ვლადიმერ სვანაძე

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.

თუმცა ამავდროულად, ირანის მთავარი სამიზნე არის დასავლეთი, შეერთებული შტატები და ისრაელი. მას ასევე გააჩნია თავისი მუდმივი ისტორიული ინტერესები კავკასიაში. ირანი წარმოადგენს რუსეთის სტრატეგიულ პარტნიორს და ისინი აქტიურად თანამშრომლობენ ბირთვულ საკითხებში, რაც თავის მხრივ დიდ უკმაყოფილებას იწვევს შეერთებულ შტატებსა და ევროკავშირში. აქვე თუ გავითვალისწინებთ იმ რეალობას, რომ საქართველო აქტიურად მიისწრაფვის ევროატლანტიკურ ინსტიტუტებში ინტეგრაციისკენ და ადრე თუ გვიან ქვეყანა შესაძლოა გახდეს როგორც ევროკავშირის, ისე NATO - ს წევრი, და საქართველო აღმოჩნდეს ირანის „მოწინააღმდეგე ბანაკში“, მაშინ შეიძლება ვივარაუდოთ, რომ ირანი გააძლიერებს თავის მოქმედებას სამხრეთ კავკასიაში, კერძოდ კი საქართველოში, რაც სავარაუდოდ გამოიხატება არა სამხედრო მოქმედებებში, რაც ირანს ზოგადად არ ახასიათებს, არამედ სწორედ კიბერშეტევების გაძლიერებაში ქვეყნის კრიტიკული ინფრასტრუქტურის მიმართ. ამიტომ, ჩვენთვის მნიშვნელოვანია წინასწარ ვიცოდეთ ირანის კიბერშესაძლებლობები, მისი კიბერუსაფრთხოების პოლიტიკა, სტრატეგია, კიბერ შეტევებში გამოყენებული ტექნიკა და ტექნოლოგიები, ასევე ორგანიზაციული სტრუქტურა.

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.

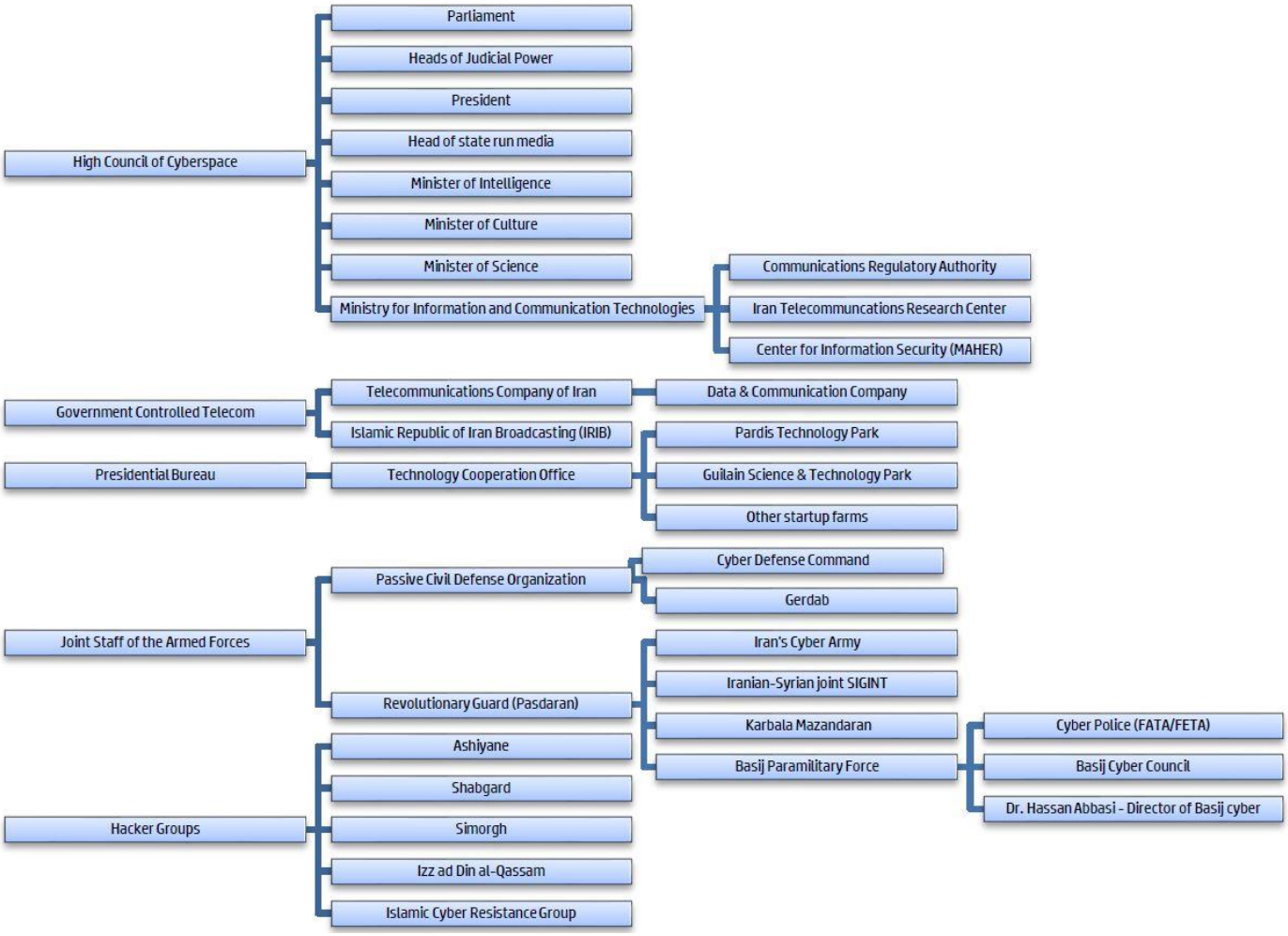
Shabgard

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.

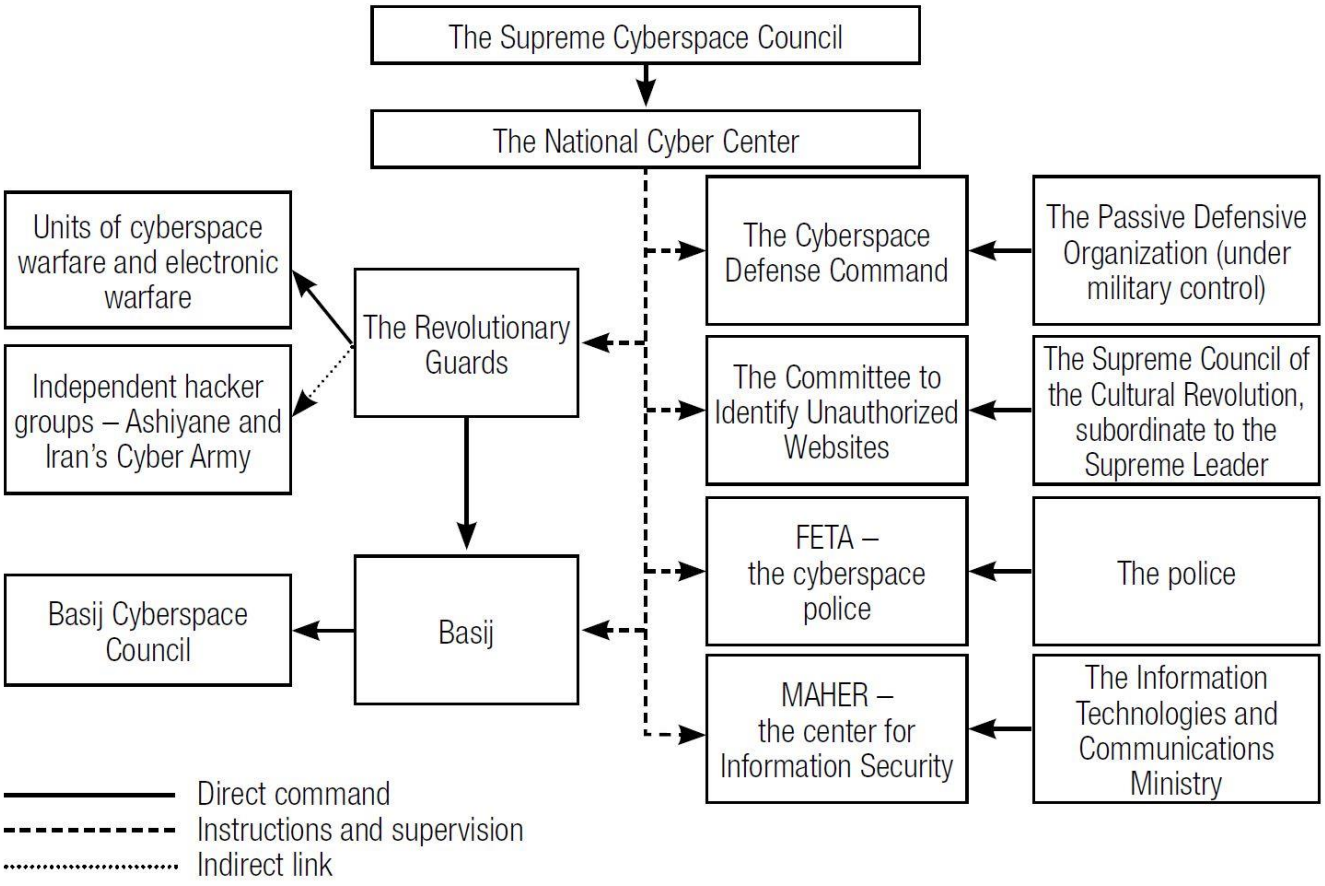
ტრენინგები მოიცავს penetration testing, application security, Android programming, networking, Debian Linux administration, PHP, Perl for penetration testers, and Python. საიტი სთავაზობს ასევე შეუერთდნენ ირანის ერთერთ პრესტიჟულ უნივერისტეტს Shahid Beheshti University, სადაც ისწავლება კომპიუტერული მეცნიერებები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

დანართი 1

Iranian cyber organizational chart



დანართი 2


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 Cyberspace Council
Basij
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 ჯგუფებასთან, 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/.