ალექსანდრე ღლონტი
გრიგოლ რობაქიძის სახელობის უნივერსიტეტი
სამართალმცოდნეობის სამაგისტრო პროგრამის I დონის სტუდენტი

კიბერდანაშაულის პრობლემა საქართველოსა და უცხოეთის ქვეყნებში

მოკლე ისტორია

როგორც სამეცნიერო კვლევის ობიექტს, კიბერდანაშაულს შეისწავლიან მე-20 საუკუნის მიწურულიდან, სწორედ იმ დროიდან, როდესაც მასობრივად დაიწყო კომპიუტერების გამოყენება. დღევანდელ დღეს კომპიუტერები და ინტერნეტ-ქსელში ჩართული სხვა მოწყობილობები გვიადვილებენ ცხოვრებას, თუმცა, ამავდროულად კიბერდანაშაულის გავრცელებასაც უწყობენ ხელს. კომპიუტერული ტექნიკის გამოყენება დანაშაულის ჩადენის ინსტრუმენტად თანამედროვე მსოფლიოსთვის ერთერთ ყველაზე სერიოზულ პრობლემას წარმოადგენს, რომელსაც აქტიურად ებრძვის მთელი საზოგადოება. Kკიბერ-ტექნიკის გამოყენება შესაძლებელია არამარტო მსოფლიო მიღწევების დასაცავად, არამედ მათზე ნეგატიური ზემოქმედებისთვისაც [9].

კომპიუტერის გამოყენებით ბოროტმოქმედს შეუძლია სერიოზული ზიანი მიაყენოს არამხოლოდ საბანკო დაწესებულებებს, მუნიციპალურ სამსახურებს, საავტორო უფლებებს, არამედ პირდაპირ დაემუქროს სახელმწიფო უსაფთხოებასა და თავდაცვის უნარიანობას [4]. FBI-ის მონაცემებით, კიბერდანაშუაულის შედეგად მხოლოდ ამერიკის შეერთებულ შტატებს 67 მილიარდი დოლარის ოდენობით ზარალი აქვს მიყენებული [8].

კიბერ-დანაშაულის განმარტება

კიბერ-დანაშაული, იგივე კომპიუტერული დანაშაული უკავშირდება ინტერნეტის ან სხვა ელექტრონული საკომუნიკაციო ქსელების ბოროტად გამოყენებას. კიბერდანაშაულს განმარტავენ, როგორც დანაშაულებრივ საქმიანობას, რომელიც მიმართულია კერძო პირთა ან პირთა ჯგუფების წინააღმდეგ; დანაშულის მიზანია პირდაპირი თუ ირიბი განზრახვით შელახოს მსხვერპლის რეპუტაცია ან ფიზიკური, ფინანსური და მორალური ზიანი მიაყენოს მას; კიბერდანაშაულის იარაღია - კომპიუტერი, საკომუნიკაციო და მობილური სატელეფონო ქსელები.

კომპიუტერის გამოყენებით შესაძლებელია მთელი რიგი დანაშაულის ჩადენა, თუმცა, მათი დაყოფა ძირითადად ორ კატეგორიად შეიძლება:

- დანაშაული, რომელიც ორიენტირებულია უშუალოდ კომპიუტერზე.
- დანაშაული, რომლის ჩადენისთვის გამოიყენება კომპიუტერი და რომლის სამიზნე დამოუკიდებელი ქსელები და აპარატებია [11].

კომპიუტერული დანაშაულის სახეობათა უმრავლესობას წარმოადგენს: ე.წ. „სპამი“, თაღლითობა, დამამცირებელი და შეურაცხმყოფელი კონტენტი, ნარკოტიკული საშუალებებითა და იარაღით ვაჭრობა, კიბერ-ტერორიზმი და კიბერ-თავდასხმები (ომები).

„მაღალტექნოლოგიური დამნაშავეები“ და მათ მიერ ჩადენილი კომპიუტერული დანაშაულის დახასიათება

დამნაშავეებმა, რომლებიც იყენებენ მაღალ ტექნოლოგიებს, ე.წ. ჰაკერებმა, დანაშაულის ახალი ფორმები და მიმართულებები შექმნეს. მათ უკვე არ იზიდავთ დანაშაულის ჩადენის ძველი მეთოდები. კომპიუტერული საშუალებები ჰაკერებს შესაძლებლობას აძლევს, მიზნის მიღწევისთვის სრულიად ახალი, აქამდე არნახული სქემები გამოიყენონ. თავიანთ ანგარებით მიზნებს ისინი კომპიუტერის მეშვეობით ახორციელებენ, კერძოდ, ქმნიან და გამოიყენებენ ე.წ. ვირუსებს ან ჩადიან სხვა სახის კიბერ დანაშაულს. არსებობს კომპიუტერული დანაშაულის სამი კატეგორია:

1. კომპიუტერი გამოიყენება, როგორც ელექტრონული ინფორმაციის შექმნის, შენახვის, მისით მანიპულაციის და ელექტრონული კომუნიკაციის საშუალება. ამ შემთხვევაში კომპიუტერი არ არის დანაშაულის იარაღი, თუმცა, მისი მეშვეობით შესაძლებელია განხორციელდეს კრიმინალურ აქტივობასთან დაკავშირებული ქმედებები, მაგალითად, ამოღებულ იქნას (გადმოიქაჩოს) ნარკოდილერის შავი ბუღალტერია.

2. კომპიუტერი შეიძლება გამოყენებულ იქნას, როგორც დანაშაულის ინსტრუმენტი. ასე მაგალითად, მისი მეშვეობით შესაძლებელია დაიბეჭდოს ყალბი ფული, გაყალბდეს საბუთები, ინტერნეტში გავრცელდეს არასრულწლოვანთა პორნოგრაფია, ჩაიტვირთოს თაღლითური ვებ-გვერდები და ა.შ.

3. კომპიუტერი ასევე შეიძლება იქცეს დანაშაულის იარაღად. ამ შემთხვევაში თავდასმა ხორციელდება ინფორმაციის მოპოვების შესაძლებლობაზე, მის მთლიანობასა და დაცულობაზე (ასეთია, მაგალითად, ინფორმაციისა და სერვისების მითვისება, კომპიუტერული ტექნიკის დაზიანება). ამ სახეობის დანაშაული უკავშირდება ვირუსების უკანონო გავცელებას, სერვისებისა და ქსელების არაავტორიზებულ დაბლოკვას. ასეთ დანაშაულს ხშირად ჩადიან ე.წ. „კიბერ- ვანდალები“. ბოლო წლებში მთელ მსოფლიოში საგრძნობლად გაიზარდა სხვადასხვა ორგანიზაციების წინააღმდეგ მიმართული კიბერ-თავდასხმების რაოდენობა [1].

კიბერდანაშაულის წინააღმდეგ საერთაშორისო კანონმდებლობის მიმოხილვა

კომპიუტერული დანაშაულის ზრდასთან ერთად, საჭირო გახდა ახალი მარეგულირებელი კანონების შემუშავება. სწორედ ამ პერიოდში მიიღეს რამოდენიმე კონვენცია. მიუხედავად

იმისა, რომ მსოფლიო აღიარებს კომპიუტერული დანაშაულის მაღალ საშიშროებას, ჯერ კიდევ არ არსებობს ცალსახად გამოკვეთილი საერთაშორისო თანამშრომლობა კიბერდანაშაულთან საბრძოლველად.

გაეროს ნარკოტიკებთან და დანაშაულთან ბრძოლის (UNODC) სამდივნომ დანაშაულობის პრევენციისა და კრიმინალური იუსტიციის გაეროს მე-12 კონგრესისთვის მოამზადა კიბერ-დანაშაულთან დაკავშირებული პროექტი. კონვენციის პროექტში აღინიშნა, რომ „კიბერ-დანაშაულის წინააღმდეგ გლობალური კონვენციის შემუშავება საჭიროებს საკითხისადმი ფრთხილ და გააზრებულ მიდგომას“. გაეროს კონგრესმა არ მიიღო კიბერ-დანაშაულან ბრძოლის რუსეთის მიერ მხარდაჭერილი პროექტი. მიუხედავად ამისა, შეთანხმდნენ, რომ საერთაშორისო თანამშრომლობა აღნიშნულ საკითხში სასიცოცხლოდ მნიშვნელოვანია მსოფლიოსთვის, რომელიც მჭიდროდაა გაერთიანებული გლობალური კომპიუტერული ქსელებით [13].

დღეისათვის ფუნქციონირებს გაეროს კონვენცია კიბერ-დანაშაულის შესახებ, რომელსაც ხელი მოეწერა ბუდაპეშტში 2001 წელს და რომელიც 2004 წლიდან შევიდა ძალაში. 2010 წლისთვის კონვენცია ხელმოწერილ იქნა 46 ქვეყნის მიერ, ხოლო მისი რატიფიცირება 26-მა ქვეყანამ მოახდინა. იმის მიუხედავად, რომ კონვენცია მიიღეს ევროსაბჭოს ეგიდით, მას შეიძლებოდა არაევროპული ქვეყნებიც (ამერიკის შეერთებული შტატები, კანადა, იაპონია, სამხრეთ აფრიკა) შეერთებოდნენ. მიუხედავად საკმაოდ ფართო მასშტაბებისა, აღნიშნულ კონვენციას ვერ ვუწოდებთ საერთაშორისოს, რადგან მსოფლიოს უამრავ ქვეყანაში ჯერ კიდევ არ ამოქმედებულა მის მიერ დადგენილი ნორმები. თუმცა, ბუდაპეშტის კონვენცია, რომელიც 11 წლის წინ იქნა მიღებული, დღესდღეობით კიბერდანაშუალთან ბრძოლის ყველაზე ფართომასშტაბიანი სამართლებრივი დოკუმენტია და მისი ხელმოწერის შესაძლებლობა მსოფლიოს ყველა ქვეყანას აქვს.

საერთაშორისო კიბერდანაშაული

ტერორიზმის ტრადიციულმა მეთოდებმა თანამედროვე სამყაროში უფრო საშიში თვისებები შეიძინეს და ე.წ. „კიბერ-ტერორიზმის“ ჩამოყალიბებას შეუწყვეს ხელი. ინფორმაციული ტექნოლოგიების ეპოქაში ტერორისტებმა შეძლეს, მიეღწიათ სასიკვდილო იარაღისა და კომპიუტერული ტექნოლოგიების კომბინაციური გამოყენებისთვის, რასაც სამართალდამცავები ჯერჯერობით არ აქცევენ სათანადო ყურადღებას. გამოწვევები იმდენად სერიოზულია, რომ სათანადო აქცენტირების გარეშე „კიბერ ტერორიზმი“ კატასტროფულ და აუნაზღაურებად ზიანს მიაყენებს მსოფლიოს. „კიბერ ტერორიზმის“ ცნება გულისხმობს კომპიუტერული ტექნოლოგიების განზრახ გამოყენებას ნეგატიური მიზნებით, რაც იწვევს სხვისი მატერიალური ან არამატერიალური ინტერესების შელახვას. მაგალითად, დამნაშავე არალეგალურად აღწევს კონკურენტი ფირმის კომპიუტერულ სისტემაში და შლის საჭირო და ფასეულ ბიზნეს-ინფორმაციის შემცველ ფაილებს; აღნიშნული კიბერ-ტერორიზმის ფორმად შეიძლება შეფასდეს.

კიბერ-ტერორიზმის პრობლემასთან დაკავშირებულ ყველაზე ციტირებად წყაროდ ითვლება დენინგის დაკითხვის ოქმი სპეციალური ზედამხედველობის კოლეგიის წინაშე (დენინგი 2000). დენინგის აზრით, "კიბერ-დანაშაული ტერორიზმისა და კიბერ სივრცის შეზავებაა (კონვერგენციაა). დამნაშავეების უკანონო მოტივაცია, განახორციელონ კომპიუტერებზე თავდასმა ან თავდასხმის მუქარა, როგორ წესი, ნათელია და მიმართულია ადამიანებისა და მთავრობების დაშინებისკენ, რათა მიღწეულ იქნას თავდამსხმელთა პოლიტიკური თუ სოციალური მიზნები. Kკიბერ-ტერორიზმის კვალიფიკაციისთვის აუცილებელია, რომ სახეზე იყოს კიბერ-თავდასხმა ადამიანებზე, ქონებაზე ან სხვა შიშის გამომწვევ შედეგებზე. Kკიბერ-ტერორიზმი შეიძლება განვიხილოთ, როგორც ვირტუალირი თავდასხმები, რომელთაც შედეგად მოჰყვა ადამიანის სიკვდილი ან სხეულის დაზიანება, აფეთქება, თვითმფრინავის კატასტროფა, წყლის დაბინძურება, მნიშვნელოვანი ეკონომიური ზარალი და ა.შ. სერიოზული თავდასხმები სტრატეგიულ ინფრასტრუქტურაზე, დამდგარი შედეგის მიხედვით, შეიძლება ჩაითვალოს კიბერ ტერორიზმად [3].

არსებობს „კიბერ ტერორიზმის“ 4 ფორმა. ესენია:

- *საიდუმლო ინფორმაციის უკანონო მიღება და მონაცემების მოპარვა.* საინფორმაციო ტექნოლოგიები შეიძლება გამოიყენონ ფასეული სახელმწიფო საიდუმლოს, კერძო ან იურიდიული პირების მონაცემების მიტაცებისათვის.
- *ელექტრონული მართვის სისტემების განადგურება.* ელექტრონული მართვის მიზანია ადამიანებისა და მოხელეების ურთიერთობების გამჭვირვალობის უზრუნველყოფა, ბიუროკრატიული ბარიერების მოშლა.

- *ვირუსების (სპამის) გავრცელება.* Kკიბერ-ტერორისტები ბლოკავენ კომპიუტერულ ქსელებს (denial of services - DDOS), რაც ხელს უშლის სახელმწიფო ელექტრონული ბაზებისა და სერვისების გამოყენებას. ისინი აინფიცირებენ სახელმწიფო ქსელში მყოფ ერთ ან რამოდენიმე არადაცულ კომპიუტერს და შემდეგ აკონტროლებენ მათ [6].

- *ქსელის დაზიანება ან მისი მუშაობის შეფერხება.* კიბერ ტერორისტების ძირითადი მიზანია ელექტრონული ქსელების წყობიდან გამოყვანა ან დაზიანება. ასეთი მეთოდებით ტერორისტები ცდილობენ უშიშროების სტრუქტურების ყურადღების გაფანტვას საკუთარი მიზნების მისაღწევად.

ზოგიერთი გახმაურებული კობერ-დანაშაული

ბოლო პერიოდში განხორციელებულმა კიბერ-თავდასხმებმა დაამტკიცა, რომ ყველაზე ძლიერი დაცვის სისტემაც უძლურია მოიგერიოს შეტევა. საყოველთაოდ მიღებული

კომპიუტერული აქსიომა გვეუბნება, რომ არ არსებობს დაცვა, რომლის „გატეხვა“ შეუძლებელია. თვალსაჩინოებისთვის შეიძლება მოვიყვანოთ შემდეგი მაგალითები [10]:

1. სასამართლო პროცესი: აშშ ოსოვსკის წინააღმდეგ (2001 წ.) - ჯოფრეი ოსოვსკი და ვილსონ თენგი მიცემულ იქნენ პასუხისგებაში Cisco Systems-ის „გატეხვისა“ და 8 მილიონი დოლარის მითვისებისთვის. Cisco Systems ერთერთი მსოფლიო ლიდერია ქსელურ გაყვანილობებში.

2. 2005 წელს პასუხისგებაში იქნა მიცემული არასრულწლოვანი, რომელმაც Microsoft Corporation-ის წინააღმდეგ განახორციელა წარმატებული კიბერ-შეტევა [7].

3. კევინ მიტნიკმა, ფინანსების მითვისების მიზნით, წარმატებით „გატეხა“ IBM, Motorola, NEC, Nokia, Fujitsu Siemens და სხვა კორპორაციები [11].

თუ ისეთი მეგაკორპორაცია, როგორიცაა Microsoft, არასრულწლოვნის თავდასხმის ობიექტად იქცა, ლოგიკურად შეიძლება ვივარაუდოთ, რომ პროფესიონალი ჰაკერი ერთ დღეს ბირთვული იარაღის მაკონტროლებელ პანელშიც შეძლებს შეღწევას.

კიბერდანაშაული საქართველოში

საქართველოში კომპიუტერიზაციის პროცესი გაცილებით გვიან დაიწყო, ვიდრე ევროპასა და ჩრდილოეთ ამერიკაში. 21-ე საკუნის დასაწყისამდე პერსონალური კომპიუტერები იშვიათობა იყო ქართველების ოჯახებში. სწორედ ამან შეუწყო ხელი კიბერ-დანაშაულის დაგვიანებულ გავრცელებას ჩვენს ქვეყანაში. გარდა კომპიუტერიზაციისა, ნიშანდობლივია, რომ ჩვენში ინტერნეტის მასობრივი გამოყენებაც საკმაოდ დაგვიანდა.

ზემოთ ხსენებული ფაქტორების მიუხედავად, დღევანდელ საქართველოში უკვე იკვეთება კიბერდანაშაულის ზოგიერთი ნიშანი. ხშირ შემთხვევაში ადგილობრივი ჰაკერები მხოლოდ ზედაპირულ ზიანს აყენებენ ეკონომიკას, ან მათი არასამართლებრივი ხელყოფის ობიექტს უფრო ხშირად ინტელექტუალური საკუთრება წარმოადგენს. ასე თუ ისე, ქართველებს ჯერ არ უწვნევიათ კომპიუტერული დანაშაულის მძიმე შედეგები, როგორიცაა, მაგალითად, კიბერ-ტერორიზმის დამანგრეველი მოქმედება. სამწუხაროდ, ამ მიმართულებით მოდუნება არ შეიძლება. თუ ქართველმა სამართალდამცავებმა სასწრაფოდ არ მიიღეს სათანადო ზომები, კიბერ- ზეწოლა ქვეყნის თავდაცვის უნარიანობაზეც შეიძლება განხორციელდეს [2].

კიბერ-დანაშაულთან დაკავშირებული მუხლები წარმოდგენილია საქართველოს სისხლის სამართლის კოდექსის 35-ე და 38-ე თავებში. ამ სახეობის დანაშაულს სულ ოთხი მუხლი ეთმობა:

მუხლი 1284. კანონით დაცულ კომპიუტერულ ინფორმაციასთან, ესე იგი მანქანამატარებელზე, ელექტროგამომთვლელ მანქანაზე (ეგმ-ზე), ეგმ-ის სისტემაში ან მათ

ქსელში ასახულ ინფორმაციასთან არამართლზომიერი შეღწევა, რამაც ინფორმაციის განადგურება, ბლოკირება, მოდიფიცირება ან მოპოვება ანდა ეგმ-ის, ეგმ-ის სისტემის ან მათი ქსელის მოშლა გამოიწვია, ასევე მობილური მოწყობილობის საერთაშორისო იდენტიფიკატორის შეცვლა.

მუხლი [1]285. ეგმ-ის დამაზიანებელი პროგრამის შექმნა ან არსებულ პროგრამაში ცვლილების შეტანა, რაც განზრახ იწვევს ინფორმაციის არასანქციონირებულ განადგურებას, ბლოკირებას, მოდიფიცირებას ან გადაღებას, ანდა ეგმ-ის, ეგმ-ის სისტემის ან მათი ქსელის მუშაობის მოშლას, აგრეთვე ასეთი პროგრამის ან ასეთი პროგრამის შემცველი მანქანა-მატარებლის გამოყენება ან გავრცელება.

მუხლი [1]286. ეგმ-ის, ეგმ-ის სისტემის ან მათი ქსელის ექსპლუატაციის წესის დარღვევა იმის მიერ, ვისაც ხელი მიუწვდებოდა ეგმ-ზე, ეგმ-ის სისტემაზე ან მათ ქსელზე, რამაც გამოიწვია ეგმ-ის კანონით დაცული ინფორმაციის განადგურება, ბლოკირება, მოდიფიცირება ან გადაღება, ანდა რამაც მნიშვნელოვანი ზიანი გამოიწვია [5].

მუხლი [1]324(1). ტექნოლოგიური ტერორიზმი, ესე იგი ბირთვული, რადიოლოგიური, ქიმიური ან ბაქტერიოლოგიური (ბიოლოგიური) იარაღის ან მისი კომპონენტის, პათოგენური მიკროორგანიზმის, რადიაქტიური ან/და ადამიანის ჯანმრთელობისათვის მავნე სხვა ნივთიერების გამოყენება ან მისი ხელში ჩაგდების ან/და გამოყენების მუქარა, მათ შორის, ბირთვული, ქიმიური ან ძლიერი ტექნოლოგიური ანდა ეკოლოგიური საშიშროების შემცველი ობიექტის ხელში ჩაგდება, რაც ხელყოფს საზოგადოებრივ უსაფრთხოებას, სახელმწიფოს სტრატეგიულ, პოლიტიკურ ან ეკონომიკურ ინტერესს, ჩადენილი მოსახლეობის დაშინების ან ფიზიკურ და იურიდიულ პირებზე, ხელისუფლების ორგანოზე, სახელმწიფოზე ან საერთაშორისო ორგანიზაციაზე ზემოქმედების მიზნით.

2010 წლის 24 სექტემბერს საქართველოს პარლამენტმა სისხლის სამართლის კოდექსში შეიტანა შემდეგი ცვლილებები:

- ✓ კიბერდანაშულის ჩამდენის სისხლისსამათლებრივი პასუხისმგებლობა;
- ✓ ინტელექტუალური საკუთრების არასამართლებრივი გავრცელება;
- ✓ „არასრულწლოვანთა პორნოგრაფიის“ კანონმდებლობის განვრცობა;
- ✓ კანონმდებლობის _ “დანაშაულებრივი შეღწევა კომპიუტერულ სისტემაში“ განვრცობა;
- ✓ კანონონმდებლობის _ „კომპიუტერული ინფორმაციის დანაშაულებრივი გამოყენება“ განვრცობა.

დასკვნა

„მაღალტექნოლოგიური დამნაშავეები“ ორი მიზეზით წარმოადგენენ სერიოზულ პრობლემას მსოფლიოს სამართალდამცავი ორგანოებისთვის. პირველი, კომპიუტერული დანაშაული ძნელად გამოსაძიებელია, რადგან პირს შეუძლია დანაშაული ჩაიდინოს ინტერნეტ-ქსელში

ჩართული ნებისმიერი კომპიუტერიდან (როგორც სახლიდან, ისე მის გარეთ). მეორე, იმის მიუხედავად, რომ ჰაკერების წინააღმდეგ არაერთი წარმატებული სპეცოპერაციაა განხორციელებული, სამართალდამცავი ორგანოები ჯერ კიდევ არ არიან საკმარისად ეკიპირებულები იმისთვის, რომ ძირფესვიანად აღმოფხვრან აღნიშნული პრობლემა. ცალსახაა, რომ მომავლის პოლიცია უკეთ უნდა მოემზადოს მოცემული ფენომენის დასაძლევად.

თანამედროვე საქართველოში კიბერ-დანაშაულთან მებრძოლი სპეციალისტების, შესაბამისი ლიტერატურის აშკარა ნაკლებობაა, რაც ხელსაყრელ პირობებს ქმნის კიბერ-დამნაშავეებისა და ტერორისტების საქმიანობისთვის. Kკიბერ-გართულებების თავიდან აცილებისთვის აუცილებელია, რომ აღნიშნული პრობლემები უმოკლეს ვადებში იქნას გადაწყვეტილი სახელმწიფო დონეზე.

გამოყენებული ლიტერატურა

1. Adler F., Mueller G, Laufer W. 2008. *Criminology and Criminal Justice System*. Edition 5th.
2. Alasania G. International Cooperation as a Strategy of Prevention and Fighting with terrorism in Georgia. *http://transcrime.cs.unitn.it/tc/fso/*
3. Gordon S., Ford R. Cyberterrorism? Symantec Security Response. http://www.symantec.com/avcenter/reference/cyberterrorism.pdf
4. Harley B. A Global Convention on Cybercrime? on March 23rd, 2010. http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/
5. Tsatsanashvili M., Sikharulidze T. 2007. Law Problems of Cyber terrorism in Georgia. *Cybersecurity.* Tbilisi.
6. საქართველოს სისხლის სამართლის კოდექსი. 2010.
7. Cyber Terrorism - The Dark Side of the Web World. http://www.legalserviceindia.com/article/l169-Cyber-Terrorism.html
8. FBI 2005 Internet crime survey. http://www.digitalriver.com/v2.0-img/operations/naievigi/site/media/pdf/FBIccs2005.pdf
9. Internet and Electronic Crimes. 11/05/2011 National Institute of Justice USA. http://nij.gov/topics/crime/internet-electronic/welcome.htm
10. United States Department of Justice – Computer Crime and Intellectual Property Section
11. Wikipedia - http://en.wikipedia.org/wiki/Kevin_Mitnick
12. Understanding and Responding to Terrorism. 2007. *NATO – Security through Science,* Vol.
13. http://www.computerweekly.com/news/1280092617/UN-rejects-international-cybercrime-treaty