამოცანებს ახორციელებს ცენტრალური სადაზვერვო სააგენტოს, საშინაო უსაფრთხოების სამინისტროს, ეროვნული უსაფრთხოების სააგენტოსა და სახელმწიფოს სხვა სტრუქტურული ერთეულების პარალელურად ან ერთობლივად, ამიტომ აუცილებელია კიბერსაფრთხეების წინააღმდეგ ერთობლივი ბრძოლა. ამ მიმართულებით, საინტერესო პრაქტიკა არის ის გარემოება, რომ სტრუქტურული ერთეულების მიერ

[149] პასუხისმგებელია ასევე ამერიკის ბირთვულ შეიარაღებასა და მართვაზე

[150] ეს სტრუქტურა მოქმედებს დღემდე და ანალოგიურის შექმნაზე მუშაობს რუსეთიც, რაც სტრუქტურის ეფექტიანობაზე მიუთითებს

ურთიერთგადამკვეთი ამოცანების გადაჭრა თავმოყრილია ერთი პიროვნების უფლებამოსილებაში, კერძოდ კიბერსარდლობის ამჟამინდელი ხელმძღვანელი ამავდროულად არის ეროვნული უსაფრთხოების სააგენტოს (NSA)[151] და უსაფრთხოების ცენტრალური სამსახურის დირექტორი.



შეიარაღებული ძალების სტრატეგიული სარდლობის ორგანიზაციულ- სტრუქტურული სქემა

[151] https://www.nsa.gov/

ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების სტრატეგიები, საერთო პრინციპები და რეკომენდაციები. საქართველოს კიბერუსაფრთხოების სტრატეგია

შესავალი

გარკვეული პერიოდის განმავლობაში, საზოგადოებრივი კეთილდღეობა და ეკონომიკური სტაბილურობა ეყრდნობოდა გადაცემის ქსელების მონაცემებისა და გამოთვლითი მომსახურების გამართულ მუშაობას, რომლის სანდოობის მაჩვენებელი საკმაოდ დიდი იყო. საერთო მოხმარების ინფორმაციული სისტემების ფუნქციონირებაზე დიდი გავლენა აქვს ისეთ ფაქტორებს, როგორებიც არის ინტერნეტზე შეტევა (attack), ფიზიკური ზემოქმედების შედეგად მიყენებული დარღვევები, პროგრამული და აპარატული უზრუნველყოფის მწყობრიდან გამოსვლა, ადამიანის როგორც მომხმარებლის მიერ მუშაობის პროცესში დაშვებული შეცდომები. ჩამოთვლილი ფაქტორები ნათლად აჩვენებს იმ გარემოებას, თუ რამდენად არის დამოკიდებული თანამედროვე საზოგადოება ინფორმაციული სისტემების სტაბილურ მუშაობაზე. მოცემულს ნათლად ასახავს კიბერუსაფრთხოების გერმანული სტრატეგია, კერძოდ: „კიბერსივრცეზე დაშვების უზრუნველყოფა, ასევე ინფორმაციის კონფიდენციალობა და სანდოობა კიბერსივრცეში გახდა ერთერთი მნიშვნელოვანი პრობლემა 21 - ე საუკუნეში. ამიტომ კიბერსივრცის დაცვა ხდება მთავარი ამოცანა სახელმწიფოს, ეკონომიკისა და საზოგადოების, როგორც ქვეყნის, ისე საერთაშორისო დონეზე“[152].

[152] გერმანიის სტრატეგია, გვ. 1 http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1

ევროკომისიის ზოგიერთ შეხვედრაზე[153] არაერთხელ განიხილებოდა და ამჟამადაც აქტიურად განიხილება ქსელისა და ინფორმაციული უსაფრთხოების მნიშვნელობა. ამ მიზნით, ასევე აქტიური განხილვის საგანია ერთიანი ევროპული ინფორმაციული სივრცის შექმნა.

ევროკომისიის ბოლო შეხვედრებზე მიღებული ნორმატიული და სამართლებრივი აქტები[154] ინფორმაციული ინფრასტრუქტურის (CII – Critical Information Infrastructure Protection) დაცვის შესახებ, გვთავაზობს პრაქტიკულ ზომებსა და რეგულაციებს ქსელების საერთო მოხმარების უსაფრთხოებისა და სანდოობის თაობაზე.

კიბერუსაფრთხოება ხშირად განიხილება როგორც სახელმწიფო მნიშვნელობის სტრატეგიული პრობლემა, რომელიც ეხება საზოგადოების ყველა ფენას. კიბერუსაფრთხოების სახელმწიფო პოლიტიკა (NCSS - National Cyber Security Strategy) არის საშუალება, რომელიც ემსახურება სახელმწიფოს ინფორმაციული სისტემებისა და მთლიანად ინფრასტრუქტურის უსაფრთხოებისა და სანდოობის გაზრდის შესაძლებლობას, რომელიც ამავდროულად მაქსიმალურად ამცირებს რისკებს. კიბერუსაფრთხოების სტრატეგიაში გამოიყენება პრობლემისადმი მაღალი დონის მიდგომა, კერძოდ: გამოიყოფა სახელმწიფოს მთელი რიგი მიზნები, ამოცანები და პრიორიტეტები, რომლებიც აუცილებელია მოცემული დროის მონაკვეთში მისაღწევად. ფაქტიურად, სტრატეგია ეს არის მოდელი, რომელიც საშუალებას იძლევა კიბერუსაფრთხოების საკითხების მოგვარებას ქვეყნის შიგნით.

ევროკავშირის წევრ - ქვეყნებში კიბერუსაფრთხოების უზრუნველყოფის გაუმჯობესებისა და კოორდინირებული მუშაობის, ასევე, საერთო პოლიტიკის შემუშავების მიზნით, შექმნილია სპეციალური სააგენტო European Union Agency for Network and Information Security – ENISA[155].

[153] მაგალითად, COM/2005/0229 final "i2010 – A European Information Society for growth and development"; COM/2006/251 "A Strategy for a Secure Information Society"; COM/2010/245 final/2 "A Digital Agenda for Europe"; COM/2009/149 on Critical Information Infrastructure Protection

[154] DIRECTIVE 2009/140/EU

[155] http://www.enisa.europa.eu/

ENISA ამუშავებს სპეციალურ სახელმძღვანელოს Good Practice Guide[156], რომელიც წარმოადგენს ევროკავშირის წევრი ქვეყნების მხარდამჭერ დოკუმენტს მათი მხრიდან კიბერუსაფრთხოების სახელმწიფო პოლიტიკის შემუშავების მთავარ მისიაში. მოცემული სახელმძღვანელო ევროკავშირის თითოეული წევრი ქვეყნისთვის იძლევა რეკომენდაციებსა და არსებულ მოწინავე პრაქტიკას კიბერუსაფრთხოების სტრატეგიის შემუშავებასა და დანერგვაში.

წინამდებარე დოკუმენტში მოკლედ არის განხილული ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოებისა და ზოგადად ევროკავშირის ინტერნეტის უსაფრთხოების სტრატეგიები, მასთან დაკავშირებული საკითხები და არსებული ვითარება. საკითხის მიმართ დიდი ინტერესიდან გამომდინარე, ქვემოთ განხილულია ასევე შეერთებული შტატების, კანადისა და იაპონიის კიბერუსაფრთხოების სტრატეგიის ძირითადი მიმართულებები. დოკუმენტში ასევე მოცემული არის სტრატეგიების საერთო მახასიათებლები, განსხვავებები, დასკვნა, რეკომენდაციები და წარმოდგენილია საქართველოს კიბერუსაფრთხოების პოლიტიკისა და სტრატეგიის მიმართულებები.

ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების სტრატეგიები

კიბერუსაფრთხოების პირველი სტრატეგია შემუშავებულ იქნა ამერიკის შეერთებულ შტატებში 2000 წლების დასაწყისში. შეერთებული შტატები გახდა ის ქვეყანა, რომელმაც დაიწყო კიბერუსაფრთხოების აღქმა, როგორც სახელმწიფო მნიშვნელობის საკითხი. 2003 წელს შეერთებულ შტატებში გამოქვეყნდა კიბერსივრცის უსაფრთხოების ეროვნული სტრატეგია (National Strategy to Secure Cyberspace)[157]. მოცემული დოკუმენტი წარმოადგენს უფრო ფართო ეროვნული უსაფრთხოების უზრუნველყოფის სტრატეგიის ნაწილს (National Strategy for Homeland Security), რომელიც შეიქმნა 2001 წლის 11 სექტემბრის ტერორისტული შეტევის პასუხად.

შემდგომ წლებში ევროპაში მთელი მასშტაბით დაიწყო ღონისძიებებისა და სტრატეგიების შემუშავება, რომელიც ემსახურებოდა კიბერუსივრცის დაცვის საკითხს.

[156] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss
[157] http://www.dhs.gov/files/publications/editorial_0329.shtm

2005 წელს გერმანია იღებს ინფორმაციული ინფრასტრუქტურის დაცვის სახელმწიფო გეგმას (National Plan for Information Infrastructure Protection - NPSI)[158]. მომავალ წელს შვედეთის მთავრობა ამუშავებს შვედეთში ინტერნეტის უსაფრთხოების გაძლიერების სტრატეგიას (Strategy to improve Internet Security in Sweden). ესტონეთმა თავისი კიბერუსაფრთხოების სტრატეგიის შემუშავება დაიწყო 2007 წელს რუსეთის მხრიდან ქვეყანაზე განხორციელებული მასიური კიბერშეტევის შემდეგ და 2008 წელს ევროკავშირის წევრ - ქვეყნებს შორის გახდა პირველი, რომელმაც გამოაქვეყნა კიბერუსაფრთხოების სახელმწიფო სტრატეგია[159]. ამის შემდეგ ევროკავშირის და უშუალოდ წევრი ქვეყნების მიერ გატარებულ იქნა მთელი რიგი ღონისძიებები და ჩატარდა დიდი სამუშაოები კიბერსივრცის უსაფრთხოების უზრუნველყოფის მიმართულებით. შედეგად, ევროკავშირის ათამდე წევრმა ქვეყანამ გამოაქვეყნა თავისი კიბერუსაფრთხოების სახელმწიფო სტრატეგია. ზოგიერთი წევრი ქვეყანა ამ დროისთვის არის სტრატეგიის დამუშავების სტადიაზე, რომლებიც ახლოსაა დასრულებასთან და მალე გამოქვეყნდება. ასევე აღსანიშნავია ის გარემოებაც, რომ ევროკავშირის რამოდენიმე წევრ - ქვეყანას გააჩნია არაოფიციალური ან არაფორმალური სტრატეგიები.

ქვემოთ განხილულია კიბერუსაფრთხოების სტარტეგიების მოკლე აღწერილობა. კერძოდ:

- **ესტონეთი** - კიბერუსაფრთხოების სტრატეგია ქვეყანამ მიიღო 2008 წელს. ესტონეთი დიდ მნიშვნელობას ანიჭებს თავისი კიბერსივრცის დაცვას და ამახვილებს ყურადღებას ინფორმაციული სისტემების უსაფრთხოებაზე. სარეკომენდაციო ღონისძიებები ატარებს სამოქალაქო ხასიათს და ეფუძნება სამართლებრივ რეგულაციებს, სწავლებასა და თანამშრომლობას;
- **ფინეთი** - ფინეთის მიერ კიბერუსაფრთხოების სტრატეგია მიღებულია 2008 წელს და მას საფუძვლად უდევს კიბერუსაფრთხოების გაგება როგორც ეკონომიკური ხასიათის პრობლემა, რომელიც მჭიდრო კავშირშია ქვეყნის ინფორმაციული სისტემებისა და საზოგადოების განვითარებასთან;

[158] http://www.bmi.bund.de/cae/servlet/contentblob/560098/publicationFile/27811/kritis_3_eng.pdf
[159] http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

- **სლოვაკეთი** - ინფორმაციული უსაფრთხოების უზრუნველყოფა განიხილება როგორც საზოგადოების ნორმალური ფუნქციონირებისა და განვითარების აუცილებელი პირობა. ამიტომ სტრატეგიის მიზანს წარმოადგენს ინფორმაციის დაცვის მჭიდრო ფუნდამენტი. სტრატეგია მიმართულია როგორც საფრთხის გაუვნებელყოფაზე, ისე ამისთვის საჭირო საშუალებების მზადყოფნასა და გაძლიერებაზე. სტარტეგია სლოვაკეთმა შეიმუშავა 2008 წელს;
- **ჩეხეთის რესპუბლიკა** - კიბერუსაფრთხოების სტრატეგიის ძირითადი მიმართულება თავისთან მოიცავს ინფორმაციული და საკომუნიკაციო სისტემების მოწყვლადი ადგილების დაცვას, ასევე რისკებისა და მოსალოდნელი საფრთხეების მაქსიმალურ შემცირებას. სტრატეგია ძირითადად ფოკუსირდება ინფორმაციულ სისტემებზე თავისუფალი დაშვების პრობლემებზე, ასევე ქვეყნის კიბერსივრცის მთლიანობასა და მონაცემთა კონფიდენციალობის დაცვაზე. სტრატეგია შემუშავდა 2011 წელს და ის კარგად არის ჰარმონიზირებული ჩეხეთის რესპუბლიკის სხვა სამართლებრივ - ნორმატიულ აქტებთან;
- **საფრანგეთი** - კიბერუსაფრთხოების სტრატეგია ქვეყნის ხელისუფლებამ მიიღო 2011 წელს, რომელიც ორიენტირებულია ინფორმაციული სისტემების შესაძლებლობებზე და ის წინ უნდა აღუდგეს კიბერსივრცეში არსებულ ისეთ მოვლენებს, რაც უარყოფითად მოქმედებს ინფორმაციის დაშვებაზე, მთლიანობასა და კონფიდენციალობის დაცვაზე. საფრანგეთი თავის სტრატეგიაში ძირითად აქცენტს აკეთებს ტექნიკური საშუალებებით ინფორმაციის დაცვაზე, კიბერდანაშაულებებთან ბრძოლასა და კიბერდაცვის გაძლიერებაზე;
- **გერმანია** - ქვეყნის კიბერუსაფრთხოების სტრატეგიას, რომელიც შემუშავებულ იქნა 2011 წელს, საფუძვლად უდევს კრიტიკული ინფორმაციული სისტემების უსაფრთხოების უზრუნველყოფა. ქვეყანა ძირითადად კონცენტრირებულია კიბერშეტევის დროულ გამოვლენაზე,

გაუვნებელყოფასა და სამართლებრივ დევნაზე, ასევე ინფორმაციული და საკომუნიკაციო ტექნოლოგიების (ICT) მოწყობილობების მწყობრიდან გამოსვლის გაუვნებელყოფაზე, რომელიც გამოწვეულია შემთხვევითი ფაქტორებით. ეს უკანასკნელი განსაკუთრებით ეხება კრიტიკულად მნიშვნელოვან ინფორმაციულ სისტემებს. სტრატეგიაში ასევე მოცემულია ანალიზი, რომელიც საშუალებას იძლევა განისაზღვროს დამატებითი ღონისძიებები მიმართული ინფორმაციული და საკომუნიკაციო ტექნოლოგიების (ICT) სისტემების დაცვაზე. სტარტეგიაში ასევე განსაზღვრულია მცირე და საშუალო ბიზნესის კიბერსივრცეში დაცვის უზრუნველყოფითი ღონისძიებები;

- **ლიტვა** - ქვეყანა ორიენტირებულია იმ მიზნებისა და ღონისძიებების განსაზღვრაზე, რომელიც მიმართულია ელექტრონული ინფორმაციის განვითარებაზე, ასევე კიბერსივრცეში კონფიდენციალობის დაცვაზე, დაშვებასა და მთლიანობაზე. გარდა ამისა, ლიტვის სტრატეგია უზრუნველყოფს კიბერსივრცეში პერსონალური მონაცემების, სატელეკომუნიკაციო ქსელის, ინფორმაციული სისტემისა და კრიტიკულად მნიშვნელოვანი ინფრასტრუქტურის დაცვას კიბერშეტევებისა და უსაფრთხოების დარღვევისგან. სტრატეგიაში, რომელიც მიღებული იყო 2011 წელს, განსაზღვრულია ღონისძიებები, რომელთა რეალიზაცია იძლევა კიბერსივრცეში მუშაობის სრულყოფილი უსაფრთხოების გარანტიებს;
- **ლუქსემბურგი** - კიბერუსაფრთხოების სტრატეგია მიღებულ იქნა 2011 წელს. მოცემული სტრატეგია აცნობიერებს იმ საფრთხეებს, რომლებიც არსებობს კიბერსივრცეში და ამის გათვალისწინებით, გამოყოფილია საზოგადოებრივი და ეკონომიკური უსაფრთხოება. სტრატეგიაში ასევე აღნიშნულია ინფორმაციული და საკომუნიკაციო ტექნოლოგიების მნიშვნელობა ეკონომიკური ზრდისთვის, ცალკეული მოქალაქეებისთვისა და ზოგადად მთელი საზოგადოებისთვის. სტრატეგია მუშაობს შემდეგი

ხუთი მიმართულით - ძირითადი ინფორმაციული ინფრასტრუქტურის დაცვა და დროული რეაგირება ინციდენტებზე; სამართლებრივ - ნორმატიული ბაზის მოდერნიზაცია; საერთაშორისო თანამშრომლობა; სწავლება და ინფორმირება; სტანდარტების დახვეწა;

- **ჰოლანდია** - ქვეყანა ერთის მხრივ მიისწრაფვის ინფორმაციული და საკომუნიკაციო სისტემების უსაფრთხო და სანდო ფუნქციონირებისკენ, და მეორეს მხრივ, აღიარებს ინტერნეტ სივრცის თავისუფლებისა და გამჭვირვალობის აუცილებლობას. 2011 წელს მიღებულ სტრატეგიაში აღსანიშნავი და მნიშვნელოვანია კიბერუსაფრთხოების განსაზღვრება, რომლის მიხედვით „კიბერუსაფრთხოება - ეს არის ინფორმაციული და საკომუნიკაციო სისტემების დაცულობა არასწორი ექსპლუატაციისგან, რომელმაც შეიძლება უარყოფითი გავლენა იქონიოს ინფორმაციული და საკომუნიკაციო სისტემებზე დაშვებასა და სანდოობაზე, ასევე რისკის ქვეშ დააყენოს სისტემებში არსებული ინფორმაციის კონფიდენციალობა და მთლიანობა“;
- **დიდი ბრიტანეთი** - გაერთიანებული სამეფოს მიდგომა ასევე მიმართულია კიბერუსაფრთხოების განვითარებაზე. სტრატეგიის მთავარი მიზანია გაიყვანოს დიდი ბრიტანეთი მოწინავე პოზიციებზე ინფორმაციული და სატელეკომუნიკაციო ტექნოლოგიების სფეროში ინოვაციების, ინვესტიციებისა და ხარისხიანი მომსახურების მიხედვით. ასევე მთლიანად ისარგებლოს კიბერსივრცის ყველა უპირატესობებითა და მიღწევებით. 2011 წელს შემოღებული სტრატეგია ასახავს მაქსიმალური რისკების შემცირებას დამნაშავეთა (მათ შორის ტერორისტების) და სხვა სახელმწიფოთა მხრიდან კიბერშეტევების მიმართ, რაც მიმართულია კიბერსივრცეში თითოეული მოქალაქის, საზოგადოებისა და ეკონომიკის უსაფრთხოებისკენ.

ევროკავშირის არაწევრი ქვეყნების კიბერუსაფრთხოების სტრატეგიები - შეერთებული შტატები, კანადა და იაპონია

როგორც ზემოთ იყო აღნიშნული, აქ მოკლედ იქნება განხილული ევროკავშირს არაწევრი ქვეყნების - შეერთებული შტატების, კანადისა და იაპონიის კიბერუსაფრთხოების სტრატეგიების მთავარი და მნიშვნელოვანი მიმართულებები. გარდა ამისა, აღსანიშნავია ის გარემოებაც, რომ ბევრ ქვეყანას უკვე აქვს გამოქვეყნებული თავისი სტრატეგიები ამ მიმართულებით. მაგალითად, კიბერუსაფრთხოების სტრატეგიები გააჩნია ინდოეთს, ავსტრალიას, ახალ ზელანდიას, კოლუმბიას და სხვა ქვეყნებს. ეს ფაქტი ნათლად მოწმობს, რომ კიბერსივრცის დაცვა აღიარებულია მთავარ პრობლემურ საკითხად მთელს მსოფლიოში.

ამერიკის შეერთებული შტატები

2011 წლის მაისში[160] შეერთებულმა შტატებმა გამოაქვეყნა თავისი სტრატეგია კიბერსივრცის დაცვაზე. სტრატეგიას საფუძვლად უდევს მთავრობას, საერთაშორისო პარტნიორებსა და კერძო სექტორს შორის თანამშრომლობის მოდელი, სადაც აღწერილია მთელი რიგი ღონისძიებები, რომლებიც აუცილებელია გატარდეს შემდეგი შვიდი მიმართულებით:

- ეკონომიკა - საერთაშორისო სტანდარტებისა და ინოვაციების მოზიდვა, ღია და ლიბერალური ბაზარი;
- ეროვნული ქსელის დაცვა - უსაფრთხოების ამაღლება, სანდოობა და მდგრადობა;
- სამართალებრივი მხარე - თანამშრომლობისა და სამართლებრივი ნორმების გაფართოება;
- სამხედრო სფერო - უსაფრთხოების თანამედროვე გამოწვევებზე მზადყოფნა;
- სამთავრობო ინტერნეტის ქსელი - სამთავრობო სტრუქტურების ეფექტურობისა და მრავალმომცველობის გაფართოება;

[160] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

- საერთაშორისო განვითარება - უსაფრთხოების ორგანიზება, საერთაშორისო კომპეტენციების განვითარება და ეკონომიკური აყვავება;
- თავისუფლება ინტერნეტში - მოქალაქეთა კერძო ცხოვრების ხელშეუხებლობისა და თავისუფლების მხარდაჭერა.

<u>კანადა</u>

2010 წელს[161] გამოქვეყნებული კიბერუსაფრთხოების სტრატეგია ეფუძნება სამ ძირითად მიმართულებას:

- სამთავრობო სისტემების დაცვა;
- თანამშრომლობა ფედერალური მთავრობის გარეთ არსებული მთავარი კიბერ - სისტემების დაცვის მიზნით;
- კიბერსივრცეში კანადის მოქალაქეთა უსაფრთხოების უზრუნველყოფა.

პირველ მიმართულებაში იგულისხმება როლებისა და პასუხისმგებლობის მკვეთრი გამიჯვნა, ფედერალურ დონეზე კიბერ - სისტემების უსაფრთხოების გაძლიერება და კიბერუსაფრთხოების სფეროში მთავრობის ინფორმირების ამაღლება. მეორე მიმართულება ეს არის სახელმწიფო დონის საპარტნიორო პროექტები კერძო და კრიტიკული ინფრასტრუქტურის სექტორების მონაწილეობით. ბოლო, მესამე მიმართულება განსაზღვრავს ბრძოლას კიბერდანაშაულებებთან და ონლაინ სივრცეში კანადის მოქალაქეთა დაცვას. აქვე აგრეთვე განხილულია პერსონალური მონაცემების დაცვის პრობლემა.

<u>იაპონია</u>

იაპონიის კიბერუსაფრთხოების სტრატეგია, რომელიც გამოქვეყნდა 2010 წლის მაისის თვეში[162], შეიძლება დაიყოს რამოდენიმე მთავარ მიმართულებად, კერძოდ:

- მასიური კიბერშეტევების წინააღმდეგ ბრძოლა და ამ პროცესზე პასუხისმგებელი ორგანოს გაძლიერება;

[161] http://publications.gc.ca/site/eng/379746/publication.html
[162] http://www.nisc.go.jp/eng/

- ინფორმაციული უსაფრთხოების სფეროში ცვლილებებზე ადვილი ადაპტირების პოლიტიკის გატარება;
- ინფორმაციული უსაფრთხოების აქტიური პოლიტიკის უპირატესობა პასიურებთან მიმართებაში.

იაპონიის კიბერუსაფრთხოების სტრატეგიაში აღწერილი მიმართულებები ასევე მოიცავს:

- ინფორმაციული და საკომუნიკაციო ტექნოლოგიების რისკების მართვას საზოგადოების უსაფრთხო ცხოვრების უზრუნველყოფის მიზნით;
- პოლიტიკის დანერგვა, რომელიც ხელს შეუწყობს სახელმწიფო უსაფრთხოების გაძლიერებას, კიბერსივრცეში კრიზისების მართვის გაუმჯობესება, რაც წინააღმდეგობაში არ მოვა ინფორმაციული და საკომუნიკაციო სისტემების გამოყენების პოლიტიკასთან, რომელსაც საფუძვლად უდევს სოციალური და ეკონომიკური მოღვაწეობა;
- სამნაწილიანი პოლიტიკა, სადაც კომპლექსურად განიხილება ეროვნული უსაფრთხოების, კრიზისების მართვისა და პიროვნებისა და საზოგადოების დაცვის პრობლემა. განსაკუთრებით, აქტიურად განიხილება პიროვნებისა და საზოგადოების ინფორმაციული უსაფრთხოების უზრუნველყოფა;
- ინფორმაციული უსაფრთხოების პოლიტიკა, რომელიც არ ეწინააღმდეგება ეკონომიკური ზრდის პოლიტიკას და მოდის მასთან თანხვედრაში;
- საერთაშორისო თანამშრომლობა და ალიანსების შექმნა.

ევროკავშირის ინტერნეტის უსაფრთხოების სტრატეგია

ამ მომენტისთვის ევროკავშირს არ გააჩნია კიბერუსაფრთხოების საერთო სტრატეგია. თუმცა 2012 წლის[163] ევროკავშირის კომისიის სამუშაო პროგრამაში დამტკიცებულია, რომ კომისია შეიმუშავებს ევროკავშირისთვის ინტერნეტის უსაფრთხოების სტრატეგიას. მოცემული სტრატეგიის შემუშავებას თავის თავზე იღებს

[163] COM (2011) 777 final VOL.1/2 http://ec.europa.eu/atwork/peogrammes/docs/cwp2012_en.pdf

DG CONNECT (DG INFOSO)[164] - ს მთავარი დირექტორატი. პროექტის მიზნები მდგომარეობს შემდეგში:

- ძირითადი რისკებისა და პრობლემების პარალელურად გამოვლინდეს ეკონომიკური და გეოპოლიტიკური შესაძლებლობები;
- მოხდეს შედარება მზადყოფნის ხარისხისა და პოლიტიკური ყურადღების და მესამე ქვეყნების ინტერნეტის უსაფრთხოების პრობლემებს შორის;
- აღინიშნოს ძირითადი და მნიშვნელოვანი პრობლემები, რომლებიც მოითხოვს დაუყოვნებლივ გადაწყვეტას;
- შეფასდეს მიმდინარე და დაგეგმილი ღონისძიებები, აგრეთვე აღინიშნოს ის პრობლემური ზონები, რომლებზეც ევროკავშირმა უნდა გაამახვილოს ყურადღება[165].

კიბერუსაფრთხოების სტრატეგია და ინტერნეტის უსაფრთხოების სტრატეგია - ეს არის ორი ერთმანეთისგან განსხვავებული თემა, თუმცა მათ გააჩნიათ ბევრი საერთოც. მაგალითად, შესაბამისი სამთავრობო მოდელის განსაზღვრა და შეთავაზება, რომელიც მიმართულია კიბერსივრცეში ინციდენტების გაუვნებელყოფაზე და მათ წინააღმდეგ ბრძოლაზე.

DG CONNECT - ის მთავარი დირექტორატის ძირითად ამოცანას წარმოადგენს გლობალურ პოლიტიკურ კონტექსტში სწორად დაალაგოს არსებული და დაგეგმილი ღონისძიებები. ინტერნეტის უსაფრთხოების პრობლემის მიმართ კომპლექსური და სტრუქტურული მიდგომის მიზნით, დირექტორატი ევროკავშირს ასევე უმზადებს და აწვდის მომავალ სამოქმედო გეგმას[166]. პროექტის რეალიზაციისთვის მარტო DG CONNECT - ის მთავარი დირექტორატის კომპეტენცია საკმარისი არ არის. ამიტომ მოცემულ თემაზე

[164] http://ec.europa.eu/dgs/connect/en/content/dg-connect
[165] COM(2011) 777 final VOL.2/2 http://ec.europa.eu/atwork/programmes/docs/cwp2012_annex_en.pdf
[166] ROADMAP: Proposal on a European Strategy for Internet Strategy http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf

მიმდინარეობს კომპლექსური და კოორდინირებული მუშაობა ევროკავშირის სხვა კომისიებთან მჭიდრო თანამშრომლობით[167].

არაერთხელ იქნა აღნიშნული ის გარემოება, რომ აუცილებელია მიღწეულ იყოს კოორდინირებული და კომპლექსური მუშაობა, რის შესახებაც საუბარია 2011 წლის ENISA - ს დოკუმენტში „კიბერუსაფრთხოება: მომავალი გამოწვევები და შესაძლებლობები“[168] და ლორდთა პალატის მიერ პარლამენტში საბჭოზე გაკეთებულ მოხსენებაში ევროკავშირის შიდა უსაფრთხოების სტრატეგიის შესახებ[169].

ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების სტრატეგიების საერთო პრინციპები და რეკომენდაციები

კიბერუსაფრთხოების განსაზღვრების შესახებ შეთანხმება საერთაშორისო დონეზე არ არსებობს[170]. ყოველ ქვეყანაში კიბერუსაფრთხოების, კიბერსივრცის, კიბერდანაშაულისა და მასთან დაკავშირებული მთავარი ტერმინების განსაზღვრება შეიძლება მკვეთრად განსხვავდებოდეს ერთმანეთისგან. ასევე განსხვავდება თითოეული ქვეყნის მიდგომა კიბერუსაფრთხოების სტრატეგიის შედგენის მიმართ. მიუხედავად იმისა, რომ საერთაშორისო თანამშრომლობის მნიშვნელობას აღიარებს ყველა ქვეყანა, მაინც საერთო მთავარი ტერმინებისა და ერთიანი ე. წ. „ენის“ არარსებობა ძალზედ ართულებს თანამშრომლობას საერთაშორისო დონეზე.

<u>საერთო პრინციპები</u>

როგორც წესი, ყოველი ქვეყნის კიბერუსაფრთხოების სტრატეგიებს მაინც გააჩნიათ საერთო პრინციპები, რომელიც შიძლება შემდეგნაირად ჩამოყალიბდეს:

- ✓ სახელმწიფო მოდელისა და პოლიტიკის შემუშავება, რომელიც მიმართულია კიბერუსაფრთხოების უზრუნველყოფაზე;

[167] SPEECH/12/204 http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/204
[168] http://www.enisa.europa.eu/publications/position-papers/cyber-security-future-challenges-and-opportunities
[169] http://www.publications.parliament.uk/pa/ld201012/ldselect/ldeucom/149/149.pdf
[170] H. Luiijf, K. Besseling, M Spoelstra, P. de Graaf, Ten National Cyber Security Strategies: a comprasion, CRITIS 2001 – 6th International Conference on Critical Information Infrastructures Security, September 2011

- ✓ სახელმწიფო პარტნიორობაზე დაფუძნებული შესაბამისი მექანიზმის განსაზღვრა, რომელიც კერძო და სახელმწიფო სექტორის დაინტერესებულ მხარეებს საშუალებას აძლევს განიხილონ და დაამტკიცონ პოლიტიკა დაკავშირებული კიბერუსაფრთხოების პრობლემებთან;
- ✓ აუცილებელი პოლიტიკისა და მექანიზმების რეგულაციების დაგეგმვა და განსაზღვრა, როლების, უფლებებისა და პასუხისმგებლობის მკვეთრი გამიჯვნა კერძო და სახელმწიფო სექტორისთვის;
- ✓ საერთაშორისო დონეზე თანამშრომლობა ინფორმაციის გაცვლაზე კიბერდანაშაულის შესახებ და ამისთვის აუცილებელი საკანონმდებლო ბაზის არსებობა. ეს საშუალებას იძლევა განხორციელდეს თანამშრომლობა საერთაშორისო დონეზე. მაგალითად, ჰოლანდია[171] და საფრანგეთი[172] აძლიერებენ თავიანთ საკანონმდებლო ბაზას მიმართულს კიბერდანაშაულის, გამოძიებისა და სამართლებრივი დევნის შესახებ;
- ✓ კრიტიკული ინფორმაციის ინფრასტრუქტურის (CII – Critical Information Infrastructure Protection) განსაზღვრა. მათ შორის ძირითადი აქტივების, მომსახურებისა და ურთიერთდამოკიდებულების განვითარება;
- ✓ მზადყოფნის ამაღლება, ინციდენტებზე რეაგირების დროის მაქსიმალურად შემცირება, დაზიანებული კრიტიკული ინფორმაციის ინფრასტრუქტურის (CII – Critical Information Infrastructure Protection) დროული აღდგენისა და დაცვის მექანიზმების გეგმის შემუშავება. ორგანიზაციული სტრუქტურების ინტეგრაციის აუცილებელი განსაზღვრა, რომელთა ვალდებულებებში შედის ამაღლებული მზადყოფნის საშუალებების, დაცვის მექანიზმებისა და დაზიანებული ინფრასტრუქტურის დროული აღდგენის გეგმების დამუშავება, დანერგვა და ტესტირება;
- ✓ რისკების სახელმწიფო მართვის მიმართ სისტემური და ინტეგრირებული მიდგომის შემუშავება;

[171] ჰოლანდიის სტრატეგია, გვ. 12
[172] საფრანგეთის სტრატეგია, გვ. 8

- ✓ ინფორმაციული პროგრამების მიზნების განსაზღვრა და აღნიშვნა, რომელიც მიმართულია შესთავაზოს მომხმარებელს ქცევისა და მუშაობის ახალი მოდელები;
- ✓ საერთაშორისო თანამშრომლობა არამარტო ევროკავშირის წევრ - ქვეყნებს შორის, არამედ იმ ქვეყნებთანაც, რომლებიც არ შედიან ევროკავშირში;
- ✓ კომპლექსური კვლევების ჩატარება და პროგრამების განვითარებაზე მუშაობა, რომელიც მიმართულია კიბერსივრცის უსაფრთხოების პრობლემების გადაჭრაზე. ინტელექტუალური რესურსების განვითარება;
- ✓ განათლების ახალი პროგრამების აუცილებლობა, რომელიც მიმართულია ინფორმაციული და საკომუნიკაციო ტექნოლოგიების სპეციალისტებისა და სხვა საჭირო ადამიანური რესურსების მომზადებაზე, გადამზადებასა და პროფესიულ განვითარებაზე კიბერუსაფრთხოების სფეროში. ასევე ტრენინგებისა და სხვა მოკლე სასწავლო კურსების ჩატარების აუცილებლობა, რომელიც ანვითარებს მომხმარებლის უნარ - ჩვევებს. მაგალითად, გაერთიანებული სამეფოს[173] კიბერუსაფრთხოების სტრატეგიაში აქტიურად არის განხილული ინფორმაციული უსაფრთხოების სპეციალისტების საგანმანათლებლო პროგრამების განვითარება, რომელიც ხელს შეუწყობს კიბერუსაფრთხოების სანდო და პროფესიული ფუნდამენტის შექმნას.

<u>რეკომენდაციები</u>

გარემოში, სადაც მუდმივად ვითარდება, თავს იჩენს და განიცდის ევოლუციას კიბერსაფრთხეები, ევროკავშირის წევრი ქვეყნები, რომლებიც მუდმივად აწყდებიან ახალ გამოწვევებსა და გლობალურ საფრთხეებს კიბერსივრცეში, მიიღებენ დიდ სარგებელს მოქნილი და ოპერატიული კიბერუსაფრთხოების სტრატეგიის არსებობის შემთხვევაში. კიბერდანაშაულის ტრანსსასაზღვრო ხასიათი წევრ - ქვეყნებს იძულებულს ხდის მჭიდროდ ითანამშრომლონ ერთმანეთთან და ზოგადად საერთაშორისო დონეზე.

[173] გაერთიანებული სამეფოს სტრატეგია, გვ. 29

მსგავსი თანამშრომლობა აუცილებელია არამარტო კიბერშეტევისთვის ეფექტური მომზადებისთვის, არამედ მათზე დროული რეაგირებისთვის. ამიტომ კიბერუსაფრთხოების მიმართ სახელმწიფო სტრატეგიის მიდგომა უნდა იყოს კომპლექსური.

ამ მიზნით, ევროკავშირი, მასში შემავალი წევრი ქვეყნების მიმართ იძლევა ზოგად რეკომენდაციებს, კერძოდ:

მოკლევადიანი პერიოდისთვის

- ✓ დაპროექტდეს, შეფასდეს და მხარი დაეჭიროს კიბერუსაფრთხოების სახელმწიფო სტრატეგიას. ასევე ის ღონისძიებები, რომლებიც აუცილებელია გატარდეს სტრატეგიის ჩარჩოში;
- ✓ მკვეთრად უნდა განისაზღვროს მოქმედების არეალი, სტრატეგიის მიზნები და თავად ტერმინი „კიბერუსაფრთხოება“;
- ✓ უნდა დარწმუნდნენ, რომ კიბერუსაფრთხოებაზე პასუხისმგებელი სახელმწიფო ორგანოს მიერ შემუსავებული წინადადებები და რეგულაციები, იქნება განხილული და მიღებული;
- ✓ სტრატეგიაში უნდა იქნას გათვალისწინებული სამეცნიერო საზოგადოების, სამრეწველო და ეკონომიკური წარმომადგენლებისა და სამოქალაქო ინტერესები;
- ✓ კიბერუსაფრთხოების კოორდინირებული და შეთანხმებული ხასიათის გარანტირებული თანამშრომლობის მიზნით, წევრმა ქვეყნებმა უნდა ითანამშრომლონ ერთმანეთთან, აგრეთვე მათ მჭიდრო ურთიერთობა უნდა გააჩნდეს ევროკავშირის კომისიასთან;
- ✓ აუცილებელია აღიარებული იქნას ის გარემოება, რომ კიბერსივრცე და კიბერუსაფრთხოება მუდმივად განიცდის განვითარებას, და ამიტომ სტრატეგია მუდმივად მოითხოვს რედაქტირებასა და გადახედვას, რათა ის შესაბამისობაში იქნას მოყვანილი ახალ გამოწვევებთან;

- ✓ აუცილებელია გავითვალისწინოთ ის ფაქტი, რომ მუდმივად არსებული რისკები და ახალი საფრთხეები საშუალებას იძლევა განვითარდეს და გაუმჯობესდეს ინფორმაციული სისტემები სახელმწიფო, კერძო და სამოქალაქო სექტორებისთვის;
- ✓ აუცილებელია თავიდან იქნას არიდებული გატარებული ღონისძიებების დუბლირება და ფოკუსირება გაკეთდეს ახალ პრობლემებსა და გამოწვევებზე;
- ✓ აუცილებელია, რომ სტრატეგია შესაბამისად იქნას გამოყენებული და მოქმედებდეს ეროვნული და ევროპული უსაფრთხოების დონის ამაღლებაზე;
- ✓ მხარი უნდა დაეჭიროს ევროკავშირის კომისიას ინტერნეტის უსაფრთხოების სტრატეგიაზე მუშაობის, შექმნისა და იმპლიმენტაციის საკითხში.

გრძელვადიანი პერიოდისთვის

- ✓ მომავალში მთლიანად ევროკავშირისთვის საერთო მიზნების მიღწევისა და ფორმულირების მიზნით, აუცილებელია შემუშავდეს და შეთანხმდეს „კიბერუსაფრთხოების“ საერთო განსაზღვრება და მასთან დაკავშირებული ტერმინოლოგია;
- ✓ აუცილებელია გათვალისწინებული იქნას ის გარემოება, რომ ევროკავშირისა და მისი წევრი ქვეყნების კიბერუსაფრთხოების სტრატეგიები არ უნდა ეწინააღმდეგებოდეს საერთაშორისო საზოგადოების მიზნებს და ადამიანის უფლებებს, თუმცა ამავდროულად, გლობალურ დონეზე მხარს უნდა უჭერდეს კიბერუსაფრთხოების პრობლემებთან ბრძოლას.

კიბერუსაფრთხოების სტრატეგიის რეალიზაციისთვის აუცილებელია კერძო და სახელმწიფო სექტორების ერთმანეთთან მჭიდრო თანამშრომლობა, რომელიც სახელმწიფო და ზოგადად ევროკავშირის დონეზე, უნდა განხორციელდეს ინფორმაციის

გაცვლის საშუალებებით, მოწინავე ტექნოლოგიებისა და პრაქტიკული ცოდნის გაზიარებით, აგრეთვე სამეცნიერო წრეების ერთმანეთთან დაახლოებითა და პრობლემაზე ერთობლივი მუშაობით.

როგორც ზემოთ იყო აღნიშნული, ENISA ევროკავშირის კომისიისა და წევრი ქვეყნებისთვის სტრატეგიის შექმნის მიზნით, შეიმუშავებს სპეციალურ სახელმძღვანელოს (Good Practices Guide). მოცემული სახელმძღვანელო შეიცავს რეკომენდაციებსა და მოწინავე პრაქტიკას კიბერუსაფრთხოების სახელმწიფო სტრატეგიის დაპროექტებისთვის, დანერგვისა და მხარდასაჭერად. ის არის სასარგებლო ინსტრუმენტი და პრაქტიკული რჩევები იმ პირებისთვის, ვინც არის სტრატეგიის დაპროექტებაზე პასუხისმგებელი ან ჩართულია ამ პროცესში. სახელმძღვანელო მუშავდება მთელი ევროპის მასშტაბით კერძო და სახელმწიფო სექტორიდან დაინტერესებული მხარეების მონაწილეობითა და ხელშეწყობით. სახელმძღვანელოს დამუშავებაში ასევე მონაწილეობას იღებენ ის საერთაშორისო ექსპერტები, რომლებიც აწარმოებენ ENISA - ს რეკომენდაციების შუალედურ ანალიზს.

საქართველოს კიბერუსაფრთხოების სტრატეგია, პოლიტიკა და გამოწვევები

2008 წლის აგვისტოში, საქართველო - რუსეთის ომის დროს, რუსეთის მხრიდან განხორციელდა მასიური კიბერშეტევა საქართველოს ინტერნეტ სივრცეზე, რის შედეგადაც გარკვეული პერიოდი პარალიზებული იყო ქვეყნის სამთავრობო და კერძო სექტორის ვებ - გვერდები, შეუძლებელი იყო დაკავშირება გარე სამყაროსთან. საქართველოს კიბერუსაფრთხოების სტრატეგიის შესავალ ნაწილში ვკითხულობთ, რომ „2008 წლის აგვისტოში რუსეთის ფედერაციის მიერ საქართველოს წინააღმდეგ განხორციელებულმა ფართომასშტაბიანმა კიბერშეტევებმა ნათლად აჩვენა, რომ საქართველოს ეროვნული უსაფრთხოება ვერ შედგება კიბერსივრცის უსაფრთხოების უზრუნველყოფის გარეშე. რუსეთ - საქართველოს ომის დროს, რუსეთის ფედერაციამ საქართველოს წინააღმდეგ სახმელეთო, საჰაერო და საზღვაო შეტევების პარალელურად, განახორციელა მიზანმიმართული და მასირებული კიბერშეტევები. აღნიშნულმა კიბერშეტევებმა აჩვენა, რომ კიბერსივრცის დაცვა ეროვნული უსაფრთხოებისთვის ისევე

მნიშვნელოვანია, როგორც სახმელეთო, საზღვაო და საჰაერო სივრცეების დაცვა“[174]. ეს კიბერშეტევა ბევრი საერთაშორისო ექსპერტის მიერ შეფასდა როგორც „ინფორმაციული/კიბერ ომი“ საქართველოს წინააღმდეგ, რასაც ქვეყანა მოუმზადებელი შეხვდა, არ არსებობდა საჭირო რესურსები, გამოცდილება და შესაბამისად საქართველომ კიბერშეტევის მოგერიება ვერ შეძლო. შედეგად ქვეყანა აღმოჩნდა სერიოზული საერთაშორისო ინფორმაციული ვაკუუმის წინაშე. პრობლემა გადაიჭრა ქვეყნის უცხოელი სტრატეგიული პარტნიორების, კერძოდ ესტონელების ჩარევის შემდეგ, რის შედეგადაც შეჩერებული და თავიდან აცილებული იქნა მთლიანი ინფრასტრუქტურის განადგურება.

2008 წლის აგვისტოს ომისა და მისი შედეგების გათვალისწინებით, რაც უკავშირდებოდა ქვეყნის დაუცველ კიბერსივრცეს, საქართველოს ხელისუფლებამ დაიწყო სამართლებრივ - ნორმატიულ ბაზაზე მუშაობა მოცემული მიმართულებით, რის შედეგად 2013 წლის მაისში გამოქვეყნდა საქართველოს კიბერუსაფრთხოების სტრატეგია, რომელიც „წარმოადგენს „ეროვნული უსაფრთხოების მიმოხილვის“ პროცესის ფარგლებში შექმნილი კონცეპტუალური და სტრატეგიული დოკუმენტების პაკეტის ნაწილს. შესაბამისად, აღნიშნული სტრატეგია ეფუძნება „საქართველოს საფრთხეების შეფასების 2010 – 2013 წ.წ. დოკუმენტს“ და „საქართველოს ეროვნული უსაფრთხოების კონცეფციას““[175].

<u>საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ</u>

კიბერუსაფრთხოების სტრატეგიის გამოქვეყნებას წინ უძღოდა 2012 წლის ივნისში[176] კანონის „ინფორმაციული უსაფრთხოების შესახებ“ გამოქვეყნება. მოცემული კანონის მიზანია „ხელი შეუწყოს ინფორმაციული უსაფრთხოების დაცვის ქმედით და ეფექტიან განხორციელებას, დააწესოს საჯარო და კერძო სექტორების უფლება - მოვალეობები ინფორმაციული უსაფრთხოების დაცვის სფეროში, აგრეთვე განსაზღვროს

[174] საქართველოს კიბერუსაფრთხოების სტრატეგია, გვ. 1
[175] საქართველოს კიბერუსაფრთხოების სტრატეგია, გვ. 1
[176] http://www.economy.ge/uploads/kanonmdebloba/kavshirgabmuloba/informaciuli_usafrtxoeba.pdf

ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების სახელმწიფო კონტროლის მექანიზმები“[177].

კანონში „ინფორმაციული უსაფრთხოების შესახებ“ მოცემულია ტერმინთა განმარტებები, რომლის თანახმად ინფორმაციული უსაფრთხოება ეს არის „საქმიანობა, რომელიც უზრუნველყოფს ინფორმაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, ავთენტიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვას“[178]. იქვე განმარტებულია კრიტიკული ინფორმაციული სისტემა და ის სუბიექტები[179], რომელთა ქვეყნის კიბერსივრცეში დაცვა აუცილებელი პირობაა ეროვნული უსაფრთხოების უზრუნველსაყოფად.

კანონი ასევე იძლევა კიბერსივრცის, კიბერშეტევისა და კომპიუტერული ინციდენტების საინტერესო განსაზღვრებას. კერძოდ:

„კიბერსივრცე - სივრცე, რომლის განმასხვავებელი ნიშანია ელექტრონული მოწყობილობებისა და ელექტრომაგნიტური სპექტრის გამოყენება ქსელით დაკავშირებული სისტემებისა და დამხმარე ფიზიკური ინფრასტრუქტურის მეშვეობით მონაცემთა შენახვისათვის, შეცვლისათვის და გაცვლისათვის;

კიბერშეტევა - ქმედება, როდესაც ელექტრონული მოწყობილობა ან/და მასთან დაკავშირებული ქსელი ან სისტემა გამოიყენება კრიტიკულ ინფორმაციულ სისტემაში შემავალი სისტემების, ქონების ან ფუნქციების მთლიანობის დარღვევის, შეფერხების ან განადგურების ან ინფორმაციის უკანონოდ მოპოვების გზით;

კომპიუტერული ინციდენტი - ინფორმაციული უსაფრთხოების პოლიტიკის რეალური ან პოტენციური დარღვევა, რომელიც ხორციელდება ინფორმაციული

[177] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, გვ. 1
[178] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, გვ. 1
[179] კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხა განსაზღვრულია საქართველოს პრეზიდენტის 2013 წლის 11 მარტის № 157 ბრძანებულებით https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=1867646&lang=ge

ტექნოლოგიის გამოყენებით და იწვევს ინფორმაციის უნებართვო წვდომას, გამჟღავნებას, დაზიანებას ან შეფერხებას ან ინფორმაციული რესურსის მიტაცებას“[180].

კანონში განსაზღვრული და ზოგადად ჩამოყალიბებულია ის პრიორიტეტული საფრთხეები[181], რომლებიც შეიძლება თან ახლდეს კიბერუსაფრთხოებას, კერძოდ:

„ა) კიბერშეტევა, რომელიც საფრთხეს უქმნის ადამიანთა სიცოცხლესა და ჯანმრთელობას, სახელმწიფო ინტერესებს ან ქვეყნის თავდაცვისუნარიანობას;

ბ) კიბერშეტევა კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული სისტემების წინააღმდეგ;

გ) კიბერშეტევა, რომელიც საფრთხეს უქმნის სახელმწიფოს, ორგანიზაციის ან კერძო პირის ფინანსურ რესურსებს ან/და საკუთრების უფლებას;

დ) სხვა ნებისმიერი ქმედება, რომელიც, მისი ხასიათიდან, მიზნიდან, წყაროდან, მოცულობიდან ან რაოდენობიდან ან მისი აღკვეთისათვის საჭირო რესურსების ოდენობიდან გამომდინარე, კრიტიკული ინფორმაციული სისტემის ნორმალური ფუნქციონირებისათვის საკმარისი საფრთხის შემცველია“.

კანონი ასევე საინტერესოა იმ თვალსაზრისით, რომ ის განსაზღვრავს კიბერუსაფრთხოებაზე პასუხიმგებელ და მაკოორდინირებელ სახელმწიფო ორგანოს. კერძოდ, კანონის მე - 3 თავში „კიბერუსაფრთხოების უზრუნველყოფა“ ვკითხულობთ, რომ „საქართველოს კიბერსივრცეში ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვას, ასევე ინფორმაციული უსაფრთხოების კოორდინაციისკენ მიმართულ სხვა, მასთან დაკავშირებულ საქმიანობას, რომელიც კიბერუსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრას ემსახურება, ახორციელებს მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი - CERT.GOV.GE“[182][183]. მოცემული ჯგუფის მოვალეობებში შედის

[180] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, გვ. 1, 2
[181] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, თავი III, მუხლი 8, გვ. 7
[182] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, თავი III, მუხლი 8, გვ. 7

კრიტიკული ინფორმაციული სისტემის ინფორმაციული უსაფრთხოების დაცვის შესახებ რეკომენდაციების გაცემა, კომპიუტერული ინციდენტების ანალიზი, აღრიცხვა, მათი დროული გამოვლენა, რეაგირება და კოორდინაციის უზრუნველყოფა და სხვა. ასევე, ჯგუფი პასუხისმგებელია მოცემულ სფეროში ცნობიერების ამაღლებაზე, საგანმანათლებლო პროცესზე და სხვა[184]. კანონში ასევე ასახულია კრიტიკული ინფორმაციული სისტემის სუბიექტის მხრიდან პასუხისმგებელი პირის განსაზღვრის აუცილებელი ვალდებულება, კერძოდ „კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია განსაზღვროს კონკრეტული პირი (პირები) ან თანამშრომელი (თანამშრომლები), რომელიც (რომლებიც) პასუხისმგებელია (პასუხისმგებელი არიან) კრიტიკული ინფორმაციული სისტემის სუბიექტის კომპიუტერული სისტემების უსაფრთხოების პრაქტიკული უზრუნველყოფისათვის (კომპიუტერული უსაფრთხოების სპეციალისტი)“[185].

საქართველოს კიბერუსაფრთხოების სტრატეგია

საქართველოს კიბერუსაფრთხოების სტრატეგია გამოქვეყნდა 2013 წლის 20 მაისს[186], საქართველოს პრეზიდენტის 2013 წლის 17 მაისის №321 ბრძანებულების მიღების თანახმად. მოცემული დოკუმენტი შემუშავდა საქართველოს ეროვნული უშიშროების საბჭოსთან არსებული ეროვნული უსაფრთხოების სტრატეგიული დოკუმენტების შემუშავების მაკოორდინირებელი მუდმივმოქმედი საუწყებათაშორისო კომისიის მიერ და ის წარმოადგენს არამარტო სტრატეგიას, არამედ მასში მოცემულია ასევე ამ სტრატეგიის განხორციელების 2013 – 2015 წ.წ. სამოქმედო გეგმაც[187].

„საქართველოს კიბერუსაფრთხოების სტრატეგია არის კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელი ძირითადი დოკუმენტი, რომელიც

---

[183] 2013 წლის 24 დეკემბერს კანონში ინფორმაციული უსაფრთხოების შესახებ შევიდა ცვლილებები, რომლის თანახმად თავდაცვის სამინისტროში შეიქმნა კიბერუსაფრთხოების ბიურო, რომელიც პასუხისმგებელია თავდაცვის სფეროში კიბერსივრცის დაცვის უზრუნველყოფაზე, მეტი ინფორმაცია შეგიძლიათ იხილოთ https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=2162943

[184] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, თავი III, მუხლი 8, გვ. 7, 8

[185] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, თავი III, მუხლი 9, გვ. 8

[186] https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=1923932

[187] საქართველოს კიბერუსაფრთხოების სტრატეგია, დანართი №2

ასახავს სტრატეგიულ მიზნებს, ძირითად პრინციპებს, აყალიბებს სამოქმედო გეგმებს და ამოცანებს. სტრატეგიაზე დაყრდნობით, საქართველოს ხელისუფლება გაატარებს ღონისძიებებს, რომლებიც ხელს შეუწყობს სახელმწიფო ორგანოების, კერძო სექტორისა და სამოქალაქო საზოგადოების კიბერსივრცეში დაცულად ფუნქციონირებას, ელექტრონული ოპერაციების უსაფრთხო განხორციელებას და ქვეყანაში ეკონომიკისა და ბიზნესის შეუფერხებლად მოქმედებას“[188].

სანამ სტრატეგიის განხილვაზე გადავიდოდეთ, ვნახოთ კანონში „ინფორმაციული უსაფრთხოების შესახებ“ თუ როგორი განსაზღვრება აქვს იმ ძირითად საკითხებს, რაც უშუალო კავშირშია კუბერუსაფრთხოების უზრუნველყოფასთან. კერძოდ:

„კრიტიკული ინფორმაციული სისტემა - ინფორმაციული სისტემა, რომლის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალური ფუნქციონირებისათვის“[189] და „კრიტიკული ინფორმაციული სისტემის სუბიექტი - სახელმწიფო ორგანო ან იურიდიული პირი, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისათვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისათვის“[190].

საქართველოს ეროვნული უსაფრთხოების კონცეფცია კიბერსივრცის დაცვის უზრუნველყოფასა და ზოგადად კიბერუსაფრთხოებას განიხილავს, როგორც ქვეყნის უსაფრთხოების ერთ - ერთ ძირითად შემადგენელ ნაწილსა და მის მნიშვნელოვან მიმართულებას. კიბერსივრცის დაცვასა და კიბერუსაფრთხოების უზრუნველყოფაზე ბევრად არის დამოკიდებული ქვეყნის შემდგომი ეკონომიკური სტაბილურობა და

[188] საქართველოს კიბერუსაფრთხოების სტრატეგია, გვ. 1
[189] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, გვ. 2
[190] იქვე, დანარჩენი ტერმინოლოგია იხილეთ საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ http://www.economy.ge/uploads/kanonmdebloba/kavshirgabmuloba/informaciuli_usafrtxoeba.pdf

სოციალური განვითარება. მოცემული მიზნის მისაღწევად, სტრატეგია განიხილავს შემდეგი თანამშრომლობის მნიშვნელოვან პრინციპებს[191]:

- საქართველოს მთავრობის ერთიანი მიდგომა;
- თანამშრომლობა სახელმწიფო და კერძო სექტორებს შორის;
- აქტიური საერთაშორისო თანამშრომლობა;
- ინდივიდუალური პასუხისმგებლობა;
- ადეკვატური ზომები.

სტრატეგიის მთავარი მიზანია კიბერშეტევის ან სხვა ქმედებების საზიანო შედეგები და რისკები მაქსიმალურად იქნას შემცირებული და უმოკლეს დროში მოხდეს დაზიანებული ინფორმაციული ინფრასტრუქტურის სრული აღდგენა. ყოველივე ამას ემატება კრიტიკული ინფორმაციული სისტემების მდგრადობისა და დაცულობის ამაღლება, ასევე დროული პრევენცია.

გლობალური ინტერნეტ სივრცის მუდმივი განვითარება და მასთან დაკავშირებული არსებული საფრთხეები, საქართველოს კიბერსივრცესა და შესაბამისად კრიტიკული ინფორმაციული ინფრასტრუქტურის სისტემის გამართულ ფუნქციონირებას მუდმივად ახალი გამოწვევების წინაშე აყენებს. სტრატეგიის თანახმად, ინფორმაციული სისტემის კრიტიკულობა და კიბერუსაფრთხოების მდგრადობა განისაზღვრება ისეთი კრიტერიუმებით, როგორიცაა მოსალოდნელი მატერიალური ზარალის სიმძიმე და მასშტაბები, ინფორმაციული სისტემის აუცილებლობა სახელმწიფოსა და საზოგადოების ნორმალური ფუნქციონირება, სისტემის მომხმარებელთა რაოდენობა და კიბერუსაფრთხოების სათანადო დონის უზრუნველყოფა საჭირო რესურსებით.

საერთაშორისო სისტემაში არსებული საფრთხეებისა და გამოწვევების გათვალისწინებით, საქართველოს უსაფრთხოების პოლიტიკის დაგეგმვა და განხორციელება განიხილავს კიბერუსაფრთხოების სფეროში შემდეგ საფრთხეებსა და გამოწვევებს:

[191] საქართველოს კიბერუსაფრთხოების სტრატეგია, გვ. 2

- კიბერომი ან/და კიბერშეტევა, რომელიც მიმართულია პოტენციური მოწინააღმდეგის მხრიდან საქართველოს მთლიანი კიბერსივრცის დაზიანებისა და მწყობრიდან გამოყვანისკენ. ამასთან, ქვეყანა კვლავ დგას მასიური კიბერშეტევის საფრთხის წინაშე;
- კიბერტერორიზმი, რომელმაც კრიტიკულ ინფორმაციულ ინფრასტრუქტურაზე კიბერშეტევით შეიძლება მნიშვნელოვანი ზიანი მიაყენოს ქვეყნის ეროვნულ უსაფრთხოებას;
- კიბერსივრცის გამოყენებით ჩადენილი სხვა ქმედებები, რომელმაც შეიძლება ზიანი მიაყენოს კრიტიკული ინფორმაციული ინფრასტრუქტურის ცალკეულ სუბიექტებს, რაც გამოიწვევს ეკონომიური, სოციალური თუ სხვა სფეროს ფუნქციონირების უარყოფით შედეგებს.

სტრატეგიაში განხილულია ასევე საქართველოს კიბერუსაფრთხოების პოლიტიკის ძირითადი მიმართულებები:

- კვლევა და ანალიზი;
- ახალი საკანონმდებლო - ნორმატიული ბაზა;
- კიბერუსაფრთხოების უზრუნველყოფის ინსტიტუციური კოორდინაცია;
- საზოგადოებრივი ცნობიერების ამაღლება და საგანამანმათლებლო ბაზის ჩამოყალიბება;
- საერთაშორისო თანამშრომლობა.

ძალზედ მნიშვნელოვანია, რომ კიბერუსაფრთხოების და მასთან დაკავშირებული ქმედებები, იქნება ეს სამართლებრივი და ნორმატიული აქტები, სხვადასხვა ინიციატივები, რეკომენდაციები, ინსტრუქციები, ასევე კიბერსივრცეში მიმდინარე პროცესები, ემყარებოდეს კვლევებსა და ანალიზს, რომელიც უზრუნველყოფს არამარტო კიბერუსაფრთხოების პოლიტიკის ეფექტიანობასა და კრიტიკული ინფორმაციული ინფრასტრუქტურის სისტემის ნორმალურ ფუნქციონირებას, არამედ ასევე დადებითად აისახება მთლიანად ეროვნული უსაფრთხოების პოლიტიკაზე.

სტრატეგიის მიხედვით, კვლევა და ანალიზი აუცილებელია განხორციელდეს შემდეგი მიმართულებებით:

- სხვა ქვეყნების საუკეთესო პრაქტიკის შესწავლა და გამოცდილების გაზიარება;
- კრიტიკული ინფორმაციული ინფრასტრუქტურის ობიექტების იდენტიფიცირების კრიტერიუმებისა და სტანდარტების კვლევა;
- კრიტიკული ინფორმაციული ინფრასტრუქტურის მდგრადობის ანალიზი;
- კიბერუსაფრთხოების სფეროში რეგიონში არსებული პრობლემატიკის შესწავლა;
- კიბერუსაფრთხოების განმსაზღვრელი სტანდარტების შემუშავება მათი შემდგომი დანერგვის მიზნით;
- საქართველოს კიბერსივრცის წინაშე მდგარი საფრთხეების და რისკების გამოვლენაზე წინადადებების პერიოდული მომზადება.

მიუხედავად მსოფლიოში არსებული ახალი გამოწვევებისა, საფრთხეებისა და პოტენციური მოწინააღმდეგების არსებობისა, დღევანდელი მდგომარეობით საქართველოს კიბერუსაფრთხოების სფეროში არ გააჩნია ეროვნული კანონმდებლობა. აუცილებელი და მნიშვნელოვანია საკანონმდებლო ბაზის შექმნა, რომელიც შესაბამისობაში იქნება მოსული საერთაშორისო სტანდარტებთან და ხელს შეუწყობს მოცემული სფეროს განვითარებას.

სტარტეგიის მიხედვით, სამართლებრივი ბაზის შექმნისა და მისი სრულყოფისათვის აუცილებელია გატარდეს შემდეგი ღონისძიებები:

- ინფორმაციული უსაფრთხოების შესახებ საკანონმდებლო აქტების ინიცირება;
- კრიტიკული ინფორმაციული ინფრასტრუქტურის განმსაზღვრელი და მისი კიბერუსაფრთხოების უზრუნველმყოფი ნორმატიული ბაზის შექმნა;
- კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის ფუნქციონირების სამართლებრივი უზრუნველყოფა;

- ევროპის საბჭოს 2001 წლის „კიბერდანაშაულის შესახებ“ კონვენციის რატიფიცირების შედეგად აღებული ვალდებულებების შესრულება;
- იმ ორგანოს ან ორგანოთა საკანონმდებლო დონეზე იდენტიფიცირება, რომელთა უფლებამოსილებაში შევა ინფორმაციული უსაფრთხოების პოლიტიკის განსაზღვრა და მაკოორდინირებელი ფუნქციის განხორციელება;
- კიბერუსფრთხოებასთან დაკავშირებული კრიზისული სიტუაციების დროს მოქმედების სარეზერვო გეგმების და პროცედურების გაწერა.

იმისთვის, რომ კიბერუსაფრთხოებამ და მასთან დაკავშირებულმა პროცესებმა ეფექტური გავლენა მოახდინოს ქვეყნის ეროვნულ უსაფრთხოებაზე და იმუშაოს ერთიან სისტემად, აუცილებელია უწყებათაშორისი საკოორდინაციო მექანიზმის შექმნა, გაძლიერება და სახელმწიფო და კერძო სექტორების მჭიდრო თანამშრომლობა.

ამ მიზნით, სტრატეგიაში მოცემულია შემდეგი ღონისძიებების გატარების აუცილებლობა:

- კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შემდგომი განვითარება;
- მაღალტექნოლოგიური დანაშაულის (კიბერდანაშაული) საერთაშორისო საკონტაქტო პუნქტის 24/7 შემდგომი განვითარება;
- კიბერდანაშაულის საქმეებზე საექსპერტო დახმარების ჯგუფის (დანაყოფი) განსაზღვრა;
- სახელმწიფო და კერძო სექტორებს შორის თანამშრომლობის ფორმატისა და მექანიზმების ჩამოყალიბება.

კიბერუსაფრთხოების სფეროში რისკების შემცირება და კიბერსივრცის მაქსიმალური დაცვის უზრუნველყოფა ბევრად არის დამოკიდებული საზოგადოებაში ცნობიერების ამაღლებაზე, შესაბამისი სპეციალისტების მომზადებასა და მათი პროფესიული დონის ამაღლებაზე, ასევე სგანმანათლებლო ბაზის შექმნა და სასწავლო პროცესის სწორად წარმართვა.

სტრატეგიის მიხედვით მოცემული პროცესი უნდა წარიმართოს შემდეგი ღონისძიებების გატარებით:

- კიბერუსაფრთხოების სფეროში საზოგადოებრივი ცნობიერების ამაღლებისა და საგანმანათლებლო პროგრამების შექმნა;
- კრიტიკული ინფორმაციული ინფრასტრუქტურის სუბიექტების და სხვა დაინტერესებული ორგანიზაციების კადრებისა და ტექნიკური პერსონალის გადამზადება ინფორმაციული უსაფრთხოების საერთაშორისო და ეროვნული სტანდარტების შესწავლისათვის;
- კიბერდანაშაულის ექსპერტების სპეციალიზებული ტრენინგები ელექტრონული მტკიცებულებების (კიბერკრიმინალისტიკის) დარგში;
- კიბერუსაფრთხოების სფეროში სამეცნიერო - კვლევითი პროექტების ხელშეწყობა;
- კვლევითი ლაბორატორიის შექმნა.

კიბერუსფრთხოების სრულყოფილი უზრუნველყოფისათვის აუცლებელია არამარტო ქვეყნის შიგნით მოხდეს კოორდინირებული მუშაობა, არამედ აუცილებელია საერთაშორისო თანამშრომლობის მუდმივი განვითარება როგორც საერთაშორისო ორგანიზაციებთან, ისე ცალკეულ ქვეყნებთან, რათა მოხდეს მათი გამოცდილების გაზიარება, გადმოტანა და მორგება ჩვენს რეალობას.

სტარტეგიაში მოცემულია ის ღონისძიებები, რომლებიც უნდა გატარდეს საერთაშორისო თანამშრომლობის განვითარებისათვის, კერძოდ:

- კიბერუსაფრთხოების საკითხებზე საერთაშორისო ურთიერთობების განმტკიცება ამ სფეროში მომუშავე საერთაშორისო ორგანიზაციებთან (OECD, EU, OSCE, CoE, UN, ITU)[192] და სახელმწიფო ორგანოებთან;

[192] The Organisation for Economic Co-operation and Development (OECD) http://www.oecd.org/
The European Union (EU) http://europa.eu/
The Organization for Security and Co-operation in Europe (OSCE) http://www.osce.org/
The Council of Europe (CE) http://www.coe.int/web/portal/home
The United Nations (UN) http://www.un.org/
The International Telecommunication Union (ITU) http://www.itu.int/en/Pages/default.aspx

- კიბერუსაფრთხოების სფეროში საერთაშორისო ინიციატივებში აქტიური მონაწილეობის მიღება და ამ ინიციატივების რეგიონის მასშტაბით მხარდაჭერა;
- სხვა ქვეყნების CERT - ებთან კიბერუსაფრთხოების სფეროში ორმხრივ და მრავალმხრივ ფორმატებში თანამშრომლობის ინიცირება.

საქართველოს კიბერუსაფრთხოების სტრატეგია არის გარდამავალი დოკუმენტი და მისი განხორციელების ვადებია 2013 – 2015 წლები, რისთვისაც შექმნილი არის სპეციალური სამოქმედო გეგმა[193] და მის განხორციელებაზე თავისი კომპეტენციის ფარგლებში პასუხისმგებელი უწყებები: საჯარო სამართლის იურიდიული პირი - მონაცემთა გაცვლის სააგენტო და საქართველოს CERT; საქართველოს შინაგან საქმეთა, იუსტიციისა და საგარეო საქმეთა სამინისტროები; საქართველოს ეროვნული უშიშროების საბჭოს აპარატი. სტრატეგიის სამოქმედო გეგმაში ასევე გათვალისწინებულია საერთაშორისო დახმარება კვლევითი ლაბორატორიის შექმნასა და ელექტრონული მტკიცებულებების (კიბერკრიმინალისტიკის) სფეროში, კიბერდანაშაულის ექსპერტების სპეციალიზებული ტრენინგების ორგანიზებაში.

რეზუმე

ნაშრომში მოკლედ, ზოგად ფორმებში არის განხილული ევროკავშირის წევრი ქვეყნებისა და შეერთებული შტატების, კანადისა და იაპონიის კიბერუსაფრთხოების სტრატეგიები, მათი პოლიტიკა და ძირითადი მიმართულებები. ასევე აქვე არის წარმოდგენილი თავად ევროკავშირის საერთო პოლიტიკა და მიდგომა ინტერნეტის უსაფრთხოების მიმართ. ფაქტიურად, ევროკავშირს არ გააჩნია ერთიანი კიბერუსაფრთხოების სტრატეგია, ის შემოიფარგლება მხოლოდ ცალკეული რეკომენდაციების გაცემით წევრი ქვეყნების მისამართით. თუმცა ამ ეტაპზე მიმდინარეობს აქტიური მუშაობა ევროკავშირის კიბერსივრცის დაცვის ერთიანი

[193] საქართველოს კიბერუსაფრთხოების სტრატეგია, დანართი №2 https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=1923932

პოლიტიკის შემუშავებაზე. წევრი ქვეყნები ინდივიდუალურად ახორციელებენ და ზრუნავენ საკუთარი კიბერსივრცის დაცვაზე. მიუხედავად ამისა, ყოველი წევრი ქვეყნის კიბერუსაფრთხოების სტრატეგიებს მაინც გააჩნიათ საერთო პრინციპები, რაც მოკლევადიანი და გრძელვადიანი პერიოდის რეკომენდაციებთან ერთად, ასევე არის წარმოდგენილი წინამდებარე ნაშრომში.

საქრთველოსთვის სულ უფრო აქტუალური ხდება საკუთარი კიბერსივრცის დაცვის უზრუნველყოფა. ნაშრომში წარმოდგენილია ქვეყნის კიბერუსაფრთხოების სტრატეგიის პრინციპები, ძირითადი მიმართულებები, პოლიტიკა და სამოქმედო გეგმა. ასევე მოკლედ არის განხილული კანონი „ინფორმაციული უსაფრთხოების შესახებ“. ფაქტიურად, რუსეთის მხრიდან 2008 წლის აგვისტოში, ომის დროს განხორციელებული მასიური კიბერშეტევის შემდეგ, ქვეყნის ხელისუფლების მხრიდან გადაიდგა გარკვეული ნაბიჯები ქვეყნის კიბერსივრცის დაცვის შექმნისა და გაძლიერების მიმართულებით. თუმცა ამ სფეროში მაინც არსებობს გარკვეული ხარვეზები, კერძოდ ამ დრომდე არ არსებობს ერთიანი მაკოორდინირებელი სტრუქტურული ერთეული, არ არის შექმნილი ეროვნული კანონმდებლობა, ძალზედ დაბალია საზოგადოების ცნობიერება ამ სფეროს მიმართ და არ არსებობს შესაბამისი საგანმანათლებლო პროგრამები, არ ტარდება სამეცნიერო - კვლევითი სამუშაოები, არ არის შექმნილი ლაბორატორია და ა. შ.

საქართველო აქტიურად მიისწრაფვის ევროინტეგრაციისკენ, ქვეყანა ცდილობს გახდეს ევროკავშირისა და ჩრდილოეთ ალიანსის სრულუფლებიანი წევრი, ხელი მოეწერა ასოცირების ხელშეკრულებას. ყოველივე ეს ნიშნავს, რომ ქვეყანა თავის თავზე იღებს ყველა იმ ვალდებულებას, რაც უზრუნველყოფს არამარტო საქართველოს უსაფრთხოებას, არამედ ევროკავშირის როგორც ცალკეული წევრი ქვეყნებისა ისე მთლიანად ევროკავშირის უსაფრთხოების შესაბამისი ნორმების დაცვას, სადაც ასევე იგულისხმება კიბერსივრცის მაქსიმალური დაცვის უზრუნველყოფა. ეს არის ქვეყნისთვის სერიოზული გამოწვევა, რადგან საქართველომ უნდა შექმნას ეროვნული კანონმდებლობა, წესრიგში მოიყვანოს და საერთაშორისო სტანდარტებს შეუსაბამოს

ქვეყნის კრიტიკული ინფორმაციული ინფრასტრუქტურის სისტემისა და ცალკეული სუბიექტების დაცვა, გაზარდოს საერთაშორისო თანამშრომლობა და რისკების შემცირების მიზნით, უნდა მოახდინოს საზოგადოების ცნობიერების ამაღლება და საგანმანათლებლო სისტემის შემუშავება.

კიბერსაფრთხეების წარმოშობის წყაროები და სახეობები. კიბერსაფრთხეებთან მებრძოლი სუბიექტები

შესავალი

„კიბერსივრცის“ ტერმინის განსაზღვრების ბევრი ვარიანტი არსებობს. თითოეული მათგანი იძლევა თავისებურ განმარტებას. თუმცა ყველა განმარტებაში განსაზღვრულია, რომ „კიბერსივრცე“ ეს არის ინფორმაციული და ტექნოლოგიური ინფრასტრუქტურის ურთიერთკავშირში არსებული კომპლექსი, სადაც შედის გლობალური ინტერნეტისა და ტელეკომუნიკაციის ქსელები, კომპიუტერული სისტემები, ასევე ჩართული პროცესორები, სერვერები და მაკონტროლირებელი მოწყობილობები, რომლებიც გამოიყენება მრეწველობის სხვადასხვა დარგში.

ახალი ტექნოლოგიების განვითარებასთან ერთად იზრდება საფრთხეები, რომლებიც დიდ ზიანს აყენებს კიბერსივრცეს და მის მომხმარებელს. სახელმწიფოს და სახელისუფლებო ორგაონოებს პირველ რიგში ადარდებთ ეროვნული უსაფრთხოების უზრუნველყოფა, კრიტიკული ინფორმაციისა და ინფორმაციული ინფრასტრუქტურის დაცვა როგორც უცხო სახელმწიფოს, ისე არასამთავრობო სუბიექტებისა და დაჯგუფებების მხრიდან ხელყოფისგან, რათა თავიდან იქნას აცილებული ინფორმაციის მოპარვა ან/და გადაცემა, ქსელის დაზიანება ან/და საერთოდ განადგურება. სახელმწიფოს უსაფრთხოების რეალურ საფრთხეს წარმოადგენს კიბერშეტევები, რომლებიც მიმართულია ისეთი სასიცოცხლო მნიშვნელობის მქონე ინფრასტრუქტურის განადგურებისკენ, როგორებიცაა სატელეკომუნიკაციო ქსელების, ენერგოგენერირებისა და ნავთობგადამამუშავებელი სიმძლავრეების სისტემები, ასევე ელექტრომომარაგების, საფინანსო, ჯანდაცვისა და სატრანსპორტო სისტემები.

ქვემოთ განხილულია კიბერსაფრთხეები და მათი სახეობები, რომლებიც ემუქრება კიბერსივრცეს და ზოგადად ინფორმაციული ინფრასტრუქტურის სისტემების

მთლიანობას. ასევე ნაჩვენებია წარმოშობის ის წყაროები, საიდანაც მომდინარეობს მოცემული კიბერსაფრთხეები. ნაშრომის მეორე ნაწილში განხილულია ის საერთაშორისო და რეგიონალური დონის სუბიექტები, რომლებიც ებრძვიან კიბერსაფრთხეებს და ცდილობენ დაიცვან კიბერსივრცე და ინფორმაციული ინფრასტრუქტურის სისტემები კიბერდამნაშავეთა ხელყოფისგან.

კიბერსაფრთხეების წარმოშობის წყაროები და სახეობები

კიბერდანაშაულთან ბრძოლის ერთერთ მთავარ პრობლემას წარმოადგენს ის ფაქტი, რომ ხშირად ძალზედ რთულია ზუსტად დაადგინო არამარტო უშუალო შემსრულებლები, არამედ მათი ადგილსამყოფელი ან ის ქვეყანა, საიდანაც განხორციელდა შეტევა. ამიტომ, დამნაშავეს ან დამნაშავეთა ჯგუფს შეუძლია ადვილად დამალოს არამარტო თავისი მონაწილეობა კიბერშეტევის ორგანიზებაში, არამედ თავისი თავი დააფიქსიროს როგორც ქსელის სხვა მომხმარებლად ან საერთოდ დარჩეს ანონიმურად.

კიბერსაფრთხეების წარმოშობის წყაროებს წარმოადგენენ როგორც სახელმწიფო და კერძო სექტორის წარმომადგენლები, ისე სხვადასხვა სახისა და ნიშნით შექმნილი ორგანიზაციები და ფიზიკური პირები. შეერთებული შტატების კონტროლის პალატის მასალების[194] მიხედვით, კიბერსაფრთხეების წარმოშობის წყაროები შეიძლება დავაკვალიფიციროთ შემდეგნაირად, კერძოდ:

- ✓ **სახელმწიფო** - უცხოეთის ქვეყნების სადაზვერვო სამსახურები კომპიუტერულ ტექნოლოგიებს იყენებენ ინფორმაციის შეგროვებისა და ჯაშუშობისთვის. მსგავსი ქმედებები სადაზვერვო სამსახურების მხრიდან შეიძლება მიმართული იყოს როგორც მეგობარი, ისე მოწინააღმდეგე ქვეყნების მიმართ, ან არასახელმწიფო სუბიექტების წინააღმდეგ. სახელმწიფო თავისი სადაზვერვო სამსახურების გამოყენებით, ახორციელებს კიბერშეტევებს პოტენციური მოწინააღმდეგე

[194] United States Government Accountability Office, Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk (Washington DC: US GAO, 2009)

სახელმწიფოების მიმართ დეზინფორმაციის, დესტაბილიზაციის, დაშინების ან ფართომასშტაბიანი კიბერომის წარმოების მიზნით. ასევე საყურადღებოა ის გარემოება, რომ ხშირად ხდება პიროვნების უსაფრთხოებისა და უფლებების დარღვევა. კერძოდ, სახელმწიფოს სპეციალურმა სამსახურებმა შეიძლება მიმართონ ისეთ ქმედებებს, რომელთა გამოყენებითაც ხდება მოქალაქეთა პერსონალური მონაცემების გადაჭერა, მოპარვა და გამოყენება. მსგავსი ქმედებები ხშირ შემთხვევაში ხდება სასამართლოს შესაბამისი ორგანოების სანქციისა და სწორი დემოკრატიული კონტროლის გარეშე;

- ✓ **კორპორაციები, კომპანიები** - დაკავებულნი არიან სამრეწველო/კორპორაციული ჯაშუშობითა და/ან დივერსიული საქმიანობით, რაშიც ისინი ხშირად იყენებენ ჰაკერებსა და ორგანიზებულ დამნაშავეთა ჯგუფებს. კომპანიების, კორპორაციებისა და კერძო სექტორის სხვა წარმომადგენლებს ასევე შეუძლიათ დაარღვიონ ადამიანის უფლებები პიროვნების პერსონალური მონაცემების შეგროვებისა და ანალიზის გზით, ან ზოგ შემთხვევაში მოცემული მონაცემების სახელმწიფო ორგანოებთან ან სხვა დაინტერესებულ პირებთან გაცვლით;
- ✓ **ჰაკერები** - იყო დრო როცა ჰაკერების მხრიდან ქსელებში არასანქცირებული შეღწევა ან პროგრამების გატეხვა დაკავშირებული იყო ჰაკერთა საზოგადოებაში ავტორიტეტის მოპოვებასთან ან წვრილმან ჰულიგნობასთან. დღესდღეისობით სურათი კარდინალურად არის შეცვლილი, კერძოდ ჰაკერთა უმრავლესობის ქმედება ატარებს კრიმინალურ ხასიათს. ადრე თუ ჰაკერებისთვის ქსელის გატეხვისათვის საჭირო იყო კომპიუტერული ტექნოლოგიების სფეროში სპეციალური უნარ - ჩვევების ცოდნა, როცა ამჟამად საკმარისია ინტერნეტიდან შესაბამისი ინსტრუქციებისა და პროტოკოლების გადმოქაჩვა და მათი გამოყენება შერჩეულ საიტზე კიბერშეტევის ორგანიზებისთვის. ამის გამო, კიბერშეტევის განხორციელება მომხმარებლისთვის გახდა უფრო ადვილად

ხელმისაწვდომი. ჰაკერთა მომსახურეობით სარგებლობენ არამარტო კორპორაციები და კომპანიები, არამედ სადაზვერვო ან სხვა სახის სპეციალური სამსახურებიც;

- ✓ **ჰაკტივისტები** - ტერმინი „ჰაკტივიზმი“ (hacktivism) წარმოიშვა ორი სიტყვის „Hack“ და “Activism” შეერთებით და ის აღნიშნავს სოციალური პროტესტის გამოხატვის ახალ მოვლენას, რომელიც წარმოადგენს თავისებურ სინთეზს რაღაცის მიმართ გამოხატული პროტესტის სოციალური აქტიურობისა და ჰაკერობის, რომელიც მიმართულია გარკვეული ვებ - გვერდების ან საფოსტო სერვისების წინააღმდეგ. თავიანთი პოლიტიკური მიზნების მისაღწევად, ჰაკტივისტები მიისწრაფვიან დააზიანონ ან საერთოდ მწყობრიდან გამოიყვანონ ზოგიერთი ვებ - გვერდი;
- ✓ **კიბერ დივერსანტები ქსელის უკმაყოფილო მომხმარებელთა რიცხვიდან** - ზოგადად, უკმაყოფილო მომხმარებლები წარმოადგენენ სერიოზულ საფრთხეს, ვინაიდან ისინი კარგად იცნობენ სისტემის მუშაობის პრინციპებს და შეუძლიათ თავიანთი ეს ცოდნა გამოიყენონ დესტრუქციული მიზნებისთვის. მაგალითად, სისტემის დასაზიანებლად ან კონფიდენციალური ინფორმაციის მოსაპარად. შეერთებული შტატების ფედერალური საგამოძიებო ბიუროს (FBI) მონაცემებით, სისტემის მომხმარებლებისა და გარე წყაროების მხრიდან კიბერშეტევის ორგანიზების შესაძლებლობის ერთმანეთთან შეფარდება შეადგენს 2:1;
- ✓ **ტერორისტები** - ცდილობენ ინფრასტრუქტურის მნიშვნელოვანი ობიექტები გამოიყვანონ მწყობრიდან, საერთოდ გაანადგურონ ან გაომიყენონ თავიანთი მიზნებისთვის. მათი ქმედება სერიოზული საფრთხის ქვეშ აყენებს ქვეყნების ეროვნულ უსაფრთხოებას, იწვევს ადამიანთა მასიურ მსხვერპლს, ასუსტებს ეკონომიკას, ასევე ზიანს აყენებს საზოგადოების მორალურ მდგომარეობასა და ამცირებს მათ სანდოობას ხელისუფლების მიმართ. ყველა ტერორისტული ორგანიზაცია და დაჯგუფება არ ფლობს საკმარის ცოდნასა და ტექნიკურ საშუალებებს

ეფექტური კიბერშეტევის განხორციელებისთვის, თუმცა არსებობს თეორიული დაშვება, რომ მათ მიიღონ მსგავსი ცოდნა და შესაძლებლობა, ან დახმარებისთვის მიმართონ ორგანიზებული დანაშაულის წარმომადგენლების მომსახურებას;

- ✓ **ბოტნეტი** - ინტერნეტ - ბოტი[195] ბოტნეტში წარმოადგენს პროგრამას, რომელიც ფარულად არის დაყენებული მსხვერპლის/ობიექტის კომპიუტერულ მოწყობილობაში, რაც დამნაშავეს/ბოროტმოქმედს საშუალებას აძლევს დავირუსებული კომპიუტერის რესურსების გამოყენებით, შეასრულოს გარკვეული ქმედებები. ჰაკერების ეს სახეობა თავისი პროგრამებით ავირუსებენ კომპიუტერების დიდ რაოდენობას, რომელთა რესურსებსაც შემდეგ იყენებენ კიბერშეტევის კოორდინირებისთვის, ასევე „სპამის“ გასაგზავნად, ფიშინგისთვის და სხვა მავნე ქმედებისთვის. მსგავსი სახის ქსელები წარმოადგენენ არალეგალური ვაჭრობის ობიექტს;
- ✓ **ფიშერები** - ეს არის ფიზიკური პირები ან პატარა დაჯგუფებები, რომლებიც იყენებენ ფიშინგის ტექნოლოგიებს[196] პერსონალური რეკვიზიტების მოპარვისა და ფასიანი ინფორმაციების გადაყიდვის მიზნით. თავიანთი მიზნების მისაღწევად ფიშერები ხშირად იყენებენ „სპამებს“ და ჯაშუშურ პროგრამებს;
- ✓ **სპამერები** - ფიზიკური ან იურიდიული პირები, რომლებიც მასიურად აგზავნიან არამოთხოვნილ ელექტრონულ ფოსტას დაფარული ან მცდარი ინფორმაციით, რომლის მიზანია ფიშინგითა და ჯაშუშური პროგრამების გამოყენებით კონკრეტულ ორგანიზაციებზე კიბერშეტევის განხორციელება;

[195] Internet bot - ეს არის სპეციალური პროგრამა, რომელიც ავტომატურად და/ან მიცემული დავალების თანახმად, ასრულებს იგივე მოქმედებებს, რასაც ჩვეულებრივი მომხმარებელი

[196] Phishing - ინტერნეტ სივრცეში მაქინაციების სახეობა, რომლის მიზანს წარმოადგენს კონკრეტული მომხმარებლის კონფიდენციალური მონაცემების - ე. წ. Login - სა და პაროლის, მიღება

- ✓ **ჯაშუშური და მავნე პროგრამების შემქმნელები** - ფიზიკური ან იურიდიული პირები, რომლებსაც გააჩნიათ დანაშაულებრივი ზრახვები კომპიუტერების მომხმარებლებზე კიბერშეტევის განსახორციელებლად;
- ✓ **პედოფილები** - ეს კატეგორია სულ უფრო აქტიურად იყენებს ინტერნეტს საბავშვო პორნოგრაფიის გასავრცელებლად, ასევე სოციალური ქსელებისა და ინტერნეტ ჩათების გამოყენებით, პოტენციური მსხვერპლების გასაცნობად.

როგორც წესი, ზემოთ მოცემულ კიბერსაფრთხეების წარმოშობის წყაროების ყველა სახეობას, გამომდინარე დასახული ამოცანის გადაჭრისა და მიზნის მისაღწევად, აქტიურად იყენებს არამარტო კრიმინალური სამყარო, არამედ ასევე სახელმწიფო სადაზვერვო ან სხვა სახის სპეციალური სამსახურები.

შეერთებული შტატების კონტროლის პალატის იგივე მასალებში განხილულია ასევე კიბერსაფრთხეების სახეობები, კერძოდ:

<u>მონაცემთა მთლიანობა</u>

კიბერშეტევების დროს შეიძლება გამოყენებული იყოს ჰაკერული მეთოდები, რომლის მიზანია მონაცემთა მთლიანობის განადგურება ან მათი დამახინჯება და ცვლილებების შეტანა. ქვესახეობები:

- *პროპაგანდა და დეზინფორმაცია* - უცხოეთის სახელმწიფოების ტერიტორიებზე მმართველი რეჟიმების დესტაბილიზაციის მოწყობის, პოლიტიკური პროცესების ან კომერციული საქმიანობის შედეგებზე გავლენის მოხდენის მიზნით, არასწორი მონაცემების შეყვანა/გავრცელება ან არსებულ მონაცემებში ცვლილებების შეტანა;
- *დაშინება* - ვებ - გვერდებზე შეტევების განხორციელების მიზანია მომხმარებლის (როგორც სახელმწიფო მოხელის, ისე ფიზიკური ან იურიდიული პირის) იძულება წაშალოს ან შეცვალოს საიტის შინაარსი /პოლიტიკა;

- *განადგურება* - უცხო სახელმწიფოებისთვის ან კონკურენტებისთვის ზარალის ან მავნებლობის მიყენების მიზნით, მონაცემების მუდმივი და მიზანმიმართული განადგურება. კერძოდ, მსგავსი შეტევები შეიძლება განხორციელდეს უფრო მასშტაბური კონფლიქტის დროს არსებული სხვა მოქმედებების პარალელურად.

<u>დაშვება</u>

სისტემაზე განხორციელებული კიბერშეტევის შედეგად, სისტემის ლეგიტიმურ მომხმარებელს ექმნება ისეთი პირობები, რომ მას არ შეუძლია სისტემაში შესვლა და აღარ აქვს დაშვება სისტემის მიერ შემოთავაზებულ რესურსებზე, ან ასეთი დაშვება არის გართულებული. ქვესახეობები:

- *საგარეო ინფორმაცია* - განხორციელებული შეტევები, რომლის შედეგად შეუძლებელია სახელმწიფო და კერძო სექტორის სერვისებზე ღია დაშვება. კერძოდ, მასიური საინფორმაციო საშუალებებისა და სახელმწიფო თუ კერძო სტრუქტურების საინფორმაციო საიტები;
- *შიდა ინფორმაცია* - სახელმწიფო და კერძო სექტორის ქსელზე ლოკალური შეტევის განხორციელება. მაგალითად, ლოკალური შეტევები ენერგეტიკული და სატრანსპორტო მართვის სისტემებზე, ელექტრონული ბანკინგის საიტებზე, ოპერატიული მმართველობის სისტემებზე, კორპორატიული სერვისების ელექტრონულ ფოსტაზე, სამაშველო სამსახურებსა და ა. შ.

<u>კონფიდენციალობა</u>

კიბერშეტევების სამიზნე შეიძლება იყოს კონფიდენციალური ინფორმაციის წყაროები[197] და ის ძირითადად ხორციელდება დანაშაულის მიზნით. ქვესახეობები:

[197] კიბერშეტევის მსხვერპლნი ხშირად ხდებიან კონფიდენციალური ინფორმაციის მატარებელი სახელმწიფო მოხელეები და მსხვილი კორპორაციების მთავარი ფიგურები. კერძოდ, ხდება არამარტო კონფიდენციალური ინფორმაციის მოპარვა, არამედ ასევე წარმოებს მსგავსი პირების პერსონალური ინფომაციის ხელყოფა, მათი მომავალში შანტაჟის მიზნით

- *ჯაშუშობა* - კორპორაციების, კომპანიებისა და ფირმების მხრიდან ინფორმაციის მოპოვება თავისი კონკურენტების მიმდინარე და მომავალი საქმიანობის შესახებ. ჯაშუშურ საქმიანობაში სახელმწიფოს მონაწილეობა, რომელიც მიმართულია უცხო ქვეყნებისა და ფიზიკური თუ იურიდიული პირების წინააღმდეგ;
- *პერსონალური მონაცემების მოპარვა* - ფიშინგის ან მსგავსი ანალოგიური შეტევების განხორციელება, რომლის მიზანია მოტყუების გზით მომხმარებელი იძულებული გახადოს აცნობოს თავისი პერსონალური მონაცემები, მაგალითად საბანკო ანგარიშები. ვირუსების დაგზავნა, რომლებიც მომხმარებლის პერსონალური კომპიუტერიდან აკეთებს მონაცემთა კოპირებასა და ჩატვირთვას;
- *„პიროვნების მოპარვა“* - იგულისხმება მომხმარებლის პერსონალური რეკვიზიტების მოპარვა. ტროიანი და მსგავსი პროგრამები გამოიყენება პირადი მონაცემების მოსაპარად;
- *ინფორმაციის მოძიება საერთაშორისო ქსელში* - სხვადასხვა სახის ინფორმაციის, კერძოდ, პერსონალური მონაცემების მოპოვების მიღების მიზნით, გამოიყენება ღია წყაროებიდან ინფორმაციის მოპოვების ტექნოლოგიები;
- *მაქინაციები* - ხშირად ხორციელდება სპამის გამოყენებით, რომელიც ვრცელდება ელექტრონული ფოსტის საშუალებით. მსგავსი მაქინაციის ყველაზე ცნობილი სახეობა არის ე. წ. „ნიგერიული წერილები 419“[198]. აქვე შეიძლება განვიხილოთ მაქინაციების ის სქემები, რომლებიც მომხმარებლებს სთავაზობს არარსებულ სერვისებსა და საქონელზე წინასწარ გადახდას.

[198] „ნიგერიული წერილები 419“ (Scam 419) - მაქინაციის გავრცელებული სახეობა, რომელიც განვითარდა ელექტრონული ფოსტის მასიური დაგზავნის გაჩენის შემდეგ. სახელწოდება მიიღო იმის გამო, რომ განსაკუთრებულად განვითარდა ნიგერიაში, სადაც ჯერ ლოკალური, ხოლო შემდეგ საერთაშორისო მასშტაბები მიიღო. აღსანიშნავია, რომ ეს არსებობდა ინტერნეტის გჩენამდე და მისი გავრცელება ხდებოდა ჩვეულებრივი საფოსტო მომსახურებით, ხოლო ახალი ტექნოლოგიებისა და ინტერნეტის გაჩენასთან ერთად „ნიგერიულმა წერილებმა 419“ მსოფლიო მასშტაბები მიიღო

კიბერსაფრთხეებთან მებრძოლი სუბიექტები

კიბერსაფრთხეებთან ბრძოლის ერთერთ მთავარ პრობლემას წარმოადგენს ის ფაქტი, რომ ინფორმაციული და საკომუნიკაციო ქსელების უმეტესობა არის კერძო სექტორის საკუთრებაში, როცა მათ უსაფრთხოებაზე პასუხისმგებლობა ეკისრება სახელმწიფოს. უნდა აღინიშნოს, რომ პროცესში კერძო სექტორის მონაწილეობა გაცილებით ართულებს ქსელების დაცვასა და მათი უსაფრთხოების უზრუნველყოფას. ორივე ჯგუფს, სახელმწიფოს და კერძო სექტორს გააჩნიათ სხვადასხვა ინტერესები და მიზნები, რაც ამცირებს კიბერსივრცის დაცვის ეფექტურობას.

ეს პროცესი კიდევ უფრო რთულდება, როცა საკითხი იღებს გლობალურ ხასიათს, რომლის გადაწყვეტაში დიდი როლი ენიჭება საერთაშორისო ნორმებსა და არსებულ სუბიექტებს. ამ უკანასკნელებმა შეიძლება შეასრულონ გარკვეული კატალიზატორის როლი მოცემულ პროცესში, მიმართული როგორც ეროვნული, ისე საერთაშორისო სამართლებრივი ბაზის სრულყოფისა და ჰარმონიზაციისკენ, სადაც იგულისხმება კიბერდამნაშავეთა სამართლებრივი დევნა, მონაცემთა შენახვა და დაცვა, ასევე ქსელის უსაფრთხოების უზრუნველყოფის პრინციპები და კიბერშეტევებზე ოპერატიული რეაგირება. აგრეთვე უნდა აღინიშნოს, რომ საკითხისადმი მსგავსი მიდგომით შესაძლებელია ინფორმაციულ სისტემებში სუსტი და მოწყვლადი ადგილები, ასევე სახელმწიფო და კერძო სექტორის სუბიექტებს შორის პარტნიორობა კიბერდამნაშავეობასთან ბრძოლის საკითხში.

საერთაშორისო დონეზე კიბერსაფრთხეებთან ბრძოლის თაობაზე მიღებულია ისეთი მნიშვნელოვანი სამართლებრივი აქტები, როგორებიცაა გაეროს გენერალური ასამბლეის 2000 წლის 4 დეკემბრის №55/63[199] და 2001 წლის 19 დეკემბრის №56/121[200] რეზოლუციები „დანაშაულებრივი მიზნებით ინფორმაციული ტექნოლოგიების გამოყენებასთან ბრძოლა“, 2008 წლის 1 – 2 აპრილს, სტრასბურგში მსოფლიო

[199] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf
[200] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf

კონფერენციაზე "თანამშრომლობა კიბერდანაშაულის წინააღმდეგ"[201] მიღებული დოკუმენტი „კიბერდანაშაულობასთან ბრძოლის სფეროში სამართალდამცავი ორგანოებისა და ინტერნეტ - პროვაიდერების ერთობლივი მუშაობის ძირითადი პრინციპები"[202]. რეგიონალურ დონეზე უნდა აღინიშნოს ევროსაბჭოს რეკომენდაციები №R[89]9 "კომპიუტერულ დანაშაულებთან ბრძოლა"[203].

კიბერდანაშაულობასთან ბრძოლის ერთერთ ძირითად სუბიექტად მოიაზრება ქსელის მომხმარებელი. ამიტომ აუცილებელია მათი ჩართვა საგანმანათლებლო ღონისძიებებში, რომლებიც დაეხმარება მომხმარებელს უფრო კარგად გაერკვნენ ისეთ საკითხში, როგორიცაა კომპიუტერული მაქინაციები, პირადი რეკვიზიტების მოპარვა, ინტერნეტში არსებული დანაშაულებები, ინტერნეტის ეთიკა და სხვა.

ქვემოთ მოცემულია ზოგიერთი ძირითადი სუბიექტი, რომლებიც მონაწილეობენ კიბერსაფრთხეებთან ბრძოლაში, კერძოდ:

საერთაშორისო და რეგიონალური ორგანიზაციები

- აზია - წყნარი ოკეანის ეკონომიკური თანამშრომლობის სამუშაო ჯგუფი ტელეკომუნიკაციებსა და ინფორმაციებში[204];
- ქსელებისა და ინფორმაციული უსაფრთხოების ევროპული სააგენტო[205];
- ნატო - ს კიბერნეტიკული დაცვის მოწინავე მეთოდების გაერთიანებული ცენტრი[206];
- სამხრეთ - აღმოსავლეთის ქვეყნების ასოციაცია[207];
- ეკონომიკური განვითარებისა და თანამშრომლობის ორგანიზაცია[208];

---

201 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_IF08-d-concl1c.pdf

202 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf

203 http://www.oas.org/juridico/english/cyber_links_coe.htm

204 http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information.aspx

205 http://www.enisa.europa.eu/

206 https://ccdcoe.org/

207 http://www.asean.org/

208 http://www.oecd.org/

- კომპიუტერულ ქსელებში საგანგებო სიტუაციებზე ოპერატიული რეაგირების ჯგუფი[209];
- ინტერნეტის მართვის ფორუმი[210];
- ელექტროკავშირის საერთაშორისო გაერთიანება[211];
- ინტერნეტის საზოგადოება[212];
- სახელებისა და ნომრების მინიჭების ინტერნეტ - კორპორაცია[213];
- სამოქალაქო ინიციატივა ინტერნეტ - პოლიტიკა „მერიდიანი“[214];
- დიდი რვიანის ლიონის ჯგუფი, მაღალი ტექნოლოგიების სფეროში დანაშაულებების ქვეჯგუფი, გაერო, ევროსაბჭო.

არასამთავრობო ორგანიზაციები[215]

- უფლებათა დამცავი ორგანიზაციები[216];
- სხვადასხვა ფონდები[217];
- ანალიტიკური ცენტრები[218].

დარგობრივი ორგანიზაციები

- ანტიფიშინგური სამუშაო ჯგუფი[219];
- ფუნქციონალურ საკითხებში დომეინის სახელების სამსახურების კვლევითი - ანალიტიკური ცენტრი[220];

[209] https://www.csirt.org/
[210] http://www.intgovforum.org/cms/
[211] http://www.itu.int/en/Pages/default.aspx
[212] http://www.internetsociety.org/
[213] https://www.icann.org/
[214] http://meridianprocess.org/default.aspx
[215] მოცემულია რამოდენიმე ძირითადი და აღიარებული ორგანიზაცია
[216] Human Rights Watch http://www.hrw.org/; საერთაშორისო ამნისტია http://www.amnesty.org/; Reporters Without Borders http://en.rsf.org/
[217] The World Wide Web Foundation http://webfoundation.org/; The Shadowserver Foundation https://www.shadowserver.org/wiki/pmwiki.php
[218] The Center for Strategic and International Studies (CSIS) http://csis.org/; http://www.rand.org/
[219] http://www.antiphishing.org/
[220] https://www.dns-oarc.net/

- სისტემებში შეტყობინებების გადაცემის მავნებლობასთან ბრძოლის სამუშაო ჯგუფი[221];
- ინტერნეტში უსაფრთხოების გაძლიერების დარგობრივი კონსორციუმი[222];
- ელექტრონიკისა და ელექტროტექნიკის ინჟინრების ინსტიტუტი[223];
- სატრანსპორტო ორგანიზაციები[224];
- სხვა დარგობრივი ორგანიზაციები, რომლებიც დაკავშირებულია კრიტიკული ინფრასტრუქტურის მართვასთან.

სახელმწიფო

- საგარეო და შინაგან საქმეთა სამინისტროები, ტრანსპორტის, ფინანსთა და იუსტიციის სამინისტროები, სადაზვერვო და სხვა სპეციალური სამსახურები, პოლიციის სამმართველოები/დეპარტამენტები, ოპერატიული უსაფრთხოების სამმართველოები/დეპარტამენტები, კიბერუსაფრთხოების საკითხებში სპეციალური სამმართველოები/დეპარტამენტები;
- ელექტრონულ ინციდენტებზე რეაგირების კომპიუტერული ჯგუფები (CERT)[225].

კერძო სექტორი

- ინტერნეტში უსაფრთხოების უზრუნველყოფის სპეციალური კომპანიები;
- პროგრამული უზრუნველყოფის შემქნელები/დეველოპერები;
- სისტემების, სერვერების, მოწყობილობების მწარმოებლები;
- ჰოსტინგ - პროვაიდერები;
- კომპანიები, რომლებიც ეწევიან საქონლით ვაჭრობას ინტერნეტში.

---

[221] https://www.maawg.org/

[222] http://www.icasi.org/

[223] https://www.ieee.org/index.html

[224] მაგალითად, აეროპორტებისა და საჰაერო გადაზიდვების მართვის უსაფრთხოების უზრუნველყოფის ორგანიზაციები

[225] მაგალითად, საქართველოს იუსტიციის სამინისტროს სსიპ „მონაცემთა გაცვლის სააგენტო“ http://www.cert.gov.ge/

ფიზიკური პირები

პერსონალური კომპიუტერების მფლობელები და მომხმარებლები.

რეზუმე

წინამდებარე ნაშრომში ნაჩვენებია ის კიბერსაფრთხეები, მათი წარმოშობის წყაროები და სახეობები, რომლებიც საფრთხეს უქმნიან და ემუქრებიან ინტერნეტის სივრცეს როგორც გლობალურ, ისე ლოკალურ დონეზე, რაც სერიოზულ სირთულეებს უქმნის ეროვნულ და საერთაშორისო უსაფრთხოების პრინციპებს.

ფაქტიურად, კიბერსივრცე დღესდღეისობით არსებული მდგომარეობით ნაკლებად დაცულია, რასაც ხელს უშლის სახელმწიფო და კერძო სექტორებს შორის ნაკლები კომუნიკაცია და იმ განსვავებული მოტივაციის, ინტერესებისა და მიზნების არსებობა, რაც ახასიათებს თითოეულ სექტორს. ყოველივეს ემატება ის გარემოებაც, რომ ტექნოლოგიური განვითარების პარალელურად ვითარდება ასევე კიბერდანაშაულებები, ვინაიდან ისინი ყოველი ნოუ ჰაუს აქტიური მომხმარებლები არიან.

მოცემულ პრობლემაში დიდი მნიშვნელობა ენიჭება არამარტო საერთაშორისო თუ რეგიონალურ დონეზე მიღებულ რეზოლუციებსა და რეკომენდაციებს, ან/და კიბერსაფრთხეებთან მებრძოლ სუბიექტებს, არამედ ასევე პიროვნების ფაქტორს როგორც ქსელისა და პერსონალური კომპიუტერული მოწყობილობის მომხმარებელს, რომლისთვისაც მოცემულ სფეროში ცნობადობის ამაღლება, საგანმანათლებლო პროგრამების მიწოდება და ინტერნეტის ეთიკის ნორმების გამომუშავებაში ხელშეწყობა აუცილებელი პირობაა ყოველი ხელისუფლებისთვის და საერთაშორისო ორგანიზაციებისთვის, რაც მაქსიმალურად შეამცირებს რისკებს როგორც გლობალურ, ისე ლოკალურ ინტერნეტ სივრცეში.

გამოყენებული ლიტერატურა

1) Democratic Governance Challenges of Cyber Security, Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler, DCAF 2010, DCAF Horizon 2015 Working Paper Series http://genevasecurityforum.org/files/DCAF-GSF-cyber-Paper.pdf; http://www.dcaf.ch/Publications/Democratic-Governance-Challenges-of-Cyber-Security;
2) United States Government Accountability Office, Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk (Washington DC: US GAO, 2009) http://www.nsi.org/pdf/reports/Information%20Security%20-%20Cyber%20Threats.pdf

კიბერუსაფრთხოების სფეროში არსებული ზოგიერთი ქვეყნის ორგანიზაციული სტრუქტურების მოკლე აღწერა. საქართველოში არსებული სუბიექტები

შესავალი

ბოლო ათწლეულში ინტერნეტ - სივრცის და მასთან დაკავშირებული პროცესების სწრაფმა განვითარებამ, ასევე მომხმარებელთა რაოდენობის მოკლე დროში კოლოსალურმა ზრდამ, გამოიწვია ახალი სახელმწიფო სუბიექტების შექმნისა და განვითარების საჭიროება. ყველა ქვეყანა ცდილობს მაქსიმალურად ეფექტური, მოქნილი და დახვეწილი ისეთი ორგანიზაციული სტრუქტურის ჩამოყალიბებას, რომელიც მაქსიმალურად უზრუნველყოფს კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვას, გაატარებს ეფექტურ ღონიძიებებს მიმართულს კიბერუსაფრთხოების უზრუნველყოფაზე, ასევე მაქსიმალურად დაიცავს პიროვნების პერსონალურ ინფორმაციას და არსებულ მონაცემთა ბაზებს. პირველ რიგში, ყველა ქვეყნის ხელისუფლება მოცემულ საკითხს განიხილავს როგორც ეროვნული უსაფრთხოების ერთერთ მნიშვნელოვან შემადგენელ ნაწილს, და შესაბამისად მსგავსი სუბიექტების დიდი ნაწილი იმყოფება თავდაცვის და შინაგან საქმეთა სამინისტროების, ან სადაზვერვო, უშიშროების ან სხვა სპეციალური სამსახურების კურატორობის ქვეშ.

მსგავს სუბიექტებს გააჩნიათ არსებობის მოკლე ისტორია. ფაქტიურად, არ არსებობდა არავითარი გამოცდილება და ყველა ქვეყანა ინდივიდუალურად ავითარებდა მოცემულ საკითხს. შეიძლება ითქვას, რომ კიბერუსაფრთხოების სფეროში სახელმწიფო თუ კერძო სუბიექტების შექმნა და მათი მომავალი განვითარება ეფუძნება იმ პრეცედენტებს, რომლებიც წარმოიშვა ინტერნეტ - სივრცეში და უკავშირდება ზოგადად, კიბერსივრცის დაცვის აუცილებლობას. ამიტომ, მოცემული სფეროს

პარალელურად მუდმივად მიმდინარეობს სახელმწიფო თუ კერძო სექტორის სუბიექტების ორგანიზაციული სტრუქტურის განვითარების პროცესი.

ნაშრომში განხილულია ზოგიერთი ქვეყნის ორგანიზაციული სტრუქტურები დაკავშირებული კიბერუსაფრთხოებასთან და ის საერთო პრინციპები, რომლებიც გააჩნიათ და ახასიათებთ სხვადასხვა ქვეყნების სახელმწიფო თუ კერძო სუბიექტებს მოცემულ სფეროში. აქვე წარმოდგენილია საქართველოში არსებული ის სუბიექტები, რომლებიც პასუხისმგებელნი არიან კომპიუტერული ქსელებისა და კიბერსივრცის, ასევე პერსონალური მონაცემების დაცვაზე და ებრძვის კიბერდანაშაულს როგორც ლოკალურ ისე საერთაშორისო დონეზე.

ზოგიერთი ქვეყნის ორგანიზაციული სტრუქტურების მოკლე მიმოხილვა

ქვემოთ მოცემული მასალა ქმნის გარკვეულ წარმოდგენას კიბერუსაფრთხოების სფეროში არსებული სახელმწიფო სუბიექტების შესახებ. კერძოდ, აქ მოკლედ არის განხილულია ევროკავშირის ზოგიერთი წევრი ქვეყნისა და სხვა ქვეყნების იმ სახელმწიფო სუბიექტების ორგანიზაციული სტრუქტურა, ფუნქციები და უწყებრივი დაქვემდებარებულობა, რომლებიც პასუხისმგებელნი არიან თავიანთ ქვეყნებში უზრუნველყონ კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვა და კიბერუსაფრთხოება, გაატარონ ყველა ის საჭირო ღონისძიებები, რომლებიც საშუალებას იძლევა მაქსიმალურად იყოს დაცული ინტერნეტის სივრცე, მონაცემთა ბაზები და მოქლაქეთა პერსონალური ინფორმაცია, ასევე ეფექტურად აწარმოონ ბრძოლა კიბერდანაშაულის წინააღმდეგ. კერძოდ, განხილულ ქვეყნებს განეკუთვნება:

- **ესტონეთი** - კიბერუსაფრთხოების სტრატეგია გამოქვეყნდა 2008 წელს. მოცემულ დოკუმენტში[226] აღწერილია სახელმწიფოში კიბერუსაფრთხოების სფეროში არსებული ვითარება და განსაზღვრავს ეროვნულ პოლიტიკას მოცემული მიმართულებით. ქვეყანაში არ არსებობს ერთიანი სახელმწიფო ორგანო, რომელიც პასუხისმგებელი იქნებოდა კიბერსივრცის დაცვის უზრუნველყოფაზე. ამ პროცესში უშუალოდ მონაწილეობს რამდენიმე

[226] https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

სამინისტრო და მათი ქვედანაყოფი. ინფორმაციული უსაფრთხოების უზრუნველყოფაში მთავარი როლი ეკუთვნის ეკონომიკისა და კავშირგაბმულობის სამინისტროს (MEAC)[227]. სამინისტროს დაქვემდებარებაში არის ცენტრალური აღმასრულებელი ხელისუფლების ორი ორგანო, რომლებიც ახდენენ კიბერუსაფრთხოების სახელმწიფო პოლიტიკის რეალიზაციას. ეს ორგანოებია: ინფორმაციული სისტემების სახელმწიფო დეპარტამენტი (RISO)[228], რომელიც არის მთავარი მაკოორდინირებელი ორგანიზაცია ინფორმაციისა და საკომუნიკაციო ტექნოლოგიების სფეროში (ICT)[229], და ესტონეთის ინფორმატიკის ცენტრი (RIA)[230], რომელიც პასუხისმგებელია მთლიანი ქსელის უსაფრთხოების უზრუნველყოფაზე, კრიტიკული ინფორმაციული ინფრასტრუქტურის სახელმწიფო სუბიექტების ტექნიკურ უსაფრთხოებაზე, ასევე სახელმწიფო ორგანიზაციების ინტერესებიდან გამომდინარე მონაცემთა გადაცემის სისტემის დამუშავება და მართვა. მოცემული ცენტრის შემადგენლობაში ფუნქციონირებს ესტონეთის საგანგებო სიტუაციებზე რეაგირების ოპერატიული ჯგუფი (CERT)[231]. უშუალოდ კრიტიკული ინფრასტრუქტურის დაცვასა (CIIP) და კიბერუსაფრთხოებას უზრუნველყოფს შინაგან საქმეთა და თავდაცვის სამინისტროების სპეციალური სტრუქტურული ერთეულები. ორივე სამინისტრო პასუხისმგებელია ქვეყნის შიდა უსაფრთხოებასა და კრიზისების მართვაზე. საფოსტო და საბაზრო ელექტრონული კავშირის მომსახურების სფეროს კოორდინირებას უწევს კავშირგაბმულობის ეროვნული საბჭო. სახელმწიფოსა და კერძო სექტორს შორის პარტნიორობისთვის შეიქმნა პროექტი „კომპიუტერული უსაფრთხოება 2009“, რომელიც მიმართულია ინფორმაციული უსაფრთხოების გაძლიერებისკენ;

[227] https://www.mkm.ee/en
[228] http://www.riso.ee/en/
[229] Information and Communication Technology
[230] https://www.ria.ee/en/
[231] https://www.ria.ee/cert-estonia

- **დიდი ბრიტანეთი** - 2009 წელს[232] მიღებული კიბერუსაფრთხოების სტრატეგია ხაზს უსვამს კიბერუსაფრთხოების უზრუნველყოფის საკითხთან კომპლექსური მიდგომის აუცილებლობას, რომლის რეალიზაციაში უნდა მონაწილეობდნენ სახელმწიფო სუბიექტები, მრეწველობის ყველა დარგის წარმომადგენლები, სამოქალაქო საზოგადოებრივი ორგანიზაციები და საერთაშორისო პარტნიორები. სტრატეგია ითვალისწინებს ორი ახალი ორგანიზაციის შექმნას[233]. პირველ რიგში ეს არის მინისტრთა კაბინეტის სტრუქტურაში შემავალი კიბერუსაფრთხოების სამმართველო (OCS)[234], რომელიც უზრუნველყოფს სტრატეგიულ ხელმძღვანელობასა და უწყებათაშორის დონეზე შეთანხმებულ მოქმედებას. ის იქნება ასევე დაკავებული კიბერდანაშაულის შესახებ საკოორდინაციო საქმიანობით. ამასთან ერთად გამოყენებული იქნება არსებული შესაძლებლობები, რომელიც გააჩნია თავდაცვის სამინისტროს, სადაზვერვო სამსახურებს და პოლიციას (ლონდონის პოლიციის ელექტრონულ დანაშაულებებთან ბრძოლის განყოფილება, ინტერნეტის ქსელის დაცვისა და ბავშვთა ექსპლუატაციის წინააღმდეგ ქმედებების ცენტრი, ასევე განსაკუთრებით საშიში და ორგანიზებული დანაშაულის სააგენტო). მეორე, ეს არის კიბერუსაფრთხოების ოპერატიული ცენტრი (CSOC), რომელიც ფუნქციონირებს სახელმწიფო კავშირგაბმულობის შტაბის[235] ბაზაზე ქ. ჩელტენჰემში. ეს არის ახალი ცენტრი, სადაც თავმოყრილია სხვადასხვა უწყებების არსებული ფუნქციები კიბერსივრცის მდგომარეობის მონიტორინგისა და ღონისძიებების კოორდინაცია ექსტრემალურ რეაგირებაზე. ცენტრი ასევე გააკეთებს ანალიზს იმ საფრთხეებზე, რომელიც ემუქრება დიდი ბრიტანეთის კომპიუტერულ ქსელებსა და მათ მომხმარებლებს,

[232] 2011 წელს მოხდა სტრატეგიის განახლება https://www.cpni.gov.uk/advice/cyber/cir/
[233] ორივე ორგანიზაციამ დაიწყო ფუნქციონირება 2010 წელს
[234] https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance
[235] http://www.gchq.gov.uk/Pages/homepage.aspx

გამოიმუშავებს შესაბამის რეკომენდაციებსა და საინფორმაციო სახელმძღვანელოებს. ეროვნული ინფრასტრუქტურის დაცვის ცენტრის (CPNI)[236] შემადგენლობაშია კომპიუტერების დახმარების სასწრაფო სამსახური (CERT Service)[237];

- **შვედეთი** - კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვით ღონისძიებებში მონაწილეობას იღებს ბევრი ორგანიზაცია. 2009 წელს შვედეთის თავდაცვის სამინისტროსთან არსებულ სამოქალაქო თავდაცვის სააგენტოს (MSB)[238] დაევალა 2010 წლის იანვრამდე წინადადებების მომზადება კომპიუტერულ ქსელებში დანაშაულებების აღკვეთის თაობაზე. გადაწყდა სააგენტოს შემადგენლობაში შექმნილიყო კიბერუსაფრთხოების ეროვნული ოპერატიული საკოორდინაციო ცენტრი, რომელიც უწყებათაშორის დონეზე, გაუწევდა კოორდინაციას ერთობლივ ღონისძიებებს და შეასრულებდა ცენტრალური ელემენტის როლს კრიზისული მენეჯმენტის სისტემაში. ამ პროცესში მთავარი როლი ეკუთვნის ასევე თავდაცვის სამინისტროსთან არსებულ საგანგებო სიტუაციების სააგენტოს (SEMA)[239]. გარდა ამისა, სამოქალაქო თავდაცვის სააგენტოს (MSB) ხელმძღვანელობით, არსებობს ინფორმაციული

[236] http://www.cpni.gov.uk/Templates/CPNI/pages/Default.aspx
[237] https://www.cpni.gov.uk/advice/cyber/cir/
[238] https://www.msb.se/en/
[239] The Swedish Emergency Management Agency (SEMA) co-ordinates the work to develop the preparedness of Swedish society to manage serious crises. SEMA works together with municipalities, county councils and government authorities, as well as the business community and several organizations, to reduce the vulnerability of society and improve the capacity to handle emergencies. The Swedish Emergency Management Agency (SEMA) supports the bodies responsible for emergency management, especially county administrative boards and municipalities, which have a special role with overall geographic area responsibility. SEMA should be able to give support to other public actors, i.e. municipalities, county councils and government authorities. SEMA does not have an operative role and does not take over any responsibility from other authorities. The support that SEMA is able to provide in the event of a crisis may include advice and expert support within areas such as crisis communication and management methodoligy. SEMA should also assist the Government Offices with updated situation reports. To carry out this task, the authority has an established network of county administrative boards, central authorities and others that may be affected by or have knowledge of an emergency situation. SEMA also co-ordinates the planning, resource allocation, follow-up and evaluation of work within the area of crisis management. Furthermore, SEMA collects knowledge through horizon scanning, strategic analyses and research to develope sociaty's emergency management.

უსაფრთხოების სფეროში ერთობლივი ოპერაციების ჯგუფი (SAMFI)[240], სადაც შედიან შვედეთის შეიარაღებული ძალების, რადიოტექნიკური თავდაცვის ეროვნული სამსახური (FRA)[241], ფოსტისა და ტელეკომუნიკაციის ეროვნული სააგენტო (PTS)[242] და პოლიციის ეროვნული დეპარტამენტის წარმომადგენლები. უწყებათაშორისო თანამშრომლობის ფარგლებში, მინისტრთა კაბინეტის დონეზე ტარდება სპეციალური სამუშაოები მიმართული საგანგებო სიტუაციების სააგენტოს (SEMA) რეკომენდაციებსა და კრიტიკული ინფორმაციული ინფრასტრუქტურის ეროვნული სისტემის მოდერნიზირებაზე. რაც შეეხება სახელმწიფოსა და კერძო სექტორის პარტნიორულ დონეზე თანამშრომლობას, აქ ხორციელდება საგანგებო სიტუაციების სააგენტოს (SEMA) მიერ მომზადებული ისეთი ინიციატივები და პროექტები, როგორებიცაა მოცემულ სფეროში სახელმწიფო და კერძო სექტორებს შორის თანამშრომლობის გაღრმავების, „სამრეწველო უსაფრთხოების დელეგაციისა“ (NSD) და „ინფორმაციის დამუშავების საზოგადოების“ (DFS) პროექტები;

- **ფინეთი** - აქ კიბერუსაფრთხოება განიხილება, როგორც მონაცემთა უსაფრთხოების პრობლემა, აგრეთვე როგორც ეკონომიკური პირობა, რომელიც მჭიდროდ არის დაკავშირებული ქვეყნის ინფორმაციული საზოგადოების განვითარებასთან. კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის საკითხებით დაკავებულია შემდეგი სამი სახელმწიფო ორგანო: ტრანსპორტისა და კავშირგაბმულობის სამინისტროს შემადგენლობაში არსებული კავშირგაბმულობის რეგულირების სამსახური (FICORA)[243], რომელიც ხელს უწყობს ინფორმაციული საზოგადოების განვითარებას და ეწევა ტექნიკური საკითხებისა და სტანდარტიზაციის

[240] http://rib.msb.se/Filer/pdf/26177.pdf
[241] http://www.fra.se/snabblankar/english.10.html
[242] http://www.pts.se/en-GB/
[243] https://www.viestintavirasto.fi/en/

რეგულირებას; მეორე, საგანგებო სიტუაციების ეროვნული სააგენტო (NESA)[244], ეწევა კრიტიკული ინფორმაციული ინფრასტრუქტურის საფრთხეებისა და რისკების შეფასებასა და ანალიზს; და მესამე, სახელმწიფო ადმინისტრაციასთან არსებული მონაცემთა უსაფრთხოების მთავარი სამმართველო (VAHTI)[245], რომელიც ინფორმაციული უსაფრთხოების უზრუნველყოფის მიზნით ამუშავებს პრინციპებისა და პრაქტიკულების სახელმძღვანელოებს. გარდა ამისა, მოცემულ სფეროში სახელმწიფოსა და კერძო სექტორს შორის პარტნიორული ურთიერთობის მიზნით შექმნილია შემდეგი სამი ორგანიზაცია საგანგებო სიტუაციების ეროვნული საბჭო (NESC), ინფორმაციული საზოგადოების საკითხთა საკონსულტაციო საბჭო და ფინეთის ინფორმაციული საზოგადოების განვითარების ცენტრი (TIEKE)[246];

- **ნიდერლანდები** - კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვისა და კიბერუსაფრთხოების უზრუნველყოფის მაკოორდინირებელ ორგანოს წარმოადგენს შინაგან საქმეთა და სამეფო საქმეთა სამინისტრო.

---

[244] http://www.nesa.fi/

[245] The Government Information and Cyber Security Management Board (VAHTI), appointed by the Ministry, is responsible for Government cooperation, steering and development efforts in this area. VAHTI sets all the main policy guidelines for information and cyber security in central government. Different administrative branches and levels of administration are represented in VAHTI.
A Government Resolution on the development of information security in central government was issued on 26 November 2009. The Resolution provides guidance to central government in developing information security as an integral part of leadership, expertise, risk management and administrative development and functions. VAHTI's effective cooperation, steering and development of information security in central government will be reinforced. The present Government has discussed the earlier government resolutions and made a decision that this resolution is to be kept in force.
VAHTI guidelines and instructions are also important reference materials for the public authorities, local government, the private sector and civil society. In addition, the results of the work are used in such international information security forums as the OECD and the EU. VAHTI publications are considered to be of high quality in international comparison.
The role and tasks of VAHTI in the development, coordination, cooperation and steering of government information and cyber security have been further developed and strengthened. VAHTI deals with all significant central government information and cyber security guidance and policy matters.
VAHTI has received several awards for improving information security in Finland. The latest OECD report on the development of the global information security culture makes several references to the operations and results of VAHTI.

[246] http://www.tieke.fi/display/English/Home

გარდა ამისა, ამ სამინისტროში არსებული კრიზისების ეროვნული ცენტრი კურირებს სხვა უწყებების საქმიანობას, ასევე საერთაშორისო პოლიტიკასა და კრიზისების მართვას. ინფორმაციული უსაფრთხოების დაცვით ღონისძიებებში ასევე მონაწილეობს საერთო დაზვერვისა და უსაფრთხოების სამსახური (AIVD)[247];

- **გერმანია** - კრიტიკული ინფრასტრუქტურის უსაფრთხოების ეროვნული სტრატეგია განსაზღვრავს მთავრობის მიზნებსა და ამოცანებს მოცემულ სფეროში, რომელიც თავის მხრივ ასახულია ინფორმაციული ინფრასტრუქტურის უსაფრთხოების სახელმწიფო პროგრამაში (NPSI). კიბერუსაფრთხოების საკითხებში მთავარი როლი ეკუთვნის შინაგან საქმეთა სამინისტროსთან არსებულ ინფორმაციული უსაფრთხოების ფედერალურ სააგენტოს (BSI), რომელიც სამოქალაქო თავდაცვისა და საგანგებო სიტუაციების ფედერალურ სააგენტოსთან (BBK), კრიმინალური პოლიციის ფედერალურ სააგენტოსთან (BKA), ფედერალურ პოლიციასთან (BPOL) და ფედერალური ინსტიტუტების ტექნიკური მხარდაჭერის სამსახურთან ერთად ახორციელებს შეფასებასა და ანალიზს, ასევე ფორმულირებას უკეთებს კიბერსივრცის დაცვის კონცეფციას. კრიტიკული ინფრასტრუქტურის დაცვის მიზნით და ამ მიმართულებით კოორდინირებული მოქმედებისთვის შექმნილი არის სამუშაო ჯგუფი (AG KRITIS)[248]. სტრატეგიის შემუშავებისა და მისი შემდგომი რეალიზების საქმიანობა მიმდინარეობს კოორდინირებულად სხვა ფედერალურ სამინისტროებთან, სააგენტოებთან და სამსახურებთან ერთად (ეკონომიკისა და ტექნოლოგიის სამინისტრო, ფედერალური კანცლერის ადმინისტრაცია, იუსტიციის, საგარეო საქმეთა და თავდაცვის ფედერალური სამინისტროები, ელექტრონული ქსელების ფედერალური

[247] https://www.aivd.nl/english/
[248] file:///C:/Users/Admin/Downloads/doc_263_259_en.pdf

სააგენტო). გარდა ამისა, წარმოებს კონსულტაციები კერძო სექტორის სტრატეგიულ პარტნიორებთან;

- **საფრანგეთი** - კრიტიკული ინფრასტრუქტურის დაცვაზე მთელი პასუხისმგებლობა ეკისრება პრემიერ - მინისტრის ადმინისტრაციასთან არსებულ ეროვნული თავდაცვის გენერალურ სამდივნოს (SGDN). ქვეყანაში კიბერუსაფრთხოება ამავდროულად განიხილება როგორც მაღალტექნოლოგიური დანაშაულის საკითხი და როგორც პრობლემა, რომელიც ხელს უშლის და ეწინააღმდეგება ინფორმაციული საზოგადოების ნორმალურ განვითარებას. მოცემულ სფეროში დანაშაულის გამოძიებაზე პასუხისმგებელი ორგანოებია 2000 წლის მაისში შექმნილი ინფორმაციისა და საკომუნიკაციო ტექნოლოგიების სფეროში დანაშაულთან ბრძოლის ცენტრალური ოფისი (OCLCTIC) და სასამართლო პოლიციის მთავარი სამმართველოს ეკონომიკური და ფინანსური საგამოძიებო განყოფილება. 2009 წლის ივლისის თვეში, თავდაცვის სამინისტროში შეიქმნა ინფორმაციული სისტემების უსაფრთხოების ეროვნული სააგენტო (Anssi)[249], რომელიც პასუხისმგებელია კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვისა და კიბერუსაფრთხოების უზრუნველყოფაზე. გარდა ამისა, ასევე ფუნქციონირებს ინფორმაციული სისტემების უსაფრთხოების უწყებათაშორისი კომისია (CISSY). სახელმწიფოსა და კერძო სექტორს შორის პარტნიორობის ფარგლებში შექმნილია ინფორმაციული ტექნოლოგიების სტრატეგიული საკონსულტაციო საბჭო (CSTI), რომელიც აერთიანებს სახელმწიფო ჩინოვნიკებს, ბიზნესისა და საწარმოთა მაღალი მმართველი რგოლისა და სამეცნიერო წრეების წარმომადგენლებს;
- **ნორვეგია** - სამოქალაქო თავდაცვისა და კრიზისების მართვის სამმართველო (DSB) არის მთავარი მაკოორდინირებელი ორგანიზაცია, რომელიც პასუხისმგებელია კრიტიკული ინფორმაციული

[249] http://www.ssi.gouv.fr/en/

ინფრასტრუქტურის დაცვითი საქმიანობის უზრუნველყოფაზე. სამმართველო იმყოფება იუსტიციისა და პოლიციის სამინისტროს დაქვემდებარებაში. ინფორმაციისა და ქსელების კავშირის უსაფრთხოება თავმოყრილია სახელმწიფო მართვისა და რეფორმების სამინისტროში. თავდაცვის სამინისტრო პასუხიმგებელია მხოლოდ სამხედრო კომპიუტერულ ქსელზე. ტრანსპორტისა და კავშირგაბმულობის სამინისტრო პასუხს აგებს კავშირგაბმულობის სექტორზე, ასევე ინფორმაციული ქსელების უსაფრთხოების ასპექტებზე. ნორვეგიის ეროვნული უსაფრთხოების სამსახური (NSA) კოორდინირებას უწევს კომპიუტერული ქსელების უსაფრთხოების უზრუნველყოფის ღონისძიებებს. ინფორმაციული უსაფრთხოების საკითხთა სახელმწიფო საკოორდინაციო საბჭო (KIS) უფლებამოსილი არ არის მიიღოს გადაწყვეტილებები, თუმცა ის უწევს კონსულტაციებს სამინისტროებსა და უწყებებს იმ საკითხებში, რომლებიც დაკავშირებულია კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვასა და კიბერუსაფრთხოებასთან. მის შემადგენლობაში შედის ექვსი სამინისტრო, პრემიერ - მინისტრის აპარატი და ათამდე სხვადასხვა სამმართველო;

- **ავსტრია** - ქვეყანაში არ არსებობს ერთიანი მაკოორდინირებელი ორგანო, რომელიც პასუხისმგებელი იქნება კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვით ღონისძიებებზე. ყოველი სამინისტრო და უწყება თავად ახორციელებს საკუთარი უსაფრთხოების ღონისძიებებს მიმართულს საგარეო კიბერშეტევებსა მონაცემთა არასანქცირებული გამოყენების გაუვნებელყოფაზე. კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვას ახორციელებს შინაგან საქმეთა სამინისტროს (BMI)[250] ზოგიერთი ქვედანაყოფი, კერძოდ, აწარმოებს მონავემთა უსაფრთხოების უზრუნველყოფასა და ბრძოლას კიბერდანაშაულებასთან. კრიმინალური პოლიციის ფედერალური სამმართველოს საზოგადოებრივი

[250] http://www.bmi.gv.at/cms/bmi/_news/bmi.aspx

უსაფრთხოების მთავარ სამმართველოსთან ფუნქციონირებს ბავშვთა პორნოგრაფიის გავრცელების საწინააღმდეგო საინფორმაციო ცენტრი. სახელმწიფო დაცვისა და ტერორიზმთან ბრძოლის ფედერალური სააგენტო (BVT)[251] პასუხს აგებს პიროვნებისა და ობიექტების უსაფრთხოების საკითხებზე. თავდაცვის სამინისტროს მეორე სამმართველო აწარმოებს თავის საქმიანობას ინფორმაციული ომის ყველა მიმართულებით და ამასთანავე მჭიდროდ თანამშრომლობს სპეციალურ სამსახურებთან. ერთერთი არის Abwehramt[252], რომელსაც გააჩნია ელექტრონული თავდაცვის სპეციალური დეპარტამენტი. ტრანსპორტის, ინოვაციებისა და ტექნოლოგიების სამინისტრო (BMVIT)[253] პასუხისმგებელია სახელმწიფო ინფორმაციული ინფრასტრუქტურის უსაფრთხოებაზე. იგივე სამინისტრო უწევს კოორდინაციას უსაფრთხოების სფეროში სამეცნიერო კვლევებისა და განვითარების ეროვნულ პროგრამებს. კიბერუსაფრთხოების სფეროში არსებული სახელმწიფო პროგრამების[254] გათვალისწინებით, ავსტრიაში კიბერუსაფრთხოება ძირითადად განიხილება მონაცემთა დაცვის ფარგლებში;

- **პოლონეთი** - კრიტიკული ინფორმაციული ინფრასტრუქტურასა და მის უსაფრთხოებაზე პასუხისმგებელია სახელმწიფო ორი უწყება. კერძოდ, მეცნიერებისა და უმაღლესი განათლებისა და შინაგან საქმეთა და ადმინისტრაციის სამინისტროები. მთავარი სუბიექტი და ერთადერთი მაკოორდინირებელი ორგანო, რომელიც მონაწილეობს სამეცნიერო -

[251] The Federal Office for the Protection of the Constitution and Counterterrorism (Bundesamt für Verfassungsschutz und Terrorismusbekämpfung, "BVT") is an Austrian police organization that acts as a domestic intelligence agency. It is tasked with the protection of constitutional organs of the Republic of Austria and their ability to function. The agency was created from the Austrian State police, as well as various special task forces targeting organized crime and terrorism that were under the direction of the Directorate General for Public Security (Generaldirektion für die öffentliche Sicherheit, "GDföS"), which itself is a department of the Federal Ministry of the Interior. The BVT publishes the Verfassungsschutzbericht, an annual report on the status of the protection of the constitution

[252] ავსტრიის საგარეო დაზვერვა

[253] http://www.bmvit.gv.at/en/

[254] ელექტრონული მთავრობის პროგრამა, ინფორმაციული უსაფრთხოების სახელმწიფო პროგრამა, მოქალაქის ელექტრონული ინტელექტუალური ბარათის შექმნის საპილოტე პროგრამა

ტექნიკური სახელმწიფო პოლიტიკის ყველა სტრატეგიის შემუშავებასა და განსაზღვრაში დაკავშირებული კრიტიკული ინფორმაციული ინფრასტრუქტურისა და მისი უსაფრთხოების უზრუნველყოფასთან, არის მეცნიერებისა და უმაღლესი განათლების სამინისტრო. ეს სამინისტრო ამუშავებს სტრატეგიულ რეკომენდაციებს ყველა დანარჩენი სამინისტროსა და უწყებებისთვის, ასევე უზრუნველყოფს სახელმწიფო კომპიუტერული ქსელების თავსებადობას. შინაგან საქმეთა და ადმინისტრაციის სამინისტრო პასუხს აგებს სახელმწიფო კომპიუტერულ ინფრასტრუქტურაზე, სახელმწიფო სატელეკომუნიკაციო და ინფორმაციული ქსელების მართვის სისტემებზე;

- **შვეიცარია** - კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვით დაკავებულია რამოდენიმე ორგანიზაცია. ამ სფეროში ერთერთი მთავარი ორგანიზაცია არის ინფორმაციული ტექნოლოგიების ფედერალური სტრატეგიული ქვედანაყოფი (FSUIT)[255]. მოცემული ორგანიზაცია არის ფინანსთა ფედერალური დეპარტამენტის სტრუქტურულ შემადგენლობაში და ის ამუშავებს ინფორმაციულ უსაფრთხოებაში ინსტრუქციებს, მეთოდოლოგიასა და პროცედურებს, ასევე კურირებას უწევს ინფორმაციული უზრუნველყოფის სპეციალურ სამუშაო ჯგუფს (SONIA) და ინფორმაციული უსაფრთხოების საკითხთა საინფორმაციო - ანალიტიკურ ცენტრს (MELANI)[256], რომელიც ახორციელებს კიბერდანაშაულთან ბრძოლის საკოორდინაციო ჯგუფის საქმიანობას (KOBIK)[257]. ორივე ეს ქვედანაყოფი იმყოფება პოლიციის ფედერალური სამმართველოს (FEDPOL)[258] უწყებრივ დაქვემდებარებაში. ინფორმაციული ტექნოლოგიების, ქსელებისა და ტელეკომუნიკაციების ფედერალური სამმართველო (FOITT)[259] ასევე წარმოადგენს ფინანსთა ფედერალური დეპარტამენტის სტრუქტურულ

[255] http://www.isb.admin.ch/index.html?lang=en
[256] http://www.melani.admin.ch/?lang=en
[257] https://www.cybercrime.admin.ch/kobik/en/home.html
[258] https://www.fedpol.admin.ch/fedpol/en/home.html
[259] http://www.bit.admin.ch/index.html?lang=en

ქვედანაყოფს და პასუხისმგებელია ოპერატიულ დონეზე ინფორმაციული ტექნოლოგიების ფედერალური სისტემების უსაფრთხოებასა და ექსტრემალურ მზადყოფნაზე. ინფორმაციული უსაფრთხოების სფეროში ასევე მოქმედებს ეკონომიკური რესურსების ფედერალური უწყების შემადგენლობაში არსებული ინფორმაციული და სატელეკომუნიკაციო ინფრასტრუქტურის სამმართველო, სამოქალაქო თავდაცვის ფედერალური სამმართველო (FOCP)[260] და ინფორმაციულ ქსელებში საგანგებო სიტუაციებზე რეაგირების სახელმწიფო ჯგუფი. სამხედრო კომპიუტერული ქსელების უსაფრთხოებაზე პასუხისმგებელია შეიარაღებული ძალების სამეთაურო მხარდაჭერის სამსახური (FUB)[261]. შვეიცარიის კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის პოლიტიკის რეალიზებაში დიდ როლს თამაშობს სახელმწიფო და კერძო სექტორს შორის არსებული საპარტნიორო ურთიერთობა;

- **რუსეთი** - ინფორმაციული უსაფრთხოების სფეროში მთავარ ორგანიზაციებად ითვლება უშიშროების საბჭო, უშიშროების ფედერალური სამსახური (ФСБ), დაცვის ფედერალური სამსახური, ტექნიკისა და ექსპერტის კონტროლის ფედერალური სამსახური და ინფორმაციული ტექნოლოგიებისა და კავშირგაბმულობის სამინისტრო. თითოეულ ორგანიზაციულ უწყებას გააჩნია თავისი კომპეტენციის ფარგლები და დაკისრებული პასუხისმგებლობა. კერძოდ, უშიშროების საბჭო განსაზღვრავს ინფორმაციულ სფეროში რუსეთის ეროვნულ ინტერესებს, ობიექტებს, სუბიექტებსა და სხვა რესურსებს, რომლებიც უნდა იყოს დაცული, ასევე კოორდინირებას უწევს ინფორმაციული უსაფრთხოების სტრატეგიის დამუშავებას. უშიშროების ფედერალური სამსახური (ФСБ)[262] პასუხისმგებელია რუსეთის ფედერაციის უსაფრთხოებასა და კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის უზრუნველყოფაზე.

[260] http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/das_babs.html
[261] http://www.vtg.admin.ch/internet/vtg/en/home/schweizerarmee/organisation/fub.html
[262] http://www.fsb.ru/

კონტრდაზვერვის სამსახურის[263] ფუნქციონირებს კომპიუტერული და ინფორმაციული უსაფრთხოების სამმართველო. იგივე უშიშროების ფედერალური სამსახური (ФСБ) აწარმოებს ინფორმაციული უსაფრთხოების სფეროში სახელმწიფოს სამეცნიერო - ტექნიკური პოლიტიკის დაგეგმვასა და რეალიზებას, უზრუნველყოფს კომპიუტერული ქსელების კრიპტოგრაფიულ და საინჟინრო - ტექნიკურ დაცვას, იცავს სახელმწიფო საიდუმლოებასა და კავშირგაბმულობის ყველა სახეობას. დაცვის ფედერალური სამსახურის შემადგენლობაშია ინფორმაციისა და სპეციალური კავშირების სამსახური, რომელმაც 2003 წლის შემდეგ აიღო იმ ფუნქციების დიდი ნაწილი, რომელიც ადრე შედიოდა ინფორმაციისა და სამთავრობო კავშირების ფედერალური სააგენტოს (ФАПСИ)[264] კომპეტენციაში. ФАПСИ - ს დანარჩენი ფუნქციები გადანაწილდა შეიარაღებული ძალების გენერალური შტაბის, უშიშროების ფედერალური სამსახურისა (ФСБ) და დაცვის სამსახურს შორის. ტექნიკისა და ექსპერტის კონტროლის ფედერალური სამსახური იმყოფება თავდაცვის სამინისტროს დაქვემდებარებაში. მოცემული სამსახურის კომპეტენციის ფარგლებში შედის უცხოეთის სახელმწიფოების ტექნიკურ ჯაშუშობასთან ბრძოლა, საიდუმლო ინფორმაციის დაცვა და კომპიუტერული ქსელებისა და სისტემების უსაფრთხოების უზრუნველყოფა. ინფორმაციული ტექნოლოგიებისა და კავშირგაბმულობის სამინისტრო რეალიზებას უკეთებს სახელმწიფო პოლიტიკასა და ახორციელებს ზედამხედველობას კავშირგაბმულობის სექტორში;

- **კანადა** - კომპიუტერულ ქსელებში საგანგებო სიტუაციებზე ოპერატიული რეაგირების ცენტრი (CCIRC)[265] ახორციელებს მონიტორინგსა და კონსულტირებას დაკავშირებულს კიბერსაფრთხეებისგან დაცვით საკითხებს, ასევე სახელმწიფო დონეზე კოორდინირებას უწევს ნებისმიერი

[263] სტრუქტურულად შედის უშიშროების ფედერალურ სამსახურში (ФСБ)
[264] http://www.agentura.ru/dossier/russia/fso/specvyaz/
[265] http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx

საგანგებო სიტუაციებზე რეაგირების ოპერატიულ ღონისძიებებს, რომლებიც პირველ რიგში უკავშირდება კრიტიკული ინფორმაციული ინფრასტრუქტურის სახელმწიფო ობიექტებს. მოცემულ ღონისძიებებში ჩართული არის სხვადასხვა სახელმწიფო უწყება, მათ შორისაა კანადის ცხენოსანთა სამეფო პოლიცია, კავშირგაბმულობის უსაფრთხოების სააგენტო და უშიშროებისა და დაზვერვის სამსახური. 2010 წელს სახელმწიფომ ბოლო ათი წლის განმავლობაში მესამედ მიიღო კიბერუსაფრთხოების ეროვნული სტრატეგია;

- **ავსტრალია** - კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვითი საკითხებით დაკავებულია კიბერუსაფრთხოების ოპერატიული მართვის ცენტრი, რომელიც შეიქმნა 2009 წელს კიბერუსაფრთხოების სახელმწიფო სტრატეგიის ფარგლებში და შედის თავდაცვის სამინისტროს კავშირგაბმულობის სამმართველოს შემადგენლობაში (DCD). ცენტრის საშტატო განაკვეთი დაკომპლექტებულია შეიარაღებული ძალების, სამხედრო დაზვერვის სამსახურის, ფედერალური პოლიციის, უშიშროებისა და დაზვერვის სამსახურების სპეციალისტებით. ცენტრი მთავრობას უწევს კონსულტაციას დაკავშირებულს კიბერსაფრთხეებისგან ქვეყნის დაცვაზე, ასევე ცოდნის, გამოცდილებისა და სადაზვერვო მონაცემების ინტეგრაციის გზით, უზრუნველყოფს კოორდინირებულ საქმიანობას. თუმცა ცენტრის საქმიანობა და მასთან დაკავშირებული საკითხები მთლიანობაში გასაიდუმლოებულია;
- **იაპონია** - კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვისა და ინფორმაციული უსაფრთხოების უზრუნველყოფის სფეროში მთავარ მოქმედ პირს წარმოადგენს მინისტრთა კაბინეტის სამდივნო. მის სტრუქტურულ შემადგენლობაში ფუნქციონირებს ინფორმაციული ტექნოლოგიების განვითარების სტრატეგიის საბჭო, სადაც შედის 20 ავტორიტეტული ექსპერტი. 2005 წელს მინისტრთა კაბინეტის სამდივნოს სტრუქტურაში შეიქმნა ინფორმაციული უსაფრთხოების პოლიტიკის საბჭო

(ISPC) და ინფორმაციული უსაფრთხოების ეროვნული ცენტრი (NISC), რომლებსაც დღეს უკავიათ წამყვანი ადგილი ეროვნული პოლიტიკის კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის სფეროში. ინფორმაციული უსაფრთხოების პოლიტიკის საბჭო (ISPC) წარმოადგენს მთავარ სახელმწიფო ორგანოს უსაფრთხოების პოლიტიკისა და სტრატეგიის მოდერნიზაციისა და დამუშავების საკითხებში. საბჭოს ხელმძღვანელობს მინისტრთა კაბინეტის სამდივნოს უფროსი და ის შედის ინფორმაციული ტექნოლოგიების სტრატეგიულ შტაბში, სადაც ასევე შედიან სხვადასხვა სამინისტროებისა და კერძო სექტორის წარმომადგენლები. ინფორმაციული უსაფრთხოების ეროვნული ცენტრი (NISC) წარმოადგენს ინფორმაციული ტექნოლოგიების უსაფრთხოების საკითხებში აღმასრულებელი ხელისუფლების ცენტრალურ ორგანოს. მინისტრთა კაბინეტის სამდივნო მოქმედებს ეკონომიკის, ვაჭრობისა და მრეწველობის სამინისტროს (METI)[266], ეროვნული პოლიციის სააგენტოს (NPA)[267] და შინაგან საქმეთა და კომუნიკაციების სამინისტროს მხარდაჭერით. ინფორმაციული ტექნოლოგიების სტრატეგიული შტაბის ხელმძღვანელობით, METI ახორციელებს ინფორმაციული პოლიტიკის დაგეგმვასა და რეალიზებას, ასევე დაკავებულია ელექტრონული ვაჭრობის საკითხებით, მონაცემთა დაცვით, ინფორმაციული ტექნოლოგიების სფეროში კვლევებითა და განვითარებით. ეროვნული პოლიციის სააგენტო (NPA) უზრუნველყოფს კომპიუტერულ და ქსელურ უსაფრთხოებას, ასევე აწარმოებს კიბერდანაშაულებების საგამოძიებო საქმიანობას. ამ მიზნით, სააგენტოს ფარგლებში მოქმედებს მაღალტექნოლოგიური დანაშაულებების სამმართველო (HTCTD), რომელიც ებრძვის მსხვილმასშტაბიან კომპიუტერულ ინციდენტებს, ასევე უფლებამოსილია განახორციელოს მოკვლევა და დაკავება. სამმართველოს ერთერთ

[266] http://www.meti.go.jp/english/
[267] http://www.npa.go.jp/english/index.htm

ქვედანაყოფს წარმოადგენს ტექნიკური მხარდაჭერის მობილური ჯგუფი, რომელიც განლაგებულია ქვეყნის მთელ ტერიტორიაზე და იმყოფება კიბერსარდლობის ცენტრის დაქვემდებარებაში. სახელმწიფოსა და კერძო სექტორს შორის პარტნიორობის ფარგლებში მოქმედებს ფინანსების დაცვის, ტექნიკური ექსპლუატაციის, ანალიზისა და რეაგირების ცენტრი (CEPTOAR), რომლის მთავარი მიზანია სახელმწიფო და კერძო სუბიექტებს შორის ინფორმაციის გაცვლის გაუმჯობესება;

- **სამხრეთ კორეის რესპუბლიკა** - კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვით ღონისძიებებს ახორციელებს ყველა სახელმწიფო ორგანიზაცია და მათი სტრუქტურული ქვედანაყოფები. მოცემულ სფეროში ყველა სამინისტროსი და უწყების საქმიანობას კოორდინაციას უწევს კიბერუსაფრთხოების ეროვნული ცენტრი (NCSC)[268] , რომელიც მუშაობს დაზვერვის ეროვნული სამსახურის (NIS)[269] ეგიდით. გარდა ამისა, კიბერუსაფრთხოების ეროვნული ცენტრი (NCSC) კიბერსაფრთხეებთან ბრძოლაში აერთიანებს კერძო, საჯარო და სამხედრო სექტორებს, ცენტრი ასევე წარმოადგენს კიბერშეტევების გამოვლენის, გაუვნებელყოფისა და კიბერსაფრთხეებზე ოპერატიული რეაგირების საკითხებში აღმასრულებელი ხელისუფლების ცენტრალურ ორგანოს. კიბერდანაშაულის პროფილაქტიკურ და საგამოძიებო საქმიანობის კოორდინაციას აწარმოებს გენერალური პროკურატურის სპეციალური სგამოძიებო ორგანო. ელექტრონიკისა და ტელეკომუნიკაციის სამეცნიერო - კვლევითი ინსტიტუტი (ETRI)[270] ახორციელებს შესაბამისი ტექნოლოგიების განვითარებასა და კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვით ღონისძიებებს. მოცემულ სფეროში ინტერნეტისა და სატელეკომუნიკაციო ქსელის უსაფრთხოების კულტურის ფორმირებაზე პასუხისმგებელია ასევე სახელმწიფო მართვისა და უსაფრთხოების

[268] http://service1.nis.go.kr/eng/intro/NCSCInfo.jsp
[269] http://eng.nis.go.kr/svc/index.do
[270] https://www.etri.re.kr/eng/main/index.etri

სამინისტრო (MOPAS)[271], კავშირგაბმულობის კომისია, ცოდნისა და ეკონომიკის სამინისტრო, ინფორმაციული უსაფრთხოების სააგენტოს (KISA)[272] შემადგენლობაში არსებული ინტერნეტის უსაფრთხოების ცენტრი (KrCERT/CC)[273]. KISA - ში შედის აგრეთვე ინფორმაციული ინფრასტრუქტურის დაცვის განყოფილება, რომელიც შედგება კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვითი ღონისძიებების დაგეგმვის, კრიტიკული ინფრასტრუქტურის უსაფრთხოების მართვისა და სერტიფიკაციის ჯგუფებისგან. ინფორმაციული უსაფრთხოების ეროვნული ალიანსი (NISA), სადაც გაერთიანებულია 22 სახელმწიფო ორგანიზაცია, 17 საწარმოს[274] ინფორმაციული უსაფრთხოების სამსახურების ხელმძღვანელი პირები, ასევე სპეციალისტები სამრეწველო და სამეცნიერო წრეებიდან, წარმოადგენს სახელმწიფოსა და კერძო სექტორებს შორის პარტნიორობას, რომელიც მიმართულია ინფორმაციის გაცვლის გზით, ინფორმაციული უსაფრთხოების ამაღლებასა და განვითარებაზე.

საქართველოში არსებული სუბიექტები

საქართველოში არ არსებობს ერთიანი ორგანო, რომელიც კოორდინაციას გაუწევს ქვეყნის კიბერსივრცის დაცვასა და უზრუნველყოფს კიბერუსაფრთხოებასთან დაკავშირებულ ღონისძიებებს სამინისტროებსა და უწყებებს შორის. განხორციელებულმა საკონსტიტუციო ცვლილებებმა და უშიშროების საბჭოს ალტერნატიული ორგანოს უსაფრთხოებისა და კრიზისების მართვის საბჭოს შექმნამ გამოიწვია მოცემული საკითხის დროებით ღიად დატოვება. კერძოდ, უშიშროების საბჭომ, რომელმაც თავის დროზე შეიმუშავა კიბერუსაფრთხოების სტრატეგია, და რომლის ფარგლებშიც უნდა ყოფილიყო კიბერსივრცის დაცვის საკითხებზე მომუშავე

[271] http://www.iclei.org/
[272] http://www.kisa.or.kr/eng/main.jsp
[273] http://eng.krcert.or.kr/krcert_cc/welcome.jsp
[274] ინფორმაციული ქსელების სახელმწიფო კომპანიები და ოპერატორები

უწყებათაშორისი კომისია[275], თავისი ფუნქციები მოცემულ სფეროში გადასცა უსაფრთხოებისა და კრიზისების მართვის საბჭოს, სადაც ჯერჯერობით ამ მიმართულებით წინსვლა არ არის. მიუხედავად ამისა, კანონში „ინფორმაციული უსაფრთხოების შესახებ“ განსაზღვრულია კიბერუსაფრთხოებაზე პასუხიმგებელი და მაკოორდინირებელი სახელმწიფო ორგანო. კერძოდ, კანონის მე - 3 თავში „კიბერუსაფრთხოების უზრუნველყოფა“ ვკითხულობთ, რომ „საქართველოს კიბერსივრცეში ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვას, ასევე ინფორმაციული უსაფრთხოების კოორდინაციისკენ მიმართულ სხვა, მასთან დაკავშირებულ საქმიანობას, რომელიც კიბერუსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრას ემსახურება, ახორციელებს მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი - CERT.GOV.GE“[276]. მოცემული ჯგუფის მოვალეობებში შედის კრიტიკული ინფორმაციული სისტემის ინფორმაციული უსაფრთხოების დაცვის შესახებ რეკომენდაციების გაცემა, კომპიუტერული ინციდენტების ანალიზი, აღრიცხვა, მათი დროული გამოვლენა, რეაგირება და კოორდინაციის უზრუნველყოფა და სხვა. ასევე, ჯგუფი პასუხისმგებელია მოცემულ სფეროში ცნობიერების ამაღლებაზე, საგანმანათლებლო პროცესზე და სხვა[277].

საქართველოში კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვაზე, კიბერუსაფრთხოებით ღონისძიებების უზრუნველყოფასა და კიბერდანაშაულთან ბრძოლას წარმართავს იუსტიციის, თავდაცვისა და შინაგან საქმეთა სამინისტროები, რომლებსაც განსაზღვრული აქვთ და მოქმედებენ თავიანთი კომპეტენციის ფარგლები. კერძოდ:

- მოცემული სამინისტროებიდან ქვეყნის კრიტიკული ინფორმაციული ინფრასტრუქტურის სისტემებისა და სუბიექტების დაცვაზე პასუხისმგებელია იუსტიციის სამინისტროს სსიპ „მონაცემთა გაცვლის

[275] კომისიაში შედიოდა ყველა სამინისტროსა და უწყებების წარმომადგენლები
[276] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, თავი III, მუხლი 8, გვ. 7
[277] საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ, თავი III, მუხლი 8, გვ. 7, 8

სააგენტო“[278], სადაც ასევე გაერთიანებულია ზემოთ ნახსენები კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი - CERT.GOV.GE. სააგენტო ასევე განსაზღვრავს ინფორმაციული უსაფრთხოების პოლიტიკას[279], კოორდინაციასა და მონიტორინგს უწევს სამინისტროებსა და უწყებებში ინფორმაციული უსაფრთხოების მიმართულებით გასატარებელ ყველა ღონისძიებას. მონაცემთა გაცვლის სააგენტო ასევე აქტიურად თანამშრომლობს საერთაშორისო დონეზე, კერძოდ ევროკავშირის წევრ ქვეყნებთან და ნატო - ს შესაბამის სტრუქტურულ ერთეულებთან. გარდა ამისა, სააგენტო წარმატებით ახორციელებს E – Governmant[280] სისტემის დანერგვის პროცესს;

- 2014 წლის თებერვალში[281] თავდაცვის სამინისტროს ფარგლებში შეიქმნა სსიპ „კიბერუსაფრთხოების ბიურო“[282], რომლის მიზანია კიბერდანაშაულთან ბრძოლის ერთიანი სახელმწიფო პოლიტიკის განხორციელება, ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავება და მისი განხორციელების ხელშეწყობა, ბიუროს კომპეტენციას მიკუთვნებული სფეროს მარეგულირებელი კანონმდებლობის შემუშავება და სრულყოფა და კანონმდებლობით დადგენილი სხვა საქმიანობის განხორციელება. ბიუროს ძირითადი საქმიანობა წარიმართება ინფორმაციული და კომუნიკაციების ტექნოლოგიების დეპარტამენტის

[278] http://dea.gov.ge/uploads/legal_acts/1/monacemta%20gacvlis%20saaagento_geo.pdf
[279] http://dea.gov.ge/uploads/legal_acts/8/Inf._Security.pdf
[280] E-government (short for electronic government, also known as e-gov, Internet government, digital government, online government, or connected government) consists of the digital interactions between a citizen and their government (C2G), between governments and government agencies (G2G), between government and citizens (G2C), between government and employees (G2E), and between government and businesses/commerce (G2B). Essentially, e-government delivery models can be briefly summed up as (Jeong, 2007):
G2G (government to governments)
G2C (government to citizens)
G2E (government to employees)
G2B (government to businesses)
[281] https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=2235212&lang=ge
[282] კიბერუსაფრთხოების ბიუროს მიზნები და ფუნქციების დიდი ნაწილი წარმოადგენს მონაცემთა გაცვლის სააგენტოს მიზნებისა და ფუნქციების ანალოგიას, რაც ყოვლად დაუშვებელია, ვინაიდან მოხდება მოცემულ სფეროში უწყებრივი ფუნქციების აღრევა და სამუშაო პროცესის წარმართვა პარალელურ რეჟიმში

მიერ, რომლის სტრუქტურული ერთეულებია: პროექტების მართვის სამმართველო; კომპიუტერულ ინციდენტებზე რეაგირების საკოორდინაციო სამმართველო CSIRT/CC); კომპიუტერულ ინციდენტებზე რეაგირების სამმართველო (CSIRT); კომპიუტერულ ინციდენტებზე რეაგირების საკომუნიკაციო მომსახურების განყოფილება;

- ინტერნეტ - სივრცეში კიბერდანაშაულების გამოვლენას, აღკვეთას, მოკვლევით და საგამოძიებო საქმიანობას, ასევე საჭიროების შემთხვევაში დაკავებას, ახორციელებს შინაგან საქმეთა ცენტრალური კრიმინალური პოლიციის დეპარტამენტის კიბერდანაშაულთან ბრძოლის სამმართველო[283]. გარდა ამისა, შინაგან საქმეთა სამინისტროში საექსპერტო–კრიმინალისტიკური მთავარი სამმართველოს შემადგენლობაში ჩამოყალიბდა კომპიუტერულ–ციფრული ექსპერტიზის ქვეგანყოფილება, რომელიც უშუალოდ ახორციელებს ციფრული მტკიცებულებების პირველად მოპყრობასა და მათ შემდგომ ექსპერტიზას. სამინისტროს შემადგენლობაში ასევე ფუნქციონირებს ოპერატიულ - ტექნიკური დეპარტამენტი, რომელიც ახორციელებს სამინისტროში ინოვაციური ინფორმაციული ტექნოლოგიების, ციფრული სატელეკომუნიკაციო სისტემების დანერგვას და ოპერირებას, აღნიშნულ სფეროებში სხვა სახელმწიფო დაწესებულებების კონსულტირებას, სამინისტროსა და მისი სტრუქტურული ქვედანაყოფების სატელეკომუნიკაციო უზრუნველყოფას და კანონმდებლობით დადგენილი წესის შესაბამისად, საგამოძიებო ღონისძიებების განხორციელების შედეგად მოპოვებული ციფრული მტკიცებულებების საექსპერტო - კრიმინალისტიკურ გამოკვლევას.

[283] 2012 წელს საქართველო შეუერთდა კიბერდანაშაულთან ბრძოლის შესახებ ევროსაბჭოს კონვენციას. ამავე წელს შსს-ს ცენტრალური კრიმინალური პოლიციის დეპარტამენტში შეიქმნა კიბერდანაშაულთან ბრძოლის სამმართველო, რომელსაც ევალება კიბერ სივრცეში ჩადენილი მართლსაწინააღმდეგო ქმედებების გამოვლენა, აღკვეთა და პრევენცია

რეზუმე

ნაშრომში მოკლედ, ზოგად ფორმებში არის განხილული ევროკავშირის ზოგიერთი წევრი ქვეყნისა და სხვა ქვეყნების სუბიექტები, რომლებიც პასუხისმგებელნი არიან კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვასა და კიბერუსაფრთხოების მიმართულებით აუცილებელი ღონისძიებების განხორციელებაზე. კიბერსივრცეში არსებული საფრთხები და რისკები არცთუ ისე დიდი ხნის წინ წარმოიშვა, თუმცა ინტერნეტისა და ტექნოლოგიების სწრაფმა განვითარებამ, დადებითი პროცესების პარალელურად, გამოიწვია ასევე კიბერდანაშაულის სწრაფი ზრდა. კიბერსივრცეში საფრთხეების მაქსიმალური შემცირების მიზნით, მსოფლიო საზოგადოებამ დაიწყო ორგანიზაციული სტრუქტურული ერთეულების შექმნისა და განვითარების პროცესი, რაც პირდაპირ კავშირშია ახალი ტექნოლოგიებისა და კიბერდანაშაულის ზრდასთან, მის ახალ გამოვლინებებთან. ფაქტიურად, მოცემულ სფეროში მუდმივად მიმდინარეობს და ვითარდება ინსტიტუციონალიზმის პროცესი.

საქართველო აქტიურად მიისწრაფვის ევროინტეგრაციისკენ, ქვეყანა ცდილობს გახდეს ევროკავშირისა და ჩრდილოეთ ალიანსის სრულუფლებიანი წევრი, ხელი მოეწერა ასოცირების ხელშეკრულებას. ყოველივე ეს ნიშნავს, რომ ქვეყანა თავის თავზე იღებს ყველა იმ ვალდებულებას, რაც უზრუნველყოფს არამარტო საქართველოს უსაფრთხოებას, არამედ ევროკავშირის როგორც ცალკეული წევრი ქვეყნებისა ისე მთლიანად ევროკავშირის უსაფრთხოების შესაბამისი ნორმების დაცვას, სადაც ასევე იგულისხმება კიბერსივრცის მაქსიმალური დაცვის უზრუნველყოფა. ეს არის ქვეყნისთვის სერიოზული გამოწვევა, რადგან საქართველომ უნდა შექმნას ეროვნული კანონმდებლობა, წესრიგში მოიყვანოს და საერთაშორისო სტანდარტებს შეუსაბამოს ქვეყნის კრიტიკული ინფორმაციული ინფრასტრუქტურის სისტემისა და ცალკეული სუბიექტების დაცვა, გაზარდოს საერთაშორისო თანამშრომლობა და რისკების შემცირების მიზნით, უნდა მოახდინოს საზოგადოების ცნობიერების ამაღლება და საგანმანათლებლო სისტემის შემუშავება. მოცემულ სფეროში აქტუალური და

აუცილებელი ხდება საქართველოს სუბიექტების, ევროკავშირის წევრი და სხვა ქვეყნების ანალოგიურ სუბიექტებთან ინტეგრაციის პროცესის სწორი მიმართულებით წარმართვა, მათი ცოდნისა და გამოცდილების გაზიარება, რაც ხელს შეუწყობს კიბერუსაფრთხოების სფეროში ქვეყნის ორგანიზაციულ სტრუქტურული სუბიექტების განვითარებას, მათ საერთაშორისო სტანდარტებთან შესაბამისობაში მოყვანას, კოორდინირებული მუშაობის ამაღლებასა და ეფექტური ღონისძიებების გატარებას კრიტიკული ინფორმაციული ინფრასტრუქტურისა და პერსონალური თუ სხვა სახის მონაცემთა დაცვის მიმართულებით.

გამოყენებული ლიტერატურა

1) Democratic Governance Challenges of Cyber Security, Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler, DCAF 2010, DCAF Horizon 2015 Working Paper Series http://genevasecurityforum.org/files/DCAF-GSF-cyber-Paper.pdf; http://www.dcaf.ch/Publications/Democratic-Governance-Challenges-of-Cyber-Security;
2) კანონი „ინფორმაციული უსაფრთხოების შესახებ“, 19/06/2012 http://www.economy.ge/uploads/kanonmdebloba/kavshirgabmuloba/informaciuli_usafrtxoeba.pdf;
3) საჯარო სამართლის იურიდიული პირის – კიბერუსაფრთხოების ბიუროს დებულების დამტკიცების შესახებ, საქართველოს თავდაცვის მინისტრის ბრძანება №8, 2014 წლის 6 თებერვალი https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=2235212&lang=ge

საერთაშორისო და რეგიონალური დონის ღონისძიებები მიმართული კიბერსივრცის დაცვაზე

შესავალი

კიბერდანაშაულთან ბრძოლისა და კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის პროცესში დიდი მნიშვნელობა ენიჭება არამარტო ეროვნულ პოლიტიკას, სტრატეგიასა თუ სხვა სახის ქმედით ზომებს, არამედ ასევე თანამშრომლობას საერთაშორისო და რეგიონალურ დონეზე. მსგავსი თანამშრომლობა კიბერსივრცის დაცვის სფეროში ითვალისწინებს და მოიცავს საერთაშორისო და რეგიონალურ კონვენციებს, ფორუმებს, ორგანიზაციებსა და ალიანსებს, შეხვედრებსა და დისკუსიებს, ერთობლივ რეზოლუციებს, გადაწყვეტილებებსა და რეკომენდაციებს, დირექტივებს.

ქვემოთ წარმოდგენილია ის საერთაშორისო და რეგიონალური დონის ორგანიზაციები, რომლებიც ცდილობენ სხვადასხვა გზებით წინ აღუდგნენ კიბერადანაშაულსა და უზრუნველყონ კიბერსივრცის დაცვა. ევროსაბჭოს, ევროკავშირის, გაერო - ს, ნატო - სა თუ სხვა წარმოდგენილი ორგანიზაციების ფარგლებში წარმოებს საქმიანობა კიბერუსაფრთხოების თემებზე.

ევროპის საბჭო

2001 წლის 23 ნოემბერს ბუდაპეშტში ხელი მოეწერა კიბერდანაშაულთან ბრძოლის ევროპულ კონვენციას (CETS 185)[284], რომელიც ძალაში შევიდა 2004 წლის 1 ივლისს. კონვენცია მომზადდა ევროპის საბჭოს ფარგლებში კანადის, შეერთებული შტატების, იაპონიისა და სამხრეთ აფრიკის რესპუბლიკის მონაწილეობით. დღესდღეისობით ეს კონვენცია არის მოცემულ სფეროში ერთადერთი აღიარებული იურიდიული დოკუმენტი, რომელიც მიღებულია საერთაშორისო დონეზე და ის არის

[284] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

ღია ყველა დაინტერესებული ქვეყნისთვის. ასევე საინტერესოა კონვენციაზე დამატებით მიღებული პროტოკოლი (CETS 189)[285] კომპიუტერულ ქსელებში ქსენოფობიისა და რასიზმის ნიადაგზე ჩადენილი დანაშაულების შესახებ, რომელსაც ხელი მოეწერა 2003 წლის იანვარში და ძალაში შევიდა 2006 წლის მარტის თვეში.

კონვენცია ხელმომწერ ქვეყნებს ავალდებულებს შექმნან სამართლებრივ - ნორმატიული ბაზა აუცილებელი კიბერდანაშაულის პრობლემის ეფექტური გადაწყვეტისთვის. ასევე ყველა ხელმომწერი ქვეყანა თავის თავზე იღებს ერთმანეთისთვის დახმარების აღმოჩენას კიბერდამნაშავეთა სამართლებრივი დევნისა და ინციდენტების გამოძიების საკითხში. ევროპული კონვენცია არის ერთერთი პირველი საერთაშორისო დოკუმენტი, სადაც განსაზღვრულია და კლასიფიცირებულია კიბერდანაშაული. კერძოდ, შემოსულია ინტერნეტ სივრცეში არასანქცირებული შეღწევისა და რესურსების არაკანონიერი გადაჭერის განსაზღვრება, კომპიუტერულ სისტემებსა და ინფორმაციის მატარებელზე არაკანონიერი ჩარევა, მოწყობილობის არასამართლებრივი გამოყენება, კომპიუტერული მაქინაციები. კონვენციის მოქმედება ასევე ვრცელდება საბავშვო პორნოგრაფიასა და საავტორო უფლებების დარღვევაზე. დოკუმენტში განსაზღვრულია კომპიუტერული დანაშაულების ეფექტური გამოძიების ინსტრუმენტები და მათთან ბრძოლა. კონვენციის მოქმედფება ვდრცელდება ყველა დანაშაულზე, რომელიც ჩადენილია კომპიუტერულ სისტემებში, ასევე ელექტრონული საშუალებებით შეგროვილი ნებისმიერი მტკიცებულებები.

ამ ეტაპზე კონვენცია რატიფიცირებულია ევროკავშირის ყველა ქვეყნისა და შეერთებული შტატების მიერ, და ხელმოწერილია ორმოცდაექვსი ქვეყნის მიერ[286]. ხუთ ქვეყანას მიეცა რეკომენდაცია და გაუკეთდა შეთავაზება მიუერთდეს კონვენციას[287]. ისეთმა დიდმა ქვეყნებმა, როგორებიცაა ჩინეთი და რუსეთი უარი თქვეს ხელი მოეწერათ

[285] http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=1&CL=ENG

[286] ევროკავშირის წევრი ქვეყნები, კანადა, იაპონიია, სამხრეთ აფრიკის რესპუბლიკა და ნატო - ს ყველა წევრი ქვეყანა

[287] ჩილე, კოსტა - რიკა, დომინიკის რესპუბლიკა, მექსიკა და ფილიპინები

კონვენციაზე და მიერთებოდნენ მას[288]. ევროპული კონვენცია გამოიყენება როგორც სახელმძღვანელო და ცნობარი მსოფლიოს ასზე მეტი ქვეყნის სტანდარტული ან ტიპიური საკანონმდებლო ბაზისათვის. გარდა ამისა, კონვენცია მხარს უჭერს ყველა სხვა ორგანიზაციას, რომლებიც იყენებენ მას თავიანთი გადაწყვეტილების მიღებაში. ეს ორგანიზაციებია ევროპის კავშირი, ამერიკის სახელმწიფოთა ორგანიზაცია (OAS)[289], ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაცია (OECD)[290], აზია - წყნარი ოკეანის ეკონომიკური თანამშრომლობის ორგანიზაცია (APEC)[291], ინტერპოლი[292], ასევე კერძო სექტორის წარმომადგენლები.

მიუხედავად იმისა, რომ მოცემულ კონვენციას აქვს ფართო საერთაშორისო აღიარება, ზოგიერთი ქვეყანა მაინც ამტკიცებს, რომ კონვენცია ითვალისწინებს კიბერდანაშაულის აღსაკვეთად საჭირო არასაკმარის ზომებს, და რამაც შეიძლება დიდი ზიანი მიაყენოს ეროვნულ უსაფრთხოებას. პირველ რიგში, კონვენცია კომპიუტერულ ქსელზე განხორციელებულ შეტევას განიხილავს როგორც კერძო და სახელმწიფო საკუთრების წინააღმდეგ ჩადენილ დანაშაულს, და არა როგორც ეროვნული უსაფრთხოების საფრთხეს. მეორე, კონვენცია ერთმანეთისგან არ ანსხვავებს შეტევებს ჩვეულებრივი კომპიუტერული ქსელებსა და კრიტიკული ინფორმაციული ინფრასტრუქტურის ობიექტებს შორის, ისევე როგორც ფართომასშტაბიან და ლოკალურ შეტევებს შორის.

თუმცა კონვენცია წარმოადგენს სტანდარტულ დოკუმენტს, რომელიც წარმოადგენს საერთაშორისო კანონმდებლობის ძალზედ მნიშვნელოვან შემადგენელ ნაწილს. მასში მოცემულია იურიდიული და ტექნიკური ნორმების ოპტიმალური კომპლექსი, რომელიც შეიძლება გამოყენებულ იქნას ამ სფეროში საერთაშორისო თანამშრომლობის გაფართოებაზე დამატებითი შეთანხმებების დამუშავების მიზნით. გამომდინარე, რომ კიბერდანაშაულს, კიბერტერორიზმსა და კიბერომს გააჩნიათ ბევრი

[288] აღნიშნული კონვენცია საქართველოსთან მიმართებაში ძალაში შევიდა 2012 წლის პირველი ოქტომბრიდან. შედეგად, საქართველო გახდა კონვენციის 34-ე წევრი სახელმწიფო
[289] Organization of American States http://www.oas.org/en/
[290] Organization for Economic Co-operation and Development http://www.oecd.org/
[291] Azia – Pacific Economic Cooperation http://www.apec.org/
[292] Interpol http://www.interpol.int/

საერთო ნიშანი და მახასიათებელი, კონვენცია ნებისმიერ კიბერშეტევაზე, მიუხედავად მათი მოტივაციისა, ითვალისწინებს, რომ მასზე ხელმომწერმა ქვეყნებმა პასუხისმგებელი უწყებების მოთხოვნაზე უნდა დააკავონ და გადასცენ ყველა კიბერდამნაშავე სამართალდამცავ ორგანოებს, მიუხედავად იმისა, განიხილებიან თუ არა ისინი საკუთარ ქვეყნებში როგორც დამნაშავეები, ტერორისტები ან კიდევ პატრიოტები.

ევროპული კავშირი

ევროკავშირი წარმოადგენს ინფორმაციული უსაფრთხოების სფეროში საერთაშორისო დონეზე არსებულ მთავარ სუბიექტს. ამავდროულად, ევროკავშირი დიდ ყურადღებას უთმობს ისეთ საკითხებს, როგორიც არის კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვა, ინფორმაციული საზოგადოების ფორმირება და ინფორმაციული დაცვა. ევროკავშირმა დაიწყო სამეცნიერო - კვლევითი და სხვა სახის პროგრამების რეალიზება, რომელიც უკავშირდება ინფორმაციული რევოლუციის ასპექტებსა და განათლებაზე, ბიზნესზე, ჯანდაცვასა და კავშირგაბმულობაზე მათ გავლენას.

2004 წლის 20 ოქტომბერს[293] ევროკავშირის კომისიის მიერ მიღებული კომუნიკე კრიტიკული ინფრასტრუქტურის დაცვაზე იძლევა კრიტიკული ინფრასტრუქტურისა და მისი ობიექტების განსაზღვრებას, ასევე ადგენს კრიტერიუმებს იმ ობიექტების მიმართ, რომლებიც შეიძლება წარმოიშვას მომავალში. 2005 წლის ნოემბერში[294] ევროკავშირის კომისიის მიერ მიღებულია კრიტიკული ინფრასტრუქტურის დაცვის ევროპული პროგრამა „მწვანე წიგნი“, სადაც განსაზღვრულია ევროკავშირის მოქმედების მიმართულებები მოცემულ სფეროში. 2008 წელს ევროკავშირის კომისია შეუდგა პროექტის რეალიზებას, რომელიც მიმართულია კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის საერთო სტრატეგიის გამომუშავებაზე.

ქვემოთ მოცემულია ევროკავშირის კომისიის სხვა პროექტები და სტრატეგიები:

[293] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm
[294] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm

- ევროკავშირის კომისიის დაკვეთით, ელექტრონული კავშირის ინფრასტრუქტურის შეღწევადობისა და საიმედოობის პრობლემების კვლევების ჩატარება (ARECI)[295];
- პროექტი „კრიტიკული ინფრასტრუქტურის საფრთხეების შეტყობინების ინფორმაციული ქსელი“ (CIWIN)[296];
- 2004 წლის მარტში შეიქმნა და 2005 წლის სექტემბერში, კუნძულ კრეტაზე დაიწყო ფუნქციონირება ქსელური და ინფორმაციული უსაფრთხოების ევროპულმა სააგენტომ (ENISA)[297]. სააგენტოს მიზანია ევროკავშირის ფარგლებში ელექტრონული ქსელების უსაფრთხოების მაღალი დონის მიღწევა;
- ტელემეტრიის ტრანსევროპული სამთავრობოთაშორისო სამსახური (TESTA)[298]. ეს არის სამთავრობოთაშორისო კავშირის ქსელი, რომელიც მოქმედებს მხოლოდ ევროკავშირის ფარგლებში. ის არ არის ჩართული ინტერნეტ - სივრცეში და სხვადასხვა უწყების თანამდებობის პირებს ერთმანეთთან ურთიერთობისას, ინფორმაციის დაზიანებისა და გადინების თავიდან აცილების საშუალებას აძლევს;

ინფორმაციული უსაფრთხოების სფეროში ევროკავშირის სამეცნიერო - კვლევითი პროექტები:

- ინფორმაციული საზოგადოების ტექნოლოგიები (პროექტები FP6[299] და FP7[300]);
- უსაფრთხოების პრობლემების ევროპული სამეცნიერო - კვლევითი პროგრამა (ESRP)[301];

[295] The Availability and Robustness of Electronic Communications Infrastructures file:///C:/Users/Admin/Downloads/StudyFinalReport.pdf
[296] The Critical Infrastructure Warning Information Network https://ciwin.europa.eu/Pages/Home.aspx
[297] The European Union Agency for Network and Information Security https://www.enisa.europa.eu/
[298] The European Software Testing Awards http://www.softwaretestingawards.com/
[299] http://ec.europa.eu/research/fp6/index_en.cfm
[300] http://ec.europa.eu/research/fp7/index_en.cfm
[301] http://www.statewatch.org/Targeted-issues/ESRP/security-research.html

- კრიტიკული ინფორმაციული ინფრასტრუქტურის პრობლემების სამეცნიერო - კვლევითი საკოორდინაციო პროექტი (CI2RCO)[302];
- ინფრასტრუქტურისა და პროექტირების არქიტექტურა[303].

ინფორმაციული უსაფრთხოების საკითხებში ევროკავშირიოს სამართლებრივ - ნორმატიული ბაზა:

- მონაცემთა დაცვის დირექტივა (1995 წელი)[304];
- ელექტრონული ხელმოწერის დირექტივა (1999 წელი)[305];
- ელექტრონულ კავშირების სფეროში კონფიდენციალობის დაცვის დირექტივა (2002 წელი)[306];
- ჩარჩო დირექტივა (2002 წელი)[307];
- ინფორმაციულ სისტემებზე შეტევის საბჭოს ჩარჩო გადაწყვეტილება (2005 წელი)[308];
- მონაცემთა შენახვის დირექტივა (2006 წელი).

უსაფრთხოებისა და ექსტრემალური რეაგირების ფორუმი (FIRST)[309]

ფორუმი დაფუძნდა 1990 წელს და წარმოადგენს ინფორმაციული უსაფრთხოების სფეროში ინციდენტებზე ექსტრემალური რეაგირების სპეციალისტების მსოფლიოში არსებულ ერთადერთ საერთაშორისო ფორუმს. ეს ორგანიზაცია წარმოადგენს ქსელებში ექსტრემალური რეაგირების სფეროში მსოფლიოში აღიარებულ ლიდერს და აერთიანებს ოპერატიული რეაგირების ჯგუფებს, რომლებიც მუშაობენ სხვადასხვა უწყებრივ დონეებზე, როგორც სახელმწიფო ისე კერძო სექტორში, მათშორის საგანმანათლებლო დაწესებულებებში. ფორუმის საქმიანობა მიმართულია ინციდენტების აღკვეთის

[302] ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/security/ci2rco-executive-summary_en.pdf
[303] http://www.service-architecture.com/articles/cloud-computing/infrastructure_as_a_service_iaas.html
[304] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 24 October 1995 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
[305] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 13 December 1999 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:en:HTML
[306] http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_en.htm
[307] http://europa.eu/legislation_summaries/information_society/legislative_framework/l24216a_en.htm
[308] http://europa.eu/legislation_summaries/information_society/internet/l33193_en.htm
[309] The Forum of Incident Response and Security Teams http://www.first.org/

გაძლიერებასა და კოორდინირებულ თანამშრომლობაზე, ასევე სწრაფი რეაგირების სფეროში შესაძლებლობების გაძლიერებაზე. ფორუმი მის წევრებსა და ზოგადად საზოგადოებას შორის ინფორმაციისა და გამოცდილების გაცვლის საშუალებას იძლევა.

დიდი რვიანი (Group of Eight – G8)

დიდი რვიანი 1995 წლიდან მოყოლებული სულ უფრო მეტ აქტიურ მონაწილეობას იღებს იმ საკითხების გადაწყვეტაში, რომლებიც უკავშირდება კიბერდანაშაულს, ინფორმაციულ საზოგადოებას, კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვას. 1995 წელს ჰალიფაქსის სამიტზე[310] შეიქმნა უფროს ექსპერტთა ჯგუფი, რომელსაც დაევალა შეეფასებინა და გაანალიზებინა არსებული საერთაშორისო შეთანხმებები, ასევე ორგანიზებულ დანაშაულთან ბრძოლის მექანიზმები. მოცემულმა ჯგუფის მიერ ჩატარებული სამუშაოს შედეგად, შემუშავდა ორმოცი ოპერატიული რეკომენდაცია, რომლებიც დამტკიცებულ იქნა 1996 წელს დიდი რვიანის ლიონის სამიტზე. ამ დროდან მოყოლებული ლიონის ჯგუფი გახდა მუდმივმოქმედი მრავალფუნქციური ორგანო, რომლის შემადგენლობაში შევიდა მთელი რიგი სპეციალური სამუშაო ჯგუფები. 2001 წლიდან, ტერორიზმთან დაკავშირებულ საკითხებზე, ლიონის ჯგუფის სხდომები მიმდინარეობს ერთობლივად რომის ჯგუფთან.

კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის სფეროში დიდი რვიანის მუშაობის მიღწევად შეიძლება ჩაითვალოს, პარიზში 2000 წელს[311] ჩატარებული კონფერენცია, სადაც მონაწილეობას იღებდა როგორც სახელმწიფო ისე კერძო სექტორი. კონფერენცია მიეძღვნა სახელმწიფოსა და კერძო სექტორს შორის უსაფრთხოებისა და კიბერსივრცის სფეროში სანდოობის ამაღლების განვითარება. კონფერენციის მიზანი იყო მარალტექნოლოგიური დანაშაულისა და ინტერნეტ - სივრცის არაკანონიერი გამოყენების ირგვლივ მსჯელობა და გადაწყვეტილების მიღება. დიდი რვიანის წევრი ქვეყნები პარიზის კონფერენციაზე შეთანხმდნენ კიბერდანაშაულთან ბრძოლის კონკრეტულ და გამჭვირვალე პრინციპებზე, რომლებიც მიმართულია ახალი

[310] http://www.chebucto.ns.ca/Current/HalifaxSummitG7/
[311] https://www.ciret.org/conferences/paris-2000/

„უსაფრთხოების კულტურის“ შექმნაზე, საერთაშორისო თანამშრომლობის გააქტიურებაზე, ასევე მონიტორინგისა და კომპიუტერულ ქსელებში საფრთხის შეტყობინების სფეროში არსებული მოწინავე გამოცდილების გაზიარებაზე. კონფერენციაზე ასევე მიღწეული იყო შეთანხმება ერთობლივი სასწავლო კურსების ჩატარებაზე, რომელმაც უნდა გამოავლინოს ქსელებში საგანგებო ინციდენტებზე რეაგირების სამსახურების მომზადების მზადყოფნა, აგრეთვე საფრთხეების შესახებ შეატყობინოს სხვა ქვეყნების მთავრობებს. კონფერენციაზე სულ მიღებული იქნა თერთმეტი პრინციპი, რომლებიც დახმარებას გაუწევს სახელმწიფოებს კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის სფეროში შექმნას და გაატაროს ეფექტური ეროვნული პოლიტიკა.

კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის პრინციპების ძირითადი ელემენტები აისახა, 2004 წელს გაეროს 78 - ე ასამბლეაზე მიღებულ №58/199 რეზოლუციაში[312] „კიბერუსაფრთხოებისა და კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის გლობალური კულტურის შექმნაზე“.

ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაცია (NATO)

2002 წელს, მას შემდეგ რაც 1990 წლების ბოლოს ბალკანებზე სამხედრო ოპერაციის დროს განხორციელდა ქსელური შეტევები, ალიანსმა შეიმუშავა და გაუშვა კიბერ - დაცვის საკუთარი პროგრამა. ალიანსის ხელმძღვანელობამ გაითვალისწინა „ბალკანეთის გაკვეთილები“, და 2002 წელს პრაღის სამიტზე[313] ნატო - ს წევრი ქვეყნების ლიდერები შეთანხმდნენ კიბერნეტიკული თავდაცვის პროგრამის შემუშავებასა და ინფორმაციულ ქსელებში ინციდენტებზე რეაგირების საკუთარი ჯგუფის (NCIRC)[314] შექმნაზე. ჯგუფის საკოორდინაციო ცენტრი განთავსებულია ბრუსელში, ნატო - ს შტაბ - ბინაში, ხოლო ალიანსის სამეთაურო ოპერაციების მართვის შტაბში[315] ორგანიზებულ იქნა NCIRC - ს ტექნიკური ცენტრი. მოცემული სტრუქტურის შექმნით, ალიანსმა

[312] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf
[313] http://www.nato.int/docu/comm/2002/0211-prague/
[314] Computer Incident Response Capability https://www.terena.org/activities/tf-csirt/meeting11/NCIRC-Anil.pdf
[315] ქ. მონსი, ბელგია

გადაწყვიტა მთელი რიგი სირთულეები დაკავშირებული კიბერუსაფრთხოების საკითხებთან. კერძოდ, ნატო - ს კომპიუტერულ ქსელებში არასანქცირებული შეღწევისა და სხვა მავნებლობების აღმოჩენა და განეიტრალება, ასევე ქსელების კრიპტოგრაფიული დაცვის ეფექტური მართვის უზრუნველყოფა.

გარდა ამისა, ალიანსის ექსპერტები უზრუნველყოფენ კომპიუტერულ ქსელებში საფრთხის წარმოქმნის საწინააღმდეგო ტექნიკურ ღონისძიებების, ასევე შეიმუშავებენ უსაფრთხოების უზრუნველყოფის რეჟიმსა და კომპიუტერულ დანაშაულებების გამოძიების მეთოდოლოგიას. ამის პარალელურად, ტალინში შეიქმნა ალიანსის კომპიუტერული თავდაცვის სფეროში მოწინავე გამოცდილების გაცვლის ცენტრი (CCDCOE)[316], ნატო - მ ასევე დააფუძნა კიბერ - თავდაცვის ღონისძიებების მართვის სპეციალური ორგანო (CDMA)[317], რომელმაც ფუნქციონირება დაიწყო 2008 წელს. ამ უკანასკნელის ფუნქციებში შედის ალიანსის კომპიუტერულ ქსელზე შეტევის შემთხვევაში „კიბერ - თავდაცვის ოპერატიული და ეფექტური ღონისძიებების“ ორგანიზება და კოორდინაცია. 2009 წელს სტრასბურგის სამიტზე[318] ნატო - ს წევრმა ქვეყნებმა ვალდებულება აიღეს დააჩქარონ კიბერ - თავდაცის თანამედროვე საშუალებების შეძენა, გახადონ კიბერდაცვა ალიანსის განუყოფელ ნაწილად, განავითარონ საერთაშორისო თანამშრომლობა არამარტო ნატო - ს წევრ - ქვეყნებს შორის, არამედ ასევე პარტნიორ ქვეყნებთან. ალიანსი ასევე ახორციელებს მხარდამჭერ პროგრამებს მიმართულს წევრი და პარტნიორი ქვეყნების კიბერუსაფრთხოების ეროვნული პოლიტიკის განვითარებისა და კიბერ - საფრთხეებზე ექსტრემალური რეაგირების ჯგუფის შექმნისკენ.

[316] Cooperative Cyber Defense Centre of Exelllence https://ccdcoe.org/tallinn-manual.html

[317] The Cyber Defense Management Authority (CDMA): The Authority was called upon to initiate and coordinate response to cyber attacks against allied member states, and NATO itself. CDMA was Created and was operational in mid-2008. It was a big step in NATO Cyber Defense because it helps member states improve their own cyber security. Rapid-Reaction Teams (RRT's) are also being created and will be available to member states in order to help them counter cyber attacks and will be available for immediate deployment http://csis.org/blog/nato-and-cyber-defense-brief-overview-and-recent-events

[318] http://www.nato.int/cps/en/natolive/news_52837.htm

კრიტიკული ინფრასტრუქტურის დაცვა არის ალიანსის ძირითადი მიმართულება ასევე სამოქალაქო თავდაცვის დაგეგმვის სფეროში. ამ სფეროში ღონისძიებების გატარების აუცილებლობაზე ნატო - ს ფარგლებში არაერთი დოკუმენტია მიღებული, სადაც ასახულია სამოქალაქო თავდაცვის დაგეგმვის პრინციპები, რომლებიც შემუშავდა წევრი ქვეყნების შესაბამისი უწყებებისთვის. გარდა ამისა, გეგმის ახალ რედაქციაში კიბერ - საფრთხეების ჭრილში, მოცემულია სამოქალაქო თავდაცვის საგანგებო სიტუაციების ისეთი მიმართულებები როგორიცაა ქიმიური, ბიოლოგიური და ატომური იარაღის გამოყენების წინააღმდეგ. ნატო - ს სამოქალაქო თავდაცვის დაგეგმვის მთავარი კომიტეტი და მისი რვა განყოფილება და კომიტეტი აგრძელებს კრიტიკული ინფრასტრუქტურის დაცვის ფუნქციონალური ასპექტების შესწავლას. ამის შედეგად, მუშავდება შესაბამისი რეკომენდაციები დაგეგმვის ყველა სახეობის მიმართულებით, რასაც ახორციელებს სათანადო განყოფილებები და კომიტეტები.

2007 წლის ნატო - ს საპარლამენტო ასამბლეაზე წარმოდეგნილ სპეციალურ მოხსენებაში, ასევე ალიანსის კრიტიკული ინფრასტრუქტურის დაცვის საკითხებზე მომზადებულ სხვა ანგარიშებში (173 DSCFC 09 E bis)[319] განსაზღვრულია ნატო - ს წევრი ქვეყნებისა და მთლიანად ალიანსის კრიტიკული ინფრასტრუქტურის დაცვის საერთო პრინციპები. ისინი განსაზღვრავენ სხვადასხვა ნორმებს, მათ მსგავსებასა და სხვაობას, ასევე კრიტიკული ინფრასტრუქტურის დაცვის დარგობრივი სტრატეგიების განვითარებისა და რეალიზაციის სფეროში განსაზღვრავენ სუბიექტებს თავისი ფუნქციებით, სადაც აგრეთვე შედის ენერგეტიკა, სამოქალაქო ავიაცია და საზღვაო პორტების უსაფრთხოება.

ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაცია (OECD)

ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციას გააჩნია დიდი გამოცდილება კომპიუტერული ქსელებისა და სისტემის უსაფრთხოების, მათ შორის კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის საკითხებზე სტრატეგიული რეკომენდაციების შემუშავებაში. ორგანიზაცია დიდ ყურადღებას უთმობს ასევე

[319] http://www.nato-pa.int/default.asp?SHORTCUT=1782

მავნებლური პროგრამული უზრუნველყოფის გამოყენებით ჩადენილ კიბერდანაშაულთან ბრძოლას. ორგანიზაცია ამზადებს ანალიტიკურ ანგარიშებს, სტატისტიკურ მონაცემებსა სტრატეგიულ რეკომენდაციებს, რომელთა საფუძველზეც სახელმწიფო და კერძო სექტორს შეუძლიათ შეიმუშავონ ეფექტური სტრატეგია საკუთარი ინფორმაციული უსაფრთხოების გაძლიერებაზე, საზოგადოებაში აამაღლონ ცნობადობის დონე ინტერნეტ - სივრცის უსაფრთხოების მნიშვნელობაზე და ხელი შეუწყონ კიბერუსაფრთხოების კულტურის განვითარებას. ორგანიზაციის ყველა წევრი ქვეყანა თანხმდება, რომ კრიტიკული ინფრასტრუქტურის დაცვა, მისი უსაფრთხო ფუნქციონირება და სანდოობა არის მნიშვნელოვანი ინტერნეტ - სივრცეში კანონიერი ვაჭრობისთვის, პერსონალური მონაცემების დაცვისა და უსაფრთხო საბანკო ოპერაციებისთვის. სწორედ ამიტომ, ორგანიზაციის ინფორმაციული უსაფრთხოებისა და კონფიდენციალობის სამუშაო ჯგუფი (WPISP)[320] აქტიურად მუშაობს ამ სფეროში საერთაშორისო დონეზე შეთანხმებული მიდგომის მიმართულებით, რომელიც ითვალისწინებს კომპიუტერულ ქსელებში ნდობის გაძლიერების მიზნით პოლიტიკის შემუშავებას. გარდა ამისა, ინფორმაციული, კომპიუტერული და საკომუნიკაციო პოლიტიკის კომიტეტი აკეთებს საერთო პრინციპების ანალიზს, რომელიც საფუძვლად უდევს ელექტრონულ ეკონომიკას, ინფორმაციულ ინფრასტრუქტურასა და საზოგადოებას.

გაერთიანებული ერების ორგანიზაცია (UN)

გაერომ 80 - იანი წლების ბოლოს დაიწყო კრიტიკული ინფორმაციული ინფრასტრუქტურის საკითხების განხილვა, თუმცა ფორმალური ზომების დანერგვა დაიწყო მხოლოდ ბოლო პერიოდში. ორგანიზაციის მიერ მის ფარგლებში მიღებულია მთელი რიგი ინიციატივები მიმართული კოორდინირებული მოქმედების გასაუმჯობესებლად. კერძოდ, ეს არის რამოდენიმე რეზოლუცია, მსოფლიო სამიტები ინფორმაციული საზოგადოების საკითხებზე (WSIS), გაეროს ზოგიერთი სტრუქტურის პროექტები.

[320] http://www.oecd.org/sti/whatistheoecdworkingpartyoninformationsecurityandprivacywpisp.htm

გლობალურ ციფრულ სივრცეში საერთაშორისო ინფორმაციული უსაფრთხოების გაძლიერების მიზნით, გაეროს განიარაღების კვლევითმა ინსტიტუტმა (UNIDIR) ჩაატარა მთელი რიგი სემინარები. თავის მხრივ, გაეროს ნარკომანიასთან და დანაშაულთან ბრძოლის სამმართველო სისტემატურად ატარებს სწავლებებს, რომლის მიზანია შეთანხმებული და კოორდინირებული მიდგომა კიბერდანაშაულის პრობლემებთან.

2000 და 2001 წლების დეკემბერში გაეროს გენერალური ასამბლეის 55 - ე და 56 - ე სესიებზე მიღებულ იქნა №55.63 და №56/121 რეზოლუციები „ინფორმაციული ტექნოლოგიების დანაშაულებრივ გამოყენებასთან ბრძოლაზე“. 2002 წლის დეკემბერში გაეროს გენერალური ასამბლეის 57 - ე სესიამ მიიღო რეზოლუცია №57/239 „კიბერუსაფრთხოების გლობალური კულტურის შექმნაზე“. 2003 წლის დეკემბერში გაეროს გენერალური ასამბლეის 58 - ე სესიაზე მიიღეს რეზოლუცია №58/199 „კიბერუსაფრთხოების გლობალური კულტურის შექმნასა და კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვაზე“. ამ რეზოლუციის დანართში ფორმულირებულია კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის თერთმეტი პრინციპი. შემდეგ წლებში გაეროს გენერალური ასამბლეა რეგულარულად იღებდა რეზოლუციებს „საერთაშორისო უსაფრთხოების კონტექსტში ინფორმაციული და სატელეკომუნიკაციო სფეროს განვითარებაზე“. 2005 და 2006 წლებში ასევე მიღებულ იქნა ორი რეზოლუცია ინფორმაციული საზოგადოების საკითხებზე გაეროს მსოფლიო სამიტების შედეგების შესახებ.

სერიოზული და მნიშვნელოვანი მოვლენა იყო, 2001 წელს გაეროს ეკონომიკური და სოციალური საბჭოს თხოვნის საფუძველზე ინფორმაციული და საკომუნიკაციო ტექნოლოგიების საკითხებზე გაეროს მიზნობრივი ჯგუფის შექმნა. ამ ჯგუფმა მიიღო უფლებამოსილება გაუწიოს საერთაშორისო საზოგადოების ძალისხმევას მობილიზება დეკლარაციის „ათასწლეულის განვითარების მიზნებზე“ იმ ნაწილს რეალიზაცია, რომელიც ეხება ინფორმაციული და საკომუნიკაციო ტექნოლოგიების განვითარებას. 2004 წლის აპრილში ნატო - ს შტაბ - ბინაში, სამიზნე ჯგუფის მიერ ორგანიზებული იყო სემინარი თემაზე „ინფორმაციული უსაფრთხოების სფეროში უსაფრთხოების საკითხები

და პოლიტიკა“. 2005 წელს სამიზნე ჯგუფმა გამოაქვეყნა პრაქტიკული სახელმძღვანელო თემაზე „ინფორმაციის დაუცველობა - კიბერსაფრთხეებისა და კიბერუსაფრთხოების „გამოუკვლევი ტერიტორიების“ ათვისების გაკვეთილები“. მოცემულ პრაქტიკულ სახელმძღვანელოში ნაჩვენებია ისეთი ახალი და სერიოზული საერთაშორისო კიბერსაფრთხეები, როგორებიც არის კიბერჰულიგნობა, კიბერტერორიზმი, კიბეროში და კიბერდანაშაული.

ინფორმაციული საზოგადოების საკითხებზე გაეროს მსოფლიო სამიტის მსვლელობისას მონაწილე ქვეყნების ლიდერებმა დაავალეს ელექტროკავშირების საერთაშორისო გაერთიანებას კიბერუსაფრთხოების სფეროში კოორდინაცია გაუწიოს საერთაშორისო მოქმედებებს. თავის მხრივ, 2007 წლის მაისში ელექტროკავშირების საერთაშორისო გაერთიანების ინიციატივით შეიქმნა კიბერუსაფრთხოების გლობალური პროგრამა (GCA), რომელმაც უნდა გამოიმუშავოს გაზრდილი კიბერსაფრთხეების წინააღმდეგ მიმართული ღონისძიებების, პრინციპებისა და მექანიზმების კოორდინირებული მოქმედების საერთო კომპლექსი. პროგრამის რეალიზების მიზნით შეიქმნა უმაღლესი დონის ექსპერტთა ჯგუფი, სადაც შედიან კიბერუსაფრთხოების სფეროში მსოფლიოში აღიარებული ასამდე სპეციალისტი, რომლებიც წარმოადგენენ კვლევით ინსტიტუტებსა და სამეცნიერო წრეებს, სახელმწიფო და კერძო სექტორს, სამრეწველო საზოგადოებებს, საერთაშორისო ორგანიზაციებს. 2007 და 2008 წლების განმავლობაში, ელექტროკავშირების საერთაშორისო გაერთიანების მიერ ჩატარდა დიდი სამუშაოები უსაფრთხოების არქიტექტურის სტანდარტიზაციაზე, კავშირის არხების კოდირების მეთოდოლოგიის შემუსავებაზე, ინფორმაციული სისტემების უსაფრთხოების მართვასა და ქსელების მომხმარებლის ავტორიზაციაზე. გარდა ამისა, მომზადდა ინფორმაციული და საკომუნიკაციო ტექნოლოგიების უსაფრთხოების სტანდარტების „გზამკვლევი“, რომელიც წარმოადგენს მონაცემთა ელექტრონულ ბაზას, რომელიც შეიცავს ინფორმაციული და საკომუნიკაციო ტექნოლოგიების უსაფრთხოების უკვე არსებულ სტანდარტებს, ასევე საერთაშორისო ნორმებსა და სტანდარტებზე მომუშავე ძირითადი ორგანიზაციების პროექტების ჩამონათვალს.

მსოფლიო ბანკის ჯგუფი (WB)

კომპიუტერული დანაშაულებები და ელექტრონულ ქსელებში არასანქცირებული შეღწევა დიდ ზიანს აყენებს ფინანსურ სექტორს. იმის გათვალისწინებით, რომ სულ უფრო იზრდება ფინანსური ინფორმაციის შენახვისა და გადაცემის მოცულობა, კომპიუტერული დამნაშავეებისთვის ასევე ადვილი ხდება ქსელებში არასანქცირებული შეღწევა და თავიანთი მავნებლური ქმედებების განხორციელება. ამიტომ მსოფლიო ბანკის ჯგუფმა ბოლო პერიოდში განახორციელა მთელი რიგი ღონისძიებები მიმართული ინფორმაციული უსაფრთხოების უზრუნველსაყოფად, განსაკუთრებით ეს ეხება განვითარებად ქვეყნებს.

გლობალური ინფორმაციული - საკომუნიკაციო ტექნოლოგიების დეპარტამენტი[321] უწევს დახმარებას განვითარებად ქვეყნებს ინფომაციული და საკომუნიკაციო ტექნოლოგიების განვითარებაში, ასევე უზრუნველყოფას მსოფლიო ბანკის ჯგუფის ძირითადი დეპარტამენტების საქმიანობას, რომელიც ეხება ინფორმაციული - საკომუნიკაციო ტექნოლოგიების სფეროში კვლევების ჩატარებას, პოლიტიკის განსაზღვრას, ინვესტიციებსა და სხვადასხვა პროგრამების განხორციელებას.

2003 წელს გამოიცა „კომპიუტერული უსაფრთხოების ცნობარი“[322], სადაც განხილულია მოწინავე გამოცდილება და რეკომენდაციები ინფორმაციული უსაფრთხოების უზრუნველყოფაში, რომელიც გამოადგება ყველა ქვეყანას, მიუხედავად მათი ტექნიკური შესაძლებლობების დონისა. ეს რეკომენდიციები მოცემულია შესაბამის ვებ - გვერდზე და ახალი ტექნოლოგიებისა და მეთოდიკის გამოჩენასთან ერთად, მუდმივად ხდება მისი განახლება.

2002 წლის ივნისში მსოფლიო ბანკმა გამოაქვეყნა სპეციალური მოხსენება „ელექტრონული უსაფრთხოება: ფინანსური ოპერაციების არსებობასთან ერთად

[321] http://www.worldbank.org/en/topic/ict

[322] Information Technology Security Handbook http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2004/09/30/000160016_20040930112655/Rendered/PDF/300750PAPER0eSecurity.pdf

რისკების შემცირება“[323]. ეს დოკუმენტი არის პუბლიკაციების ციკლის გაგრძელება, სადაც ელექტრონული ქსელების უსაფრთხოება განიხილება როგორც ერთერთი ძირითადი პირობა ელექტრონული გადახდების ბაზრის ეფექტური ფუნქციონირებისთვის.

2004 წლის იანვარსა და მაისში გამოვიდა შემდეგი პუბლიკაცია სახელწოდებით „ტექნოლოგიური რისკების საკონტროლო სია“[324], სადაც მოცემულია ელექტრონული უსაფრთხოების ოცდაათამდე დონის აღწერა, ასევე განხილულია ის რისკები, რომლებიც უკავშირდება ქსელების ინფრასტრუქტურის პროგრამულ უზრუნველყოფას. ყოველი მოცემული დონისთვის გათვალისწინებულია რისკების მართვის, კიბერდაზვერვისა და ინტელექტუალური ცენტრალიზებული მართვის ღონისძიებები; დაშვებისა და ავტორიზაციის კონტროლი; ქსელთაშორისი დაცვა და კონტენტის ფილტრაცია; შეღწევის აღმოჩენისა და ანტივირუსული სისტემები; კოდირების საშუალებები და მოწყვლადობის ტესტირება; სისტემური ადმინისტრირების ღონისძიებები; შეღწევის შემთხვევაში ექსტრემალური ღონისძიებების გეგმები. 2005 წელს გამოვიდა კიდევ ორი დოკუმენტი[325] დაკავშირებული ელექტრონული გადახდების სისტემების უსაფრთხოებასთან, სადაც განხილულია საფრთხეები, რომლებიც მოდის ბოტ - ქსელებისგან, აგრეთვე კიბერსივრცეში ფულის გათეთრების პრობლემები.

ინსტიტუტის „აღმოსავლეთი - დასავლეთის“ გლობალური კიბერუსაფრთხოების ინიციატივა (WCI)[326]

2007 წელს ინსტიტუტის „აღმოსავლეთი - დასავლეთი“ ამერიკულმა ჯგუფმა „სტრატეგიული დიალოგები“, გენერალ ჯეიმს ჯონსონის[327] ხელმძღვანელობით, კიბერუსაფრთხოების სფეროში საერთაშორისო თანამშრომლობის თაობაზე ჩაატარა

[323] Electronic Security: Risk Mitigation in Financial Transactions - Public Policy Issues https://openknowledge.worldbank.org/bitstream/handle/10986/19261/multi0page.pdf?sequence=1

[324] Technology Risk Checklist http://archive.rdec.gov.tw/public/Data/851413535571.pdf

[325] http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/CyberSecurity.pdf

[326] World Cyber Initiative http://www.ewi.info/cyber

[327] ევროპაში ნატო - ს გაერთიანებული შეიარაღებული ძალების ყოფილი უმაღლესი მთავარსადრდალი, ამჟამად შეერთებული შტატების ეროვნული უსაფრთხოების მრჩეველი

შეხვედრების სერია ჩინეთისა და რუსეთის ხელმძღვანელ პირებთან. ეს შეხვედრები გაგრძელდა კიდევ უფრო მაღალ დონეზე, რომლის დროს გამართულმა დისკუსიებმა გამოავლინა შეერთებული შტატების, ჩინეთისა და რუსეთის საერთო აღშფოთება არასახელმწიფო სუბიექტების სწრაფად მზარდი შესაძლებლობები, რომლებსაც შესწევთ უნარი დიდი ზიანი მიაყენოს მსოფლიო ეკონომიკას და საფრთხის ქვეშ დააყენოს როგორც თითოეული ქვეყნის ეროვნული უსაფრთხოება ისე დიდი საფრთხე შეუქმნას საერთაშორისო და რეგიონალურ უსაფრთხოებას. შეხვედრების შედეგად, თითოეულმა ქვეყანამ გადახედა კიბერუსაფრთხოების საკითხების შეფასებას, ხოლო შეერთებულმა შტატებმა კიბერსაფრთხეებს მისცა ატომური საფრთხის ტოლფასი შეფასება.

დღეს ინსტიტუტის „აღმოსავლეთი - დასავლეთი“ ხელმძღვანელობით, გლობალური კიბერუსაფრთხოების ინიციატივის ფარგლებში მიმდინარეობს აქტიური თანამშრომლობა შეერთებული შტატების, რუსეთსა და ჩინეთს შორის. ამ თანამშრომლობას უკვე შეუერთდნენ ევროკავშირისა და დიდი ოცეულის ქვეყნები, ასევე კერძო სექტორის, პროფესიული ასოციაციებისა და საერთაშორისო ორგანიზაციების წარმომადგენლები.

გლობალური კიბერუსაფრთხოების ინიციატივის საკონსულტაციო ჯგუფს სათავეში ჩაუდგა “Deloitte” კიბერინოვაციების ცენტრის დირექტორი გენერალი ჰარრი რეიდუედჯი. ეს ჯგუფი სთავაზობს პრობლემის გადაჭრას შემდეგ ორ დონეზე: (1) სანდოობის ამაღლება კიბერუსაფრთხოების კონკრეტული პრობლემის ერთობლივი თანამშრომლობისა და გადაწტვეტილების მიღების გზით, სადაც ჩართული არიან ორი ან ორზე მეტი ქვეყნის ექსპერტთა ჯგუფები; და (2) საზოგადოებრივი პროცესის ინიცირება, რომელიც საშუალებას იძლევა გადაიდგას პირველი ნაბიჯები კიბერსივრცეში საერთაშორისო უსაფრთხოების პოლიტიკის რეალიზების მიმართულებით, როგორც ეს უკვე არსებობს საზღვაო, საჰაერო და კოსმოსური სივრცისთვის. მეორე მიმართულებით საქმიანობა, ინსტიტუტის „აღმოსავლეთ - დასავლეთი“ ეგიდით, დაიწყო 2010 წლის მაისში, როცა კიბერუსაფრთხოების საკითხების მსოფლიო პირველი სამიტის

ფარგლებში „კიბერ - 40“[328] - ის 200 - მდე ლიდერი შეიკრიბა დალასში (აშშ). ეს სამიტი გახდა უმაღლეს დონეზე სახელმწიფოსა და კერძო სექტორს შორის საპარტნიორო მოძრაობის შექმნის პირველი მცდელობა, რომელიც ეძღვნება კრიტიკული ინფრასტრუქტურის[329] კიბერდაცვის საკითხებს.

„ჰორიზონტი 2015“[330]

ბოლო დროს სულ უფრო მეტი ყურადღება ექცევა სამხედრო, უსაფრთხოებისა თუ დაცვის კერძო ორგანიზაციების ჩართვას უსაფრთხოების სექტორის რეფორმირებისა და მართვის პროცესებში. ამ თემაზე უკვე არსებობს დიდი რაოდენობის პუბლიკაციები და მასალა, თუმცა არცთუ ისე ბევრ ნაშრომშია განხილული მოცემული სუბიექტების როლის დიდი მნიშვნელობა სახელმწიფო თუ კერძო სექტორის უსაფრთხოების უფრო ფართო პრობლემების მართვასთან დაკავშირებით. უახლოეს წლებში უნდა მოხდეს ანალიტიკური კვლევების ჩარჩოების გაფართოება და უსაფრთხოების სექტორის რეფორმირებისა და მართვის ახალი მიდგომების შემუშავება. დროა უკვე უარი ვთქვათ მოძველებულ „სახელმწიფო მართვის ერთიან“[331] მიდგომაზე, სადაც მხოლოდ სახელმწიფო სექტორის უწყებები და სამსახურები მონაწილეობენ. აუცილებელი ხდება პრობლემის მიმართ სისტემური მიდგომა, რომელიც უსაფრთხოების სექტორს განიხილავს როგორც ერთიან ორგანიზმს, ხოლო პრობლემის გადაჭრის მასშტაბები სცილდება არსებულ სახელმწიფო ჩარჩოებს და მოიცავს ასევე კერძო თუ საერთაშორისო ორგანიზაციებსაც.

---

[328] დიდ ოცეულთან ერთად გაერთიანებულია კიბერსივრცის კიდევ მსოფლიოს ოცი წამყვანი ქვეყანა

[329] აქ, კრიტიკულ ინფრასტრუქტურაში შედის საფინანსო სექტორი, ენერგეტიკა, სატელეკომუნიკაციო და ძირითადი სახელმწიფო უწყებები და სამსახურები

[330] პროექტი ინიცირებულია ორგანიზაცია „შეიარაღებულ ძალებზე დემოკრატიული კონტროლის“ (DCAF) http://www.dcaf.ch/ მიერ 2010 წელს, სადაც ერთ ერთ მნიშვნელოვან პრობლემად განხილულია კიბერუსაფრთხოება http://www.dcaf.ch/Project/Horizon-2015

[331] იგივეა, რაც ცენტრალიზებული მმართველობა, რომლის დროსაც ესა თუ ის პრობლემა გადაიჭრება არა ცალკეული უწყებების მიერ, არამედ მთლიანად სახელმწიფო დონეზე. მსგავსი მიდგომა წარმოიქმნა ამ სფეროში რეფორმირების პირველ ეტაპზე და ამჟამად წარმოადგენს ნაკლებად ეფექტურ საშუალებას, ამიტომ აუცილებელია დაიწყოს რეფორმირების მეორე ეტაპი, რაც მოიცავს ასევე კერძო სექტორის ჩართულობას

პროექტი „ჰორიზონტი 2015“ ერთმანეთში აერთიანებს დაინტერესებულ სახელმწიფო და არასახელმწიფო სტრუქტურების წარმომადგენლებს, რომელთა შორის იმართება თემატური მრგვალი მაგიდები. ყოველი მსგავსი მრგვალი მაგიდის შემდეგ იქმნება მოცულობითი სამუშაო დოკუმენტი, რომელიც შეიცავს პრობლემის მოკლე აღწერილობას, თეორიულ და პრაქტიკულ საკითხებს, კონტროლისა და ზედამხედველობის მექანიზმებს, რაც ზრდის გამჭვირვალობასა და დემოკრატიულ მმართველობას მთლიანად. თუმცა ეს დოკუმენტები არ იძლევა საკითხის გადაჭრას, ისინი უფრო წამოჭრიან პრობლემას და საფუძველს უდებს სამეცნიერო კვლევების განვითარებას. ანალოგიური პროცესი მიმდინარეობს ასევე კიბერუსაფრთხოების თემების განხილვისას, როცა ასევე მიიღება შესაბამისი დოკუმენტები[332].

რეზუმე

ზემოთ მოკლედ განხილული იყო ევროკავშირის, ევროსაბჭოს, გაეროს, ნატოს, დიდი რვიანისა და სხვა საერთაშორისო თუ რეგიონალური დონის ორგანიზაციების ფარგლებში მიღებული გადაწყვეტილებები, რეკომენდაციები, დირექტივები და რეზოლუციები კიბერუსაფრთხოებაზე, რომელმაც უნდა უზრუნველყოს კიბერსივრცის დაცვა და კიბერდანაშაულთან ბრძოლის ეფექტურობა როგორც საერთაშორისო თუ რეგიონალურ, ისე ეროვნულ დონეებზე.

[332] file:///C:/Users/Admin/Downloads/OnCyberwarfare-Schreier.pdf

სოციალური მედია და ეროვნული უსაფრთხოება

შესავალი

მასობრივი ინფორმაციის საშუალებას ყოველთვის შეეძლო გარკვეული დადებითი თუ უარყოფითი როლი ეთამაშა ნებისმიერი ქვეყნის ეროვნული უსაფრთხოების საკითხებში და მასზე გარკვეული ზეგავლენა ექონია, მთავარი იყო მხოლოდ რა მიმართულებით? ვინ და საიდან? და როგორ გამოიყენებდა ტრადიციულ მედია საშუალებებს.

XXI საუკუნის დასაწყისის ბოლო ათწლეულში ძალზედ პოპულარული და გამოყენებადი გახდა სოციალური მედიით სარგებლობა. შეიცვალა საშუალებები, ხოლო მიზნები და ამოცანები, ისევე როგორც ზემოთ მოცემული კითხვები, იგივე დარჩა. ეროვნულ უსაფრთხოებაზე ისევ ისეთი გავლენა აქვს მედია საშუალებებს, როგორც ტრადიციულ მედიას, მხოლოდ ყოველივე ეს დროში დაჩქარდა, უფრო სწრაფად ხდება მოვლენათა განვითარება და გავრცელება.

სოციალურმა მედიამ თავისი არსებობა დაიწყო XXI საუკუნეში აშშ - ში, და მას აქეთ ვითარდება გეომეტრიული პროგრესიით. 2010 წლის მონაცემებით, სოციალური მედიის მომხმარებელმა შეადგინა დაახლოებით ორი მილიარდი, პლანეტის მთლიანი მოსახლეობის თითქმის მესამედი.

განვითარების პირველ ეტაპზე, 2000 – 2005 წლებში, სოციალური მედია გავრცელებული იყო მაღალი ტექნოლოგიების მქონე ქვეყნებში, სადაც დემოკრატიულობის ინდექსის ნიშნულის მაჩვენებელი საკმაოდ მაღალ დონეზე არის. 2005 წლიდან სოციალური მედია საშუალება გავრცელებას იწყებს შედარებით დაბალგანვითარებულ ქვეყნებში, სადაც დემოკრატიულობის ინდექსის მაჩვენებელი შედარებით დაბალია, ზოგან კი საერთოდ არ არსებობს. ეს ფაქტი ძალზედ აისახება არა მარტო ქვეყნის ეროვნულ უსაფრთხოებაზე, არამედ რეგიონალურ და ხშირ შემთხვევაში საერთაშორისო უსაფრთხოებაზე.

ტრადიციულად სოციალურ მედიაში იგულისხმება ისეთი ცნობილი სოციალური ქსელები, როგორებიც არის Facebook, LinkedIn, MySpace, Twitter, YouTube, Flickr, WordPress, Blogger, Typepad, LiveJournal, Wikipedia, Wetpaint, Wikidot, Second Life, Del.icio.us, Digg, Reddit, Lulu.

სოციალური ქსელების მომხმარებელთა რაოდენობა დღითიდღე იზრდება. მის სწრაფ გლობალურ გავრცელებას ხელს უწყობს სოციალური მედიისთვის დამახასიათებელი, მომხმარებლისთვის მნიშვნელოვანი ისეთი საშუალებები, როგორიც არის ოპერატიულობა, ინფორმაციის სწრაფი გადაცემა და ორმხრივი კომუნიკაციის შესაძლებლობა, იაფფასიანობა და ა. შ. მომხმარებელთა მუდმივი ზრდა.

თუმცა სოციალურ მედიას გააჩნია როგორც დადებითი ისე უარყოფითი მხარეები. მისი არასწორი მიმართულებით გამოყენებამ შეიძლება ცუდი გავლენა იქონიოს ქვეყნის ეროვნულ უსაფრთხოებაზე. თუმცა ამავე დროს სოციალურ მედიას შეუძლია დადებითი ეფექტის მოტანა ქვეყნისთვის, მისი საშუალებით შესაძლებელია სტრატეგიული თუ ტაქტიკური მიზნების მიღწევა, საფრთხეებზე მუშაობა და მათი დროული პრევენცია.

სოციალური მედია ძალზედ სწრაფად ვითარდება, და აუცილებელია მისი საშუალებით გეო - პოლიტიკურ, გეო - ეკონომიკურ, თუ სხვა სახის პროცესებზე მუდმივი მონიტორინგი სახელმწიფოს მხრიდან. მთლიანობაში, კომპლექსურად ეს პროცესი საშუალებას მოგვცემს თავიდან ავიცილოთ საგარეო საფრთხეები და მათი გავლენა საშინაო მოვლენებზე. შეიძლება ითქვას, რომ სოციალურ მედიას საკმაოდ წარმატებით იყენებენ საერთაშორისო დამნაშავე ჯგუფები, მათ შორის ტერორისტული ორგანიზაციები. თავისი მიზნების მისაღწევად, სოციალურ მედიას თავის ინტერესებში გამოყენებას არ ერიდებიან აგრეთვე პოტენციურად მოწინააღმდეგე ქვეყნები და ალიანსები.

აუცილებელია ვიცოდეთ, როგორ და რამდენად შეუძლია სოციალურ მედიას გაუწიოს დახმარება სახელმწიფოს აღკვეთოს საფრთხეები და დაიცვას სტრატეგიული ინტერესები. აუცილებელია სწორად იქნას გამოყენებული სოციალური მედიის

შესაძლებლობა, თუმცა აქვე გასათვალისწინებელია ის გარემოება, რომ არ უნდა დაირღვეს მომხმარებლის, როგორც პიროვნების უფლებები.

საქართველოში სოციალურ მედიას რატომღაც სწავლობენ და იჩემებენ საკითხის კომპეტენტურობას ჟურნალისტები, როცა ეს თემა თავისი აქტუალობიდან, შინაარსიდან და დატვირთულობიდან გამომდინარე წარმოადგენს საერთაშორისო ურთიერთობის, საერთაშორისო უსაფრთხოების კვლევის საგანს.

სანამ მთავარი საკითხის განხილვას დავიწყებდეთ, ნათელი წარმოდგენის შექმნისთვის, ორიოდე სიტყვით შევეხოთ სოციალური მედიის განსაზღვრებას, მის დეფინიციას, განსხვავებას ტრადიციულ მედიასთან და სოციალური ქსელების მომხმარებლის კატეგორიებს. აგრეთვე, საუბარი იქნება ინფორმაციული ომის შესახებ და ამ ომში სოციალური მედიის როლსა და ადგილზე.

სოციალური მედიის განსაზღვრება და შედარება ტრადიციულ მედიასთან

რა არის ზოგადად სოციალური მედია? თითქმის ათი წელი გავიდა მას შემდეგ, რაც ინტერნეტში გაჩნდა სოციალური მედია, და როგორც წესი მსგავსი სიახლეები ელვის სისწრაფით ვრცელდება. ფაქტიურად სოციალური მედიის გავრცელებამ და გამოყენებამ აშკარად გაუსწრო მისი შესწავლის პროცესს, რაც გახდა ძირითადად მიზეზი ოპონენტთა შორის მწვავე დებატებისა და აზრთა სხვადასხვაობისა.

შეიძლება ითქვას, რომ საკითხი ბოლომდე შესწავლილი არ არის, ჯერ არ ჩატარებულა საკმარისი კვლევები და მის შესახებ ერთიანი ჩამოყალიბებული აზრი არ არსებობს, შესაბამისად სოციალური მედიის დეფინიციაც ზოგად ხასიათს ატარებს. მაგალითად, the US Congressional Research Service (CRS) ანალიტიკოსი ბრუს ლინდსი სოციალურ მედიას განსაზღვრავს შემდეგნაირად: „ტერმინი სოციალური მედიის შესახებ განეკუთვნება ინტერნეტ - ბმულებს, რომლებიც იძლევა ადამიანთა შორის ურთიერთობის საშუალებას, რესურსებისა და ინფორმაციის ერთობლივ გამოყენებას. სოცილური მედია თავისთან მოიცავს სადისკუსიო ფორუმებს, ბლოგებს, ჩათებს, YouTube channels, LinkedIn, Facebook და Twitter. სოციალურ მედიასთან დაშვება შეიძლება

მივიღოთ კომპიუტერის დახმარებით, აგრეთვე სმარტფონების, ფიჭური კავშირისა და მობილური ტელეფონების მოკლე ტექსტური შეტყობინების საშუალებით“.

სტრატეგიული კომუნიკაციების ექსპერტი და Oklahoma State University პროფესორი ბობი ლუისი სოციალურ მედიას განსაზღვრავს, როგორც „ბლოგების, YouTube, Flickr, MySpace და Facebook ისეთ ინტერნეტ - საშუალებას, რაც ჩვეულებრივ ადამიანს საშუალებას აძლევს შექმნას კონტენტი, რომელსაც გაუზიარებს მსოფლიო აუდიტორიას. მოცემული საშუალებების ინტერაქტიულმა ხასიათმა შეცვალა მასიური საინფორმაციო საშუალებების ცალმხრივი გავრცელებიდან ორმხრივი დიალოგისკენ“.

როგორც ზემოთ არის აღნიშნული, სოციალური მედიის ზუსტი განსაზღვრების შესახებ ერთი ჩამოყალიბებული აზრი არ არსებობს, და ამაზე შეჩერება ცოტა შორს წაგვიყვანდა, მხოლოდ ბოლოში მოვიშველიებ სკონსულტაციო ფირმა Burston – Marsteller ვერსიას სოციალური მედიის აღწერის შესახებ, კერძოდ „ეს არის გადართვა, სადაც ადამიანები აკეთებენ ახალ აღმოჩენებს, კითხულობენ და უზიარებენ ერთმანეთს ახალ ამბებს, ინფორმაციასა და კონტენტებს, მათ შორის წერით, ვიდეო, ფოტო და აუდიო“.

მოკლედ შეგვიძლია ვთქვათ, რომ სოციალური მედია ეს არის კიბერ სივრცეში მიღწევადი კავშირისა და კომუნიკაციის საშუალება, რომელიც ოპერატიულად ფუნქციონირებს ტექნოლოგიური მოწყობილობების ბაზაზე (ინტერნეტი, მობილური ტელეფონები, კომპიუტერები და სხვა) და გააჩნია პროგრამული უზრუნველყოფის (Facebook, Twitter, MySpace, LinkedIn, YouTube, etc.) პლატფორმა. ყოველივე აღნიშნულის დახმარებით მომხმარებლებს შეუძლიათ:

- ერთმანეთთან ურთიერთობა;
- სხვადასხვა სახის კონტენტების (ვიდეო, ფოტო, აუდიო, და სხვა) გაზიარება;
- ქსელური გაერთიანებების შექმნა (პროფესიული, რელიგირი, კულტურული, ნაცნობები, პოლიტიკური და ა. შ.);
- სოციალური იდენტურობის განსაზღვრა და განვითარება.

სოციალურ მედიას, ტრადიციული მასიური საინფორმაციო საშუალებებისგან განსხვავებით, გააჩნია მომხმარებელთა შორის ძალზედ მაღალი დონის ინტერაქტიული ურთიერთდამოკიდებულება. ტრადიციული მედია საშუალებები არის ინფორმაციის ცალმხრივად გამავრცელებელი, როცა სოციალური მედიის მომხმარებლები არიან როგორც ინფორმაციის მიმღებნი, ისე მისი შემქმნელნი და გამავრცელებელნი.

ტრადიციული და სოციალური მედიის შედარებისას, ეს უკანასკნელი არის უფრო დინამიური, პირადი და ინტერაქტიული. აგრეთვე მას ახასიათებს ოპერატიულობა და ინფორმაციულობის გავრცელების სისწრაფე მთელს მსოფლიოში, მისთვის მიუღებელია დრო და სივრცე, ის მარტივი და იაფია. სოციალური მედიის გამოყენებისას მომხმარებელს ვირტუალურ სივრცეში შეუძლია შექმნას, გააქტიუროს და მართოს თავისი პირადი პროფილი, დაიმკვიდროს თავისი ადგილი არარეალურ სამყაროში.

სოციალური მედიის მომხმარებელი

სოციალური მედიის მომხმარებლები შეიძლება დაიყოს რამოდენიმე კატეგორიად. პირველ რიგში ესენი არიან ჩვეულებრივი პიროვნებები, რომლებიც იყენებენ სოციალური მედიის ისეთ საშუალებებს, როგორიც არის ინფორმაციისა და კონტენტის გაცვლა - გაზიარება, კომუნიკაცია, პიროვნული იდენტურობის ამაღლება სოციალური ქსელის გამოყენებით. ფაქტიურად სოციალური მედია ცალკეულ პირებს საშუალებას აძლევს დაიკმაყოფილოს თითქმის ყველა თავისი მოთხოვნა, ფიზიოლოგიურის (ჭამა, სმა, ძილი) გარდა. ეს კი ზრდის მომხმარებლის დამოკიდებულებას სხვადასხვა სოციალურ ქსელებზე, ხშირ შემთხვევაში, ასეთ დამოკიდებულებას სპეციალისტები უკვე ადარებენ ალკოჰოლზე, ნარკოტიკულ ნივთიერებაზე, ყავაზე დამოკიდებულებას.

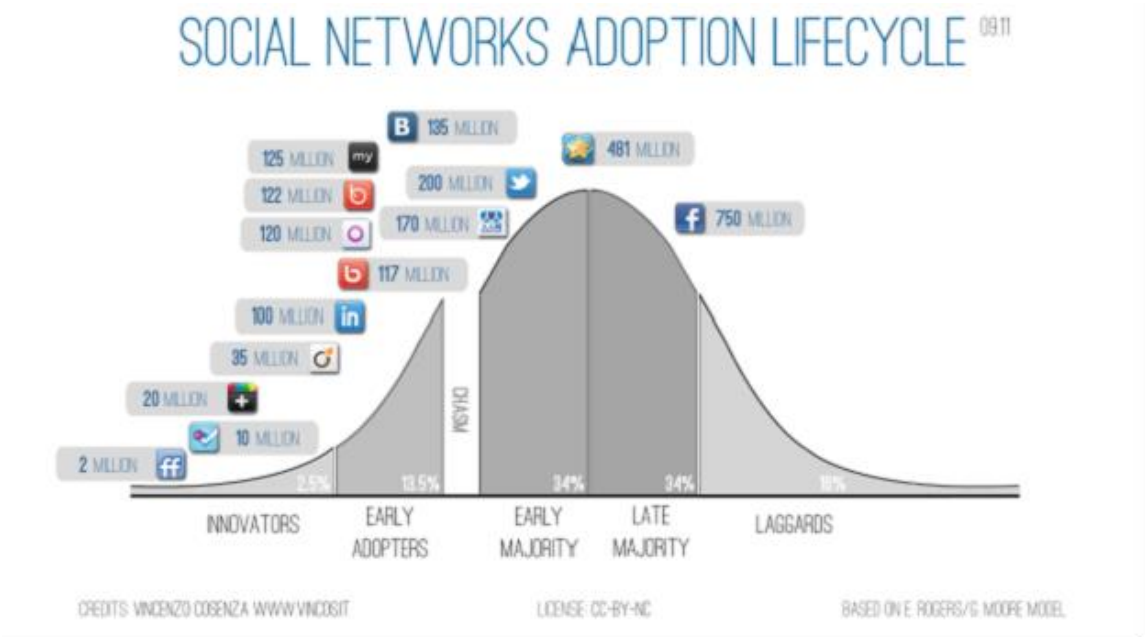
2011 წლის სტატისტიკის მიხედვით სოციალური მედიის მომხმარებელია:

- ინტერნეტის მომხმარებლის 75%, რომელთაც გააჩნიათ თავიანთი პროფილი;
- დაახლოებით 40% - ს აქვს მობილურიდან წვდომის საშუალება, რომელსაც იყენებენ აქტიურად;

- 55 წელს გადაცილებულები იყენებენ მხოლოდ საკუთარ კომპიუტერს;
- ქალები უფრო ხშირად იყენებენ სოციალურ მედიას ვიდრე მამაკაცები;
- სოციალური ქსელების აქტიური მომხმარებლის ასაკია 18 – 35 წელი.

ჰააგის სტრატეგიული კვლევების ცენტრის მონაცემებით, სულ უფრო იზრდება სოციალური მედიის შეღწევა ჩვენს ყოველდღიურ ცხოვრებაში, და როგორც მოსალოდნელია უახლოეს მომავალში კიდევ უფრო გაიზრდება. საზოგადოებრივ ცხოვრებაში სოციალური შეღწევადობის დონის სწრაფი გაზრდა დამოკიდებულია რამოდენიმე ფაქტორზე, რომელთაგან მთავარ როლს თამაშობს ქსელში დაშვების სიმარტივე და ნდობის უფრო მაღალი ხარისხი. ეს ფაქტორები კიდევ უფრო იზრდება და შესაბამისად გაიზრდება სოციალური ქსელების მომხმარებელთა რიცხვი.

ქვემოთ გრაფიკზე მოცემულია სოციალური ქსელების სიცოცხლის ციკლი, რაც პირდაპირპროპორციულად არის დამოკიდებული სოციალური ქსელის მომხმარებელთა რაოდენობაზე.



წყარო: ალფონსო მონტაგნესე

ცალკეულ პირებს შეუძლიათ გამოიყენონ სოციალური ქსელი არა მარტო პირადი მიზნებისთვის, არამედ სხვა ინტერესებშიც, მაგალითად, თავის თანამოაზრეებთან ერთად შექმნან ჯგუფი მათთვის საინტერესო სფეროში. სოციალურ ქსელში შექმნილი ჯგუფი არის პოტენციური მომხმარებელი და მას ფაქტიურად, მართავს ჯგუფის ერთი ან რამოდენიმე წევრი, ყველა მასში გაერთიანებული პირის სახელით. ხშირ შემთხვევაში, სოციალური ქსელის ჯგუფები ემსახურება მცირე წრის პირად ინტერესებს, რომელიც შეიძლება იყოს როგორც ყოფითი, ისე საზოგადო. უკვე გაჩნდა სპეციალისტების გაფრთხილება მომხმარებლისადმი სოციალურ ქსელებთან მუშაობის პროცესში მეტი ყურადღებისა და სიფრთხილის გამოჩენის შესახებ.

სოციალური მედია და ინფორმაციული ომი

სანამ სოციალური მედიის როლსა და ადგილზე ვისაუბრებდეთ ინფორმაციულ ომში, ვნახოთ რა არის ინფორმაციული ომი, რა მეთოდებს იყენებენ და რა ძირითადი მახასიათებლებით გამოირჩევა?

ამერიკის შეერთებული შტატების თავდაცვის დეპარტამენტის განსაზღვრებით, Information War (IW) ანუ როგორც მას ეძახიან აგრეთვე Information Operations (IO) - ეს არის ქმედება მიმართული საკუთარი ინფორმაციული სისტემის შენარჩუნებისკენ, რათა არ მოხდეს არასასურველი შეღწევა გარედან, ქვეყნის თავდაცვისუნარიანობის დარღვევის მიზნით. ამავდროულად, ეს არის ქმედება, რომელიც მიმართულია მოწინააღმდეგის საინფორმაციო სისტემის პარალიზებისკენ, ამ უკანასკნელზე უპირატესობის მოპოვების მიზნით.

თუმცა არსებობს კიდევ სხვა სახის განმარტება, კერძოდ IW/IO მოიხსენიებენ, როგორც მოწინააღმდეგე ან სხვა ქვეყნის მოსახლეობასა და სამხედრო მოსამსახურეებზე, ინფორმაციის გავრცელების გზით, ფსიქოლოგიურ ზემოქმედებას, პოლიტიკური და სამხედრო უპირატესობის მოპოვების მიზნით. ასეთი განსაზღვრებით IW/IO ხშირად მოიხსენიებენ, როგორც „ინფორმაციულ - ფსიქოლოგიურ ომს“.

IW/IO წარმოების დროს ძირითად მეთოდად გამოიყენება დეზინფორმაციის გავრცელება, ან ვრცელდება საჭირო კონტექსტის შემცველი ინფორმაცია. მსგავსი მეთოდები საშუალებას იძლევა შეცვალოს საზოგადოებრივი აზრი ამა თუ იმ მოვლენებზე.

IW/IO წარმოებას ძირითადად ახასიათებს:

- ინფორმაციული ზემოქმედება შეიძლება განხორციელდეს როგორც ინფორმაციული ბუმის ფონზე, ისე ინფორმაციული ვაკუუმის დროს;
- საშუალებად გამოიყენება ტრადიციული და სოციალური მედია საშუალებები, აგრეთვე ფოსტა და ჭორები;
- ინფორმაციული ზემოქმედება შეიცავს დამახინჯებულ ფაქტებს და ობიექტს ემოციურ ფონზე თავს ახვევს გამავრცელებლისთვის მისაღებ ინფორმაციას;
- ინფორმაციული ზემოქმედების ობიექტებად ითვლება როგორც მოსახლეობა მთლიანად, ისე ინდივიდები. ინდივიდუალური ზემოქმედების ობიექტებად მიჩნეულია ქვეყნის მმართველი პირები (პრეზიდენტი, პრემიერ - მინისტრი, მინისტრები, პოლიტიკოსები, სახელმწიფო თუ საზოგადო მოღვაწეები, კომპანიების ტოპ - მენეჯერები და ა. შ.) და მისი ძირითადი მიზანია მიაღებინოს მათ სასურველი გადაწყვეტილება. ხოლო მოსახლეობის შემთხვევაში, ხდება ცნობიერებაზე მასიური ზემოქმედება, რაც ფსიქოთერაპიის ანალოგად შეიძლება იქნეს მიჩნეული;
- ინფორმაციული ზემოქმედების დროს არ არის აუცილებელი ფსიქოაქტიური საშუალებების გამოყენება (შანტაჟი, დაშინება, ფიზიკური ზემოქმედება, მოსყიდვა და ა. შ.), თუმცა შეიძლება ღონისძიების კომპლექსურად ჩატარება.

IW/IO წარმოების დროს აქტიურად გამოიყენება სოციალური მედია საშუალებები. მისი გამოყენებისას ორგანიზებული ჯგუფები ცდილობენ მოიპოვონ თავიანთ მოწინააღმდეგეზე უპირატესობა, გახდნენ უფრო კონკურენტუნარიანები.

სოციალური მედია შეიძლება გახდეს IW/IO ეფექტური ინსტრუმენტი, ვინაიდან ის თავის მომხმარებელს აძლევს საშუალებას:

1) სტრატეგიული და ტაქტიკური თვალსაზრისით იძლევა მნიშვნელოვან შედეგებს:
   - მოქმედებს დომეინის ფარგლებში (კიბერ სივრცე), განსხვავებით ტრადიციული სამხედრო სახეობებისგან (სახმელეთო, საზღვაო, საჰაერო);
   - ზომებსა და მასშტაბებში, განსხვავებით ტრადიციული ომის წარმოებისგან;
   - ობიექტებად სამხედროების გარდა მიღებულია აგრეთვე სოციალური საზოგადოება (ეთნიკური, რელიგიური, პროფესიული და კულტურული);
2) შესაძლებელია მიზნის მიღწევა მინიმალური ფინანსური დანახარჯებით;
3) მნიშვნელოვანი შედეგების მიღწევა ყოველგვარი კონტროლისა და მონიტორინგის, აგრეთვე გამოძიების შესძლებლობის ჩატარების გარეშე;
4) ასიმეტრიული კონფლიქტების მართვა, კერძოდ, ზემოქმედება ხდება მცირე და საშუალო ჯგუფებზე, როცა რეალური სამიზნე არის უფრო დიდი დაჯგუფება ან მთლიანად სახელმწიფო.

ინფორმაციული ომის წარმოებას სოციალური მედია საშუალებების გამოყენებით, შეიძლება გააჩნდეს სხვადასხვა ნიშანი, დამოკიდებული ორგანიზებული ჯგუფის ხასიათზე (ტერორისტული ან დანაშაულებრივი ჯგუფი, სახელმწიფო, კომპანია და ა. შ.) და მათ წინაშე დასახულ ამოცანაზე. მოცემული შეიძლება დაიყოს შემდეგნაირად:

1) კიბერ - ომი (კიბერ - შეტევა) - „სახელმწიფოს - ერის მოქმედება მიმართული სხვა სახელმწიფოს კომპიუტერულ ქსელში შესაღწევად, ამ უკანასკნელისთვის ზიანის მიყენების ან საერთოდ მწყობრიდან გამოყვანის მიზნით“ (Richard Clarke, USA national security expert) ანუ სხვა სიტყვებით, რომ ვთქვათ ეს არის შეტევითი ღონისძიებების

კომპლექსი, რომელიც ხორციელდება კიბერ სივრცეში ერთი ან რამდენიმე სახელმწიფოს მიერ, და მიმართულია სხვა სახელმწიფოს ან საერთაშორისო დონის არასახელმწიფო სუბიექტის წინააღმდეგ;

2) კიბერ - ტერორიზმი, რაც გამოიყენება ტერორისტული ორგანიზაციების მიერ კიბერ სივრცეში და მიმართულია ქვეყნის ეროვნული უსაფრთხოების წინააღმდეგ;
3) ანტი კიბერ - ტერორიზმი, გამოიყენება ტერორისტული ორგანიზაციების წინააღმდეგ და ხორციელდება კიბერ სივრცეში;
4) კიბერ - დანაშაული, გამოიყენება სხვადასხვა დამნაშავე ან ტრანსნაციონალური ჯგუფების მიერ, რომლის დროსაც კიბერ სივრცის გამოყენებით ხდება ქურდობა, ინფორმაციის მოპარვა, თაღლითობა და ა. შ. მათი ობიექტები შეიძლება იყოს როგორც ცალკეული პირები, ისე მსხვილი კომპანიები. მისი მიზანია ეკონომიკური მოგების მიღება;
5) ანტი კიბერ - დანაშაული, ეს მოიცავს სახელმწიფოს სამართალდამცავების ან კერძო პირებისა და კომპანიების მხრიდან დაცვით ღონისძიებებს მიმართულს კიბერ დამნაშავეების წინააღმდეგ.

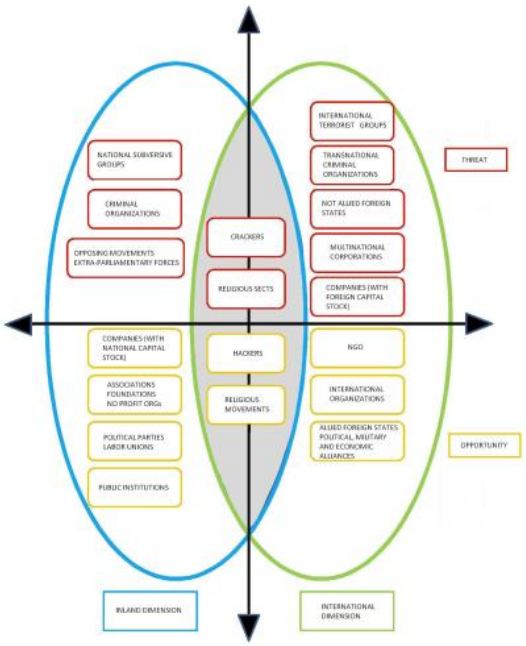
აქ შეიძლება აღინიშნოს ის გარემოება, რომ სპეციალისტები და ექსპერტები ცალკე საკითხად გამოყოფენ კიბერ - შეტევას, და განასხვავებენ მას კიბერ - ომისგან. თუმცა უნდა აღინიშნოს ისიც, რომ ხშირ შემთხვევაში ძალზედ ძნელია განასხვავო კიბერ - ომი კიბერ - შეტევისგან, ჯერ ფაქტიურად, დადგენილი არ არის ზღვარი მოცემულ ორ მცნებას შორის, და არ არის კონკრეტულად განსაზღვრული ის კრიტერიუმები, რომლითაც უნდა შეფასდეს ან ერთი, ან მეორე ქმედება.

სოციალური მედია შეიძლება გამოყენებულ იქნას ადგილობრივი და საერთაშორისო დამნაშავე ჯგუფების მიერ, რომელიც პირდაპირ უქმნიან საფრთხეს ეროვნულ უსაფრთხოებას. ასეთ ჯგუფებად მოიაზრებიან:

- ეროვნული დივერსიული ჯგუფები (მარქსისტულ - ლენინური დაჯგუფებები, ანარქისტები);
- ეროვნული და ტრანსნაციონალური დამნაშავე ჯგუფები (მაფია, იაკუძა, ტრიადა, კამორა);
- ტერორისტული ორგანიზაციები;
- მულტინაციონალური კომპანიები თავისი ფინანსური საშუალებებით;
- კომპანიები საგარეო კაპიტალით;
- ექსტრა საპარლამენტო ოპოზიციური ჯგუფები (მემარჯვენე ექსტრემისტები, ქსენოფობიური ჯგუფები);
- რელიგიური სექტები;
- ჰაკერთა დაჯგუფებები;
- სხვა სახელმწიფოსი და ეროვნული სამხედრო - პოლიტიკური, აგრეთვე ფინანსური გაერთიანებები;
- ასოციაციები, ფონდები, არაკომერციული ორგანიზაციები;
- არასამთავრობო და საერთაშორისო ორგანიზაციები;
- პოლიტიკური ორგანიზაციები და პროფკავშირები;
- სახელმწიფო დაწესებულებები.

სოციალური მედია საშუალებები ვითარდება სწრაფად და ის ვრცელდება მთელს მსოფლიოში, სადაც კი არის ინერნეტ წვდომა. ეს ფაქტი საშუალებას იძლევა ჩამოყალიბდეს და შეიქმნას კიდევ ახალი ტიპისა და თავისი საქმიანობით განსხვავებული უცნობი დაჯგუფებები, რომელთა რეალური მიზნები და მისწრაფებები გარკვეულ დრომდე ცნობილი არ არის, და შესაძლებელია ის იყოს გარკვეული საფრთხის შემცველი, რომლის შესწავლას სჭირდება გარკვეული დრო. ყოველივე ეს აშკარად უარყოფითად აისახება ეროვნულ უსაფრთხოებაზე. ამიტომ ეს თემა არის მუდმივი კვლევისა და შესწავლის საგანი. აგრეთვე, შეიძლება ითქვას, რომ საჭიროა მუდმივი მონიტორინგი სოციალურ მედიაზე, თუმცა არ უნდა დაირღვეს პიროვნების უფლებები და ჯდებოდეს კონსტიტუციით განსაზღვრულ ფარგლებში.

ქვემოთ მოყვანილი სქემა აჩვენებს თუ როგორ შეიძლება ცალკეულმა ჯგუფებმა იქონიონ დადებითი ან უარყოფითი გავლენა ეროვნულ უსაფრთხოებაზე.



წყარო: ალფონსო მონტაგნესე

ეროვნული უსაფრთხოება

სანამ კონკრეტულად საფრთხეებზე დავიწყებდეთ საუბარს, ორიოდე სიტყვით ვთქვათ თუ რას წარმოადგენს ეროვნული უსაფრთხოება, რას მოიცავს და რის დაცვას უზრუნველყოფს, აგრეთვე რომელი სახელმწიფო სტრუქტურები ახორციელებენ ეროვნული უსაფრთხოების დაცვას?

არსებობს ეროვნული უსაფრთხოების ბევრი განმარტება, რომელთაგან წარმოგიდგენთ რამოდენიმე ვარიანტს, კერძოდ:

1. ეროვნული უსაფრთხოება - ეს არის პიროვნების, საზოგადოებისა და სახელმწიფოს სასიცოცხლოდ მნიშვნელოვანი ინტერესების დაცვა

გარე და შიდა საფრთხეებისგან, ქვეყნის სტაბილური განვითარების უზრუნველყოფა;

2. ეროვნული უსაფრთხოება - ეს არის ერის შესაძლებლობა, არსებული მდგომარეობის საბაზისო ღირებულებებისთვის მინიმალური საფრთხის მიყენების გათვალისწინებით, მოთხოვნილებების დაკმაყოფილება აუცილებელი თვითდამკვიდრებისა და თვითგადარჩენისთვის;
3. ეროვნული უსაფრთხოება - ეს არის სტაბილურობა, რომელიც შეიძლება შენარჩუნებულ იქნას ხანგრძლივი პერიოდის განმავლობაში, ამავდროულად, წინასწარ შეფასდეს და გამოვლინდეს არსებული საფრთხეები, მათი დროული ნეიტრალიზაციის მიზნით;
4. ეროვნული უსაფრთხოება - ეს არის სახელმწიფო სტრატეგიისა და მიზნების ოფიციალურად მიღებული შეხედულებების ერთობლიობა, რომელიც უზრუნველყოფს პიროვნების, საზოგადოებისა და სახელმწიფოს დაცვას პოლიტიკური, ეკონომიკური, სოციალური, სამხედრო, ინფორმაციული, ტექნოგენური, ეკოლოგიური ან სხვა ხასიათის გარე და შიდა საფრთხეებისგან, არსებული რესურსებისა და შესაძლებლობების გათვალწნებით.

მოყვანილი განმარტებების გათვალისწინებით ეროვნული უსაფრთხოება თავისთან მოიცავს და შედგება შემდეგი კომპონენტებისგან:

- სახელმწიფო უშიშროება;
- საზოგადოებრივი უსაფრთხოება;
- ტექნოგენური უსაფრთხოება;
- ეკოლოგიური უსაფრთხოება;
- პოლიტიკური უსაფრთხოება;

- სამხედრო უსაფრთხოება;
- ეკონომიკური უსაფრთხოება;
- ენერგეტიკული უსაფრთხოება;
- ინფორმაციული უსაფრთხოება;
- პიროვნების უსაფრთხოება.

ეროვნული უსაფრთხოების უზრუნველყოფა - ეს არის პოლიტიკური, ეკონომიკური, სოციალური, სამხედრო, ჯანდაცვისა და სამართალდაცვითი ღონისძიებების ერთობლიობა, მიმართული ერის ნორმალური ცხოვრების უზრუნველყოფისკენ და შესაძლო საფრთხეების დროული პრევენციისკენ. მის მთავარ ამოცანად შეიძლება ჩაითვალოს მოქალაქის სტაბილური ეკონომიური მდგომარეობის ჩამოყალიბება, დაცვა და მისი კეთილდღეობის განვითარება სხვა ქვეყნის მოქალაქეებთან მიმართებაში.

ეროვნული უსაფრთხოების უზრუნველყოფა თავისთან მოიცავს:

- სახელმწიფო და საზოგადოებრივი წყობის დაცვას;
- სუვერენიტეტისა და ტერიტორიული დაურღვევლობის უზრუნველყოფას;
- ერის პოლიტიკური და ეკონომიკური დამოუკიდებლობის უზრუნველყოფას;
- ერის ჯანმრთელობის უზრუნველყოფას;
- საზოგადოებრივი წესრიგის დაცვას;
- დანაშაულებასთან ბრძოლას;
- ტექნოგენური უსაფრთხოების უზრუნველყოფასა და სტიქიური უბედურებისგან დაცვას.

ეროვნული უსაფრთხოების დაცვაში კომპლექსურად ჩართულია სახელმწიფოს ყველა არსებული რესურსი, თუმცა მის დაცვას ძირითადად უზრუნველყოფს არმია, დაზვერვისა და კონტრ - დაზვერვის სამსახურები, სამართალდამცავი და ჯანდაცვის სტრუქტურები.

ეროვნული უსაფრთხოებისთვის სოციალური მედიის გამოყენებით შექმნილი საფრთხე

სოციალურ მედიას შეიძლება გააჩნდეს როგორც დადებითი ისე უარყოფითი ეფექტი ქვეყნის ეროვნულ უსაფრთხოებაზე. რაც უფრო მაღალია ქვეყნის ინფორმატიზაციის დონე, მით მაღალია საფრთხის შემცველი რისკ - ფაქტორები, მიმართული ქვეყნის სტრატეგიული ინტერესებისა და მიზნების წინააღმდეგ. მსაგავსი საფრთხეები ეროვნულ უსაფრთხოებას შეიძლება შეექმნას სოციალური მედიის გამოყენებით.

ტერორისტული ორგანიზაციები

სოციალური მედია საშუალებებს სულ უფრო აქტიურად გამოიყენებს ტერორისტული ორგანიზაციები. ამ გზით წარმოებს ინფორმაციის გაცვლა და კომუნიკაცია, იდეოლოგიის გავრცელება, დაქირავების პროცესი და ტრენინგები.

დღესდღეისობით ყველაზე აქტიურად სოციალური მედიის საშუალებებს გამოიყენებს ისლამისტურ - ჯიჰადისტური ტერორისტული ორგანიზაციები. მაგალითად, ალ - ქაედას მიერ ხშირად გამოიყენება Facebook - სა და YouTube - ს არხები „ისლამის მებრძოლთა“ დაქირავებისთვის და ფუნდამენტური ისლამის იდეოლოგიის გავრცელებისთვის, აგრეთვე, ცდილობს სულ უფრო მეტი მომხრე შეიძინოს, განსაკუთრებით დასავლეთში. გარდა ამისა, სოციალური ქსელები აქტიურად გამოიყენება ტერორისტულ ორგანიზაციებს შორის ინფორმაციისა და რჩევების გასაცვლელად.

სოციალური მედია საშუალებებით, და ზოგადად ინტერნეტით ტერორისტული ორგანიზაციები ავრცელებენ ექსტრემისტულ მასალებსა და იდეებს, რაც მათ საშუალებას აძლევს მოახდინონ რეკრუიტმენტი, ყოველგვარი შუამავლის გარეშე.

ამის გარდა, სოციალური მედია საშუალებები გამოიყენება პროპაგანდისტული მიზნების მისაღწევად, კერძოდ, გაავრცელონ ინფორმაცია და შესაბამისი მასალები წარმატებულად ჩატარებული ტერორისტული ღონისძიებების შესახებ, რითაც თესავენ

მოსახლეობაში პანიკას. აგრეთვე, ვრცელდება სხვადასხვა ხასიათის დეზინფორმაციული მასალები და ინფორმაცია ტერაქტის ჩატარების შესახებ, რომლის მიზანს ასევე წარმოადგენს პანიკა. ამ დროს მოსახლეობის გარდა, სავარაუდო თავდასხმის ობიექტს შეიძლება წარმოადგენდეს კონკრეტული პირი, ფინანსური ინსტიტუტები, პოლიტიკური ორგანიზაციები ან მსხვილი კომპანიები.

აშშ - ს კვლევითი სამსახურების ვარაუდით, ზოგიერთი ტერორისტული ორგანიზაციების მხრიდან სოციალური მედიის გამოყენება ხდება მიზანმიმართული ტყუილის გავრცელება სტიქიური უბედურების დროს ან მისი დამთავრებისთანავე, რათა ზედმეტად უარყოფითად იქნას წარმოჩენილი ზემოქმედება, და ქვეყნის მხრიდან დაგვიანებული რეაქცია.

აშშ - ს არმიის განცხადებით, სოციალური მედია საშუალებები ზოგიერთი ტერორისტული ორგანიზაციის მიერ შეიძლება გამოყენებულ იქნას კომპიუტერული და მობილური ტექნიკის მიზანმიმართული დაზიანებისკენ. პროპაგანდისტული მასალების გავრცელების გარდა, სოციალური ქსელის საშუალებით, ძირითადად Facebook - სა და YouTube - ს არხების გამოყენებით, იგზავნება სპეციალურად დავირუსებული პროგრამები, რომელსაც მწყობრიდან გამოჰყავს მომხმარებლის ტექნიკა.

ყველაზე უფრო კარგად და წარმატებულად სოციალური მედიის გამომყენებლად შეიძლება ჩაითვალოს ალ - ქაედა, კერძოდ, ანვარ ალ - ავლაქი, რომელმაც შეიმუშავა მთელი სტრატეგია ინტერნეტის საშუალებით სასურველი ინფორმაციის გავრცელებისთვის, პროპაგანდისთვისა და დაქირავებისთვის. ის მოკლეს 2011 წლის 30 სექტემბერს, იემენში, აშშ - სადაზვერვო სამსახურების სპეციალურმა ძალებმა. ანვერ ალ - ავლაქის „წარმატებულ“ იდეოლოგიურ ოპერაციად შეიძლება ჩაითვალოს აშშ - ს არმიის მაიორის ნადილ ჰასანის მიერ, ალ - ავლაქის სოციალური ქსელით გავრცელებული პროპაგნდის ზემოქმედებით, 13 ამერიკელი სამხედროს მკვლელობა და 43 - ს დაჭრა, რომელიც მოხდა აშშ - ში, სამხედრო ბაზაზე, ერაყში გამგზავრების წინ. ნადილ ჰასანი პროფესიით იყო ფსიქოლოგი და სამხედროებს უტარებდა ფსიქოლოგიური მომზადების კურსებს.

კრიმინალური ორგანიზაციები

კრიმინალური ორგანიზაციები, თავიანთი არაკანონიერი საქმიანობის განხორციელებისთვის, სოციალურ მედია საშუალებებს იყენებენ მხოლოდ მხარდაჭერის მიზნით. ასეთი არაკანონიერი საქმიანო შეიძლება იყოს ან ინფორმაციის გავრცელება (მაგალითად, საბავშვო პორნოგრაფია, ვირუსების გავრცელება, პიროვნების პირადი ინფორმაციის მოპარვა და სხვა) ან ტრადიციული საქმიანობა (მაგალითად, ნარკოტიკების კონტრაბანდა, ტრეფიკინგი, ფულის გათეთრება, მოპარული დოკუმენტების გადაცემა, კორპორატიული შპიონაჟი).

კრიმინალური დაჯგუფებები შეიძლება იყოს ერთ ადგილას, ლოკალურად თავმოყრილი ადამიანთა ჯგუფი, რომლებიც ერთმანეთს პირადად იცნობენ, ან მსოფლიოს სხვადასხვა კუთხეში გაბნეული პირები, რომლებსაც ერთმანეთთან მხოლოდ ვირტუალური შეხება გააჩნიათ. ასეთი ჯგუფები იმართება ე. წ. მოდერატორების მიერ, რომლებიც აღჭურვილნი არიან განსაკუთრებული მმართველობითი უფლებებით, მათ შეუძლიათ გააგდონ ნაკლებად აქტიური წევრები, ან „დააწინაურონ“ კარგი შედეგის მაჩვენებლები.

სოციალურ მედიაში კრიმინალური ქსელი სულ უფრო ფართოვდება და სულ უფრო მასშტაბურ ხასიათს იძენს.

ომი

NATO - ს მიერ ჩატარებული კვლევების მიხედვით, მომავალში კონფლიქტები წარმოიქმნება იმ გარემოში, რომელსაც ახასიათებს საინფორმაციო და საკომუნიკაციო უახლესი ტექნოლოგიების, მათ შორის სოციალური მედია საშუალებების აქტიური გამოყენება.

სამხედრო ოპერაციების ჩატარების დროს პარალელურად წარმოებს მხარდამჭერი ღონისძიებები სოციალური მედია საშუალებებით. მაგალითად, ისრაელსა და ლიბანს შორის მომხდარი ბოლო ორი კონფლიქტი. 2006 წელს, მეორე კონფლიქტის დროს, ჰეზბოლამ ჩაატარა რამოდენიმე IW ოპერაცია სოციალური მედია საშუალებით, კერძოდ,

YouTube - ს გამოყენებით გამოაქვეყნეს რამოდენიმე მათთვის სასურველი ვიდეო და ფოტო მასალა, რის საპასუხოდ ისრაელმა მომავალი კონფლიქტების პერიოდში, იგივე სოციალური მედიის გამოყენებით გაუშვა კონტრ - ინფორმაციები.

საპროტესტო მოძრაობები და რევოლუციები

ახალი ტექნოლოგიები, და კერძოდ, სოციალური მედია საშუალებები ძალზედ მნიშვნელოვან, და ხშირ შემთხვევაში, გადამწყვეტ როლსაც თამაშობს საპროტესტო მოძრაობებსა და რევოლუციების ორგანიზებაში. ასეთ შემთხვევაში რევოლუციური ჯგუფების მიერ სოციალური ქსელები გამოიყენება მასობრივი გამოსვლებისთვის, მათი კოორდინაციისათვის და მოქმედების სტიმულირებისათვის, აგრეთვე, საპროტესტო გამოსვლების ტაქტიკური და ოპერატიული მართვის მიზნით.

თუ გავითვალისწინებთ იმ გარემოებას, რომ სოციალური მედია სულ უფრო სწრაფად ვითარდება, მაშინ დაბეჯითებით შეიძლება ითქვას, რომ შესაბამისად გაიზრდება საპროტესტო გამოსვლებისა და რევოლუციების რაოდენობა. Stratfor - ის ანალიტიკოსების განცხადებით, სოციალური მედია წარმოადგენს ინსტრუმენტს, რომელიც რევოლუციურ ჯგუფებს საშუალებას აძლევს შეამცირონ დანახარჯები ღონისძიების ორგანიზებაზე, მონაწილეობაზე, დაქირავებასა და ტრენინგზე.

ტუნისსა და ეგვიპტეში საპროტესტო გამოსვლების შესწავლისას გაირკვა, რომ:

- პროტესტში მოსახლეობის სტიმულირებასა და მართვაში, ძალზედ გაიზარდა სოციალური მედიის როლი;
- მობილურ ტელეფონთან ერთად, გაიზარდა მოქმედების სისწრაფე და გავრცელების არეალი;
- სიიაფის გამო, რევოლუციურ მოძრაობას საშუალება აქვს იმოქმედოს უფრო ავტონომიურად, ის საერთოდ არ არის დამოკიდებული საგარეო ფინანსებზე;
- ნაკლებად ან საერთოდ არ იზღუდება ცენზურისგან;

- საპროტესტო გამოსვლები და რევოლუციური ცვლილებები ხდება იმ ქვეყნებში, სადაც სახელმწიფოს ან კერძო კომპანიების მხრიდან არის მკაცრი ცენზურა ტრადიციულ მედია საშუალებებზე. ამ დროს სოციალური მედია საშუალება მოსახლეობისთვის წარმოადგენს ბრძოლის უნიკალურ შესაძლებლობას არსებულ რეჟიმთან, აგრეთვე თავიანთი სიტყვის თავისუფლებისა და უფლებების დაცვაში.

<u>სახელმწიფო მოხელეების მიერ სოციალური მედიის არასწორი გამოყენება</u>

სულ უფრო ხშირია სოციალური მედიის საშუალებით კონფიდენციალური და საიდუმლო მასალების გამოქვეყნება, რაც სერიოზულ ზიანს აყენებს ეროვნულ უსაფრთხოებას. გამოხატვისა და კომუნიკაციის თავისუფლება უნდა გაჩერდეს იქ, სადაც საქმე ეხება კონფიდენციალურობის შემცველ მასალებს. სახელმწიფო სტრუქტურები თავიანთ საქმიანობაში სულ უფრო აქტიურად იყენებენ სოციალურ მედიას, რომლის დროსაც არ არის გამორიცხული უნებურად საიდუმლო მასალის გავრცელება. ამიტომ, რისკების შემცირების მიზნით აუცილებელია სახელმწიფო ჩინოვნიკების მუდმივი ინფორმირება სოციალური ქსელის სწორად გამოყენებასა და უსაფრთხოების კულტურის ამაღლებაზე.

ეროვნული უსაფრთხოების დაცვის შესაძლებლობები

სოციალური მედია საშუალებები სახელმწიფო სტრუქტურების მიერ, ეროვნული უსაფრთხოების დაცვის მიზნით, შეიძლება გამოყენებული იქნას, როგორც თავდაცვით ისე თავდასხმით საშუალებად. კერძოდ, თავდაცვით ღონისძიებებში იგულისხმება პროფილაქტიკა, გაფრთხილება, კრიზისების მართვა, პროპაგანდასთან ბრძოლა, ხოლო თავდასხმითი მოქმედებები თავისთან მოიცავს ზემოქმედებას, პროპაგანდასა და ტყუილს.

სოციალური მედიის მუდმივი მონიტორინგი სადაზვერვო სამსახურების მხრიდან საშუალებას იძლევა მოპოვებულ იქნას წინმსწრები ინფორმაციები ეროვნული

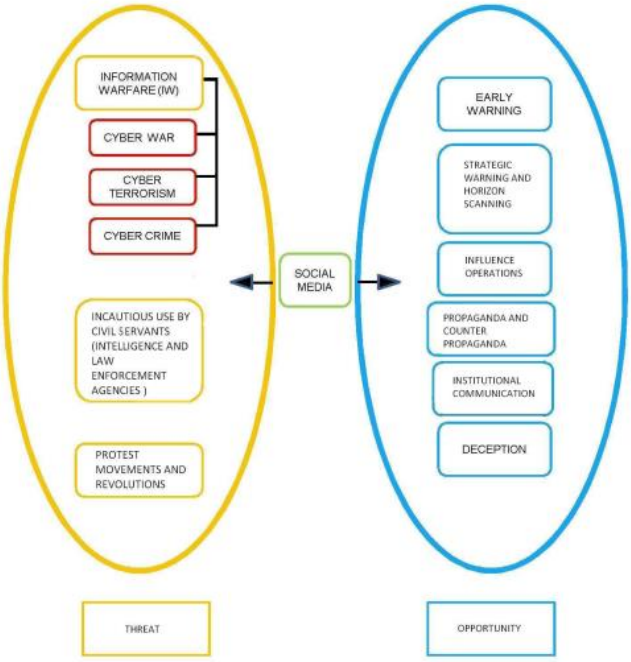
უსაფრთხოებისთვის შემცველი არსებული და მომავალი საფრთხეების შესახებ, და დროულად იქნას აღკვეთილი.

მონიტორინგის მუდმივი პროცესი ასევე იძლევა საშუალებას განისაზღვროს მოკლე-, საშუალო- და გრძელვადიანი პოლიტიკური, ეკონომიკური და სამხედრო პერსპექტივები, მოხდეს მოვლენათა ზუსტი შეფასება და გაკეთდეს მაქსიმალურად სწორი დასკვნები.

ეროვნული უსაფრთხოების სტაბილურობა ბევრად არის დამოკიდებული საერთაშორისო უსაფრთხოების შემადგენელ თითოეულ ცალკეულ კომპონენტზე. დღეს მსოფლიოში ერთ - ერთ მთავარ და ძირითად კომპონენტად განიხილება სწორედ კიბერსივრციდან მომდინარე საფრთხეები იქნება ეს კიბერ ომი თუ კიბერ შეტევა, ან სხვადასხვა სახის კიბერ დანაშაულება, რომლებმაც შესაძლოა სერიოზული საფრთხის წინაშე დააყენოს ეროვნული უსაფრთხოება და ქვეყნის სტრატეგიული ინტერესები. ამიტომ მსგავსი საფრთხეების პრევენციისა და რისკების შემცირების მიზნით, აუცილებელია მსხვილი მოთამაშე დიდი სახელმწიფოების მხრიდან გადადგმული იქნას შესაბამისი ნაბიჯები ურთიერთანამშრომლობისკენ, რითაც დაცული იქნება კიბერსივრცეში მოქმედების გარკვეული ბალანსი.

შეერთებულ შტატებსა და რუსეთს შორის უკვე დასასრულს უახლოვდება ორმხრივი მოლაპარაკებები, რაც ხელს შეუწყობს კიბერსივრცეში საფრთხეების შემცირებას, გამჭვირვალობასა და ურთიერთკოორდინაციას. კიბერსივრციდან მომდინარე საფრთხეები, ისევე როგორც ბირთვული საფრთხე, შეყვანილი იქნება დაცული კავშირის არხში, რომლის საშუალებითაც მოხდება ერთმანეთის გაფრთხილება და ინფორმაციის გაცვლა. ეს ხელს შეუწყობს მომხდარი ფაქტის მართებული სურათის წარმოსახვას და გამორიცხავს ე. წ. „ტყუილი განგაშის“ თემას, სადაც შესაძლოა ჩართული იყოს მესამე მოქმედი პირი ან არ მოხდეს ერთმანეთის შეცდომაში შეყვანა, რამაც შესაძლოა გამოიწვიოს საბრძოლო მოქმედებების დაწყება ან სხვა დიდი კატასტროფა, მათ შორის ბირთვული ომიც.

მსგავსი შეთანხმება არის წინგადადგული ნაბიჯი პირველ რიგში ორი ქვეყნის ეროვნული უსაფრთხოების დაცვის საკითხში, და შემდეგ მთელი მსოფლიოს საერთაშორისო უსაფრთხოებაში. ვინაიდან მოლაპარაკება ხდება ორ დიდ სახელმწიფოს შორის, რომლებიც დიდი, შეიძლება გადამწყვეტ როლს თამაშობენ მსოფლიო უსაფრთხოების საკითხში.



წყარო: ალფონსო მონტანეგსე

გამოყენებული ლიტერატურა

1. LINDSAY B. R., (2011), Social Media and Disasters: Current Uses, Future Options, and Policy Considerations, Congressional Research Service, Washington, DC;
2. LEWIS B. K., (2010), Social Media and Strategic Communication: Attitudes and Perceptions Among College Students, Public Relations Jouurnal vol. 4, New York;
3. BURSON - MARSTELLER, (2010), Social Media Check-up: a Burson – Marsteller Evidence – Based Tool, New York;
4. US DEPARTMENT OF DEFENSE, (2011), Department of Defense Strategy for Operatung in Cyberspace, Arligton Country, VA;
5. US GOVERNMENT, (2010), National Security Strategy 2010, Washington, DC;
6. CLARKER A., (2010), Cyber War: The Next Threat to National Security and What to do About it, Harper Collins, New York;
7. BURSON – MASTELLER, (2011), The Global Social Media Check – up 2011, New York;
8. http://www.hcss.nl;
9. THE HAGUE CENTRE FOR STRATEGIC STUDIES, (2011), Social Networking – The security shakedown of shared information, Future Issue n. 11/2011, The Hague;
10. http://www.vincos.it;
11. http://www.nmincite.com;
12. http://www.bbc.co.uk;
13. INTELLIGENCE AND NATIONAL SECURITY ALLIANCE, (2011), Cyber Intelligence: setting the landscape for an emerging discipline, Arlington, VA;
14. NATO Allied Command Transformation, (2009), Multiple Futures Project – Navigating Towards 2030, Norfolk;
15. PAPIC M., NOONAN S., (2011), Social Media as a Tool for Protest, STRATFOR, Austin, TX;
16. WEINBERG S., (2011), The Spy Who Tweeted Me: Intelligence Wants to Monitor Social Media, Wired, San Francisco;
17. Capt. CC ALFONSO MONTAGNESE, (2012), Impact of Social Medea on National Security, Centro Militare di Studi Strategici;
18. თამთა კახაძე, კიბერუსაფრთხოება და XXI საუკუნის გამოწვევა, გაზეთი „24 საათი“, 7 ნოემბერი, 2011 http://24saati.ge/index.php/category/news/2011-11-07/21449;

19. ლონდონის კონფერენცია კიბერსივრცის შესახებ, ჟურნალი „ტაბულა“ 17 ოქტომბერი, 2011 http://www.tabula.ge/article-6058.html;
20. Ellen Nakashima, In U.S. – Russia deal, nuclearcommunication system may be used for cybersecurity, The Washington Post, 26 April, 2012;
21. Ellen Nakashima, U.S. Web site covering China scandal disputed by cyberattack, The Washington Post, 21 April, 2012;
22. Ellen Nakashima, Cyber-intruder sparks massive federal response – and debate over dealig with threats, The Washington Post, 9 December, 2011.

სოციალური ქსელები - დემოკრატია თუ უსაფრთხოება?

ინტერნეტის სწრაფმა განვითარებამ სათავე დაუდო უზარმაზარი ეკონომიკური და სოციალური შესაძლებლობების შექმნას. 2012 წლის მონაცემებით, სოციალური მედიის მომხმარებელმა ორ მილიარდზე მეტი შეადგინა, პლანეტის მთლიანი მოსახლეობის თითქმის მესამედი. არსებული გამოკვლევებითა და დაკვირვებით, ინტერნეტ ქსელის გაფართოება პირდაპირპროპორციულად აისახება მთლიანი შიდა პროდუქტის გლობალურ მაჩვენებელზე, რაც ხელს უწყობს კონკურენციის ზრდასა და ახალი ბაზრების შექმნას. ინტერნეტ სივრცეში მსოფლიო მასშტაბით წარმოებული კომერცია გულისხმობს რვა ტრილიონ აშშ დოლარის წლიურ ბრუნვას, ხოლო კიბერდამნაშავეთა მიერ მიყენებული ფინანსური ზარალი წელიწადში ერთ ტრილიონ აშშ დოლარს აღწევს. ინტერნეტ ქსელის მომხმარებელთა რიცხვი ყოველდღიურად იზრდება (მაგალითად, Google - ს ყოველდღიურმა მომხმარებელმა ერთ მილიარდს მიაღწია) და მისმა სწრაფმა განვითარებამ წარმოშვა ისეთი სერიოზული პრობლემები, რომლებიც ინტერნეტის გამოყენების დადებითი ნაწილის უპირატესობის მნიშვნელობას საგრძნობლად ამცირებს და საფრთხეს უქმნის კიბერსივრცის შესაძლებლობების სრულ გამოყენებას. ფაქტიურად, განვითარებულ ქვეყნებს გააჩნიათ ინფორმაციული ტექნოლოგიების ინოვაციური მომავლის შესაძლებლობა, მაგრამ ამავდროულად ისინიც და მთელი მსოფლიოც დგას საფრთხის წინაშე, რომ ყოველ ნოუ ჰაუს ასევე შეუძლია დიდი ზიანის მოტანა.

ახალი ინფორმაციული ტექნოლოგიები საკმაოდ დიდ შესაძლებლობებს აძლევს კრიმინალურ სამყაროსა და ტერორისტულ ორგანიზაციებს. მათ მიერ სოციალური ქსელების გამოყენებით წარმოებს მოტყუება, დაშანტაჟება, იდეების მოპარვა, იდეოლოგიის გავრცელება, კორპორატიული თუ სამრეწველო შპიონაჟი და ა. შ. ინფორმაციული ტექნოლოგიების მიღწევები ასევე ბოროტად გამოიყენება რეპრესიული ხელისუფლებისა და ავტორიტარული რეჟიმების მხრიდანაც. კერძოდ, ისინი ზღუდავენ თავიანთ მოქალაქეთა უფლებებს, კრძალავენ სიტყვის თავისუფლებას და ხელს უშლიან

სხვისთვის ადვილად ხელმისაწვდომი ინფორმაციის გავრცელებას. მაგალითად, რუსეთში საპრეზიდენტო არჩევნების წინა პერიოდში ოპოზიციური ძალების პარალიზების მიზნით, ხელისფულების მხრიდან მათ ბლოგებზე განხორციელდა კიბერშეტევები. ხოლო თურქეთში, ასევე არჩევნების პერიოდში დროებით დაიხურა Facebook - სა და სხვა სოციალურ ქსელებზე წვდომის შესაძლებლობა. კიბერსივრცეში ახალი ტექნოლოგიების შექმნამ ასევე წარმოშვა „კიბერ ომის“ ცნება, რაც თავისთან მოიცავს სახელმწიფოებისა და ალიანსების მხრიდან ერთმანეთისთვის ინფრასტრუქტურის განადგურების და მაქსიმალური ზიანის მიყენებას.

სოციალური ქსელებიდან მომდინარე საფრთხეებს დიდი ზიანის მიყენება შეუძლია მსოფლიო ცივილიზებული სამყაროსთვის და ისინი პირდაპირ ემუქრებიან ეროვნულ თუ საერთაშორისო უსაფრთხოებას. ამიტომ ცივილიზებული მსოფლიო ცდილობს შეინარჩუნოს ინტერნეტის უზარმაზარი შესაძლებლობები, არ შეფერხდეს ინფორმაციული ტექნოლოგიების ინოვაციური განვითარება, არ დაირღვეს ადამიანის უფლებები და ამავდროულად, ყოველივე ამის ფონზე მაქსიმალურად იყოს დაცული უსაფრთხოება თავის ყველა დონეზე.

უსაფრთხოების უზრუნველყოფაზე ფიქრისას მუდმივად ვაწყდებით გარკვეულ შეუთავსებლობას, რაც თავის მხრივ წარმოშობს დილემურ კითხვას - უფრო მეტი დემოკრატია თუ სათანადო უსაფრთხოება? ანუ სად მთავრდება დემოკრატიული პრინციპები და საიდან იწყება უსაფრთხოება, იქნება ეს ეროვნული თუ საერთაშორისო? ყოველი ქვეყნის ხელისუფლების საზრუნავს წარმოადგენს მოცემულ ორ ცნებას შორის სწორი არჩევანის გაკეთება და მათ შორის გარკვეული ბალანსის დამყარება.

ავტორიტარული მმართველობის ქვეყნებში, ხელისუფლება ცდილობს თავის კონტროლს დაუქვემდებაროს სოციალურ ქსელებზე მომხმარებლის წვდომა და მისი აქტიურობა. თუმცა უნდა ითქვას, რომ დემოკრატიულ ქვეყნებშიც წარმოიშვა მსგავსი პრობლემები, განსაკუთრებით „არაბული გაზაფხულის“, „დავიკავოთ უოლსტრიტისა“ და ლონდონში მასიური გამოსვლების შემდეგ. ყოველივე ორგანიზებული იყო ბლოგერების მიერ სოციალური ქსელების საშუალებით. ყველა გამოსვლამ გამოიწვია

დასავლეთის დიდი შეშფოთება და შიში იმისა, რომ საპროტესტო აქციებს უფრო მასშტაბური ხასიათი არ მიეღო, არ გადაზრდილიყო პოლიტიკურში და არ ყოფილიყო გამოყენებული ულტრა - მემარცხენე ოპოზიციური ძალების მიერ.

ფაქტიურად, დასავლეთი აღმოჩნდა სერიოზული პრობლემის წინაშე. კერძოდ. სოციალური ქსელები, რომლებიც საზოგადოების ძალიან დიდ ნაწილს მოიცავს, კარგად გამოიყენება დესტაბილიზაციის მიზნებისთვის, შიდა პოლიტიკური, ეკონომიური თუ სოციალური ტემპერატურის კონტროლისთვის. ამის გამო სოციალური ქსელების სწორად გამოყენების გზებს მსოფლიოს მთელი საზოგადოება ეძებს. ხელისუფლების მხრიდან სოციალურ ქსელებზე მონიტორინგის განხორციელება და კონტროლის დაწესება გარკვეულწილად ადამიანის უფლებების დარღვევად აღიქმება, როცა არდაწესებამ შეიძლება წარმოშვას სერიოზული საფრთხეები. ეს ფაქტი კი ერთგვარი დილემის წინაშე აყენებს ამა თუ იმ ქვეყნის მთავრობებს, რომლებიც ცდილობენ პრობლემა თავისებურად მოაგვარონ, რაც ხშირ შემთხვევაში უშედეგოდ მთავრდება. მაგალითად, დიდი ბრიტანეთის პრემიერ - მინისტრის დევიდ ქემერონის მხრიდან გაკეთებულმა განცხადებამ სოციალურ ქსელებზე სახელმწიფო კონტროლისა და მონიტორინგის დაწესების შესახებ საზოგადოებრიობის დიდი უკმაყოფილება გამოიწვია და დემოკრატიული პრინციპებიდან გამომდინარე, მთავრობაც იძულებული იყო წასულიყო დათმობებზე.

ამერიკელი მეცნიერების კვლევები აჩვენებს, რომ სოციალური ქსელების კონტროლი საკმაოდ იოლი ყოფილა, რაც პირდაპირ კავშირშია თავად ქსელის სტრუქტურასთან და მის ჰომოგენურობასთან. სოციალური ქსელის საშუალებით სასურველი შედეგის მისაღწევად, აუცილებელია ქსელის მხოლოდ 20 პროცენტ მომხმარებელში საჭირო ინფორმაციის გავრცელება. თუმცა უნდა აღინიშნოს, რომ ამ მეთოდითაც გარკვეულწილად იზღუდება პიროვნების თავისუფალი არჩევანისა და ნების გამოხატულობის საშუალება. ფაქტიურად, სოციალური ქსელის მეშვეობით მომხმარებელს გარკვეული ფორმით მიეწოდება ისეთი ინფორმაცია, რაც პირდაპირ კავშირშია მისაღები შედეგის დადგომასთან და იწვევს შენთვის სასურველი მიზნის

მიღწევას, რაშიც ქსელის მომხმარებელი, მისდაგაუცნობიერებლად „გეხმარება“. ესეც შეიძლება მიჩნეულ იქნას სოციალურ ქსელებზე კონტროლის დაწესების ერთ - ერთ მეთოდად.

საკმაოდ რთული გადასაწყვეტია პრობლემა დაკავშირებული ადამიანის როგორც სოციალური ქსელების მომხმარებლის უფლებებთან. ეს უფლება ადამიანს მინიჭებული აქვს კონსტიტუციით, სხვადასხვა ქარტიებითა და საერთაშორისო აქტებით, მისი ხელყოფა კი დემოკრატიულობის პრინციპებიდან გამომდინარე ყოვლად დაუშვებელია. მის დარღვევას ან თუნდაც ნაწილობრივ შეზღუდვას ერიდება დემოკრატიულობის ინდექსის მაღალი თუ საშუალო ნიშნულის მაჩვენებელი ყველა ქვეყნის ხელისუფლება, რადგან ეს მისთვის პოლიტიკურად აშკარად წამგებიანი ნაბიჯი იქნება. ამიტომაც პოლიტიკური ლიდერები სოციალური ქსელების არასწორი გამოყენების პროცესს ხშირ შემთხვევაში უკავშირებენ ეროვნულ და საერთაშორისო უსაფრთხოებას, ქვეყნის სტრატეგიულ ინტერესებს, რაც ხშირად ხდება ხელისუფლების მხრიდან სოციალურ ქსელებზე არასანქცირებული ფარული მონიტორინგისა და კონტროლის განხორციელების მცდელობის მიზეზი. სწორედ აქ სრულდება დემოკრატია და იზღუდება მისი ფასეულობები. თუმცა ასევე მნიშვნელოვანია იმის გათვალისწინება, რომ უნდა ამაღლდეს სამოქალაქო ცნობიერება დაკავშირებული ქვეყნის უსაფრთხოების საკითხებთან და მოქალაქეთა მხრიდან სოციალური ქსელების სწორად გამოყენებასთან, რათა არ მოხდეს ქვეყნის სტრატეგიული ინტერესებისათვის რაიმე სახის ზიანის მიყენება.

ანდრია გოცირიძე

პოსტსაბჭოთა სივრცის კონფლიქტების კიბერასპექტები და საქართველო

კიბერელემენტების გამოყენება თანამედროვე კონფლიქტებში

საქართველოსთვის, როგორც მცირე რესურსის მქონე ქვეყნისათვის მეტად მნიშვნელოვანია ძლიერ მოწინააღმდეგესთან კონფლიქტისას მოწინააღმდეგის გამოფიტვისკენ მიმართული ასიმეტრიული პასუხების გამოყენება. ასეთ გარემოში, ცხადია დიდ მნიშვნელობას იძენს სახელმწიფო უსაფრთხოების კიბერმდგენელი. უკანასკნელ ათწლეულში კიბერდომეინი საჰაერო, სახმელეთო, საზღვაო და კოსმოსურის შემდეგ, დაპირისპირების მეხუთე სივრცედ დამკვიდრდა და იგი სულ უფრო ხშირად გამოიყენება პოლიტიკური თუ სამხედრო მიზნების, გეოპოლიტიკური უპირატესობის მისაღწევად.

თუკი პოსტსაბჭოთა სივრცეში რუსეთის მონაწილეობით მიმდინარე კონფლიქტებს გავაანალიზებთ, ცხადი ხდება რომ იგი კონფლიქტის ტერიტორიებს განიხილავს, როგორც შეიარაღების კინეტიკური სახეობების, ასევე კიბერშეტევითი პოტენციალის გამოსაცდელ ერთგავრ პოლიგონად. ამის ნათელი მაგალითია რუსეთის მხრიდან თუნდაც საქართველოზე განხორციელებული კიბერშეტევის პერიოდიდან უკრაინაში ამ მხრივ მიღწეული „პროგრესი“ და კიბერელემენტის გამოყენების არეალის მკვეთრი ზრდა. უკრაინის კრიზისი ნატოს მიერ აღიარებულია ინფორმაციული ოპერაციების, პროვოკაციების, კიბერთავდასხმების სამხედრო ოპერაციებთან სტრატეგიული ინტეგრაციის მაგალითად. ამდენად, საქართველოსთვის სასიცოცხლოდ აუცილებელია აღნიშნული კონფლიქტის და რუსეთის დაინტერესების სფეროში ამ მხრივ პარალელურად მიმდინარე პროცესების დეტალური ანალიზი და სწორი დასკვნების გამოტანა. საქართველოსთვის, როგორც ევროატლანტიკურ სივრცეში ინტეგრირების მსურველი ქვეყნისთვის, უაღრესად მნიშვნელოვანია

კიბერუსაფრთხოების ინტეგრირება სამხედრო ოპერაციების ჭრილში. უნდა გვახსოვდეს, რომ არ არსებობს „სუფთა კიბერომი“ და ყოველი კიბეროპერაცია, როგორც წესი, საინფორმაციო, შეზღუდული მასშტაბის, ჰიბრიდული თუ სრულმასშტაბიანი ომის ნაწილია.

კიბერელემენტი დღესდღეობით უკვე წარმოადგენს ყველა ომისა და კონფლიქტის მნიშვნელოვან შემადგენელ ნაწილს. საქართველოსთვის, როგორც რუსეთის დაინტერესების მუდმივი ობიექტისთვის, კიბერსივრცის დაცვა მისი ეროვნული უსაფრთხოების და თავდაცვის წინააღმდეგ გამოყენებისაგან პრიორიტეტულ მიმართულებად უნდა იქნას აღიარებული. მიუხედავად იმისა, რომ სამხედრო პოტენციალის თვალსაზრისით განსხვავება ჩვენსა და მოწინააღმდეგეს შორის კოლოსალურია, კიბერსივრცე ის არეალია, სადაც პატარა ქვეყანას რეალურად შეუძლია წინააღმდეგობა გაუწიოს აგრესორს და იგი შესაძლოა გახდეს მის ქმედებებზე ასიმეტრიული პასუხის ერთ ერთი წარმატებული ელემენტი ან წინააღმდეგობის მოქმედი ფრონტი. ყველასათვის კარგად ცნობილი პროგრამა-დივერსანტი “Stuxnet”, რომლის სამიზნე ირანის ბირთვული პროგრამა იყო, ზემოქმედების კლასიკური მეთოდების (ავიადარტყმების მუქარა, პოლიტიკური ზეწოლა, ეკონომიური სანქციები) კიბერსაშუალებებით შევსების კარგი მაგალითია. აღნიშნული ცხადყოფს, რომ ძლიერი და განვითარებული ქვეყნებიც კი კარგად აცნობიერებენ, რომ კიბერშეიარაღება წარმოადგენს რეალურ ასიმეტრიულ ინსტრუმენტს იმ ქვეყნებისა თუ დაჯგუფებების წინააღმდეგ, რომლებიც ხელყოფენ საერთაშორისო წესრიგსა და უსაფრთხოებას. მითუმეტეს მნიშვნელოვანია აღნიშნული მიმართულება, როგორც შესაძლო ასიმეტრიული პასუხის ერთ ერთი მდგენელი, მცირე სახელმწიფოთათვის.

ზემოთქმულიდან გამომდინარე, უკიდურესად მნიშვნელოვანია განვიხილოთ საომარ თუ კრიზისულ ვითარებებში კიბერელემენტის გამოყენების უკანასნელი ტენდენციები და პოსტსაბჭოთა სივრცეში რუსეთის მონაწილეობით მიმდინარე კონფლიქტებში კიბერთავდასხმების გამოყენების სპეციფიკა. სწორედ აღნიშნული ფაქტორების გათვალისწინებით უნდა წარიმართოს საქართველოში კიბერთავდაცვითი

პოტენციალის განვითარება, კიბერელემენტის ინტეგრაცია სამხედრო შესაძლებლობებთან, რაც საერთო ჯამში მსოფლიო უსაფრთხოების არქიტექტურაში საქართველოს საიმედო პარტნიორად და სანდო მოთამაშედ აქცევს.

კიბერსივრცე, როგორც მხარეთა დაპირისპირების არეალი ყოველდღიურად უფრო მეტ მნიშვნელობას იძენს. განვითარებული ქვეყნების კიბერუსაფრთხოების სფეროში ჩართული დანაყოფების რიცხვი ყოველდღიურად იზრდება, ბიუჯეტი კი მილიარდობით დოლარს უტოლდება. კიბერდომეინის მიმართ ქვეყნების მზარდ ინტერესს ის გარემოებაც ადასტურებს, რომ მიუხედავად ეკონომიური კრიზისებისა თუ ფინანსური სირთულეებისა, ჯერ არც ერთ სახელმწიფოს ეს ხარჯი არ შეუმცირებია. ცხადია, ეს სისტემები მხოლოდ თავდაცვას არ ემსახურება. ნატოს უელსის სამიტის წინ გაჟღერებული მონაცემებით, ოცდაათამდე ქვეყანას უკვე გააჩნია შემტევი პოტენციალი, რაც მოწინააღმდეგის კრიტიკულ ინფრასტრუქტურაზე კიბერდივერსიებსაც გულისხმობს.

ცხადია, რთულია ზუსტი პროპორციის დადგენა შემტევ და თავდაცვით საშუალებებზე დახარჯულ თანხებს შორის, თუმცა უნდა ვივარაუდოთ, რომ შეტევით პოტენციალზე არსებული მონაცემები ხელოვნურად შემცირებულია.

შემტევი კიბერპოტენციალის თვალსაზრისით, რუსეთი ერთ ერთ მოწინავე პოზიციას იკავებს. რუსეთის ფედერაციის უშიშროების საბჭოს მდივანი ნ. პატრუშევი ხაზგასმით აღნიშნავს, რომ ეროვნული უსაფრთხოების საფუძვლების უზრუნველყოფის მიზნით სტრატეგიული დაგეგმვის კორექტირებულ დოკუმენტებში, რომლებიც 2020 წლამდე ამოცანებს განსაზღვრავს, რუსეთის ფედერაციის საინფორმაციო უსაფრთხოების დოქტრინას მნიშვნელოვანი ადგილი უჭირავს. პატრუშევის მოსაზრებით, “პირველ რიგში ეს გამოწვეულია ახალი სამხედრო საფრთხეების და მუქარების წარმოქმნით. მათი გამოჩენა თვალსაჩინოა “არაბული გაზაფხულის” მოვლენებში, სირიასა და ერაყში, უკრაინასა და მის გარშემო მიმდინარე პროცესებში. გამოიკვეთა სამხედრო საფრთხეების წანაცვლება საინფორმაციო სივრცეში”. კიბერ- და საინფორმაციო უსაფრთხოების საკითხების სპეციალიზირებული კონფერენციებიდან

საჯარო პოლიტიკის სფეროში გადანაცვლება მარტო რუსული ტრენდი არ არის. ყურადსაღებია ის გარემოებაც, რომ რუსეთისა და ჩინეთის მიერ ხელმოწერილ იქნა შეთანხმება საერთაშორისო საინფორმაციო უსაფრთხოების უზრუნველყოფის თაობაზე. აღნიშნული შეთანხმების მიზეზები ცალკე განხილვის საგანს წარმოადგენს, თუმცა მხედველობის მიღმა არ უნდა დარჩეს ის გარემოება, რომ კიბერთავდაცვით სფეროში (ცხადია, ეს შემტევ პოტენციალსაც გულისხმობს) არსებული სამი უდიდესი მოთამაშისგან (აშშ, რუსეთი, ჩინეთი), კიბერთავდასხმებზე ბრალდება მუდმივად რუსეთისა და ჩინეთის მისამართით ისმის, მაშინ, როდესაც ამ ორ სახელმწიფოს შორის კიბერსაფრთხეების სფეროში რაიმე ხმაურიან ინციდენტს ადგილი არ ჰქონია, რაც თავისთავად ლოგიკურს ხდის მათ ალიანსს; აქვე უნდა აღინიშნოს, რომ თუკი ჩინეთის მხრიდან ორგანიზებული კიბერთავდასხმების სამიზნეს ძირითადად კომერციული საიდუმლო ინფორმაცია წარმოადგენს და ამდენად საქართველოსთვის ნაკლები საფრთხის შემცველია, რუსეთი აქტიურად იყენებს კიბერელემენტს სახელმწიფოებრივი მიზნების, ამოცანების გადასაჭრელად, მათ შორის სამხედრო თუ გეოპოლიტიკური უპირატესობის მოსაპოვებლად. ცხადია, ეს გარემოება საქართველოსთვის უაღრესად დიდ საშიშროებას წარმოადგენს.

უკანასკნელი პერიოდის აქტიური საბრძოლო დაპირისპირებების უმრავლესობას თან ახლდა ამა თუ იმ ფორმით კიბერელემენტი. კიბერდაპირისპირება ახასიათებდა ლიბიის ომს, ნაწილობრივ სირიის კონფლიქტს, ხოლო კიბერშპიონაჟი და კიბერდივერსიები საერთაშორისო ურთიერთობებს მუდმივ ფონად გასდევს. Stuxnet-ის ეპიზოდი, ჯაშუშური ვირუსებისა თუ ქსელების (Duqu, Flame, Gauss, Miniduke, Red October, Wiper) აღმოჩენა - კიბერშპიონაჟისა თუ დივერსიების ეს არასრული ჩამონათვალი 21-ე საუკუნის პირველი ათწლეულის ბოლოდან დღითიდღე იზრდება და მზარდ მნიშვნელობას იძენს. საქართველოს წინააღმდეგ კიბერჯაშუშობის მასშტაბებზე თუნდაც ამერიკული ნახევრადსამთავრობო ორგანიზაციის Fire Eye-ს ანგარიშში არსებული მონაცემებიც მოწმობს, რომლის თანახმადაც წლების მანძილზე ვირუსის ზემოქმედებას დაექვემდებარა სამთავრობო და ძალოვან სტრუქტურათა რესურსები, სამხედრო ატაშეების ოფისები, ნატო-საქართველოს ურთიერთობასთან დაკავშირებული

დოკუმენტაცია და სხვა სენსიტიური მასალები. ცალკე უნდა განვიხილოთ ის მიზანმიმართული ჯაშუშური ქმედებები, რომელთა სამიზნეც სამხედრო სამრეწველო სფეროს საიდუმლო პროექტებია.

ობიექტური რეალობაა, რომ კიბერსივრცეში საიმედო დაცვის შექმნა უკიდურესად რთული ამოცანაა, მასშტაბური კიბერშეტევის თავიდან აცილება და ადექვატური პასუხი კი თითქმის შეუძლებელი; სახელმწიფოები ცდილობენ აქცენტი შემტევ ოპერაციებზე გააკეთონ, რათა ეფექტურად გამოიყენონ კიბერსივრცე მიზნების მისაღწევად.

კიბერშეიარაღების კონტროლის ან გამოყენების აკრძალვის საერთაშორისო სისტემების შექმნის მცდელობები გრძელდება, თუმცა უახლოეს პერიოდში რაიმე მნიშვნელოვან შედეგს ამ ქმედებებისაგან არ უნდა ველოდეთ, რაც კიბერიარაღის თვისებებით, განსაკუთრებით კი მისი იდენტიფიკაციის შეუძლებლობით არის განპირობებული. სიტუაციას ამძაფრებს ის გარემოებაც, რომ შეტევა ამ სფეროში ყოველთვის დარჩება უფრო იაფ და დამანგრეველი შედეგების მქონე ქმედებად, ხოლო დაცვა - ძვირადღირებულ და უკიდურესად რთულ პროცესად.

რუსეთ - უკრაინის კონფლიქტი

კონფლიქტებში კიბერელემენტების გამოყენების შესწავლისათვის მნიშვნელოვანია უკრაინა-რუსეთის კონფლიქტის აქტიური ფაზის განხილვა, რომელიც ექსპერტთა მიერ ჰიბრიდული ომის წარმატებულ მაგალითად არის აღიარებული. კიბერთავდასხმების, როგორც ჰიბრიდული ომის შემადგენელის გამოყენება რუსეთმა და მასთან დაკავშირებულმა ჯგუფებმა უკრაინის კონფლიქტში ყირიმის ანექსიის მომენტიდან დაიწყეს, თუმცა ზოგიერთი მონაცემით კიბერშეტევები ევრომაიდანის დროიდან იღებს სათავეს. განხორციელდა მასშტაბური შეტევები სამთავრობო საინფორმაციო რესსურსსა თუ ზოგიერთი პოლიტიკოსის და საზოგადო მოღვაწის პერსონალურ მონაცემებზე. განსაკუთრებული მნიშვნელობის იყო DDoS შეტევები საგარეო საქმეთა სამინისტროს, უსაფრთხოების თუ თავდაცვის სექტორის, უკრაინის პრეზიდენტის საიტებზე, მიზანმიმართული თავდასხმები თაღლითური

ელექტრონული ფოსტის მეშვეობით, ცენტრალური საარჩევნო კომისის მუშაობის მოშლის მცდელობები საპრეზიდენტო და საპარლამენტო არჩევნებისას 2014 წელს, ვირუს Uroboros-ის მოქმედება, რამაც დააზარალა სამთავრობო, განსაკუთრებით კი ძალოვანი სტრუქტურების რესურსები, კიბერდარტყმის ქვეშ მოექცა ასევე საინფორმაციო საშუალებების, საფინანსო დაწესებულებებისა თუ მსხვილი სამრეწველო ობიექტების ვებ-რესურსი.

მთელ კონფლიქტს ფონად გასდევდა კიბერზემოქმედების ათეულობით მცდელობა. ცნობილი კომპანიის, ESET-ის მონაცემებით, უკრაინისა და ნაწილობრივ პოლონეთის წინააღმდეგ მიზანმიმართულად იქნა გამოყენებული ვირუსი Blachenergy. ამ ვირუსის ზემოქედების ქვეშ მოექცა სახელმწიფო ორგანიზაციებისა და ბიზნეს-სტრუქტურების რესურსი, ასევე სამრეწველო სექტორის გარკვეული ნაწილი. გამოყენებულ იქნა ვირუსი Cosmicduke, ასევე არსებობს მონაცემები თანამდებობის პირთა მიმართ ვირუს Fireeye-ს გამოყენების შესახებ. ზემოაღნიშნული მავნე პროგრამების დანიშნულებას ინფორმაციაზე არასანქცირებული წვდომა წარმოადგენდა, რაც გარკვეული წარმატებით იქნა კიდევაც განხორციელებული. გარდა აღნიშნულისა, არსებობს მრავალი მონაცემი სოციალურ ქსელებში ყალბი ანგარიშებით განხორციელებულ დეზინფორმაციის გავრცელებასა და ტრადიციული სოციალური ინჟინერიის მეშვეობით განხორციელებულ შეტევებზე.

უკრაინის კონფლიქტმა კიდევ ერთხელ ცხადყო, რომ კიბერშპიონაჟი თუ კიბერდივერსიები დიდ საფრთხეს უქმნის ქვეყნის თავდაცვისუნარიანობას. რუსეთის სპეცსამსახურებმა, უკრაინელი ექსპერტების მონაცემებით, შეძლეს გამოეყენებინათ მსხვილი მობილური ოპერატორების შესაძლებლობა აბონენტებზე ფარული მოსმენებისათვის, მათი ადგილმდებარეობის განსაზღვრისა თუ სხვა მონაცემთა მიღებისათვის. ამგვარი ინფორმაციის გამოყენება მრავალმხრივაა შესაძლებელი: დაწყებული ფსიქოლოგიური ზემოქმედებიდან თუ ინფორმაციის მოხსნიდან და დასრულებული საარტილერიო დარტყმისთვის კოორდინატების გადასაცემად ადგილმდებარეობის განსაზღვრით. არსებული მონაცემების ანალიზი ცხადყოფს, რომ

სახეზეა ერთ ერთი მხარის მიერ კიბერსივრცის, კერძოდ კი მისი სატელეკომუნიკაციო მდგენელის დესტრუქციული მიზნებისათვის გამოყენება.

რუსეთის მხრიდან კიბერშესაძლებლობების ზრდის ტენდენცია და მისი ფართოდ გამოყენება კონფლიქტურ სიტუაციებში წარმოშობს სეროზულ საფრთხეს, რომ მომავალი ესკალაციის შემთხვევაში მოხდება კრიტიკული ინფრასტრუქტურის წინააღმდეგ მიმართული შეტევა, რასაც შესაძლოა დიდი მსხვერპლი და მასიური ნგრევა მოჰყვეს.

ჰიბრიდული ომის ნიშნები პოლონეთის წინააღმდეგ

უკრაინის კრიზისის მსვლელობისას პოლონეთი იყო მოწინავე სახელმწიფო ევროპაში, რომელმაც მხარდაჭერა გამოუცხადა ოფიციალურ კიევს რუსეთის წინააღმდეგ ბრძოლის პროცესში. იგი ხუთ სხვა სახელმწიფოსთან ერთად აქტიურ მხარდამჭერად მოგვევლინა 2008 წლის რუსეთ-საქართველოს ომის დროსაც. ცხადია, აღნიშნული მკვეთრი პოზიცია ექსპერტებს აძლევს ვარაუდის საფუძველს, რომ პოლონეთი შესაძლოა გახდეს რუსეთის ჰიბრიდული ომის ლოგიკური სამიზნე.

პოლონეთის შიდა უსაფრთხოების სააგენტოს სამთავრობო კომპიუტერული უსაფრთხოების ინციდენტებზე რეაგირების ჯგუფის (CERT) მოხსენების თანახმად, შეინიშნება პოლონეთის სამთავრობო რესურსზე განხორციელებული კიბერშეტევების ზრდის ტენდენცია. 2011-12 წლებში დაფიქსირებული ასეულობით დადასტურებული კიბერშეტევის რიცხვი 2013 წელს 5670, ხოლო 2014 წელს 7498-მდე გაიზარდა. პოლონელი ექსპერტების მონაცემებით, რეგისტრირებული კიბერშეტევების დონე და მათგან მომდინარე საფრთხე მკვეთრად გაზრდილია წინა წლებთან შედარებით. ხშირშემთხვევაში შეინისნება უცხო ქვეყნის მხარდაჭერის კვალიც.

2014 წელს განხორციელდა გახმაურებული ჰაკერული და ე.წ DDoS თავდასხმები პოლონეთის საკვანძო სახელმწიფო და ფინანსურ საიტებზე, მათ შორის პოლონეთის პრეზიდენტისა და ვარშავის საფონდო ბირჟის გვერდებზე. ზემოხსენებულ ინციდენტებთან დაკავშირებით პასუხისმგებლობა აიღო „კიბერ-ბერკუტმა“, მიზეზად კი

პოლონეთის მთავრობის წინააღმდეგ შურისძიება დაასახელა „პოსტ - ევრომაიდანზე“ უკრაინელი სამართალდამცავი ორგანოებისათვის გამოხატული მხარდაჭერის გამო. აღიარებულ ტენდენციად გვევლინება ის გარემოება, რომ ამ ორგანიზაციის აქტივობები ხშირ შემთხვევაში რუსეთის მონაწილეობით მიმდინარე კონფლიქტის შემადგენელი ნაწილია და არა განყენებული „შურისძიების აქტი“.

უკრაინასა თუ პოლონეთის კიბერსივრცეში მიმდინარე მოვლენებმა ცხადყო, რომ კიბერელემენტი შესაძლებელია გამოყენებულ იქნას არა მხოლოდ ინფორმაციაზე არასანქცირებული წვდომის ან რესურსის წყობიდან გამოყვანის მიზნით; კიბერსივრცეში იკვეთება პოსტსაბჭოთა ქვეყნების მიმართ წარმოებული „საინფორმაციო ომის“ ახალი ტენდენცია, რომელიც მოიცავს უცხოური პროპაგანდისა და დეზინფორმაციის გავრცელებას ბლოგერებისა და ავტორების მიერ ონლაინ სადისკუსიო ფორუმებისა და ვებ-გვერდების კომენტარებში. აღნიშნული ტენდენცია მეტად ყურადსაღებია საქართველოსთვის, როგორც ევროატლანტიკური მისწრაფების მქონე ქვეყნისათვის. პოლონური CERT-ის მონაცემებით, ბევრი ასეთი ბლოგერი ანაზღაურებას იღებს უცხოური სახელმწიფოსგან, თუმცა არ გამოირიცხება გულუბრყვილო, დეზინფორმაციით შეცდომაში შეყვანილ ან იდეოლოგიურად ანგაჟირებულ პირთა შეხედულებებისა და მიდგომების, გამოყენება უცხო ქვეყნის ინტერესების გასატარებლად.

ყირიმის ანექსიის შემდეგ პრორუსული ხასიათის ინფორმაციით პოლონური საიტების გაჯერების ტენდენციას პოლონური საინფორმაციო გამოშვებები ცალსახად უწოდებენ რუსეთის ჰიბრიდულ ომს პოლონეთის წინააღმდეგ. ბოლო ათწლეულში ტრადიციულად ქცეული კიბერთავდასხმების გარდა, მიმდინარე სამხედრო ოპერაციის საინფორმაციო უზრუნველყოფა უკვე იქცა ჰიბრიდული ომის ძირითად, საკვანძო ელემენტად. თუკი ესტონეთისა და საქართველოს წინააღმდეგ განხორციელებული კიბერშეტევები ამ სახელმწიფოთა საინფორმაციო არხების განადგურებას ისახავდა მიზნად, დღესდღეობით კიბერსივრცის გამოყენება რუსეთის მხრიდან სულ უფრო და

უფრო ხშირად ხდება მოწინააღმდეგის არხების საკუთარი პროპაგანდისტული მიზნებისათვის გამოსაყენებლად.

ამ ფონზე არ არის გასაკვირი პოლონეთის ხელისუფლების შეშფოთება თებერვალში რუსეთის სახელმწიფო საინფორმაციო სააგენტოს პოლონურ ენაზე მაუწყებლობის დაწყებამ. "სპუტნიკი" 2014 წლის მიწურულს ჩამოყალიბდა და ოცზე მეტ ენაზე მაუწყებლობს. ევროპელი ექსპერტების შეფასებით, აღნიშნული სააგენტო სამიზნედ 30-ზე მეტ ქვეყანას განსაზღვრავს და რეალურად რუსული პროპაგანდის მნიშვნელოვან არხს წარმოადგენს.

პროპაგანდის აღნიშნული ფორმა არ არის ერთადერთი საშუალება რუსეთის არსენალში. 2015 წლის დასაწყისში ფეისბუკში შექმნილი პოლონურენოვანი გვერდებით გავრცელებული მოწოდება ვილნიუსისა და ლვოვის პოლონური რესპუბლიკების შექმნის თაობაზე, საერთო შეფასებით უკრაინასთან და ლიტვასთან გამთიშავი პროპაგანდის შემადგენელი ნაწილია და ცხადია, რუსეთთან ასოცირდება, თუნდაც იმ ნიშნით, რომ ამგვარი ვირტუალური ჯგუფების მსგავსება მოსკოვის მიერ მხარდაჭერილ დონეცკისა თუ ლუგანსკის "სახალხო რესპუბლიკებთან" თვალსაჩინოა. დაახლოებით იგივე მეთოდი იქნა გამოყენებული საქართველოს შეიარაღებული ძალების ISAF მისიაში მონაწილეობისადმი ნეგატიური ფონის შექმნის მიზნით, "ჯიჰადისტური" ვიდეორგოლის გავრცელებით, რომელიც ქართველი ჯარისკაცების დაღუპვის მეტად რთულ პერიოდს დაემთხვა და სამართალდამცავი ორგანოების მონაცემებით, სეპარატისტული რეგიონიდან იმართებოდა. ზემოხსენებული ფეისბუკ-ჯგუფების არსებობამ გამოხმაურება გამოიწვია რეგიონში, რადგან აღნიშნული საკითხი განსაკუთრებით მტკივნეულია ლიტვისთვის, სადაც პოლონური უმცირესობა პრორუსულია და რუსულ ენაზე იღებს ინფორმაციას.

პოლონეთის წინააღმდეგ წარმოებულ ჰიბრიდულ აქტივობებში, გარდა პირდაპირი კიბერთავდასხმებისა სახელისუფლებო თუ ფინანსურ ინსტიტუტებზე, კიბერელემენტი მინიმუმ სამი მიზნის მიღწევაშია ჩართული. პირველი, ეს არის პოლიტიკური თუ ეკონომიური არასტაბილურობის განცდის დათესვა, რაც მართვადი

სატელეკომუნიკაციო სივრცისა და სამაუწყებლო არხების მეშვეობით მიიღწევა; მეორე - პრორუსულ ელიტაზე გავლენის მოხდენა და მოსაზრების დანერგვა, რომ პრორუსული ძალები შესაძლოა მოხვდნენ პარლამენტში ან სულაც მთავრობის ფორმირებაში მიიღონ მონაწილეობა, რისთვისაც პრორუსული პოლიტიკური პარტიების საინფორმაციო მხარდაჭერის კიბერარხების შექმნა ხდება და მესამე - სოციალური ქსელებისა თუ კიბერსივრცის სხვა სეგმენტის გამოყენება ძირგამომთხრელი საქმიანობის მიმართულებით, განსაკუთრებით მეზობლებთან ურთიერთობის კონტექსტში, რაც ჩანასახშივე სპობს მოსალოდნელი აგრესიისადმი კოლექტიური წინააღმდეგობის შესაძლებლობას და კონსენსუსის მიღწევას კოლექტიურ პასუხზე.

ერთის მხრივ, იმედის მომცემია ის გარემოება, რომ პოლონეთს პრაქტიკულად არ გააჩნია მნიშვნელოვანი რუსულენოვანი უმცირესობა და გაცილებით უფრო მეტადაა ინტეგრირებული ევროატლანტიკურ სივრცეში, ვიდრე უკრაინა, რაც პრაქტიკულად გამორიცხავს ესკალაციას ყირიმის სცენარით, მითუმეტეს "მწვანე კაცუნების" და კინეტიკური საშუალებების გამოყენებით, თუმცა ეს კიდევ უფრო ზრდის რისკს, რომ კიბერსივრცეში აქტიურობები გაიზრდება და შესაძლოა მეტად მწვავე და სახიფათო ფორმებიც კი მიიღოს.

საქართველოს გამოწვევები კიბერთავდაცვის სფეროში

კრემლი საქართველოს მისი გავლენის სფეროდ მოიაზრებს და უკრაინისა და თუნდაც პოლონეთის მაგალითი არის მკაფიო ინდიკატორი იმისა, რომ ჩვენი ქვეყანა წარმოადგენს რუსეთის ჰიბრიდული ომის სამიზნეს. როგორი უნდა იყოს საქართველოს სტრატეგიული ხედვა კიბერთავდაცვის განვითარების თვალსაზრისით? ჩრდილოატლანტიკური ალიანსი, რომლის წევრობისკენაც მიისწაფვის საქართველო, აცნობიერებს, რომ მჭიდრო და ეფექტური თანამშრომლობის გარეშე იგი ვერ შეძლებს სრულყოფილად შეასრულოს თავისი როლი კიბერსივრცეში. დადებითად შესაფასებელი და გამოსაყენებელია ის ფაქტი, რომ კიბერუსაფრთხოების მიმართულებით ინფორმაციის გაცვლა, ორმხრივი თანამშრომლობა უფრო და უფრო ღრმავდება ალიანსში, როგორც წევრ ქვეყნებს შორის, ასევე მოკავშირეებისთვისაც. ამავდროულად,

საქართველოს გაცნობიერებული აქვს, რომ კიბერთავდაცვის უზრუნველყოფა ქვეყნის შიგნით უნდა დაიწყოს და ცდილობს, გამოყოს ადამიანური და ფულადი რესურსი საკუთარი კიბერშესაძლებლობების განვითარებისათვის. თუ სახელმწიფოს სურს, ისარგებლოს ალიანსის ერთობლივი შესაძლებლობებით კიბერსფეროში, მაშინ დიდი ძალისხმევა უნდა გასწიოს საკუთარი კიბერუსაფრთხოების განსავითარებლად. ამ მხრივ საჭიროა დიდი მოცულობის სამუშაოს დაგეგმვა და შესრულება, როგორც ქმედითი და თანამედროვე სტრატეგიული დოკუმენტების შექმნის, ასევე კიბერშესაძლებლობების სამხედრო ოპერაციებთან ინტეგრაციის თვალსაზრისით.

საქართველო სრულად იზიარებს ნატოს პოზიციას, რომ საიმედო ერთობლივი კიბერუსაფრთხოების საწყისი სწორედ საკუთარი ქვეყნის კიბერთავდაცვაა. უკანასკნელ წლებში რუსეთის მონაწილეობით მიმდინარე კონფლიქტების ანალიზმა ცხადყო, რომ კიბერშესაძლებლობების განვითარების პროცესში საქართველოს რამოდენიმე გამოწვევის გათვალისწინება მოუწევს.

პირველი, როგორ უნდა მოხდეს კიბერშესაძლებლობების ინტეგრირება სხვა სამხედრო ოპერაციებთან? ეს სფერო ჯერჯერობით შეუსწავლელი რჩება. კიბერუსაფრთხოება ხშირად განიხილება, როგორც დამოუკიდებელი თემა. უპირველესი გამოწვევა, როგორც ზემოთაც აღინიშნა, არის კიბერუსაფრთხოების ინტეგრირება უფრო ფართო სტრატეგიულ და ოპერაციულ ჭრილში, როგორც თავდაცვის, ისე თავდასხმის მიმართულებით. სამწუხაროდ, იგივე ნატოს ოფიციალურ პირთა შეფასებით, ამგვარი სტრატეგიული ინტეგრაციის საუკეთესო მაგალითი რუსეთის ქმედებებია უკრაინის კრიზისისას. მისი მიდგომა ითვალისწინებს ჩვეულებრივ სამხედრო ძალებთან ერთად საინფორმაციო ოპერაციების, პროვოკაციების, კიბერ და ეკონომიური ქმედებების განხორციელებას. რუსული ჰიბრიდული ომის ტაქტიკა გულისხმობს ენერგიის, როგორც იარაღის, ეკონომიური ზეწოლის, კორუფციის, შანტაჟის, სადაზვერვო ოპერაციების გამოყენებას ბირთვული ომის ზღვარზე ბალანსირებასთან კომბინაციაში და მოიცავს სპეციალური ძალების, არარეგულარული "პარტიზანული" ფორმირებების და რეგულარული შეიარაღებული

ძალების მხარდაჭერის გამოყენებას. კიბერელემენტს, როგორც ბოლო დროს განვითარებულმა მოვლენებმა ცხადყო, აღნიშნულ ტაქტიკაში ერთ ერთი საკვანძო ადგილი უჭირავს და სულ უფრო მეტი ამოცანის გადასაჭრელად გამოიყენება. ამ გამოწვევის განხილვისას გარკვეულ იმედს იძლევა ბოლო დროს ჩვენი ქვეყნის მასშტაბით სამხედრო წვრთნებში კიბერელემენტის მუდმივი ჩართულობა და საერთაშორისო კიბერსავარჯიშოებში ქართული უწყებების მონაწილეობა, თუმცა ძირითადი სამუშაო ამ მხრივ ჯერ კიდევ გასაწევია და თავად გამოწვევაც, საერთო შეფასებით ინტელექტუალური უფროა, ვიდრე ტექნიკური.

მეორე გამოწვევას კიბერთავდასხმის იმ ზღვარის განსაზღვრა წარმოადგენს, რომლის გადალახვაც პასუხის აუცილებლობას იწვევს. აღნიშნული პრობლემა ნატოს წევრი ქვეყნებისათვის და ალიანსისთვისაც აქტუალურია. უელსის სამიტამდე ალიანსმა განაახლა კიბერთავდაცვის პოლიტიკა, იმ მიზნით, რომ მეხუთე მუხლით გათვალისწინებული ყოფილიყო წევრ ქვეყნებზე განხორციელებული „ციფრული შეტევა“ და მისგან ერთობლივი თავდაცვა. ეს თავისთავად ძალიან სერიოზული განაცხადია და კიბერსივრცის დაცვის მნიშვნელობას უსვამს ხაზს, მაგრამ პრეცენდენტის არარსებობის გამო უპასუხოდ რჩება კითხვა: რა შემთხვევა განაპირობებს მეხუთე მუხლის ამოქმედებას? როდის ჩაითვლება ერთი ქვეყნის მიმართ განხორციელებული კიბერშეტევა ყველა წევრი ქვეყნის მიმართ განხორციელებულ კიბერშეტევად? წევრ ქვეყნებს და გარკვეულწილად პარტნიორებსაც უნდა გააჩნდეთ რწმენა იმისა, რომ ალიანსი გამოიყენებს თავის ნებას და შესაძლებლობებს, უზრუნველყოს შესაბამისი რეაქცია იმ შემთხვევაში, თუკი მოხდება კიბერშეტევა ნებისმიერ მათგანზე. დიდი ალბათობით, კიბერშეტევა, რომელიც გამოიწვევს მეხუთე მუხლის გამოყენებას, უნდა ითვალისწინებდეს მასობრივ კატასტროფასა და ფიზიკურ ზარალს, თუმცა გადაწყვეტილება კოლექტიური პასუხის შესახებ ყოველთვის პოლიტიკური ხასიათის იქნება, ისევე როგორც ფიზიკური შეტევის შემთხვევაში და იგი მიღებულ იქნება ყოველი კონკრეტული შეთხვევის კონტექსტში. მეორეს მხრივ, სახიფათო იქნებოდა პოლიტიკაში მკაფიოდ დაფიქსირებულიყო ზუსტი ზღვარი კოლექტიური თავდაცვის ამოქმედებისა. ცხადია, არ იქნება მიზანშეწონილი განისაზღვროს თუ რა არის მისაღები და რა არა,

რადგან მოწინააღმდეგე გამიზნულად იმოქმედებს ღია ომის საზღვრებს მიღმა, რათა თავიდან აიცილოს ნატოს ერთიანი საპასუხო ქმედებები. მართალია, საქართველოს არ არის ალიანსის წევრი და კოლექტიური თავდაცვის მექანიზმის ამოქმედება ჩვენს შემთხვევაში არარეალურია, თუმცა მნიშვნელოვანია არსებობდეს მკაფიო განცდა იმისა თუ რა ფორმიტ და რა საშუალებებით უნდა გასცეს ქვეყანამ პასუხი კიბერთავდასხმას.

დაბოლოს, სერიოზულ გამოწვევად რჩება კოლოსალური განსხვავება საქართველოსა და ნატოს კიბერშესაძლებლობების (თავდაცვა, შეტევა და დაზვერვა) განვითარების კუთხით. დისკუსიები და პრაქტიკული სამუშაოები არასდროს იქნება საკმარისი თუ არ იარსებებს რეალური შესაძლებლობები. ნატოს ოფიციალურ პირთა შეფასებით, ამ ეტაპისათვის ალიანსის უახლოეს მოკავშირეებს შორისაც კი არსებობს გარკვეული ეჭვები თუ რამდენად გამოიყენებენ განვითარებული წევრი ქვეყნები თავიანთი დაზვერვისა და შეტევით შესაძლებლობებს სხვა წევრი ქვეყნების დასახმარებლად, თუმცა დადებითად შესაფასებელია ის ფაქტი, რომ კიბერუსაფრთხოების მიმართულებით ინფორმაციის გაცვლა, ორმხრივი თანამშრომლობა თავად ნატოსთან თუ მის წევრებთან უფრო და უფრო ღრმავდება და საქართველო ამ მხრივ მრავალ პროექტსა თუ მიმდინარე წვრთნებშია ჩართული. აღნიშნულის მაგალითად თუნდაც სულ ახლახანს, 2015 წლის აპრილის თვეში ნატოს ეგიდით ჩატარებულ ყოველწლიურ კიბერწვრთნებში “Locked Shields 2015” საქართველოს დაშვებაც გამოდგება. მჭიდრო და ეფექტური თანამშრომლობის გარეშე საქართველო ვერ შეძლებს სრულყოფილად შეასრულოს სანდო პარტნიორის როლი კიბერსივრცეში, ეფექტური კიბერშესაძლებლობების გარეშე კი 21-ე საუკუნეში უსაფრთხოების სფეროში საიმედო მოთამაშის პოზიციის შენარჩუნება წარმოუდგენელია.

პარიზის ტერაქტი და ახალი გამოწვევები კიბერსივრცეში

პარიზში, 7 იანვარს ფრანგულ სატირულ ყოველკვირეულ ჟურნალზე Charlie Hebdo - ზე განხორციელებულ ტერაქტს წინ უძღოდა საკმაოდ მასირებული ჰაკერული კიბერშეტევების სერია ფრანგულ კიბერსივრცეზე. ჰაკერების მხრიდან შეტევის ობიექტები გახდნენ როგორც სახელმწიფო ისე კერძო სექტორის და ასევე იმ უცხოური კომპანიების ვებ - გვერდები, რომელთა საქმიანობა სხვადასხვა ფორმით უკავშირდება საფრანგეთსა და ფრანგულ კომპანიებს. კიბერშეტევების რიცხვი კიდევ უფრო გაიზარდა ტერაქტის შემდეგ. კერძოდ, 15 იანვარს abc NEWS, ფრანგი ოფიციალური პირების განცხადებებზე დაყრდნობით, ავრცელებს ინფორმაციას, რომ 7 იანვრის შემდეგ ჰაკერული თავდასხმა განხორციელდა 19, 000 ფრანგულ ვებ - გვერდზე, რაც არ მომხდარა არასდროს და არის პირველი შემთხვევა საფრანგეთის ისტორიაში. იგივე abc NEWS - ის ინფორმაციით, მხოლოდ ბოლო 24 საათის განმავლობაში განხორციელდა დაახლოებით 1, 000 - ზე მეტი შეტევა. ფრანგული ოფიციოზის განცხადებით, ჰაკერულ თავდასხმაში ეჭვმიტანილ ჰაკერულ დაჯგუფებებს შორის არიან: „ახლო აღმოსავლეთის კიბერ არმია“ (the Middle Eastern Cyber Army - MECA), Fallaga Hackers Team და Cyber Caliphate. აღსანიშნავია, რომ ამ უკანასკნელმა 12 იანვარს ერთმანეთის მიყოლებით განახორციელა რამოდენიმე კიბერშეტევა აშშ - ს ცენტრალური სარდლობის Twitter - ისა და YouTube - ს ანგარიშებზე.

აღსანიშნავია, რომ საქართველოს ინტერნეტ - სივრცეც და ქართული დომეინიც იქცნენ ჰაკერების შეტევის ობიექტებად. კერძოდ, 10 იანვარს ფრანგული ჰიპერმარკეტის Carrefour - ის ოფიციალური ვებ - გვერდი http://carrefour.com.ge/ დაჰაკერებული იქნა „ახლო აღმოსავლეთის კიბერ არმიის“ (the Middle Eastern Cyber Army - MECA) მიერ. ვებ - გვერდის გატეხვასთან დაკავშირებით შსს-მ გამოძიება სისხლის სამართლის კოდექსის 284-ე მუხლის 1-ელი ნაწილით დაიწყო, რაც კომპიუტერულ ინფორმაციასთან არამართლზომიერ შეღწევას გულისხმობს. აქვე შეიძლება ავღნიშნოთ, რომ საქართველოს კანონმდებლობა კერძო კომპანიებს არ ავალდებულებს ითანამშრომლონ

სახელმწიფოს შესაბამის უწყებებთან, ამ შემთხვევაში იუსტიციის სამინისტროს „სსიპ მონაცემთა გაცვლის სააგენტოსთან“, ინტერნეტ - სივრცის დაცვის საკითხებში, ეს არის მხოლოდ ნებაყოფლობითი კერძო კომპანიების მხრიდან სურვილის შემთხვევაში, რაც არის ყოვლად მიუღებელი, გამომდინარე, რომ რისკის ქვეშ დგება ქვეყნის კრიტიკული ინფრასტრუქტურა, ობიექტები და ინტერნეტის ნებისმიერი მომხმარებელი. ეს კი პირდაპირ კავშირშია ქვეყნის ეროვნული უსაფრთხოების სენსიტიურ საკითხებთან.

ბოლო წლებში, განსაკუთრებით სირიაში საომარი მოქმედებებისა და ახლო აღმოსავლეთში ე. წ. „ისლამური სახელმწიფოს“ (ISIS) ასპარეზზე გამოსვლის შემდეგ, ერთი - ორად გაიზარდა კიბერშეტევების რიცხვი. ამ მიმართულებით, განსაკუთრებით აქტიურობენ ზემოთ მოცემული ჰაკერული დაჯგუფებები „ახლო აღმოსავლეთის კიბერ არმია“ (the Middle Eastern Cyber Army - MECA), Fallaga Hackers Team და Cyber Caliphate, ასევე „სირიის ელექტრონული არმია“ (SEA).

„სირიის ელექტრონული არმია“ (the Syrian Electronic Army SEA), რომელსაც ასევე ხშირად უწოდებენ „სირიის კიბერ არმიას“ (the Syrian Cyber Army) სირიის პრეზიდენტის ბაშარ ალ - ასადის მხარდაჭერით სარგებლობს. ეს არის არაბულ სამყაროში პირველი ვირტუალური საჯარო არმია (http://sea.sy/index/en), რომლის სამიზნეებია ქვეყნის პოლიტიკური ოპოზიციის წარმომადგენლებისა და დასავლური ვებ - გვერდები. „სირიის ელექტრონული არმიის“ (the Syrian Electronic Army SEA) ჰაკერული თავდასხმის ობიექტები არის BBC News, the Associated Press, National Public Radio, CBC News, Al Jazeera, Financial Times, The Daily Telegraph, The Washington Post, სირიის სატელიტური მაუწყებელი Orient TV და al-Arabia TV. ასევე მობილურის სხვადასხვა VoIP აპლიკაციები, მათშორის Viber და Tango. აღსანიშნავია ისიც, რომ „არმიამ“ განახორციელა არაერთი კიბერშეტევა აშშ - ს პრეზიდენტის ბარაქ ობამასა და თეთრი სახლის, ასევე Human Rights Watch - ის ვებ - გვერდებზე. „სირიის ელექტრონული არმია“ (the Syrian Electronic Army SEA) ამ ეტაპზეც აგრძელებს აქტიურ ჰაკერულ საქმიანობას.

სრულიად უცნობ ჰაკერულ დაჯგუფებას წარმოადგენს „ახლო აღმოსავლეთის კიბერ არმია“ (the Middle Eastern Cyber Army - MECA), რომელიც ასპარეზზე გამოჩნდა

გასული 2014 წლის 23 სექტემბერს, როცა მან განახორციელა ჰაკერული თავდასხმები აშშ - ს კიბერსივრცეზე. არ არსებობს არავითარი ინფორმაცია იმის შესახებ, თუ ვინ შეიძლება იდგეს MECA - ს უკან. თუმცა შეიძლება ითქვას, რომ ეს შეიძლება იყოს როგორც რომელიმე ტერორისტული დაჯგუფება ან სახელმწიფო, ისე კერძო პირი. 15 იანვრის მონაცემებით, „ახლო აღმოსავლეთის კიბერ არმიამ“ (the Middle Eastern Cyber Army - MECA) განახორციელა მასიური შეტევა ნიდერლანდების ვებ - გვერდებზე.

The National Interest - ის ინფორმაციით, Cyber Caliphate უკავშირდება ე. წ. „ისლამური სახელმწიფოს“ (ISIS). თუმცა მის შესახებ ბევრი რამ ცნობილი არ არის. მაგრამ ზოგიერთის ვარაუდით, მოცემული ჰაკერული დაჯგუფების ერთერთი ლიდერი არის ბრიტანელი Junaid Hussain, რომელიც ერთხელ იყო უკვე დაპატიმრებული გაერთიანებული სამეფოს ყოფილი პრემიერ - მინისტრის ტონი ბლერის Gmail - ის ანგარიშის დაჰაკერების გამო. ის ასევე დაკავშირებული იყო ჰაკერთა ჯგუფთან Team Poison, რომელთა მტკიცებით, მათ აქვთ არასანქცირებული წვდომა Blackberry - სა და NATO - ს ქსელებთან, ასევე გაერთიანებული არიან “Anonymous” - თან, საბანკო ანგარიშებზე შეღწევის მიზნით. სხვა წყაროების მიხედვით, Junaid Hussain ახორციელებს ციფრული სფეროს ექსპერტების გადაბირებას სირიისა და ე. წ. „ისლამური სახელმწიფოსთვის“ (ISIS). მოცემული მიმართულების ანალიზი ნათლად აჩვენებს, რომ Cyber Caliphate არის სწრაფად მზარდი ჰაკერული ორგანიზაცია და ექპერტებს მიაჩნიათ, რომ მისი შესაძლებლობები უახლოეს მომავალში გაცილებით დიდი იქნება. ბოლო ერთ თვეში Cyber Caliphate - მა ორჯერ დააჰაკერა Albuquerque Journal - ის, New Mexico’s Mountain View Telegraph - ისა და მერილანდის WBOC 16 TV - ს ვებ - გვერდები, ასევე Twitter. როგორც ზემოთ იყო აღნიშნული, Cyber Caliphate - მა 12 იანვარს ერთმანეთის მიყოლებით განახორციელა რამოდენიმე კიბერშეტევა აშშ - ს ცენტრალური სარდლობის Twitter - ისა და YouTube - ს ანგარიშებზე.

ბოლო დროს კიბერსივრცეში განვითარებული მოვლენები ნათლად აჩვენებს, რომ სულ უფრო აქტიურად ხდება ჰაკერული დაჯგუფებების გამოყენება ტერორისტული ორგანიზაციებისა და მათთან ასოცირებული კერძო პირების მიერ, წარმოებს მათი

არასანქცირებული შეღწევა და ჰაკერული თავდასხმები სახელმწიფო თუ კერძო სექტორის ვებ - გვერდებზე, რაც პირდაპირ საფრთხეს უქმნის როგორც ცალკეულ ორგანიზაციებსა და მომხმარებლებს, ისე მთლიანად საერთაშორისო, რეგიონალურ თუ ეროვნულ უსაფრთხოებას. ვითარებას კიდევ უფრო ართულებს ის გარემოება, რომ დანაშაულებრივ ქმედებებში გამოიყენება უახლესი კომპიუტერული და პროგრამული ტექნოლოგიების მიღწევები.

ერთი - ორი სიტყვით, Charlie Hebdo არის ფრანგული სატირული ყოველკვირეული ჟურნალი, რომელიც ასახავს კარიკატურებს, რეპორტაჟებს, პოლემიკებსა და ხუმრობებს, რომელთაც ნონ - კონფორმისტული სტილი აქვთ. აქვეყნებს სტატიებს რელიგიის, პოლიტიკის, კულტურისა და სხვა საკითხების შესახებ. ჟურნალი დაარსდა 1970 წელს როგორც ჟურნალ „ჰარა-კირის“ მემკვიდრე, რომელიც საფრანგეთის მთავრობამ 1969 წელს დახურა შარლ დე გოლის შესახებ უხამსი კარიკატურების ბეჭდის გამო. ჟურნალი გამოდის ყოველ ოთხშაბათს და მისი ტირაჟი შეადგენდა დაახლოებით 50 ათას ეგზემპლარს. ჟურნალი ცნობილი გახდა წინასწარმეტყველ მუჰამედის კარიკატურებთან დაკავშირებული სკანდალით 2006 წელს, როდესაც იმავე წლის თებერვალში გამოქვეყნდა მუჰამედის კარიკატურები, რომელმაც ფართო პროტესტი გამოიწვია მუსლიმურ სამყაროში. ამის შემდეგ რედაქცია მუდმივად ღებულობდა თავისი მისამართით მუქარას. თუმცა ყველაფრის მიუხედავად, გამომცემლობის ყველაზე ცნობილი კარიკატურისტები აგრძელებდნენ თავიანთი ნახატების გამოქვეყნებას, რომელიც მიმართული იყო მსოფლიოს სხვადასხვა ადგილებში მოღვაწე რელიგიური ფანატიკოსების წინააღმდეგ. პირველი ტერორისტული შეტევა გამომცემლობაზე განხორციელდა 2011 წელს, როცა ნოემბერში ჟურნალმა „შარლი ებდომ“ გამოუშვა ნომერი სახელწოდებით „შარიათ ებდო“. ჟურნალის ეს ნომერი გავრცელდა 400, 000 ეგზემპლარით და ტუნისელი ისლამისტების გამარჯვებას მიეძღვნა. ნომრის გამოსვლისთანავე ღამით რედაქციის შენობა მთლიანად დაიწვა, ვინაიდან უცნობმა პირებმა შენობას დაუშინეს ბოთლები ცეცხლგამჩენ ნივთიერებებთან ერთად. ინციდენტის შედეგად არავინ არ დაშავებულა.

საქართველოს კიბერსივრცეში არსებული საფრთხეები

ზოგადი მიმოხილვა

თანამედროვე განმარტებით, კიბერშეტევა წარმოადგენს კომპიუტერული ქსელებისა და ელექტრონული სერვისების კონფიდენციალურობაზე, ერთიანობასა და ხელმისაწვდომობაზე ზემოქმედების განზრახულ მცდელობას. ასეთი ქმედება შესაძლოა, მიზანად ისახავდეს, როგორც სერვისის დააზიანებას ან შეფერხებას, ასევე კომპიუტერული ქსელის გამოყენებას თავდამსხმელის მიზნებისთვის, ინფორმაციის/მონაცემთა ბაზის გაჟონვას და მასზე სამომავლო არასანქცირებულ წვდომას უზრუნველყოფას.

სახელმწიფოთა მხრიდან დღესდღეობით აქტიურად განიხილება საფრთხე ინფორმაციის კონფიდენციალურობისა და ხელმისაწვდომობის მიმართ. თუკი კიბერშპიონაჟი საფრთხეს უქმნის და არღვევს კონფიდენციალობას, DDOS ოპერაციები, მონაცემთა განადგურება, სერვისების შეზღუდვა აფერხებს მონაცემთა ხელმისაწვდომობას. უკანასკნელი წლების მანძილზე შეინიშნება ტენდენცია, რომ კიბერთავდასხმები, ნაცვლად ინფორმაციის წაშლის ან მასზე წვდომის შეზღუდვისა, მიმართული იქნება ინფორმაციის შეცვლის, მისით მანიპულირებისაკენ ინფორმაციის ერთიანობის (სიზუსტე და სანდოობა) კომპრომეტირების მიზნით. ცხადია, არასწორ, სახეცვლილ ინფორმაციაზე დაყრდნობით მიღებული გადაწყვეტილებები სამოქალაქო თუ სამხედრო სფეროში სახელმწიფოსთვის დიდი საფრთხის შემცველია. ასევე ზიანის მომტანია მოვლენათა ამგვარი განვითარება ინტერნეტ-პროვაიდერებისა თუ კავშირგაბმულობის საწარმოთათვის, საბანკო თუ სადაზღვევო სექტორისათვის, ენერგეტიკისა და წყალმომარაგების, კვების მრეწველობის, ჯანდაცვის სფეროს წარმომადგენლებისთვის, რომელთა გამგებლობაშიც არის ქვეყნის თავდაცვის სფეროს კრიტიკული სერვისების დიდი ნაწილი.

თავდაცვის სფეროსთვის ასევე მნიშვნელოვანია ის საფრთხე, რომელიც წარმოიქმნება სამხედრო მოსამსახურეთა მიერ სოციალურ მედიაში, ელექტრონული ტრანზაქციების ფორმებში, საძიებო მექანიზმებში თუ სხვადასხვა მონაცემთა ბაზაში შეყვანილი პერსონალური ინფორმაციის გაჟონვით.

დღესდღეობით მიმდინარეობს თავდაცვის სექტორში არსებული საჯარო ინფორმაციის ციფრულ ფორმატში გადაყვანის პროცესი, რის შედეგადაც ელექტრონული ჩანაწერები - საზოგადოების ცხოვრების განუყოფელი ნაწილი - უფრო მეტად ხელმისაწვდომი ხდება დაინტერესებულ პირთათვის. ცხადია, ასეთ შემთხვევაში მოსამსახურე, მისი ოჯახის წევრები, თანამშრომლები, დაახლოებულ პირთა წრე შესაძლოა გახდეს როგორც უცხო ქვეყნის სპეცსამსახურის, ასევე ტერორისტული ორგანიზაციის სამიზნე. ამ პირობებში თავს იჩენს კონტრდაზვერვითი რისკები, რაც სპეციალური სამსახურების განსაკუთრებულ ყურადღებას მოითხოვს.

კიბერსივრცის აქტორების, თავდასხმის მეთოდების და სამიზნე სისტემების გაფართოების კვალდაკვალ, იზრდება სახელმწიფოს წინაშე მდგარი კიბერსაფრთხეების მასშტაბი, მათი სირთულე და საშიშროების დონე.

სამთავრობო საინფორმაციო-კომუნიკაციური ქსელები, სამხედრო, კომერციული თუ სხვა სახის პროექტები უფრო და უფრო მოწყვლადი ხდება კიბერშპიონაჟისა თუ კიბერთავდასხმისათვის. საქართველოში მიმდინარე ინფორმატიზაციის პროცესები აღნიშნულ ტენდენციას ჩვენი ქვეყნისთვის აქტუალურს ხდის, რასაც ემატება პოტენციური მოწინააღმდეგის მხრიდან კიბერელემენტების წარმატებული გამოყენება რეგიონში მიმდინარე კონფლიქტებსა თუ გეოპოლიტიკურ პროცესებში. წამყვანი ქვეყნების სადაზვერვო მონაცემებით, “კიბერ არმაგედონის” სცენარის განვითარება ნაკლებად სავარაუდოა, თუმცა სხვადასხვა აქტორის მხრიდან განხორციელებულ კიბერშეტევებს სერიოზული ზიანი შეუძლია მიაყენოს საქართველოს ინფრასტრუქტურას, მის ეკონომიურსა და ეროვნულ უსაფრთხოებას.

მიუხედავად ქსელების დაცვის მექანიზმების მუდმივი განვითარებისა, ჰაკერული შეღწევის, წარმოების პროცესსა თუ ლოჯისტიკური ოპერაციების მეშვეობით

დავირუსებული ტექნიკური მოწყობილობებისა ან პროგრამული უზრუნველყოფის, მომხმარებელთა შეცდომის საფრთხე მუდმივად არსებობს, რაც კიდევ ერთხელ ადასტურებს, რომ კიბერსაფრთხეების აღმოფხვრა შეუძლებელია და საჭიროა ქვეყანაში არსებობდეს რისკების მართვის ეფექტური მექანიზმი. თუ გავითვალისწინებთ კრიტიკული ინფორმაციული სისტემის სხვადასხვა სუბიექტის ურთიერთდამოკიდებულებასა და გარედან მომდინარე კიბერსაფრთხეებს, ცხადი ხდება, რომ ეფექტური კიბერთავდაცვის სისტემის შექმნა შეუძლებელია კერძო სექტორთან თანამშრომლობის გარეშე. უფრო ზუსტად, სამხედრო საკომუნიკაციო ქსელების დაცვა ჯერ კიდევ არ ნიშნავს ეფექტური კიბერთავდაცვითი სისტემის არსებობას, რადგან თანამედროვე სახელმწიფოში კრიტიკული სერვისების დიდი ნაწილი კერძო სექტორშია კონცენტრირებული (მაგ. წყალმომარაგება, კვება, საბანკო თუ სადაზღვევო მომსახურება) და მასზე თუნდაც კომერციული ინტერესით განპირობებული თავდასხმა ცალსახად ნეგატიურად აისახება ქვეყნის თავდაცვისუნარიანობაზე. მაგალითად, უკანასკნელი წლების განმავლობაში, ირანისა და ჩრდილოეთ კორეის მიერ ფართოდ გამოიყენებოდა თავდასხმითი კიბეროპერაციები აშშ კერძო სექტორის წინააღმდეგ საკუთარი ეკონომიკური თუ საგარეო პოლიტიკური მიზნების განსახორციელებლად.

უკანასკნელ პერიოდში მნიშვნელოვანი პროგრესი იქნა მიღწეული კიბერთავდასხმების წყაროს აღმოჩენასა და სახელმწიფოსადმი კუთვნილების დადგენაში. ამ მხრივ საქართველოს წინააღმდეგ განხორციელებულ კიბერშეტევებზეც იქნა წარმოდგენილი სარწმუნო ინფორმაცია:

- 2015 წლის 21-25 მაისს ქართულ საფინანსო ორგანიზაციებზე განხორციელდა მასიური DDoS შეტევა. სულ შეტევაში მონაწილეობდა 300 000-მდე უნიკალური IP მისამართი 160-ზე მეტი ქვეყნიდან. შეტევის მასშტაბიდან, მომზადების ხარისხიდან და რეგიონისადმი გეოპოლიტიკური ინტერესიდან გამომდინარე, უნდა ვივარაუდოთ, რომ აღნიშნული შეტევის უკან რუსეთთან დაკავშირებული ჰაკერული ჯგუფი იდგა. იმის გათვალისწინებით, რომ ასეთ

მასშტაბური შეტევა არ იყო ორიენტირებული ფინანსურ ზარალზე, დიდი ალბათობით, იგი მიზნად ისახავდა ყურადღების გადატანას სხვა, შესაძლოა უფრო მეტად ზიანის მომტანი შეტევისაგან;

- შეერთებული შტატების კიბერუსაფრთხოების სფეროში მოღვაწე ავტორიტეტულმა კომპანიამ „FireEye“ აღმოაჩინა ჰაკერული დაჯგუფება, რომელსაც დიდი ალბათობით რუსეთის ფედერაციის უშიშროების სამსახური მართავს. კომპანიის განცხადებით, ჰაკერული დაჯგუფება, რომელსაც პირობითად უწოდეს „APT28“ მიზანს კომერციული ინფორმაციის მიღება კი არა, არამედ თავდაცვისა და გეოპოლიტიკურ საკითხებზე ინფორმაციის შეგროვება წარმოადგენს, რაც მხოლოდ სახელმწიფოსათვის შეიძლებოდა ყოფილიყო საინტერესო. APT28, რომელიც სულ მცირე 2007 წლიდან არსებობს, შეტევებს ახორციელებდა რუსეთის საერთაშორისო ინტერესების შესაბამისი სადაზვერვო ინფორმაციის მოსაპოვებლად ძირითადად სამი მიმართულებით: კავკასიის რეგიონი, კერძოდ, კი საქართველო; აღმოსავლეთ ევროპის რეგიონი, კერძოდ უნგრეთი და პოლონეთი; ევროპული და ევროატლანტიკური უსაფრთხოების ორგანიზაციები: NATO და ეუთო.

მიუხედავად იდენტიფიცირების გაზრდილი შესაძლებლობისა, დღევანდელი საერთაშორისო სამართალი ვერ უზრუნველყოფს კიბერშპიონაჟისა თუ კიბერთავდასხმების ეფექტურ შემაკავებელ გარემოს. არ არსებობს კიბერსივრცეში უნივერსალურად მიღებული და სამართლებრივად სანქციერებული წესები. იმ შემთხვევაშიც, თუკი დგინდება კონკრეტული კიბერშეტევის განმახორციელებელი აქტორი, შეტევასა და თავდამსხმელის იდენტიფიცირებას შორის არსებული ხანგრძლივი პერიოდი დანაშაულის გამოძიებისათვის არახელსაყრელ გარემოს ქმნის. შემტევი ოპერაციების სიმარტივისა და ეფექტურობის გამო, კიბერშპიონაჟისა და კიბერშეტევების განხორციელების მოტივაცია მაღალია, ზოგიერთი სახელმწიფო კი მუდმივად განაგრძობს დაინტერესების ობიექტის ტექნიკური შესაძლებლობებისა თუ კიბერუსაფრთხოების მდგომარეობის ტესტირებას.

ცხადია, გარკვეულ სირთულეებთანაა დაკავშირებული საფრთხის წარმომავლობის ქვეყნებში სახელმწიფო და არასახელმწიფო აქტორებს შორის მკვეთრი ზღვარის გავლება, მითუმეტეს, როდესაც სახეზეა მათი აქტიური თანამშრომლობა და ურთიერთქმედება მაგალითად იგივე რუსეთის შემთხვევაში. ხშირია პრაქტიკა, როდესაც სხვა ქვეყნისთვის ზიანის მომტანი კრიმინალური ქმედებები წარმომავლობის ქვეყნის სამართალდამცავი ორგანოებისათვის "შეუმჩნეველი'' რჩება ან უფრო მეტიც, არსებობს პირდაპირი ნიშნები "სახელმწიფო ხელშეწყობისა" (მაგ. "კიბერბერკუტი", საქართველოს წინააღმდეგ 2012-14 წლებში განხორციელებული კიბერშპიონაჟის ფაქტები, პოლონეთის, უკრაინის წინააღმდეგ მიმართული კიბერშეტევები 2014 წელს და სხვა).

საქართველოს კიბერსივრცისთვის საფრთხის შემცველი აქტორები

კიბერელემენტების გამოყენება პოლიტიკური, ეკონომიკური თუ სამხედრო მიზნების მისაღწევად, გეოპლიტიკური უპირატესობის მოსაპოვებლად, თანამედროვე მსოფლიოს რეალობაა. დასავლელი ექსპერტები სულ უფრო ხშირად მსჯელობენ იმ ტენდენციაზე, რომელიც კიბერომის ქსელურ ომად გარდაქმნას ახლავს თან. კიბერომი ინფორმაციული და საკომუნიკაციო სისტემების განადგურებისაკენ მიმართული ქმედებაა, მაშინ, როდესაც ქსელური ომი არის განზრახ ქმედება, რომელიც გულისხმობს ერთი ან რამდენიმე აქტორის მცდელობას, ღია ან ფარული არხების მეშვეობით იმგვარად შეცვალოს სამიზნე აქტორის აღქმა, რომ ამ ცვლილებამ შემდგომში შემტევისათვის სასურველი შედეგი მოიტანოს.

გამონაკლისს ამ მხრივ არც საქართველოს კიბერსივრცე წარმოადგენს. უკანასკნელი წლების პოსტსაბჭოთა სივრცეში მიმდინარე კონფლიქტები ცხადყოფს, რომ პოლიტიკურად მოტივირებული კიბერშეტევები საქართველოსთვისაც აქტუალურია. გარდა ეროვნული მნიშვნელობის კრიტიკული ინფრასტრუქტურისა, ანტიტერორისტული კოალიციის აქტიური წევრობისა და ქვეყნის მკაფიოდ გამოხატული ევროატლანტიკური ვექტორის გათვალისწინებით, დამატებით სამიზნეს წარმოადგენს საქართველოში არსებული სხვა ქვეყნების, საერთაშორისო

ორგანიზაციების და საზღვარგარეთული კომერციული სტრუქტურების საინფორმაციო ქსელები და ინფრასტრუქტურა.

ჩამოთვლილ ობიექტების მიმართ საფრთხე შესაძლოა მომდინარეობდეს ისეთი აქტორებისაგან, როგორიცაა:

- მაღალგანვითარებული კიბერშეტევითი პოტენციალის მქონე ქვეყნები (რუსეთი, ჩინეთი, ირანი);
- ტერორისტული ორგანიზაციების კიბერდანაყოფები და იდეოლოგიურად მოტივირებული ან ექსტრემისტულად განწყობილი ჰაკერები;
- ფინანსურად მოტივირებული კიბერდამნაშავეები.

განვიხილოთ თითოეული ჯგუფის ცალკეული აქტორები, რომელთა შესაძლებლობების შესწავლა საქართველოსთვის აქტუალურია.

<u>რუსეთის ფედერაცია</u>

რუსეთის თავდაცვის სამინისტრო აყალიბებს საკუთარ კიბერსარდლობას, რომელიც, არსებული ინფორმაციით, პასუხისმგებელი იქნება შემტევი კიბერღონისძიებების ჩატარებაზე, მათ შორის პროპაგანდაზე ორიენტირებულ ქმედებებზე და მოწინააღმდეგის მართვისა და კონტროლის სისტემებში მავნებელი პროგრამული უზრუნველყოფის ჩანერგვაზე.

რუსეთის შეიარაღებულ ძალებში ყალიბდება კომპიუტერული ქსელების ოპერაციებზე სპეციალიზირებული სხვა დანაყოფებიც. გავრცელებული ინფორმაციით, რუსეთი აქტიურად ავითარებს კრიტიკული ინფრასტრუქტურის საწარმოო პროცესის კონტროლის სისტემებზე (industrial control systems - ICS) დისტანციური წვდომის საშუალებებს. ექსპერტთა მონაცემებით, უცნობმა რუსმა აქტორებმა წარმატებულად განახორციელეს რამდენიმე ICS მწარმოებლის პროგრამის დაზიანება და ლეგალური პროგრამული უზრუნველყოფის განახლებებში მავნე პროგრამული კოდის ჩანერგვა და ამ გზით მომხმარებლის ვებგვარდთან პირდაპირი წვდომის დამყარება.

დღესდღეობით, ეჭვს აღარ იწვევს ის გარემოება, რომ რუსეთის ხელისუფლება პოლიტიკური მიზნებისთვის აქტიურად იყენებს ე.წ. ინფორმაციულ-ფსიქოლოგიური ზემოქმედების მეთოდს, რომელსაც, დასავლელი მკვლევარები ახასიათებენ, როგორც თანამედროვე რუსული კონფლიქტის წარმოების საწყის ფაზას. აღნიშნული ფაზა მოიცავს არაკონვენციური ოპერაციების ჩატარებას საზოგადოებრივი აზრის მანიპულირების მიზნით ქვეყნის შიგნით, სამიზნე ქვეყანაში და საერთაშორისო მედიაში. ინტენსიური აქტიური რონისძიებების ფონზე რუსული საბრძოლო დანაყოფები იწყებენ სამიზნე ტერიტორიაზე შეღწევას ადგილობრივი შეიარაღებული ფორმირებების საფარქვეშ. ამით სრულდება არაკონვენციური ოპერაციების ფაზა. თუ ოპერაცია წარმატებული აღმოჩნდა, იწყება ინტერვენციის ლეგიტიმაციისაკენ მიმართული ღონისძიებები „უმცირესობის უფლებათა დაცვის“ ლეგენდით. მეორე ფაზა უკვე კონვენციურ ქმედებებს გულისხმობს, თუმცა ყირიმის ანექსიის პირველი, არაკონვენციური ფაზის წარმატებამ ძალზედ გაამარტივა კონფლიქტის კონვენციური ფაზა რუსეთის სასარგებლოდ.

რუსეთის პოლიტიკური ელიტა ინფორმაციას განიხილავს როგორც ძალაუფლების წყაროს, რაც ქმნის მყარ საფუძველს ქვეყნის მიერ ინფორმაციული ოპერაციების განსახორციელებლად. ეროვნული უსაფრთხოების კონცეფციის თანახმად, რუსეთი საფრთხედ მიიჩნევს ნაციონალისტურ, სეპარატისტულ და რადიკალურ რელიგიურ სააგიტაციო ღონისძიებებს და მათთან გასამკლავებლად საჭიროდ მიიჩნევს „ჭეშმარიტი“ ინფორმაციის გავრცელებას და ადგილობრივი პლატფორმის განვითარებას (მაგ. საკუთარი სოციალური მედია). ამავე დოკუმენტში სამომავლო საფრთხეების ანალიზისას აღნიშნულია, რომ „გლობალური საინფორმაციო ბრძოლა კიდევ უფრო გააქტიურდება". აქედან გამომდინარე, კომპიუტერული ქსელური ოპერაციები განიხილება როგორც ინფორმაციული უსაფრთხოების ორგანული, უცვლელი ნაწილი. რუსეთი ცდილობს დაამუშავოს ინფორმაციის არა მხოლოდ ტექნიკური მხარე, არამედ მიაღწიოს ინფორმაციის შემეცნებითი მდგენელის კონტროლსაც. სწორედ ამიტომ, ექსპერტთა მოსაზრებით, აპრობირებული ცნება „კიბერუსაფრთხოება“ რუსულ

დოქტრინებსა და კონცეპტუალურ დოკუმენტებში ჩანაცვლებულია ტერმინით „ინფორმაციული უსაფრთხოება“.

თუკი პოსტსაბჭოთა საივრცეში რუსეთის მონაწილეობით მიმდინარე კონფლიქტებს გავაანალიზებთ, ცხადი ხდება, რომ იგი კონფლიქტის ტერიტორიებს განიხილავს, როგორც შეიარაღების კინეტიკური სახეობების, ასევე კიბერშეტევითი პოტენციალის გამოსაცდელ ერთგავრ პოლიგონად. ამდენად, საქართველოსთვის სასიცოცხლოდ აუცილებელია რუსეთის კიბერღონისძიებებისა და საინფორმაციო ომის ერთობლიობის დეტალური ანალიზი და წარმოშობილი რისკების ეფექტური მართვა. გასათვალისწინებელია, რომ თუნდაც ტექნოლოგიურად ნაკლებად განვითარებული შეტევები, როგორიცაა მაგალითად „DDoS“ -შეტევა ან ვებ-გვერდების ე.წ „defacement“-ი როგორც წესი რუსეთის მიერ წარმოებული კიბერ-საინფორმაციო ომის ნაწილად უნდა ჩაითვალოს.

<u>ჩინეთი</u>

გავრცელებული მონაცემებით, ჩინეთის კიბეროპერაციები ძირითადად კომერციულ მიზნებს ემსახურება და, შესაბამისად, საქართველოსთვის პირდაპირი საფრთხის შემცველი არ არის, თუმცა არ უნდა გამოგვრჩეს ჩვენს ქვეყანაში არსებული განვითარებული ქვეყნების სამთავრობო თუ კომერციული სტრუქტურების ქსელები და მათ მონაცემთა ბაზებში არსებული ინფორმაცია.

მიუხედავად კიბერსეფროში თანამშრომლობის შესახებ გაფორმებული მემორანდუმისა, ჩინეთის კიბერშპიონაჟის მთავარ სამიზნედ კვლავ რჩება აშშ. დაინტერესების საკითხების სპექტრი ფართოა, ეროვნულ უსაფრთხოებასთან დაკავშირებული ინფორმაციით დაწყებული, სენსიტიური ეკონომიკური მონაცემებითა და აშშ 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.

ირანის ისლამური რესპუბლიკა

ჩინეთისა და რუსეთისგან განსხვავებით, ირანი ჰაკერებს ძირითადად რელიგიურ იდეოლოგიაზე დაყრდნობით ამზადებს. კერძოდ, ირანმა ბოლო ხუთი წლის განმავლობაში ათასამდე ჰაკერი ფუნდამენტალური რელიგიური პათოსის გავლენით მოამზადა. მათი მიზანია იდეოლოგიური მოწინააღმდგის კრიტიკული ინფრასტრუქტურის განადგურება. ირანი პასუხისმგებელია 2012-2013 წლების აშშ ფინანსურ ინსტიტუტებზე განხორციელებულ DDoS შეტევებსა და 2014 წლის თებერვალში Las Vegas Sands კაზინოზე განხორციელებულ თავდასხმაში. აშშ სადაზვევრო თანამეგობრობის მონაცემებით, ირანი საკუთარ კიბერპროგრამას განიხილავს, როგორც პოლიტიკური მოწინააღმდეგეების წინააღმდეგ ასიმეტრიული, მაგრამ პროპორციული ქმედებების წარმოებისა და სადაზვერვო ინფორმაციის მოძიების საშუალებას. ის ფაქტი, რომ აშშ აპირებს ირანისათვის დაწესებული სანქციების შემსუბუქებას და მის დაბრუნებას ნავთობის საერთაშორისო ბაზარზე, არ გამოიწვევს კიბერსივრცეში დასავლეთთან და ისრაელთან დაპირისპირების შემცირებას. ავტორიტეტული ამერიკელი ექსპერტების შეფასებით, ირანი კიბერშეტევებს აუცილებლად გაზრდის, მიუხედავად იმისა, იქნება თუ არა სანქციები. უფრო მეტიც, სანქციების შემსუბუქების შემთხვევაში ირანი შეძლებს ფინანსური საშუალებების მობილიზებასა და მიმართვას თავისი კიბერშესაძლებლობების განვითარებისთვის, რაც თავისთავად გამოიწვევს ჰაკერული დაჯგუფებების კვალიფიკაციის ზრდასა და მათი მოქმედების მეთოდების დახვეწას. 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 მიერ ქართული კიბერქსელების პროპაგანდისტული მიზნებით გამოყენება.

მოგებაზე ორიენტირებული კრიმინალური აქტორები

მოგებაზე ორიენტირებული კიბერ დამნაშავეების ძირითადი დასაყრდენი იმპროვიზირებული ელეტრონული ბაზრებია, რომლებიც თავისი არსით წარმოადგენენ ფორუმს არალეგალური სერვისების, ინფრასტრუქტურის, მოპარული პერსონალური ინფორმაციისა და ფინანსური მონაცემების შესყიდვისთვის.

კიბერდამნაშავეები წარმატებით ახორციელებენ საცალო ბიზნესისა და ფინანასური ინსტიტუტების ქსელებში შეღწევას, რათა მოიპოვონ ფინანსური ინფორმაცია, პერსონალური მონაცემები, საცხოვრებელი თუ ელ. ფოსტის მისამართები და სამედიცინო ჩანაწერები, რაც წარმოადგენს საბაზისო ინფორმაციას კრიმინალური ოპერაციებისათვის. თავდაცვის სექტორისთვის ამ მხრივ მნიშვნელოვანია კრიტიკული სერვისების პროვაიდერებში არსებული მონაცემთა ის ბაზები, სადაც, გარდა პერსონალურისა კონცენტრირებულია ინფორმაცია ქვეყნის თავდაცვისუნარიანობის შესახებ. აუცილებელია აღინიშნოს, რომ თანამედროვე ქვეყნებში კრიტიკული ინფრასტრუქტურის დიდი ნაწილი კერძო სექტორშია კონცენტრირებული, რაც კიდევ ერთხელ ადასტურებს კიბერუსაფრთხოების სფეროში კერძო და საჯარო სექტორის თანამშრომლობის გარდაუვალობას.

უკანასკნელ პერიოდში კიბერკრიმინალის წინააღმდეგ ბრძოლის წარმატებულ მაგალითად უნდა ჩაითვალოს აშშ და გერმანიის სპეცსამსახურების ერთობლივი ოპერაცია ერქან ფინდიკოღლუს (Ercan Findikoglu) - თურქეთის მოქალაქის, ექსტრადირების მიზნით. ეს უკანასკნელი იმხილება 2011-2013 წ. ჩადენილ კიბერდანაშაულებში, რომელთა შედეგადაც აშშ საფინანსო სექტორიდან მოპარულ იქნა 55 მილიონი აშშ დოლარი. ფინდიკოღლუ დაკავებულ იქნა გერმანული ფედერალური პოლიციის მიერ 2013 წლის დეკემბერში, აშშ საიდუმლო სამსახურის ინფორმაციის საფუძველზე. ასევე მნიშვნელოვანი წარმატებას მიაღწია 2015 წელს 20 ქვეყნისაგან შემდგარმა საერთაშორისო კოალიციამ FBI-ს მეთურობით, რომელმაც დაშალა ელექტრონული კრიმინალური ფორუმი - Darkode. აშშ იუსტიციის დეპარტამენტის ცნობით, აღნიშნული ფორუმი წარმოადგენდა ერთ-ერთ ყველაზე სერიოზულ საფრთხეს

მსოფლიოს მოწინავე ქვეყნების საინფორმაციო სისტემებში არსებული მონაცემების მთლიანობისთვის.

ტერორისტული ორგანიზაციების კიბერდანაყოფები

ტერორისტული დაჯგუფების ან ექსტრემისტულად განწყობილ პირთა მიერ კომპიუტერული ქსელებისა და ელექტრონული სერვისების კონფიდენციალურობაზე, ერთიანობასა და ხელმისაწვდომობაზე ზემოქმედებისკენ მიმართული შეტევები ძირითადად მოიცავს კომპიუტერულ ქსელების დაზიანების, სერვისის შეფერხების და კომპიუტერული ქსელის ან არასანქცირებული წვდომის შედეგად ქსელიდან მიღებული ინფორმაციის ტერორისტული მიზნებით გამოყენების მცდელობებს.

არსებული ვითარების შეფასებით, ტერორისტული დაჯგუფებები დღესდღეობით არ ფლობენ მნიშვნელოვანი ზიანის გამოსაწვევად საკმარის კიბერსაშუალებებს. მსოფლიოში ყველაზე ხშირად განხორციელებული კიბერტერორისტული შეტევის ფორმა არის დაუცველი ვებ-გვერდებისა და სოციალური მედიისათვის ზიანის მიყენება. ცხადია, ამ მხრივ გამონაკლისს არც ჩვენი ქვეყანა წარმოადგენს. საქართველოს კიბერსივრცეში ვებ-გვერდების დაზიანების მიზნით განხორციელებული ე.წ. Defacement შეტევების სამიზნეს ძირითადად შედარებით მოწყვლადი, სუსტად დაცული ვებ-გვერდები წარმოადგენს. როგორც წესი, აღნიშნული სახის შეტევა მხოლოდ მცირე შეფერხებებს იწვევს.

სუსტად დაცული ვებ-გვერდების დაზიანების სიმარტივის არასწორად აღქმის გამო, ტერორისტული ორგანიზაციების კიბერშესაძლებლობები მედიის და საზოგადოების მხრიდან ხშირად გადაჭარბებულადაა შეფასებული. მითუმეტეს, საქართველოში დაუცველი ვებ-გვერდების რაოდენობა კერძო სექტორსა თუ სახელმწიფო დაწესებულებებში დიდია ერთის მხრივ ცნობიერების არასათანადო დონისა და მეორეს მხრივ, არასაკმარისი ფინანსური რესურსის გამო. აღნიშნულ ტენდენციას ხელს უწყობს საკუთარი კიბერშესაძლებლობების გაზვიადება ექსტრემისტულად განწყობილი ჰაკერების მხრიდან რეპუტაციის ამაღლებისა თუ ფსიქოლოგიური ზემოქმედების მიზნით. უკანასკნელ პერიოდში ღია წყაროებში გაჩნდა

არაერთი ტექნიკური დადასტურება გაჩნდა იმისა, რომ კიბერტერორისტების მიერ განხორციელებული ყველაზე რეზონანსული თავდასხმა ფრანგულ სამაუწყებლო კომპანია - TV5Monde-ზე რუსეთის სახელმწიფოს მიერ მხარდაჭერილი კიბერშეტევას წარმოადგენდა “Cyber Chaliphate”-ს ლეგენდით. აღნიშნულ მოსაზრებას ამყარებს კიბერშეტევის ხელწერა და მავნე კოდებში კირილიცის ელემენტების შემცველობა, რომელიც რუსულ, მთავრობის კონტროლქვეშ მოქმედ ჰაკერულ დაჯგუფება APT28-ს ხელწერის იდენტურია. აქვე გასათვალისწინებელია, რომ შეტევის დრო ემთხვევა ფრანგულ-რუსული ურთიერთობების გაუარესებას (მისტრალის საკითხი, ფ.ოლანდის უარი მოსკოვში 9 მაისის ღონისძიებებში მონაწილეობის მიღებაზე და სხვა).

მსოფლიოს მოწინავე სპეცსამსახურების ანალიზით, ახლო მომავალში, ტერორისტული დაჯგუფებები სავარაუდოდ ისევ კონვენციური შეტევებს მიანიჭებენ უპირატესობას, როგორც მნიშვნელოვანი ზიანისა თუ შიშის გამომწვევი ამ ეტაპზე მათ ხელთ არსებული ერთადერთი მექანიზმს.

ამავდროულად, უნდა აღინიშნოს, რომ ექსტრემისტთა მეტად კომპიუტერიზებული თაობის და რამდენიმე წარმატებული კიბერშეტევის ფონზე, კიბერტერორიზმის საფრთხე მზარდია; ასევე, რეალურია კიბერსივრცის გამოყენება ტერორისტული ორგანიზაციების მხრივ სადაზვერვო ინფორმაციის მოპოვების, ფინანსური თაღლითობის, პროპაგანდისტული მიზნების ან რეკრუტის განხორციელების მიზნით.

ზემოთქმულის ნათელი მაგალითია ახლო წარსულში დაწყებული მასშტაბური, მრავალპლატფორმიანი კამპანია სოციალურ ქსელებში, რომელსაც ათასობით ონლაინ მხარდამჭერი მიუერთდა მსოფლიოში და საქართველოშიც. სოციალური მედია საშუალებას იძლევა გავრცელდეს პროპაგანდა მაქსიმალურად ფართო მასებში და მოზიდულ იქნას ახალი წევრები ტერორისტული საქმიანობისათვის.

ტერორისტული ორგანიზაციების მხრიდან უახლოეს პერიოდში მოსალოდნელი შეტევები ძირითადად ვებ-გვერდების დაზიანებითა და სერვისების გათიშვით შემოიფარგლება. უპირველეს ყოვლისა ასეთი სეტევები ხორციელდება

ანტიტერორისტული კოალიციის წევრი ქვეყნების საქართველოში განთავსებულ ინფრასტრუქტურაზე (ბიზნესი, დიპლომატიური წარმომადგენლობები და სხვა), რომელთა ზოგიერთი პროდუქტიც, სავსებით შესაძლებელია საქართველოს თავდაცვის სექტორისათვის კრიტიკულ სერვისს წარმოადგენდეს. აღნიშნულ მოსაზრებას ადასტურებს სუპერმარკეტ კარფურის ქსელზე განხორციელებული კიბერშეტევა, რომელიც „Charlie Hebdo“-ს მოვლენების გამოძახილი იყო საქართველოში. ეს შეტევა მნიშვნელოვანი ზიანის გარეშე იქნა დაძლეული, თუმცა დაუცველ ან სუსტად დაცულ მნიშვნელოვან ობიექტზე ასეთი მარტივი თავდასხმაც კი შესაძლოა არაპროპორციული ზიანის მომტანი იყოს სახელმწიფოსთვის.

გაცილებით სერიოზული იქნება საფრთხე, თუკი თავიანთი კიბერშესაძლებლობების არსებითად გასაუმჯობესებლად, ტერორისტული ორგანიზაციები ითანამშრომლებენ რომელიმე განვითარებული კიბერშესაძლებლობების მქონე სახელმწიფოსთან, ელიტარულ კრიმინალურ ჰაკერებთან ან მოახდენენ სპეციალისტების რეკრუტირებას. თუმცა, ტერორისტულ ორგანიზაციასთან თანამშრომლობა სახელმწიფოთათვის პოლიტიკური რისკის შემცველია, ამასთან სახელმწიფოთა კიბერშესაძლებლობები ისედაც შეზღუდულია. ასევე, ჯერჯერობით ნაკლებად შეინიშნება ექსტრემისტებს და კრიმინალურ კიბერ აქტორებს შორის თანამშრომლობის ფაქტები.

მიუხედავად აღნიშნულისა, ტერორისტული დაჯგუფებები კვლავ განაგრძობენ კიბერშესაძლებლობების განვითარებას, რამაც შესაძლოა გაზარდოს მათგან მომდინარე საფრთხეები.

დასკვნა

ზემოთქმულიდან გამომდინარე, საქართველოს წინაშე მდგარი კიბერსაფრთხეების მასშტაბი მზარდია, როგორც სირთულის, ისე მრავალფეროვნების თვალსაზრისით. საჭიროა განსაკუთრებული ყურადღება დაეთმოს კიბერაქტორების განზრახვების, შესაძლებლობებისა თუ ღონისძიებების შესახებ ინფორმაციის

მოპოვებისა და ანალიზის მექანიზმის ჩამოყალიბებას და ამ მხრივ აქტიური მუშაობის წარმართვას.

ყველაზე რეალური საფრთხის შემცველი საქართველოს კიბერსივრიცისათვის არის რუსეთის კიბერაქტივობები, რომელიც მიმართულია როგორც კრიტიკული ინფრასტრუქტურის მოშლის, ასევე საკუთარი მიზნებისათვის გამოყენებისაკენ. ხაზგასმით უნდა აღინიშნოს, რომ ისეთი დაბალტექნოლოგიური თავდასხმებიც კი, როგორიცაა DDoS და Defacement შეტევა, სუსტად დაცული ინფრასტრუქტურის პირობებში შესაძლოა არაპროპორციული ზარალის მიზეზი გახდეს. ცალსახად უნდა აღინისნოს, რომ რუსეთის მიერ განხორციელებულმა ან მხარდაჭერილმა კიბერშეტევამ საქართველოში შესაძლოა გამოიწვიოს მნისვნელოვანი ზარალი და მსხვერპლიც კი.

რაც შეეხება ირანისა და ჩინეთის მხრიდან მომდინარე კიბერსაფრთხეებს, აქ, უპირველეს ყოვლისა, არ უნდა გამოგვრჩეს საქართველოში განთავსებული იმ სახელმწიფოების ინფრასტრუქტურა და მონაცემთა ბაზები, რომელთაც ეს ქვეყნები საკუთარ მოწინააღმდეგედ განიხილავენ. ასეთებს განეკუთვნება საქართველოს სტრატეგიული პარტნიორი აშშ, ჩრდილოატლანტიკური ალიანსისა და ევროკავშირის წევრი ქვეყნები და თავად ამ საერთაშორისო ორგანიზაცების სისტემები. ჩინეთის კიბერშეტევები ძირ

ტერორისტული ორგანიზაციების მხრიდან დიდია ალბათობა ისეთი კიბერშეტევის განხორციელებისა, რომელიც გამოიწვევს ელექტრონული სერვისების და ვებ-გვერდების დროებით, ლოკალურ დაზიანებას. მასობრივი ზიანის ან მსხვერპლის გამომწვევი კიბერშეტევის ორგანიზება და განხორციელება ამ ეტაპზე ნაკლებად სავარაუდოა.

რთულად პროგნოზირებადია მოგებაზე ორიენტირებულ კიბერდამნაშავეთაგან მომდინარე საფრთხეების ალბათობა. ამ მხრივ მეტად მნისვნელოვანია საზოგადოებრივი ცნობიერების ამაღლება, მუდმივი კონტაქტი კერძო სექტორში განთავსებულ კრიტიკულ ინფრასტრუქტურასთან, ადგილობრივი კანონმდებლობის

საერთაშორისოსთან ჰარმონიზაცია და კიბერკრიმინალთან ბრძოლის სართაშორისო თანამშრომლობის მექანიზმების აქტიური გამოყენება.

საქართველო და ახალი გამოწვევები კიბერსივრცეში

მიმდინარე წლის 13 ივნისს, თეირანში ირანსა და რუსეთს შორის მიღწეულ იქნა შეთანხმება კიბერუსაფრთხოების სფეროში თანამშრომლობის შესახებ, რომელიც ორიენტირებული იქნება მოცემულ დარგში სადაზვერვო ინფორმაციის გაცვლაზე, საფრთხეების წინააღმდეგ ურთიერთმოქმედებასა და საერთო თავდაცვაზე.

ბოლო ერთ თვეში, ეს არის რუსეთის მიერ მიღწეული თანამშრომლობის მეორე შეთანხმება. მანამდე, 8 მაისს რუსეთმა ჩინეთთან მოაწერა ხელი თანამშრომლობის თორმეტპუნქტიან ხელშეკრულებას, სადაც ერთი მოზრდილი პუნქტი დათმობილი აქვს კიბერუსაფრთხოების სფეროში ურთიერთობას.

რუსეთის მხრიდან კიბერუსაფრთხოებაში მსგავსი გააქტიურება საერთაშორისო დონეზე არის პირდაპირი პასუხი, მიმდინარე წელს შეერთებული შტატების მიერ ახალი კიბერუსაფრთხოების სტრატეგიის მიღებაზე. სტრატეგიაში პირველად იქნა დაკონკრეტებული ქვეყნები, საიდანაც შეერთებული შტატები უნდა მოელოდნენ კიბერ საფრთხეებს. ასეთ ქვეყნებად სტრატეგიაში დასახელდა რუსეთი, ჩინეთი, ირანი და ჩრდილოეთ კორეა. ამის გათვალისწინებით, კიბერუსაფრთხოების მიმართულებით, უნდა ველოდოთ რუსეთსა და ჩრდილოეთ კორეას შორის თანამშრომლობის დაწყების ახალ ეტაპს. ფაქტიურად, შეიძლება ითქვას, რომ კიბერუსაფრთხოების სფეროში იქმნება ახალი „კოალიცია“, სადაც გაერთიანებულ ქვეყნებს გააჩნიათ საერთო ინტერესები მიმართული შეერთებული შტატების, ისრაელისა და ზოგადად, დასავლეთისა და მისი მოკავშირეების წინააღმდეგ.

დარგის აღიარებული ექსპერტები მიიჩნევენ, რომ საფრთხეები ელექტრონული მმართველობის განვითარების პარალელურად, კიდევ უფრო გაიზრდება. იგივე ექსპერტები პროგნოზირებენ კიბერუსაფრთხოების ახლო მომავალს, კერძოდ, გაციფროვნების პროცესი გაგრძელდება სულ უფრო მეტი ინტენსივობით და ის შეაღწევს ჩვენი ცხოვრების ყველა ასპექტში და ჩვენი საზოგადოების ფუნქციებში.

ადამიანები სულ უფრო და უფრო დამოკიდებულები გახდებიან ციფრულ მომსახურებასა და სხვადასხვა სახის ინფორმაციულ და საკომუნიკაციო ტექნოლოგიებზე, რაც ხელს შეუწყობს საზოგადოებრიობის როგორც მოქალაქეების, ისე მედია საშუალებების ინტერესს კიბერუსაფრთხოების მიმართ. მომავალში თანამედროვე საზოგადოება გახდება სულ უფრო მოწყვლადი, რადგან რთულია ერთმანეთთან დაკავშირებული და დამოკიდებული სისტემების სრულად აღქმა და დაცვა. გაიზრდება გლობალური და შიდა საზოგადოებრივი დამოკიდებულებები, რაც კიბერუსაფრთხოების გამოწვევებს სულ უფრო გლობალურ ხასიათს აძლევს და ამდენად, არსებობს კიბერ საფრთხეებზე საერთაშორისო რეაგირების აუცილებლობა. ახალი ტექნოლოგიური ინოვაციები ძირითადად მოდის კერძო სექტორიდან და ეს პროცესი სულ უფრო მზარდი იქნება, რაც ერთი - ორად ზრდის ასევე უსაფრთხოების უზრუნველყოფის საჭიროებას. იქვე, ამის პარალელურად არის ახალი ტექნოლოგიები, რომლებიც უზრუნველყოფენ კიბერუსაფრთხოებას და მიუხედავად ამისა, კიბერ სივრცეში გაიზრდება გამალებული შეიარაღების პროცესი. კიბერდანაშაულებები კვლავ იქნება გამოწვევა საზოგადოებისთვის და ეკონომიკური დანაკარგები სულ უფრო გაიზრდება, რაც სხვა მხრივ ხელს შეუწყობს სახელმწიფოსა და კერძო სექტორს შორის თანამშრომლობის განვითარებას. კიბერ შესაძლებლობების კონცეფციას გავლენა ექნება საერთაშორისო პოლიტიკაზე და ძალაუფლებისთვის გლობალურ ბრძოლაზე, რაც ასევე შეუწყობს ხელს კიბერ სივრცეში გამალებული შეიარაღების პროცესის გაზრდის ტენდენციას. სავსებით შესაძლებელია, რომ ახლო მომავალში მოხდება გლობალური კიბერ კატასტროფა, რაც მთლიანად შეცვლის ჩვენს მიდგომას არამარტო კიბერუსაფრთხოების, არამედ მთლიანად კიბერსივრცეში საერთაშორისო თანამშრომლობის მიმართ. კიბერის ახალ ეპოქაში გამარჯვებული იქნება ის, ვინც შეძლებს საბაზრო ეკონომიკის გათვალისწინებით უსაფრთხოების საკითხების კომპლექსურ გადაწყვეტას; გააჩნიათ საუკეთესო ტალანტების მობილიზების შესაძლებლობა; და შესწევთ ადაპტაციის უნარი და ყოველგვარი ძალისხმევის გარეშე იმუშაონ მრავალეროვან გარემოში.

ფაქტიურად, კიბერუსაფრთხოება გახდა საგარეო პოლიტიკის შემადგენელი ნაწილი და ის სულ უფრო აქტიურ როლს თამაშობს საერთაშორისო ურთიერთობების საკითხში. საინტერესოა ამ მხრივ რა მდგომარეობაა საქართველოში?

უკვე 2008 წლის აგვისტოს ომის შემდეგ, როცა რუსეთის მხრიდან მოხდა მასირებული კიბერ შეტევა ქვეყნის ინფრასტრუქტურაზე, სამთავრობო ვებ-გვერდებზე. ქვეყანა დადგა სერიოზული პრობლემის წინაშე, იყო საფრთხე, რომ საქართველო მოქცეულიყო ინფორმაციულ ვაკუუმში. მიღებული ცუდი გამოცდილების გათვალისწინებით, ხელისუფლებამ დაიწყო კიბერუსაფრთხოების სფეროს განვითარებაზე ფიქრი. კერძოდ, იუსტიციის სამინისტროში შეიქმნა სსიპ - მონაცემთა დაცვის სააგენტო, განისაზღვრა კრიტიკული ინფორმაციული ინფრასტრუქტურის სუბიექტები, რომელთა დაცვა დაევალა მონაცემთა გაცვლის სააგენტოს, შეიქმნა კანონი „ინფორმაციული უსაფრთხოების შესახებ“ და „კიბერუსაფრთხოების სტრატეგია“, ასევე თავდაცვის სამინისტროში ახალი შექმნილია სსიპ - კიბერუსაფრთხოების ბიურო, რომელიც პასუხისმგებელია თავდაცვის სფეროში კიბერუსაფრთხოებითი ღონისძიებების გატარებაზე. ასევე შინაგან საქმეთა სამინისტროს ცენტრალური კრიმინალური პოლიციის დეპარტამენტში არსებობს კიბერდანაშაულთან ბრძოლის სამმართველო, და ბოლოს რაც ასევე მნიშვნელოვანია შეიქმნა კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელი მთავარი დოკუმენტი – საქართველოს კიბერუსაფრთხოების 2013-2015 წლების სტრატეგია. აქვე შეიძლება ავღნიშნოთ ორგანიზაცია „გრენას“ დადებითი როლი და საქმიანობა ამ მიმართულებით.

მიუხედავად ამისა, კიბერუსაფრთხოების სფეროს მიმართულებით ქვეყანაში არსებობს სერიოზული პრობლემები, რაც პირველ რიგში უკავშირდება საჭირო საკანონმდებლო ბაზის არ არსებობას, რომელიც დაარეგულირებს უკვე არსებული თითოეული სუბიექტის - მონაცემთა გაცვლის სააგენტოს, კიბერუსაფრთხოების ბიუროსა და შსს კიბერდანაშაულთან ბრძოლის სამმართველოს ურთიერთკოორდინირებულ საქმიანობას, განსაზღვრავს თითოეული სუბიექტის მოქმედების ფარგლებსა და დამატებით ვალდებულებებს, ასევე რაც ყველაზე

მნიშვნელოვანია კანონმდებლობაში უნდა იყოს განსაზღვრული კერძო სექტორის, ინტერნეტ მომწოდებლების ვალდებულებები და მათთან ყველა ზემოთნახსენები სახელმწიფო სუბიექტის კოორდინირებული მუშაობის კონკრეტული ასპექტები. სხვათა შორის, მოცემულ დარგში სახელმწიფოსა და კერძო სექტორს შორის მუშაობა წარმოადგენს დიდ პრობლემას არა მარტო ჩვენთან, არამედ ბევრ წამყვან ქვეყანაში. სახელმწიფოსა და კერძო სექტორს შორის თანამშრომლობა აუცილებელი პირობაა კიბერ სივრცის დაცვის უზრუნველყოფისთვის. ერთის მხრივ სახელმწიფო ეროვნული უსაფრთხოების უზრუნველყოფიდან გამომდინარე, ვალდებულია დაიცვას ქვეყნის მთლიანი ინფრასტრუქტურა არასანქცირებული შეღწევისგან, მაგრამ არ ფლობს ყველა საჭირო რესურსს, ვინაიდან რესურსის დიდი ნაწილი არის კერძო სექტორის მფლობელობაში. ეს საბაზრო ეკონომიკის პირობებში ნორმალური და აუცილებელი მოვლენაა. მეორეს მხრივ, კერძო სექტორს არ გააჩნია არავითარი სამართლებრივი ვალდებულებები ითანამშრომლოს სახელმწიფოსთან და გამოაყენებინოს მის ხელთ არსებული რესურსი. აქ ისევ და ისევ მივდივართ საჭირო საკანონმდებლო ბაზის არარსებობის პრობლემასთან და შესაბამისად არც კერძო სექტორს არ გააჩნია არავითარი ვალდებულებები. აქ ძირითადად საუბარია ინტერნეტ პროვაიდერებზე, რომელთა მფლობელობაშიც არის ქსელები, რომლებიც თავის მხრივ ინტერნეტით უზრუნველყოფენ სამთავრობო სტრუქტურებს, სტრატეგიული დანიშნულების ობიექტებს, კერძო მომხმარებლებს, სამრეწველო ობიექტებსა და მსხვილ კომპანიებს, მათშორის მსხვილ ბანკებს, დიპლომატიურ და სხვა უცხოურ მისიებსა თუ წარმომადგენლობებს.

ასევე დიდი მნიშვნელობა ენიჭება საზოგადოების ცნობადობის ამაღლებასა და დარგის აკადემიურ დონეზე განვითარებას, რაც ჩვენთან ფაქტიურად არ ხორციელდება. საზოგადოების ცნობადობის ამაღლება და დარგის აკადემიურ დონეზე განვითარება, რაც ასევე გულისხმობს სამეცნიერო-კვლევითი და ანალიტიკური საქმიანობის წარმოებას, გაცილებით ამცირებს კიბერსივრციდან მომდინარე საფრთხეებს. აქვე ცალკე გამოვყოფდი საჭირო პროფესიული კადრებისა და სპეციალისტების არარსებობას. მაგალითად, ქვეყანას არ ჰყავს კიბერ-ანალიტიკოსები, არ არის კიბერ სამართლის

დარგის სპეციალისტები, არ გვყავს კრიპტოგრაფები, რაც კიბერ თავდაცვითი საქმიანობის განვითარებისთვის აუცილებელ პირობას წარმოადგენს.

მსოფლიო საზოგადოება დადგა ახალი კიბერ საფრთხის წინაშე, რაც მომდინარეობს ისლამური ჰაკერული ჯგუფებიდან და დაჯგუფებებიდან. უახლოეს მომავალში იგივე საფრთხის წინაშე აღმოჩნდება საქართველოც, რომლის საგარეო პოლიტიკა მიმართულია ევროპულ ინსტიტუტებში ინტეგრაციისკენ, ქვეყანა უნდა გახდეს ევროკავშირისა და ჩრდილოეთ ატლანტიკური ალიანსის წევრი, საქართველომ ხელი მოაწერა ევროპასთან ასოცირების ხელშეკრულებას, სადაც ერთერთ პუნქტად ჩადებულია უსაფრთხოების საკითხების უზრუნველყოფა. ყოველივე ეს გამოიწვევს, ქვეყანაში დასავლური კომპანიების, ახალი მისიებისა და წარმომადგენლობითი ოფისების გახსნას. ეს პროცესი სულ უფრო გაიზრდება, რაც თავის მხრივ, ჩვენი ქვეყნის მიმართ კიდევ უფრო ზრდის საფრთხეებს ისლამური ფუნდამენტალიზმის მხრიდან, რის პარალელურადაც იზრდება კიბერ საფრთხეებიც. მაგალითისთვის, 2015 წლის იანვარიდან დღემდე განხორციელდა რამოდენიმე კიბერშეტევა, რომელიც მოდიოდა ისლამური ჰაკერული დაჯგუფებებისგან. აქ აღსანიშნავია მიმდინარე წლის 10 იანვარს ფრანგულ კომპანია "კარფურის" საქართველოს ფილიალის ვებ-გვერდზე განხორციელებულ კიბერ შეტევას, რომელიც განახორციელა "ახლო აღმოსავლეთის კიბერ არმიამ". სხვათა შორის, იმ პერიოდში განხორციელდა საკმაოდ მასიური კიბერ შეტევა ფრანგულ კომპანიებსა და მათ წარმომადგენლობით ოფისებზე მთელს მსოფლიოში, სადაც ასევე ფიგურირებდა "კარფურის" საქართველოს ფილიალი. ეს ფაქტი ყურადღებას იმსახურებს და ის უნდა განვიხილოთ, როგორც პრეცედენტი ჩვენი ქვეყნისთვის, რომელსაც მომავალშიც ექნება ადგილი, და ეს არ შემცირდება, პირიქით უფრო გაიზრდება. ასევე ამა წლის 16 აპრილს ისლამური ჰაკერული დაჯგუფება "ელ მოჰაჯირის" მიერ განხორციელდა თავდასხმა "საქართველოს მოსამართლეთა ერთობის" ვებ-გვერდზე.

გარდა ამისა, დასავლეთის პრესა და ექსპერტები სულ უფრო ხშირად წერენ, რომ რუსეთი "ჰიბრიდული ომების" შემადგენელი ელემენტების გამოყენებას, უკრაინის

შემდეგ იწყებს ბალტიისპირეთის ქვეყნებისა და პოლონეთის წინააღმდეგ. აქ საუბარია მიზანმიმართულ კიბერ შეტევებსა და "საინფორმაციო ომზე". არ უნდა გამოვრიცხოთ ასევე ახლო მომავალში მსგავსი ქმედებები საქართველოს წინააღმდეგ, თუმცა მანამდე ჩვენი ქვეყნის მიმართ განხორციელდა სხვა კიბერ შეტევები. მაგალითისთვის, ამერიკული ავტორიტეტული ორგანიზაცია "FireEye"-ს კვლევისა და ანალიზის მიხედვით, 2008 – 2014 წლებში რუსეთის მხრიდან მუდმივად ხორციელდებოდა კიბერ შეტევები, რომელთა ობიექტები იყო საქართველოს საგარეო და შინაგან საქმეთა და თავდაცვის სამინისტროები, ასევე სხვადასხვა საინფორმაციო სააგენტოები. კიბერ შეტევების ხასიათი იყო ჯაშუშური და მიზნად ისახავდა დასავლურ ინსტიტუტებთან დაკავშირებით ქვეყნის მიზნებისა და ამოცანების შესახებ ინფორმაციის მოპარვას.

კიბერუსაფრთხოების ელემენტების განხილვა უნდა მოხდეს ეროვნული უსაფრთხოების დონეზე, მიმდინარე და ახალი საფრთხეები აუცილებლად გათვალისწინებული და ასახული უნდა იყოს ეროვნული უსაფრთხოების კონცეფციაში.

რეკომენდირებული ლიტერატურა

1) Cybersecurity and Cyberwar: What Everyone Needs to Know®, *by P.W. Singer, Allan Friedman*, January 3, 2014;
2) The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, *by Jason Andress*, June 10, 2011;
3) The Hacker Playbook: Practical Guide To Penetration Testing, *by Peter Kim*, March 13, 2014;
4) Cyber Security Principles: Mobile Devices - Security Hazards and Threats - 2nd Edition, *by Walter Spivak*, Mar 27, 2015;
5) Cyber War: The Next Threat to National Security and What to Do About It, *by Richard A. Clarke*, April 10, 2012;
6) Cyber Warfare: A Multidisciplinary Analysis (Routledge Studies in Conflict, Security and Technology), *by James A. Green*, April 21, 2015;
7) The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice, *by Steve Winterfeld and Jason Andress*, Nov 30, 2012;
8) Cyber Warfare: "A New DoD Core Mission Area" (Defense), *by Joint Forces Staff College*, August 5, 2014;
9) International Cyber Incidents: Legal Considerations, *by Eneken Tikk, Kadri Kaska, Liis Vihul*, 2010;
10) Information Security Management Handbook, Sixth Edition, Volume 7, *by Richard O'Hanley, James S. Tiller*, August 29, 2013;
11) The Quick Guide to Cloud Computing and Cyber Security, *by Marcia R.T. Pistorious*, Dec 17, 2012;
12) Windows Cyber Security 101: The Beginner's Guide To Hacking: Hacking Essentials You Must Know, *by Irwin Starr*, Jun 18, 2015;
13) Essentials of Cyber Security, *by Dr Gurpreet S Dhillon*, May 14, 2014;
14) Cyber Fraud: The Web of Lies, *by Bryan Seely and Jonathan David Chicquette*, Jul 15, 2015;

15) Cyber Nation: How Venture Capital & Startups Are Protecting America from Cyber Criminals, Threats and Cyber Attacks, *by Ross Blankenship*, Jul 9, 2015;

16) CYBER WARFARE: Targeted Assured Destruction (We the people...), *by John F. Harnish*, Dec 23, 2014;

17) CyberWar Vengeance, *by T.B. Giboney*, Jan 19, 2014;

18) Cyber Security: Analytics, Technology and Automation (Intelligent Systems, Control and Automation: Science and..., *by Martti Lehto and Pekka Neittaanmäki*, May 31, 2015;

19) End Code (The NextWorld Series Book 3), *by Jaron Lee Knuth*, Aug 1, 2015;

20) Threat Modeling: Designing for Security, *by* Adam Shostack, Feb 17, 2014;

21) Cyber Security, *by Edward Amoroso*, Sep 27, 2006;

22) Inside the Black Box: Data, Metadata, and Cyber Attacks, *by Lance Nevin*, Jun 21, 2015;

23) Data-Driven Security: Analysis, Visualization and Dashboards, *by Jay Jacobs and Bob Rudis*, Feb 24, 2014;

24) Cyberpower and National Security (National Defense University), *by Franklin Kramer*, Apr 1, 2009;

25) The Legal Challenges of Cyber Security, *by Tilahun Mishago*, Mar 11, 2013;

26) Cyber Warfare, Second Edition: Techniques, Tactics and Tools for Security Practitioners, *by Jason Andress and Steve Winterfeld*, Oct 30, 2013;

27) Cyber-Physical Attacks: A Growing Invisible Threat, *by George Loukas*, Jun 18, 2015;

28) The Cyber Threat, *by Bob Gourley*, Sep 3, 2014;

29) @War: The Rise of the Military-Internet Complex, *by Shane Harris*, Nov 11, 2014;

30) Cyber Security Policy Guidebook, *by Jennifer L. Bayuk and Jason Healey*, Apr 24, 2012;

31) Cyber Security and IT Infrastructure Protection, *by John R. Vacca*, Sep 9, 2013;

32) Cyber Security Management: A Governance, Risk and Compliance Framework, *by Peter Trim and Yang-im Lee*, Sep 28, 2014;

33) Cyber War versus Cyber Realities: Cyber Conflict in the International System, *by Brandon Valeriano and Ryan C. Maness*, May 26, 2015;

34) Cyber Security and Cyber Warfare: 11 Facts You Need to Know, *by Garrett Singapore*, Nov 15, 2014.