

სიფრულო საფრთხეების ეკონომიკური გავლენა

რათი აბულაძე

ეკონომიკის დოქტორი,
სტუ-ს ასოცირებული პროფესორი

რეზიუმე

ეკონომიკა სულ უფრო დამოკიდებული ხდება ტექნოლოგიებზე. ინტერნეტ-ტექნოლოგიები აფართოებს, როგორც სოციალურ-ეკონომიკურ სარგებელს, ისე საფრთხეებს, ინვესტს სოციალურ ცვლილებებს, ზრდის საზოგადოებრივ გაურკვევლობას, წარმოაჩენს სახელმწიფოს კიბერ საფრთხეებსა და მონყვლად ადგილებს.

სამეცნიერო ნაშრომში ნაჩვენებია ინტეგრირებული კიბერგარემოს ფორმირების საფუძველი და მოსალოდნელი ტენდენციები. აღნიშნულია კიბერთავდასხმების ზრდისა და ინტერნეტ-ეკონომიკის ზრდის ტემპის შემცირების კავშირი. ნაჩვენებია, კიბერთავდასხმების მზარდი საფრთხე, რომელიც მსოფლიო ეკონომიკას დიდ ზიანს აყენებს.

კვლევების საფუძველზე დადგენილია საქართველოს კიბერგარემოს გამოწვევები. კვლევით ნაშრომში აღნიშნულია, რომ ქვეყანაში არ ხდება ელექტრონული ბიზნეს სივრცის ათვისება და ვერ ყალიბდება მძლავრი ელექტრონული მმართველობითი სისტემა,

სტატიაში გამოკვეთილია კიბერერიშიშმითანილი სფეროები, სახელმწიფოს კიბერდაცვისათვის საჭირო ღონისძიებები და პრევენციის მექანიზმები.

დასკვნის სახით ჩამოყალიბებულია ქვეყნის კეთილდღეობისათვის საჭირო რეკომენდაციები და კონკრეტულ ღონისძიებათა სისტემა.

საკვანძო სიტყვები: ეკონომიკური გავლენა, ციფრული საფრთხე, კიბერთავდასხმა

Economic Impact of Digital Threats

Rati Abuladze, Associated prof. of Gtu

Summary

The economy is becoming increasingly dependent on technologies. Internet technology expands the socio-economic benefits, as well as the threats, leads to social changes, increases social uncertainty, highlights cyber threats and vulnerable areas of the State.

The scientific work deals with the basis for the formation of an integrated cyber environment and the expected trends. It considers the connection between the growth of cyber-attacks and the slowdown of the Internet economy. The paper discusses the growing threat of cyber attacks, which causes serious damage to the world economy.

Based on the studies, the challenges of Georgian cyber environment are identified. Research paper points out that

the E-business space is not utilized and powerful E-governance system can not be formed.

The article outlines the cyber attacked areas, cyber security measures and prevention mechanisms of the state.

In conclusion, the recommendations and system of specific measures required for prosperity of the country are outlined.

შესავალი

ეკონომიკა სულ უფრო დამოკიდებული ხდება ტექნოლოგიებზე. ინტერნეტ-ტექნოლოგიები აფართოებს, როგორც სოციალურ-ეკონომიკურ სარგებელს, ისე საფრთხეებს, ინვესტს სოციალურ ცვლილებებს, ზრდის საზოგადოებრივ გაურკვევლობას, წარმოაჩენს სახელმწიფოს კიბერ საფრთხეებსა და მონყვლად ადგილებს.

კვლევები ადასტურებს, რომ საერთაშორისო ორგანიზაციების შეფასებით 10 წელიწადში მოსახლეობის 90% ჩართული იქნება ინტერნეტში, ხოლო ინტერნეტ-საგნების შექმნით ციფრული და ფიზიკური სამყაროს გაერთიანდება. აღნიშნული მოცემულობის შედეგი ინტეგრირებული კიბერგარემოს ფორმირება იქნება.

აღსანიშნავია, რომ მიზეზშედეგობრივი კავშირი არსებობს კიბერთავდასხმების ზრდასა და ინტერნეტ-ეკონომიკის ზრდის ტემპის შემცირებას შორის. ამასთან, კიბერეკოსისტემის კასკადზე სულ უფრო იზრდება კიბერთავდასხმების პრეცედენტები. კიბერთავდასხმები წარმოადგენს ინფორმაციული ომის ახალ ფურცელს. იგი არის მზარდი საფრთხე, რომელიც ქვეყნის ეკონომიკას დიდ ზიანს აყენებს.

ციფრული საფრთხეები ქმნის სახელმწიფოს დასუსტების პირობას, სხვადასხვა ეკონომიკური, პოლიტიკური, ფსიქოლოგიური გავლენით. იგი დიდ გავლენას ახდენს საფინანსო ბაზრებზე, სახელმწიფოს რეპუტაციასა და ნდობაზე.

I. ციფრული საფრთხეების კლასიფიცირება

კიბერსივრცედ მხოლოდ ინტერნეტი აღარ განიხილება, რადგან ინტერნეტში ჩართულია საყოფაცხოვრებო ნივთები, ტექნიკა, საგნები, აქსესუარები, ნებისმიერი ფიზიკური სივრცე. აღნიშნული მოცემულობა ნიშნავს, რომ კიბერსაფრთხეები პირდაპირ თუ ირიბ გავლენას ახდენს არამხოლოდ ციფრულ სივრცეში, არამედ ფიზიკურ სივრცეში ადამიანთა კეთილდღეობასა და ცხოვრებაზე [1].

IBM-ის 2016 წლის კვლევის შედეგებით, გამოკვე-

თილია კიბერსივრცის სფეროები, მათ შორის [2]:

1. ჯანდაცვის სფერო (ელექტრონული მედიცინის ბარათები შეიცავს ინფორმაციას მოქალაქის პირად მონაცემებს, საკრედიტო ბარათის, ელექტრონული ფოსტის, სოციალური უზრუნველყოფის ნომრისა და სხვა იდენტიფიცირების მონაცემს. 2015 წელს, ჯანდაცვის 100 მლნ ჩანაწერი იქნა დაკარგული);

2. მრეწველობა (მანქანათმშენებლობას, ელექტროტექნიკის, ტექსტილის, ფარმაცევტული პროდუქტის წარმოება);

3. საფინანსო მომსახურება (ბანკები, მობაილ ბანკი, საკრედიტო ბარათი, საინვესტიციო ფონდები);

4. სახელმწიფო მმართველობა (საჯარო მოსამსახურეებზე არსებული ინფორმაციის გაჟონვა, შპიონაჟი);

5. ტრანსპორტირება (ავიაკომპანიის, ავტობუსის, მეტროს, რკინიგზის, საზღვაო ტრანსპორტის სფეროში არსებული ინფორმაცია). აღნიშნული დარგი ემსახურება მსოფლიო ვაჭრობას, მის გარეშე მსოფლიო ეკონომიკა ადვილად დაიშლება.

არსებითია, რომ პოლიტიკურად მოტივირებული კიბერდანაშაულები მიმართულია მასობრივი ქაოსის, მმართველობითი და პოლიტიკური კრიზისის შექმნის, პოლიტიკური ნდობის შემცირების, სახელმწიფო სისტემის მდგრადობის შესუსტებისკენ. თუმცა გამორიცხავს ფინანსურ სარგებელს.

ინტერნეტის უნივერსალური სივრცეში, ყველა ქვეყნისათვის ერთნაირია კიბერსაფრთხეები ფორმები, თუმცა განსხვავებულია პრევენციის ღონისძიებები და საფრთხეების მასშტაბები.

Deloitte-ის კვლევის ანგარიშით, ინტერნეტ-გარემოს დინამიური განვითარების პარალელურად მნიშვნელოვანი გამოწვევების წინაშეა სახელმწიფოს კიბერდაცვა, მათ შორის შეიძლება აღინიშნოს [3]:

- ელექტრონული კომერცია ვითარდება ფიქსირებული, ინტერნეტ და მობილური მონეობილობების გამოყენებით;
- საერთო დანაშაულებში, განსაკუთრებული ზრდით ხასიათდება კიბერდანაშაულები;
- ტერორიზმის მასშტაბები ფართოვდება ტექნოლოგიების საფუძველზე;
- იზრდება ინტერნეტშია ჩართული საგნები, რომელიც ზრდის როგორც კეთილდღეობას, ისე საფრთხეებს;
- წარმოჩენილია გლობალური ინტერნეტ-ბაზრის საინვესტიციო მიმზიდველობითა და გლობალური გამოწვევებით .

კიბერსივრცის დაცვის საკითხები მნიშვნელოვან სირთულეებს ქმნის ნაციონალურ თუ საერთაშორისო დონეზე. შესაბამისად, სახელმწიფოს კიბერთა-დაცვის პოლიტიკა საჭიროებს:

§ ტრანსნაციონალური თანამშრომლობა;

§ იურისდიქციის პრობლემატიკის მოწესრიგებას;

§ ციფრული სივრცის საერთაშორისო სამართლის კონცეფციის თეორიტიზირებას;

§ კიბერთაგდასხმის შემთხვევაში კონკრეტული ღონისძიებების გატარებას;

ქვეყანაში, ციფრული საფრთხეების ეკონომიკური გავლენის შემცირების მიზნით, გლობალური და ლოკალური კიბერსაფრთხეები საჭიროებს ტაქტიკურ მიდგომებს. ასეთი მიდგომებიდან შეიძლება აღვნიშნოთ საერთაშორისო ორგანიზაცია The World Economic Forum-ის მიერ წარმოდგენილი 8 მიმართულება [4] :

1. ციფრული იდენტიფიცირება: ციფრული თანამშრომლობა, ციფრული მოქალაქეობრიობა, ციფრული მენარმეობა;

2. ციფრული უფლებების დაცვა: სიტყვის თავისუფლება, ინტელექტუალური საკუთრების დაცვა, პირადი ცხოვრების ხელშეუხებლობა;

3. ციფრული წიგნიერება: კომპიუტერული უნარ-ჩვევები და აზროვნება, კონტენტის შექმნა, კრიტიკული აზროვნება;

4. ციფრული კომუნიკაცია: ონლაინ თანამშრომლობა, ონლაინ კომუნიკაცია, ციფრული „ნაკვალევი“;

5. ციფრული უსაფრთხოება: უსაფრთხოების კოდების დაცვა, ინტერნეტ უსაფრთხოება, მობილური უსაფრთხოება;

6. ციფრული დაცვა: კონტენტის რისკი, კონტაქტების რისკი, სამომხმარებლო რისკი;

7. ციფრული მოხმარება: კომპიუტერთან მუშაობის დრო, საზოგადოების ჩართულობა, ციფრული კეთილდღეობა და ჯანმრთელობა;

8. ციფრული ემოციური ინტელექტი: სოციალურ & ემოციური ცნობიერების ამაღლება, ემოციების რეგულირება/მართვა, ემპათია.

კვლევები ადასტურებს, რომ გლობალურ და ლოკალურ სივრცეში, კიბერთაგდასხმებთან და კიბერტერორიზმთან ბრძოლის აღიარებული მეთოდები [5]:

პროგრამების, პოლიტიკისა და პროცედურების შემუშავება;

კიბერჯგუფების შექმნა და ინციდენტებზე რეაგირების მექანიზმების შემუშავება;

ბიზნეს უწყვეტობისა და საზოგადოების უსაფრთხოებისათვის, სამივე სექტორის კოორდინირებული კიბერაქტივობა;

სამართლებრივი პასუხისმგებლობის გამკაცრება;

კადრების მომზადება;

ტექნიკური უსაფრთხოების შეფასება და მონიტორინგი.

II. გლობალური ციფრული საფრთხეების სოციალურ-ეკონომიკური გავლენა

მნიშვნელოვანია აღინიშნოს, რომ გლობალურ ეკონომიკურ დანაშაულებში, კიბერკრიმინალი ერთ-ერთი ფართოდ გავრცელებული ეკონომიკური დანაშაულია. PWC -ს კვლევის ანგარიშით (Global Economic Crime Survey 2016), გლობალურ ეკონომიკურ

დანაშაულებში პირველ ადგილს იკავებს აქტივების უკანონო მითვისება 64%, მეორე ადგილზეა კიბერკრიმინალი 32%-ით, ხოლო სამეულში შედის მექართამეობა და კორუფცია 24%-ით^[9].

კრიმინალის გლობალური მასშტაბები და მისი წილი მსოფლიოს მშპ-ში საკმაოდ სოლიდურია, მათ შორის გლობალურ მშპ-ში: ტრანსნაციონალური დანაშაულების წილი შეადგენს 1.2%-ს, ნარკოტიკების - 0.9%-ს, კიბერკრიმინალის - 0.8%-ს, გაყალბება/საავტორო უფლებების დარღვევა-0.89%-ს, ხოლო საზღვაო პირატობა - 0.02%-ს^[7].

2014 წელს, მსოფლიოში, კიბერკრიმინალის ზარალი აღწევდა 445 მლრდ დოლარს^[8], ხოლო დღეს 1 ტრლნ დოლარს. პროგნოზით, მსოფლიოში, კიბერკრიმინალის დანაკარგები 2019 წელს 2 ტრლნ-ს მი-აღწევს ^[9].

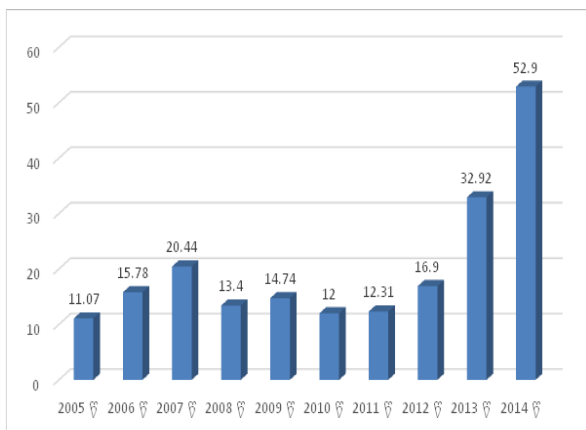
გლობალური ინდექსით (გლობალ პეაცე ინდექსი), 163 ქვეყნის კონფლიქტი, ტერორიზმი და პოლიტიკური არასტაბილურობა 2015 წელს შეფასდა 13.6 ტრლნ დოლარით^[10].

ტერორიზმის გავლენის შეფასებისათვის, შეიძლება განხილული იქნას The Institute for Economics and Peace (IEP)-ის მიერ ჩატარებული კვლევა, რომელმაც 162 ქვეყნის საფუძველზე წარმოადგინა გლობალური ტერორიზმის ინდექსი (კვლევა მოიცავს მოსახლეობის 99,6%-ს, ტერორიზმის ფსიქოლოგიურ გავლენას, დანაკარგებს, ზარალს, საკუთრების დაზიანებას). აღნიშნული ინდექსის მაღალი დონე აჩვენა შემდეგმა ქვეყნებმა: ერაყი, ავღანეთი, ნიგერია, პაკისტანი, სირია, ინდოეთი, იემენი, სომალი^[11].

The Symantec-ის ანგარიშით, კიბერკრიმინალის შედეგად, პლანეტის მოსახლეობამ დაკარგა 158 მლრდ დოლარი^[12].

მსოფლიო ეკონომიკური ფორუმის კვლევის ანგარიშით, ძალადობრივი დანაშაულები და მკვლელ-ობები 2014 წელს შეფასდა 1.7 ტრლნ დოლარით, ხოლო ტერორიზმის გლობალური ეკონომიკური გავლენა 2000-2014 წწ-ში 4.9 მლრდ დოლარიდან 52.9 მლრდ დოლარამდე გაიზარდა (იხ. დიაგრამა) ^[13].

ტერორიზმის გლობალური ეკონომიკური გავლენა (მლრდ დოლარი)



მსოფლიოში, 50 წლის განმავლობაში, 475 სახელმწიფო გადატრიალება მოხდა, მათგან 236 ინციდენტი წარმატებით დასრულდა. 2010 წლიდან დღემდე 19 სახელმწიფო გადატრიალება მოხდა, მათგან 9 ინციდენტი წარმატებით დასრულდა (წარუმატებელი აღმოჩნდა სახელმწიფო გადატრიალება თურქეთში^[14].

სხვადასხვა შეფასებით, გლობალური უთანასწორობის გადაჭრა და ძალადობის შემცირება საჭიროებს 1.36 ტრლნ დოლარს. აღნიშნული კი შეადგენს მსოფლიოს საკვები პროდუქტების ექსპორტის ექვივალენტს^[15]. პროგნოზით, მომავალ 5 წელიწადში 1 ტრლნ დოლარი იქნება დახარჯული გლობალური კიბერუსაფრთხოების უზრუნველყოფისათვის^[16].

კიბერკრიმინალი წარმოადგენს საკმაოდ მზარდ ინდუსტრიას, რომლის სარგებელი დიდი, ხოლო რისკები დაბალია. სხვადასხვა შეფასებით, კიბერკრიმინალის პრევენციაზე, გლობალური ეკონომიკის განეული დანახარჯები 575 მლრდ დოლარს აჭარბებს^[17].

გაეროს მიერ სამშვიდობო ოპერაციებზე განეულმა დანახარჯმა 8.27 მლრდ დოლარი შეადგინა (ბოლო ერთ წელიწადში) ^[18].

III. საქართველოს ციფრული საფრთხეები

კვლევები ადასტურებს, რომ საქართველოს კიბერსაფრთხეების სოციალური და ეკონომიკური გავლენის კომპლექსური კვლევა და შეფასება რთულია. საქართველოს კიბერსაფრთხეებისა და კიბერ ტერორიზმის ანალიზი, ძირითადად საერთაშორისო კვლევითი ინსტიტუტებისა და ორგანიზაციების კვლევის საფუძველზეა შესაძლებელი. მაგალითად, IEP-ის კვლევითი ინსტიტუტის ანგარიშით, საქართველო თუ 2015 წლის რეიტინგში იმყოფებოდა ტერორიზმის ყველაზე დაბალი გავლენის მქონე ქვეყნების სიაში^[19], 2016 წლის გლობალური მშვიდობის ინდექსის რეიტინგში (GLOBAL PEACE INDEX 2016) საქართველოს გარემოს საფრთხეები საშუალო დონით ფასდება^[20].

საქართველოს კიბერგარემოს კომპლექსური ანალიზი და შეფასება რთულია, ვინაიდან და რადგანაც, ქვეყანაში არ წარმოებს (ან ფრაგმენტულია) კიბერგარემოს კომპლექსური კვლევა, არ ხდება ელექტრონული ბიზნეს სივრცის ათვისება, არ იქმნება სახელმწიფო კვლევითი ინსტიტუტები, ჯერ კიდევ ვერ ყალიბდება მძლავრი ელექტრონული მმართველობითი სისტემა, ბუნებრივია, ქართულ კიბერსივრცეზე არსებული ფრაგმენტული კვლევის მონაცემები ზუსტი დასკვნების წარდგენის შესაძლებლობას არ იძლევა.

ფაქტია, რომ კიბერსაფრთხეები გადაიჭრება ნაციონალურ დონეზე. ამისათვის თითოეული ქვეყანა ქმნის კიბერინციდენტებზე რეაგირების ჯგუფს, ინტენსიურად იკვლევს და ანალიზებს საფრთხეებს, ამუშავებს კიბერკრიმინალთან ბრძოლისა და კიბერსივრცის უსაფრთხოების შენარჩუნების მეთოდებს.

დასკვნა

ჯამში, შეიძლება აღინიშნოს, რომ კიბერთავდასხმების ზომებისა და თანმდევი შედეგების (ზიანის) მასშტაბების ანალიზის აქტუალობის მუხიდან, კიბერკრიმინალის ეკონომიკური გავლენის რაოდენობრივი შეფასება საკმაოდ რთულ ამოცანას წარმოადგენს. ეს კი მსოფლიოს ქვეყნებში, კიბერთავდასხმებით გამოწვეული დანაკარგების გაზომვის შეზღუდული შესაძლებლობითაა გამოწვეული [21].

საჭიროა ქვეყანაში შეფასდეს კიბერ რისკები, მათ შორის:

მონაცემთა დაკარგვით გამოწვეული ზიანის ოდენობა,

კიბერდანაშაულების შემთხვევების რაოდენობა;

კიბერ ტერორიზმისა და კიბერთავდასხმების პრეცედენტების გავლენა ქვეყნის იმიჯზე;

კიბერსაფრთხეებთან ბრძოლის მექანიზმების ფორმირება.

საჭიროა ქვეყანაში დამკვიდრდეს მეცნიერ-მკვლევარებთან თანამშრომლობის პრაქტიკა, რაც უნდა გამოიხატებოდეს:

კიბერ საფრთხეების ინტენსიური კვლევითა და შეფასებით;

სახელმწიფოსა და სამეცნიერ სექტორის თანამშრომლობა, კვლევების დაკვეთის პრაქტიკის დანერგვა;

სახელმწიფო-სამეცნიერო კვლევითი ინსტიტუტის შექმნის ხელშეწყობით;

სამეცნიერო-კვლევითი მუშაობის აქტივიზირების ხელშეწყობით;

საზოგადოების ინფორმირების ზრდის მიზნით აქტიური აგიტაცია-პროპაგანდით;

გლობალური და ლოკალური გამოწვევების ფონზე, როგორც სახელმწიფოს კიბერსივრცის თავდაცვისუნარიანობის ზრდის მიზნით, ისე საზოგადოების დაცულობისა და გარემოს ჯანსაღებისათვის, საჭიროა:

კიბერსივრცის საფრთხეებზე ზრუნვა საზოგადოების სამივე სექტორის თანამშრომლობით :

ქოლ-ცენტრის შექმნა კიბერსაფრთხეებზე მყისიერი რეაგირებისათვის;

სახელმწიფოს კიბერუსაფრთხოებაზე პასუხისმგებელი ერთი უწყება (რომელიც საზოგადოებას კიბერგამოწვევებზე გაუწევს კონსულტაციას, გამოიძიებს ინტერნეტ-კრიმინალს, შეამოწმებს საეჭვო საიტებს, ბავშვებს დაიცავს არასასურველი კონტენტისაგან, დაიცავს ინტერნეტ-მოხმარებლების უფლებებს);

კიბერპატრულის, კიბერრეზერვისა და კიბერარმიის შექმნა და კოორდინირება სახელმწიფოს უსაფრთხოების სამსახურის მიერ;

კანონმდებლობის კონტროლ ქვეშ მოექცეს კიბერშეტევების მასშტაბი და დონე;

ინტერნეტ-საზღვრების იურისდიქციის პრობლემები საჭიროებს საერთაშორისო დონეზე

თანამშრომლობას (მაგრამ ეს არ გულისხმობს, რომ სხვა ქვეყნების იმედად ვიყოთ);

ქვეყანაში საუბრობენ მხოლოდ კიბერსივრცის თავდაცვითი ღონისძიებებსა და პრევენციის მექანიზმებზე, თუმცა გასათვალისწინებელია, რომ სახელმწიფოს ასევე სჭირდება თავდასხმითი გეგმა ქვეყნის უსაფრთხოების ძლიერებისათვის.

ჯამში, შეიძლება ითქვას, რომ მნიშვნელოვანად იზრდება კიბერკრიმინალის მასშტაბები (ასევე, კიბერსივრცის სოციალურ-ეკონომიკური ფასეულობა), რომელზე რეაგირებაც კერძო და სახელმწიფო სექტორის მიერ საკმაოდ დაგვიანდა (რადგან პრევენციის მექანიზმები, პოლიტიკა, სტრატეგია, კიბერ-სტრუქტურები ახლა ფორმირდება).

დასასრულს, აღვნიშნავთ, რომ ქვეყანაში საჭიროა „ელექტრონული მმართველობის სახელმწიფო სამეცნიერო კვლევითი ინსტიტუტის შექმნა“, რომელიც მეცნიერ-მკვლევარების, ბიზნეს და სახელმწიფო სექტორის კოორდინირებით ხელს შეუწყობს ქვეყნის გლობალური და ლოკალური გამოწვევების გადაჭრას, როგორც ფიზიკურ სივრცეში ისე კიბერ გარემოში.

გამოყენებული ლიტერატურა:

- 1 https://www.weforum.org/agenda/2015/09/video-how-should-we-govern-cyberspace/?utm_content=buffer6e063&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer
- 2 <http://www-01.ibm.com/common/ssi/cgi-bin/ssia/liaas?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF>
- 3 Deloitte. Cyber opportunity analysis report 2016 Positioned to lead. https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/IE_ERS_CyberAnalysisReport.pdf
- 4 https://www.weforum.org/agenda/2016/06/8-digital-skills-we-must-teach-our-children?utm_content=bufferd8a7f&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer
- 5 <http://www.emrisk.com/knowledge-center/newsletters/cyber-terrorism-emerging-threat>
- 6 <https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf>
- 7 <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf>
- 8 <http://www.tripwire.com/state-of-security/latest-security-news/economic-impact-of-cybercrime-estimated-at-445-billion-worldwide/>
- 9 <http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#4e4d2c873bb0>
- 10 <https://www.theguardian.com/global-development/2016/jun/08/conflict-and-terrorism-cost-the-world-trillions-says-global-peace-index>
- 11 The Institute for Economics and Peace (IEP) .

Global Terrorism Index. 2015. MEASURING AND UNDERSTANDING THE IMPACT OF TERRORISM. <http://economicsandpeace.org/wp-content/uploads/2015/11/Global-Terrorism-Index-2015.pdf>

12 <http://www.forbes.com/sites/stevemorgan/2016/01/24/how-consumers-lost-158-billion-to-cyber-crime-in-the-past-year-and-what-to-do-about-it/#ce9001b6b6fe>

13 MyersJ. is the economic impact of terrorism?. 19 November 2015. <https://www.weforum.org/agenda/2015/11/what-is-the-economic-impact-of-terrorism/>

14 https://www.washingtonpost.com/news/world-views/wp/2016/07/22/map-the-world-of-coups-since-1950/?tid=sm_fb

15 <https://www.theguardian.com/global-development/2016/jun/08/conflict-and-terrorism-cost-the-world-trillions-says-global-peace-index>

16 <http://cybersecurityventures.com/cybersecurity-market-report/>

17 <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf>

18 <http://www.un.org/en/peacekeeping/operations/financing.shtml>

19 The Institute for Economics and Peace (IEP) . Global Terrorism Index. 2015. MEASURING AND UNDERSTANDING THE IMPACT OF TERRORISM. <http://economicsandpeace.org/wp-content/uploads/2015/11/Global-Terrorism-Index-2015.pdf>

20 The Institute for Economics and Peace (IEP) . Global Peace Index 2016. ten years of measuring peace. http://static.visionofhumanity.org/sites/default/files/GPI%202016%20Report_2.pdf

21 <http://tesi.eprints.luiss.it/11390/1/pupillo-cecilia-tesi-2013.pdf>