კიბერდანაშაული – აწმყო და მომავალი*

პროფესორი, სამართლის დოქ. ***მარტინ პაულ ვასმერი***, კიოლნის უნივერსიტეტი

I. შესავალი

კომპიუტერული დანაშაულის წინააღმდეგ ბრძოლის შესახებ სისხლისსამართლებრივი ნორმები გერმანიაში ჯერ კიდევ 30 წლის წინ იქნა მიღებული. აღნიშნულმა ნორმებმა მას შემდეგ მოდიფიცირება და სრულყოფა განიცადეს, რათა არ ჩამორჩენოდნენ ტექნოლოგიურ პროგრესს, განსაკუთრებით კი ინტერნეტდანაშაულის განვითარებას და ევროკავშირისა და საერთაშორისო სამართლით დადგენილ ვალდებულებებს. საფრთხის ძლიერ აქტუალობაზე მეტყველებს ბიზნეს საკონსულტაციო კომპანია KPMG-ის კვლევები. აღნიშნული კვლევების მიხედვით, გერმანიაში 2015-2016 წლებში გამოკითხულ 504 საწარმოთა 38%-ს შეეხო ე. წ. ელექტრონული დანაშაული და გამოკითხულ საწარმოთა 88%-ის მხრიდან ეს დანაშაული, როგორც მაღალ ან/და როგორც ძალიან მაღალ რისკად შეფასდა.

ამასთან, გასათვალისწინებელია ის საფრთხეები, რომლებიც ინფრასტრუქტურას ემუქრება. საქართველო 2008 წელს, როდესაც რუსეთის ჯარი შემოიჭრა, გახდა ფართომასშტაბიანი კიბერთავდასხმის მსხვერპლი.[1] ინტერნეტგვერდზე „stopgeorgia.ru“ შესაძლებელი იყო დამაზიანებელი პროგრამის, სახელწოდებით „war.bat“, ჩამოტვირთვა, რომელიც იძლეოდა ქართულ ინტერნეტქსელებზე თავდასხმის შესაძლებლობას. აღნიშნულის შედეგად შესაძლებელი გახდა, არამხოლოდ პრეზიდენტის პირადი გვერდის მოქმედების შეჩერება, არამედ ფინანსურმა ინსტიტუტებმაც ეროვნული ბანკის განკარგულებით 10 დღით შეაჩერეს თავიანთი ელექტრონული საბანკო მიმოქცევა. გარდა ამისა, ჰაკერებმა გააყალბეს არაერთ საიტზე მოცემული ინფორმაცია. სხვებთან ერთად მაგალითისათვის აღსანიშნავია საგარეო საქმეთა სამინისტროს ვებგვერდზე გამოსახული კოლაჟი საქართველოს პრეზიდენტის მიხეილ სააკაშვილისა და ადოლფ ჰიტლერის პორტრეტებით.

II. კიბერდანაშაულის დეფინიცია

კიბერდანაშაულის დეფინიციის განსაზღვრა რთულია. ფართო გაგების მიხედვით, აღნიშნულის ქვეშ მოიაზრება ყველა სისხლისსამართლებრივი დანაშაული, რომელიც ჩადენილია საინფორმაციო ან საკომუნიკაციო ტექნოლოგიების გამოყენებით ან მათ მიმართ. გავრცელებულია დიფერენციაცია **„კომპიუტერულ დანაშაულსა“** და **„ინტერნეტ დანაშაულს“** შორის, კერძოდ, დანაშაულებს შორის, რომელთა ჩადენის დროსაც დანაშაულის ჩადენის საშუალებას ან დანაშაულის ობიექტს კომპიუტერი ან ინტერნეტი წარმოადგენს.[2] თუმცა ეს დაყოფა მკაცრი არ არის, რადგან მათი სფეროების გადაფარვა ხდება. მიუხედავად ამისა, დანაშაულის საპოლიციო სტატისტიკა (PKS) აღნიშნულ დაყოფას ეყრდნობა, როდესაც აღწერს „ინტერნეტს, როგორც დანაშაულის საშუალებას“ და „კომპიუტერულ დანაშაულს“, როგორც დანაშაულის სპეციალურ ფორმას. „კიბერდანაშაულის შესახებ ფედერაციაში არსებული მდგომარეობის ამსახველი ანგარიშიც“ (Bundeslagebild Cybercrime) ერთმანეთისაგან ასხვავებს დანაშაულებს, რომლებიც ინტერნეტის, მონაცემთა ბაზების, საინფორმაციო ტექნოლოგიური სისტემების ან მათი მონაცემების წინააღმდეგ არის მიმართული **(კიბერდანაშაული ვიწრო გაგებით)** და დანაშაულებს, რომლებიც აღნიშნული ტექნიკის გამოყენებით ხორციელდება **(კიბერდანაშაული ფართო გაგებით).**[3]

---

* წინამდებარე სტატია წარმოადგენს ავტორის მიერ საქართველოს უნივერსიტეტში (თბილისი) 2017 წლის 24 ოქტომბერს გაკეთებული მოხსენების წერილობით ვერსიას, თავისი სქოლიოებით.
სტატია ქართულად თარგმნა ჟურნალის სამუშაო ჯგუფის წევრმა *თამარ ასათიანმა.*

[1] შეად. *Goetz, John, Rosenbach, Marcel, Szandar, Alexander,* Krieg der Zukunft, Spiegel 7/2009, ხელმისაწვდომია: http://www.spiegel.de/spiegel/a-606165-5.html.

[2] შეად. *Gercke, Marco*, in: Gercke, Marco/Brunst, Philipp, Praxishandbuch Internetstrafrecht, 2009, Rn. 73.

[3] Bundeskriminalamt, Bundeslagebild Cybercrime 2016, 4 ff. (ხელმისაწვდომია: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html).

III. პრაქტიკული მნიშვნელობა

1. კომპიუტერული დანაშაული

PKS-ის მიხედვით, 2016 წელს კომპიუტერული დანაშაულის **107.751 შემთხვევა** დაფიქსირდა, რაც წინა წელთან შედარებით 50%-ზე მეტ ზრდაზე მიუთითებს. აღნიშნული ზრდა დანაშაულის აღრიცხვის ცვლილებებმაც გამოიწვია,[4] რომლის მიხედვითაც, ამიერიდან დანაშაულები, რომელთა ჩადენაც მართლსაწინააღმდეგოდ მოპოვებული საგადასახადო ბარათების გამოყენებით ხდება, ფასდება არა როგორც თაღლითობა (გერმანიის სისხლის სამართლის კოდექსის[5] §263), არამედ კომპიუტერის გამოყენებით ჩადენილი თაღლითობა (გერმანიის სსკ-ის §263a). თუმცა აღრიცხვა მაინც საკმაოდ არასრულყოფილია. ამგვარად, ხარვეზს წარმოადგენს ის ფაქტი, რომ იგი მხოლოდ იმ დანაშაულებს მოიცავს, რომელთა დანაშაულის შემადგენლობაც გერმანიის ფარგლებში ხორციელდება[6], რადგან კომპიუტერული დანაშაულის შემთხვევაში დანაშაულის ჩადენის ადგილს სწორედ ინტერნეტის გამო არ აქვს დიდი **მნიშვნელობა**. ამავდროულად, ახლებური გააზრებაც გვაქვს სახეზე: 2017 წლიდან PKS მოიცავს როგორც საზღვარგარეთიდან, ისე დაუდგენელი ადგილმდებარეობიდან ჩადენილ დანაშაულებს,[7] რის საფუძველზეც რაოდენობრივი მაჩვენებელი კვლავ მნიშვნელოვნად გაიზრდება. და ბოლოს, როგორც პოლიტიკურად, ისე დაზვერვითი მიზნებით მოტივირებული დანაშაულები აღარ იქნება მოცული.[8] დანაშაულის გახსნის მაჩვენებელი 2016 წლისთვის 37,7%-ს შეადგენდა და ამით საშუალოზე დაბალი იყო (დანაშაულები მთლიანობაში უცხოური კანონმდებლობის დარღვევის გარეშე: 54,0%),[9] რაც ინტერნეტის გლობალურობისა და ანონიმურობიდან გამომდინარე, რა თქმა უნდა, გასაკვირი არაა.

კიბერდანაშაულის შესახებ ფედერაციაში არსებული მდგომარეობის ანგარიში **ვიწრო გაგებით კიბერდანაშაულთან** ერთად, კომპიუტერული დანაშაულის ყველაზე მნიშვნელოვან ნაწილსაც ასახავს. 2016 წელს[10] მთლიანობაში **82.649 შემთხვევა** იქნა რეგისტრირებული, რაც წინა წელთან შედარებით 80%-იან ზრდას ნიშნავს. ამ შემთხვევაშიც, როგორც უკვე აღინიშნა, დანაშაულის აღრიცხვაში განხორციელებულ ცვლილებებთან გვაქვს საქმე, რადგან მხოლოდ კომპიუტერის გამოყენებით განხორციელებული თაღლითობის 58.620 შემთხვევა დაფიქსირდა. აქედან „სატელეკომუნიკაციო მომსახურების ბოროტად გამოყენების“ 811 შემთხვევა იყო სახეზე, რომლებიც ასევე კომპიუტერულ თაღლითობას განეკუთვნებიან. ამით აღნიშნული დანაშაული ყველა რეგისტრირებული სისხლისსამართლებრივი დანაშაულის 70%-ზე მეტის გამომწვევია. დანარჩენ სისხლისსამართლებრივ დანაშაულებზე უფრო ნაკლები წილი მოდის: ჯაშუშობა და მონაცემების ხელში ჩაგდება მოსამზადებელ ქმედებებთან ერთად (გერმანიის სსკ-ის §§202a, 202b, 202c) – 12,9%; მტკიცებულების მნიშვნელობის მქონე მონაცემების გაყალბება და სამართლებრივ ბრუნვაში მონაცემების დამუშავების პროცესში მათი გაყალბება (გერმანიის სსკ-ის §§ 269, 270) – 9,9%; მონაცემების შეცვლა და კომპიუტერული საბოტაჟი (გერმანიის სსკ-ის §§ 303a, 303b) – 5,4 %. 2016 წლის განმავლობაში[11] აღნიშნული დანაშაულების საფუძველზე მიყენებული ზიანის ოდენობამ 51,63 მლნ. ევრო შეადგინა. თუმცა, აქ გათვალისწინებულია მხოლოდ კომპიუტერული თაღლითობის

[4] Bundeskriminalamt, Polizeiliche Kriminalstatistik 2016, Band 4, 167 (ხელმისაწვდომია: https://www.bka.de).

[5] ტექსტში სისხლის სამართლის კოდექსი შემოკლებულია, როგორც სსკ.

[6] Bundeskriminalamt, Bundeslagebild Cybercrime 2016, 3 (ხელმისაწვდომია: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html).

[7] Bundeskriminalamt, Bundeslagebild Cybercrime 2015, 5, Fußnote 01 (ხელმისაწვდომია: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2015.html).

[8] Bundeskriminalamt, Bundeslagebild Cybercrime 2015, 5 (ხელმისაწვდომია: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2015.html).

[9] Bundeskriminalamt, Polizeiliche Kriminalstatistik 2016, Band 1, 8.

[10] Bundeskriminalamt, Bundeslagebild Cybercrime 2016, 6 (ხელმისაწვდომია: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html).

[11] Bundeskriminalamt, Bundeslagebild Cybercrime 2016, 7 (ხელმისაწვდომია: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html).

საფუძველზე დამდგარი ზიანი, რაც გულისხმობს იმას, რომ ზუსტი დასკვნების გაკეთება რთულია.

2. ინტერნეტი, როგორც დანაშაულის ჩადენის საშუალება

„ინტერნეტი, როგორც დანაშაულის ჩადენის საშუალება“ [12] – ამ აღნიშვნის ქვეშ PKS აერთიანებს ყველა სისხლისსამართლებრივ დანაშაულს, რომელთა ჩადენაც ინტერნეტის გამოყენებით ხდება. ეს დანაშაულები შესაძლოა დანაშაულის ნებისმიერ სახეს წარმოადგენდნენ. 2016 წელს **253.290 შემთხვევა** დაფიქსირდა, რაც წინა წელთან შედარებით 3,6%-იან ზრდას გულისხმობს. ეს მონაცემი აჩვენებს, რომ დანაშაულის ჩადენის აღნიშნული საშუალების გამოყენება გვხვდება სისხლისსამართლებრივი დანაშაულების 4,3%-ის შემთხვევაში (გარდა უცხო ქვეყნის კანონმდებლობის დარღვევის შემთხვევებისა). მაშასადამე, სისხლისსამართლებრივი დანაშაულების 95%-ზე მეტის ჩადენა ე. წ. „offline“ ხდება. უმეტესად საქმე ეხება მოტყუებით ჩადენილ დანაშაულებს (გერმანიის სსკ-ის §§ 263 და შემდგომნი; 72,5%), განსაკუთრებით ქონებრივ დაზიანებას მოტყუებით (27,8%). კომპიუტერული დანაშაულის გარდა (იხ. ზემოთ III.1.), დარჩენილი წილი მოდის პორნოგრაფიული პუბლიკაციების მომზადებაზე (გერმანიის სსკ-ის §§ 184 და შემდგომნი – 2,3%) და საავტორო სამართალთან დაკავშირებულ სისხლის სამართლის დანაშაულებზე (საავტორო უფლებების შესახებ გერმანიის ფედერალური კანონის §§ 106 და შემდგომნი – 1,5%).

3. გამოუვლენელი დანაშაულები

ამასთან, ხაზგასასმელია, რომ სწორედ კიბერდანაშაულის შემთხვევაში გვხვდება **გამოუვლენელი დანაშაულების ძალიან დიდი ოდენობა,** როგორც ამას ბევრი კვლევა აჩვენებს.[13] ამიტომ, სტატისტიკურ მონაცემებში კიბერდანაშაულის რეალური ოდენობის მხოლოდ მცირე ნაწილი აისახება. აღნიშნულის მიზეზები იმ ფაქტში უნდა ვეძებოთ, რომ უამრავი დანაშაული უსაფრთხოების გაუმჯობესებული ტექნიკური ღონისძიებების გამო შეუმჩნეველი რჩება ან არ სცდება დანაშაულის მცდელობის სტადიას, ხშირად ზიანი არ დგება და დაზარალებულები, განსაკუთრებით საწარმოები, ცდილობენ არ აღრიცხონ ეს დანაშაულები, რათა მათ არ დაკარგონ მყარი და საიმედო პარტნიორის რეპუტაცია.[14]

IV. კიბერდანაშაული ვიწრო გაგებით

კიბერდანაშაულის მთავარ ბირთვს ქმნის კიბერდანაშაული ვიწრო გაგებით, რადგან მის შემთხვევაში დანაშაულის განხორციელებისათვის **მონაცემთა დამუშავება** არსებითი მნიშვნელობის მქონეა. გერმანიაში სათანადო სისხლისსამართლებრივი დანაშაულები გერმანიის სსკ-ის სხვადასხვა თავში გვხვდება, რადგან ისინი **„ელექტრონული გზით ჩადენის“** შემთხვევებში ანაცვლებენ ტრადიციულ დანაშაულის შემადგენლობებს (თაღლითობა, დოკუმენტის გაყალბება, პირადი ცხოვრების ხელშეუხებლობის დარღვევა, ქონებრივი ზიანის მიყენება).

1. კომპიუტერული თაღლითობა (გერმანიის სსკ-ის § 263a)

გერმანიის სსკ-ის §263a ეკონომიკური დანაშაულების წინააღმდეგ ბრძოლის შესახებ მეორე კანონის 15.5.1986[15] **(2. WiKG)** საფუძველზე იქნა მიღებული, რათა შევსებულიყო სისხლისსამართლებრივი დასჯადობის არსებული ხარვეზები. თაღლითობა (გერმანიის სსკ-ის § 263) არ მოიცავს მონაცემთა დამუშავების პროცესში განხორციელებულ ქმედებებს, რადგან ამ შემთხვევაში სახეზე არ არის ადამიანის მოტყუება, შეცდომაში შეყვანა ან მისი ქონების განკარგვა.[16] სისხლის სამართლის

[12] Bundeskriminalamt, Polizeiliche Kriminalstatistik 2016, 15.

[13] Bundeskriminalamt, Bundeslagebild Cybercrime 2015, 3, 7 m. w. N. (ხელმისაწვდომია: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2015.html).

[14] Bundeskriminalamt, Bundeslagebild Cybercrime 2015, 8 (ხელმისაწვდომია: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2015.html).

[15] Bundesgesetzblatt (BGBl) I, 721.

[16] Bundestagsdrucksache (BT-Drucks.) 10/318, 18; Bundestagsdrucksache (BT-Drucks.) 10/5058, 20.

კოდექსში ცვლილებების განხორციელების შესახებ 2003 წლის 22 დეკემბრის[17] 35-ე კანონით 2003 წლის 28 დეკემბერს თაღლითობისა და უნაღდო ანგარიშსწორების საშუალებებთან დაკავშირებული[18] გაყალბების წინააღმდეგ ბრძოლის შესახებ ევროკავშირის N:2001/413/JI ჩარჩო გადაწყვეტილების იმპლემენტირებისათვის მე-3 და მე-4 აბზაცები იქნა შემოღებული, რათა თავად მოსამზადებელი ქმედებებიც დასჯადი გამხდარიყო. [19]

ა) დანაშაულის ძირითადი შემადგენლობა (გერმანიის სსკ-ის § 263a-ის პირველი აბზაცი) თაღლითობის მსგავსადაა შექმნილი და გაბატონებული შეხედულების თანახმად,[20] მასთან მჭიდრო კავშირში უნდა განიმარტოს (ე. წ. თაღლითობისათვის დამახასიათებელი განმარტება). იგი შეიცავს დანაშაულის ოთხ ალტერნატივას. 5 წლამდე თავისუფლების აღკვეთით ან ფულადი ჯარიმით ისჯება პირი, რომელიც საკუთარი თავისათვის ან მესამე პირისათვის მართლსაწინააღმდეგო გზით ქონებრივი სარგებლის მიღების განზრახვით, სხვა პირის ქონებას იმით აზიანებს, რომ მონაცემთა დამუშავებით მიღებულ შედეგს მოიპოვებს: 1. პროგრამის არასწორად აწყობის საფუძველზე (1.Aალტერნატივა, **პროგრამული მანიპულაცია**), 2. არასწორი ან არასრულყოფილი მონაცემების გამოყენების საფუძველზე (2. ალტერნატივა, **მიწოდების მანიპულაცია**), მონაცემების არაავტორიზებული გამოყენებით (3. ალტერნატივა, **მონაცემთა ბოროტად გამოყენება**) ან არასანქცირებული ზეგავლენით პროგრამის მოქმედების პროცესში (4. ალტერნატივა ე. წ. **მონაცემთა შეგროვების შემადგენლობა**). თაღლითობაზე (გერმანიის სსკ-ის § 263a მეორე აბზაცი) **მითითებიდან** გამომდინარე, დასჯადია არამხოლოდ დანაშაულის ჩადენის მცდელობა, არამედ გერმანიის სსკ-ის § 263 მესამე აბზაცის შესაბამისად, განსაკუთრებით მძიმე შემთხვევებიც გვაქვს სახეზე, რომელთა მიმართაც გაზრდილი სასჯელია გათვალისწინებული, კერძოდ, თავისუფლების აღკვეთა 6 თვიდან 10 წლამდე. გარდა ამისა, ჯგუფურად და პროფესიული საქმიანობის გამოყენების გზით დანაშაულის ჩადენისას გამოიყენება გერმანიის სსკ-ის § 263 მე-5 აბზაცი, რომელიც ითვალისწინებს თავისუფლების აღკვეთას ერთიდან 10 წლამდე და, შესაბამისად, დანაშაულს წარმოადგენს.

კიბერდანაშაულისათვის გერმანიის სსკ-ის **§263a განსაკუთრებული მნიშვნელობისაა.** პრაქტიკაში დომინირებს მოპარული ან გაყალბებული საბანკო და საკრედიტო ბარათების არასანქცირებული გამოყენება ბანკომატებთან ან სალაროებთან.[21] ამასთან, საქმე ეხება შემთხვევებს, რომლის დროსაც დამნაშავე წვდომის მონაცემებს (მომხმარებლის დასახელებას, პინკოდს, ტრანზაქციის ავტორიზაციის ნომერს) ე. წ. „Phishing"-ის მეშვეობით (Mail/SMS/Instant Message-ის გამოყენებით) ან ე. წ. „Pharming"-ის მეშვეობით (გაყალბებულ გვერდებზე გადამისამართებით) მოიპოვებს და შემდეგ მას „ინტერნეტ ბანკინგში" იყენებს.[22] აგრეთვე, საქმე ეხება „სატელეკომუნიკაციო მომსახურების ბოროტად გამოყენებას", განსაკუთრებით ე. წ. „Phreaking-ს", რომლის დროსაც სატელეფონო ან/და მონაცემთა ბაზები უცხო შემაერთებლის ხარჯზე მოქმედებს, ასევე ე. წ. „პირატული ბარათების" გამოყენებას ე. წ. Pay-TV გადაცემების დეკოდირებისათვის და კოდირებული უკაბელო ინტერნეტის არაავტორიზებულ გამოყენებას. [23]

ბ) გერმანიის სსკ-ის § 263a მე-3 აბზაცი დანაშაულის მომზადებისათვის განხორციელებულ ქმედებებს დასჯადად მიიჩნევს. 3 წლამდე თავისუფლების აღკვეთით ან ფულადი ჯარიმით ისჯება ის, ვინც დაამზადებს, თავისთვის ან სხვისთვის მოიპოვებს, თავისუფლად განათავსებს, შეინახავს ან სხვას გადასცემს კომპიუტერულ პროგრამებს, რომელთა მიზანიც გერმანიის სსკ-ის § 263a პირ-

[17] Bundesgesetzblatt (BGBl) I, 2838.

[18] Amtsblatt (ABl.) L 149, 1; იხ. ასევე *Waßmer, Martin Paul*, in Pötz/Grützner/Kreß, Internationaler Rechtshilfeverkehr in Strafsachen, 3. Aufl. 2012, III C 4.9.

[19] Bundestagsdrucksache (BT-Drucks.) 15/1720, 10.

[20] Sammlung der Entscheidungen des BGH in Strafsachen (BGHSt) 38, 120, 124; 47, 160, 162 s.; *Waßmer, Martin Paul*, Computerbetrug (§ 263a StGB), in: Leitner, Werner/Rosenau, Henning, Wirtschafts- und Steuerstrafrecht, 2017, Rn. 37 ff. m. w. N.

[21] Bundeskriminalamt, Bundeslagebild Cybercrime 2016, 4 (ხელმისაწვდომია: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html).

[22] *Waßmer, Martin Paul*, Computerbetrug (§ 263a StGB), in: Leitner, Werner/Rosenau, Henning, Wirtschafts- und Steuerstrafrecht, 2017, Rn. 54 m. w. N.

[23] *Waßmer, Martin Paul*, Computerbetrug (§ 263a StGB), in: Leitner, Werner/Rosenau, Henning, Wirtschafts- und Steuerstrafrecht, 2017, Rn. 56 f. m. w. N.

ველი აბზაცის შესაბამისი სისხლისსამართლებრივი დანაშაულის ჩადენაა. გერმანიის სსკ-ის § 263a მე-4 აბზაცი ადრეულ ეტაპზე დამთავრების გამო გერმანიის სსკ-ის § 149 მე-2 და მე-3 აბზაცებით გათვალისწინებული ქმედითი მონანიების შესახებ ნორმების სათანადო გამოყენებას ითვალისწინებს. კანონის დასაბუთების თანახმად პროგრამა არ უნდა იყოს განსაზღვრული მხოლოდ კომპიუტერული თაღლითობის ჩასადენად.[24] ეს მიდგომა პრობლემურია, რადგან ბევრი პროგრამა შესაძლოა გამოყენებულ იქნას როგორც ლეგალური, ასევე არალეგალური მიზნებით (ე. წ. **Dual-Use-Tools**). ამიტომ შეზღუდულად მოითხოვება, რომ პროგრამა „ძირითადად"[25] სისხლისსამართლებრივი დანაშაულის ჩადენას ემსახურებოდეს ან აღნიშნული მის „არსებით"[26] მიზანს წარმოადგენდეს. გერმანიის სსკ-ის § 202c-თან დაკავშირებულ საკონსტიტუციო მართლმსაჯულებაში[27] შეზღუდულად მოითხოვება, რომ პროგრამა სუბიექტურად იმ მიზნით უნდა იყოს შექმნილი ან მოდიფიცირებული, რომ გამოყენებულ იქნას სისხლისსამართლებრივი დანაშაულების ჩადენისას და ეს განზრახვა ობიექტურად უნდა იყოს გაცხადებული (მაგალითად, ინტერნეტში რეკლამის მეშვეობით). [28]

2. ჯაშუშობა და მონაცემების ხელში ჩაგდება (გერმანიის სსკ-ის §§ 202a, 202b, 202c)

გერმანიის სსკ-ის §202a-ც 1986 წლის 2. WiKG კანონით იქნა მიღებული, რათა შევსებულიყო ის სისხლისსამართლებრივი სიცარიელეები, რომლებიც არსებობდა პირადი ცხოვრების ხელშეუხებლობისა და საიდუმლოების დაცვის სფეროსთან დაკავშირებით.[29] სისხლის სამართლის კოდექსში ცვლილებების განხორციელების შესახებ 2007 წლის 7 აგვისტოს[30] 41-ე კანონით კიბერდანაშაულის შესახებ ევროსაბჭოს 2001 წლის 8 ნოემბრის კონვენციის[31] და საინფორმაციო სისტემებზე თავდასხმების შესახებ[32] ევროკავშირის 2005 წლის 24 თებერვლის N:2005/222/JI ჩარჩო გადაწყვეტილების იმპლემენტაციისათვის კი 2007 წლის 8 ნოემბრისათვის გაფართოვდა არამხოლოდ დანაშაულის შემადგენლობები, არამედ ასევე შემოღებულ იქნა გერმანიის სსკ-ის შემდგომი პარაგრაფები: §§ 202b, 202c. პრაქტიკაში აღნიშნული დანაშაულები მოიცავენ განსაკუთრებით ელექტრონული იდენტობების, საკრედიტო ბარათების, ელექტრონული ვაჭრობისა და ანგარიშების მონაცემების, განსაკუთრებით Phishing-ისა და Pharming-ის გამოყენებით „ქურდობას". მოპოვებული მონაცემების გამოყენება ხდება ან თავად დამნაშავის მიერ ან სხვისდება ე. წ. შავ ინტერნეტ ბაზარზე.[33]

ა) **გერმანიის სსკ-ის §202a-ის პირველი აბზაცის (ჯაშუშობის გზით მონაცემთა მოპარვა)** მიხედვით, 3 წლამდე თავისუფლების აღკვეთით ან ფულადი ჯარიმით ისჯება პირი, რომელიც უფლებამოსილების გარეშე, მონაცემებზე უსაფრთხო წვდომის დარღვევით თავად ეუფლება ან სხვას ეხმარება იმ მონაცემებზე დაშვების მიღებაში, რომლებიც მისთვის არაა განკუთვნილი და არაუფლებამოსილი დაშვებისაგან განსაკუთრებულადაა დაცული. მონაცემებს გერმანიის სსკ-ის §202a-ის მეორე აბზაცის გაგებით, წარმოადგენს ის მონაცემები, რომლებიც ელექტრონულად, მაგნიტურად ან სხვაგვარად პირდაპირ მიუწვდომლად არის შენახული ან რომელთა გადაცემაც ამგვარი გზით ხორციელდება. აქედან გამომდინარე, მონაცემების დეფინიცია ძალიან ფართოა, მასში ასევე მოიაზრება მონაცემები, რომლებიც ინახება მაგნიტურ ფირებზე, მაგნიტურ დისკეტებზე, მყარ დისკებზე, ფლეშ მეხსიერებებზე, მეხსიერების ბარათებზე (ასევე სმარტფონებზე), საკრედიტო ბარათებზე, CD ან DVD დისკებზე. [34]

[24] Bundestagsdrucksache (BT-Drucks.) 15/1720, 11.

[25] *Heger, Martin,* in: Lackner/Kühl (Hrsg.), StGB, 28. Aufl. 2014, § 263a Rn. 26b.

[26] *Fischer, Thomas*, StGB, 64. Aufl. 2017, Rn. 31.

[27] Bundesverfassungsgericht – Computer und Recht 2009, 673.

[28] *Waßmer, Martin Paul*, Computerbetrug (§ 263a StGB), in: Leitner, Werner/Rosenau, Henning, Wirtschafts- und Steuerstrafrecht, 2017, Rn. 107 m. w. N.

[29] Bundestagsdrucksache (BT-Drs.) 10/5085, 28.

[30] Bundesgesetzblatt (BGBl) I, 1786.

[31] ETS-Nr. 185.

[32] Amtsblatt (ABl.) L 69, 67.

[33] შეად. Bundeskriminalamt, Bundeslagebild Cybercrime 2016, 4, 12 (ხელმისაწვდომია: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html).

[34] *Hilgendorf, Eric/Valerius, Brian,* Computer- und Internetstrafrecht, 2. Aufl. 2012, Rn. 538.

დანაშაულის შემადგენლობა, პირველ რიგში, მოითხოვს მონაცემების განსაკუთრებული დაცულობის არსებობას. აღნიშნული გულისხმობს უსაფრთხოების იმგვარი ზომების არსებობას, რომლებიც გამორიცხავენ მონაცემებზე დაშვებას ან, სულ მცირე, უმნიშვნელოდ არ ართულებენ მას.[35] მეორე, აუცილებელია წვდომის უსაფრთხოება იქნას დაძლეული, რისთვისაც უნდა არსებობდეს უფლებამოსილების გარეშე კონკრეტულ დროის მონაკვეთში განხორციელებული ან ტექნიკური სახის მცდელობა.[36] ამიტომ, გაბატონებული შეხედულების მიხედვით,[37] ე. წ. Skimming, მაშასადამე, გადახდის ბარათის მაგნიტურ ლენტზე ჩაწერილი მონაცემების უბრალო წაკითხვა არ ქმნის დანაშაულის შემადგენლობას. თუმცა შესაძლოა ეს შემთხვევები მოიცვას გერმანიის სსკ-ის §202c-მა (იხ. ქვემოთ IV.2.გ.) მოცემული დანაშაულის მომზადების შემადგენლობამ, თუკი გამოყენებული იქნება კომპიუტერული პროგრამები.[38] მესამე შეზღუდვას ქმნის ნიშანი **„არაუფლებამოსილი“,** რომლითაც გარანტირებულია, რომ მაგალითად, დანაშაულის შემადგენლობა არ მოიცავს შემთხვევას, რომლის დროსაც მონაცემთა გაჟონვა ხდება მონაცემთა დამუშავების ელექტრონული სისტემის უსაფრთხოების ხარვეზებიდან გამომდინარე, როცა „ჰაკერს“ ეს დავალება საწარმოს მხრიდან გადაეცა.[39]

ბ) **გერმანიის სსკ-ის § 202b (მონაცემების ხელში ჩაგდება)** მიხედვით, პირი, რომელიც უფლებამოსილების გარეშე თავისთვის ან სხვა პირისთვის ტექნიკური საშუალებების გამოყენებით მონაცემთა არასაჯარო გაცვლის პროცესში ჩარევით ან მონაცემთა დამუშავების სისტემის ელექტრომაგნიტური გამოსხივების საფუძველზე მოიპოვებს მონაცემებს, რომლებიც მისთვის არაა განკუთვნილი (გერმანიის სსკ-ის § 202a მე-2 აბზაცი)**,** ისჯება 2 წლამდე თავისუფლების აღკვეთით ან ფულადი ჯარიმით. ამ შემთხვევაში მოიაზრება მონაცემთა გადაცემის ნებისმიერი ფორმა (მაგალითად, უკაბელო ინტერნეტის, ელექტრონული შეტყობინების, ტელეფონის, ხმოვანი შეტყობინების, ფაქსის მეშვეობით). დანაშაულის შემადგენლობა მოითხოვს **„არასაჯაროობის“** ელემენტის არსებობას, რისთვისაც გადამწყვეტია არა მონაცემების სახეობა და შინაარსი, არამედ მონაცემების გადაცემის პროცესი.[40] მონაცემთა მოპოვებისათვის არ აქვს მნიშვნელობა მონაცემთა კოდირების ფაქტის არსებობას.[41] ამ შემთხვევაში არ მოიაზრება მაგალითად, ე. წ. Phishing, რომლის დროსაც, მსხვერპლი წვდომის მონაცემებს თავისი სურვილით უგზავნის დამნაშავეს.[42]

გ) **გერმანიის სსკ-ის § 202c** მიხედვით, 2 წლამდე თავისუფლების აღკვეთით ან ფულადი ჯარიმით ისჯება პირი, რომელიც ამზადებს გერმანიის სსკ-ის § 202a და § 202b გათვალისწინებულ დანაშაულებს. კერძოდ, პირი, რომელიც ამზადებს, თავისთვის ან სხვისთვის მოიპოვებს, ასხვისებს, სხვა პირს გადასცემს, ავრცელებს ან სხვაგვარად ხელმისაწვდომს ხდის (1.) პაროლებს ან უსაფრთხოების სხვა კოდებს, რომლითაც შესაძლებელია მონაცემებზე დაშვება, ან (2.) კომპიუტერულ პროგრამებს, რომელთა მიზანიც ამგვარი დანაშაულის ჩადენაა. ამასთან აქ გამოყენებულ უნდა იქნეს გერმანიის სსკ-ის § 149 მე-2 და მე-3 აბზაცით გათვალისწინებული რეგულაციები ქმედითი მონანიების შესახებ. კანონმდებელს ამ რეგულაციით ყველაზე მეტად სურდა მოეცვა ის ჰაკერული მექანიზმები, რომლებიც ინტერნეტში ფართოდაა გავრცელებული.[43] ამასთან, აქ პრობლემა არის ის, რომ ე. წ. ორმაგი მიზნით გამოყენებადი მექანიზმები **(Dual-Use-Tools)** უსაფრთხოების დამცავი კომპანიების მიერ სატესტო პროგრამის სახით შესაძლოა იქნას გამოყენებული. აქედან გამომდინარე, საკონსტიტუციო სასამართლოს მიხედვით, (შეად. IV.1.ბ.) ნორმა შეზღუდულად უნდა განიმარტოს.

[35] Bundestagsdrucksache (BT-Drs.) 16/3656, 10.

[36] Bundestagsdrucksache (BT-Drs.) 16/3656, 10.

[37] Bundesgerichtshof – Neue Zeitschrift für Strafrecht (BGH NStZ) 2011, 154.

[38] *Waßmer, Martin Paul*, Computerbetrug (§ 263a StGB), in: Leitner, Werner/Rosenau, Henning, Wirtschafts- und Steuerstrafrecht, 2017, Rn. 108 m. w. N.

[39] Bundestagsdrucksache (BT-Drs.) 16/3656, 10.

[40] Bundestagsdrucksache (BT-Drs.) 16/3565, 11.

[41] *Eisele, Jörg,* in: Schönke, Adolf/Schröder, Horst, StGB, 29. Aufl. 2014, Rn. 4a.

[42] *Eisele, Jörg,* in: Schönke, Adolf/Schröder, Horst, StGB, 29. Aufl. 2014, Rn. 4.

[43] Bundestagsdrucksache (BT-Drs.) 16/3656, 12.

3. მტკიცებულების ძალის მქონე მონაცემების გაყალბება და შეცდომაში შეყვანა სამართალბრუნვისას მონაცემთა დამუშავების პროცესში (გერმანიის სსკ-ის §§ 269, 270)

გერმანიის სსკ-ის §§ 269, 270 ასევე **2. WiKG** კანონის საფუძველზე იქნა მიღებული, რათა ამოვსებულიყო დასჯადობასთან დაკავშირებული ხარვეზები, რადგან გერმანიის სსკ-ის § 267 (დოკუმენტების გაყალბება) არ გამოიყენება, როდესაც კომპიუტერში შენახული მონაცემები ვიზუალურად აღქმადი სახით არ იცვლება.[44]

გერმანიის სსკ-ის § 269-ის პირველი აბზაცის მიხედვით, 5 წლამდე თავისუფლების აღკვეთით ან ფულადი ჯარიმით ისჯება პირი, რომელიც სამართალბრუნვისას შეცდომაში შეყვანის მიზნით, მტკიცებულების ძალის მქონე მონაცემებს იმგვარად ჩაწერს ან შეცვლის, რომ მისი აღქმით ეს დოკუმენტი მცდარი ან გაყალბებულია, ან გამოიყენებს ამგვარად ჩაწერილ ან შეცვლილ მონაცემებს. **გერმანიის სსკ-ის § 270-ის** მიხედვით, სამართალბრუნვისას შეცდომაში შეყვანა უთანაბრდება სამართალბრუნვისას მონაცემთა დამუშავების პროცესზე არასწორ ზემოქმედებას. ეს გათანაბრება სამართლებრივ სიცხადეს ქმნის იმ შემთხვევებისათვის, რომელთა დროსაც დამნაშავე დოკუმენტებს და მონაცემებს კონკრეტულ პირს კი არ გადაუგზავნის, არამედ კომპიუტერში კითხულობს.[45] პრაქტიკაში დანაშაულის შემადგენლობებს შესაძლოა წარმოადგენდეს არამხოლოდ ის შემთხვევები, რომელთა დროსაც პირები ელექტრონული მისამართის ან საკრედიტო ბარათების მონაცემების დაკარგვის მიზნით შეცდომაში შეჰყავთ კონკრეტულ იდენტობას ან კომპანიის სახელს ამოფარებული ელექტრონული შეტყობინებების მიღებით, არამედ აქ ასევე მოიაზრება მაგალითად, ელექტრონულ მისამართებზე ზიანის მიმყენებელი პროგრამების გაგზავნა, რომლებიც გადასახადების გადახდის ქვითრების სახით არიან შენიღბულნი.[46] ამ დანაშაულების მცდელობაც დასჯადია (გერმანიის სსკ-ის § 269 მე-2 აბზაცი). უფრო მეტიც, არამხოლოდ განსაკუთრებით მძიმე შემთხვევებისათვის არსებობს უფრო დიდი სასჯელის საფრთხე (გერმანიის სსკ-ის § 269 მე-3 აბზაცი), არამედ ასევე ჯგუფურად ან პროფესიული საქმიანობის გამოყენებით დანაშაულის ჩადენის შემთხვევებშიც (გერმანიის სსკ-ის § 269 მე-4 აბზაცი).

4. მონაცემთა შეცვლა და კომპიუტერული საბოტაჟი (გერმანიის სსკ-ის §§ 303a, 303b)

და ბოლოს, 2. WiKG კანონით შემოღებულ იქნა გერმანიის სსკ-ის §§ 303a, 303b, რათა ამოვსებულიყო დასჯადობის ის სიცარიელეები„ რომლებიც არსებობდა ქონებრივ დაზიანებასთან დაკავშირებით (გერმანიის სსკ-ის § 303).[47] სისხლის სამართლის კოდექსი ცვლილებების განხორციელების შესახებ 41-ე კანონის (IV.2.) საფუძველზე, 2007 წლის 11 ნოემბერს შეივსო სისხლისსამართლებრივი ნორმები და მოსამზადებელი ქმედებებიც დასჯადი გახდა. პრაქტიკაში დანაშაულის შემადგენლობების ქვეშ მოიაზრება **„ქონების ელექტრონული დაზიანების“** მრავალი ფორმა კომპიუტერულ სისტემებზე თავდასხმებთან ერთად (ე. წ. DoS-/DDos თავდასხმები), ზიანის მიმყენებელი პროგრამების (ე. წ. Trojaner-ის, ვირუსების, ე. წ. ქსელური ჭიების) გამოყენება და მომზადება.[48]

გერმანიის სსკ-ის §303a მესამე აბზაცით (მონაცემთა შეცვლა), ორ წლამდე თავისუფლების აღკვეთა ან ფულადი ჯარიმა ემუქრება პირს, რომელიც მართლსაწინააღმდეგოდ წაშლის ან დამალავს მონაცემებს, შეცვლის ან შეუძლებელს გახდის მათ გამოყენებას. გარდა ამისა, **გერმანიის სსკ-ის § 303b პირველი აბზაცით (კომპიუტერული საბოტაჟი),** სამ წლამდე თავისუფლების აღკვეთით ან ფულადი ჯარიმით ისჯება პირი, რომელიც სხვა პირისათვის არსებითი მნიშვნელობის მქონე მონაცემთა დამუშავების პროცესს იმით უშლის მნიშვნელოვნად ხელს, რომ იგი (1.) გერმანიის სსკ-ის

[44] Bundestagsdrucksache (BT-Drs.) 10/318, 31.

[45] Bundestagsdrucksache (BT-Drs.) 10/318, 34.

[46] Bundeskriminalamt, Bundeslagebild Cybercrime 2016, 5 (ხელმისაწვდომია: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html).

[47] Bundestagsdrucksache (BT-Drs.) 10/5058, 34.

[48] Bundeskriminalamt, Bundeslagebild Cybercrime 2016, 5 (ხელმისაწვდომია: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html).

§ 303a პირველი აბზაცით გათვალისწინებულ დანაშაულს ჩადის, (2.) მონაცემებში შედის იმ მიზნით, რომ ზიანი გამოიწვიოს ან მათ გადამისამართებას ახდენს ან (3.) მონაცემების დამუშავების სისტემას ან მონაცემთა მატარებელს აზიანებს, ანადგურებს, მის გამოყენებას შეუძლებელს ხდის, შლის ან ცვლის. თუკი მონაცემთა დამუშავება უცხო საწარმოსთვის, უცხო კომპანიისათვის ან სახელმწიფო ორგანოსათვის არსებითი მნიშვნელობის მქონეა მაშინ გერმანიის სსკ-ის § 303a მე-2 აბზაცი სასჯელის სახით 5 წლით თავისუფლების აღკვეთას ან ფულად ჯარიმას ითვალისწინებს. ამ შემთხვევაშიც დანაშაულის მცდელობა დასჯადია (გერმანიის სსკ-ის § 303a მე-2 აბზაცი და § 303b მე-3 აბზაცი) და არსებობს რეგულაცია განსაკუთრებით მძიმე შემთხვევებისათვისაც (გერმანიის სსკ-ის §303b მე-4 აბზაცი). დანაშაულის მომზადებისათვის გერმანიის სსკ-ის §202c შესაბამისად გამოიყენება (გერმანიის სსკ-ის § 303a მე-3 აბზაცი და § 303b მე-5 აბზაცი).

V. თვალსაზირი

კიბერდანაშაულის გამოვლინების მრავალი ფორმის წინააღმდეგ ბრძოლა გერმანიაში სისხლისსამართლებრივი ნორმების გამოყენებით ხდება, რომლებიც დანაშაულის სხვადასხვა სფეროს ქვეშ არიან თავმოყრილნი და თავიანთი გადაკვეთის წერტილებით დაცვის საკმაოდ მსხვილ ქსელს ქმნიან. აღნიშნულით გათვალისწინებული დაცვის მექანიზმი დღეისათვის საკმარისია. აღნიშნული ჩანს ასევე იმაში, რომ ჩრდილოეთ რაინ ვესტფალიის მიწის იუსტიციის მინისტრის 2017 წლის აგვისტოს ინიციატივა, რომლის თანახმადაც, „სახლის მყუდროებაში ელექტრონული გზით ჩარევა“ დამოუკიდებელი სისხლისსამართლებრივი ნორმით დასჯადი უნდა გამხდარიყო, დღემდე ფართოდაა უარყოფილი.[49] რადგან სისხლისსამართლებრივი დასჯადობის ხარვეზები, მაგალითად, კომპიუტერის მომხმარებლების მიერ ვებკამერების მეშვეობით ფარული გადაღების შემთხვევაში, რომელიც კონტროლდება სპეციალური ჯგუფური პროგრამების, ე. წ. Botnet-ების მიერ, ამ დროისათვის არ არსებობს. სწორედ ამიტომ, ფედერაციული მიწის – ჰესენის – 2016 წლის[50] საკანონმდებლო განაცხადი, რომლის თანახმადაც, ასევე სახლის მყუდროებაში ელექტრონული გზით ჩარევა სისხლისსამართლებრივად დასჯადი უნდა გამხდარიყო, ფედერალური მთავრობის მხრიდან უარყოფილ იქნა.[51] მიუხედავად ამისა, არსებული სისხლისსამართლებრივი ნორმები განმარტებისას ნაწილობრივ პრობლემებს მაინც ქმნიან. ამიტომ უმჯობესი იქნება, რომ მათ უკეთესად სისტემატიზირებული ხასიათი ჰქონდეთ და უფრო მკაცრად შემოსაზღვრულნი იყვნენ,[52] რათა პრაქტიკოსებს მათზე მუშაობა გაუმარტივდეთ.

მხედველობიდან არ უნდა გამოგვრჩეს, რომ **საფრთხის შექმნისა და ზიანის მიყენების პოტენციალი** მუდმივად იზრდება, რადგან ინტერნეტის მნიშვნელობა, როგორც პირადი, ასევე საქმიანი ურთიერთობების სფეროში კვლავ იზრდება. ეს, ერთი მხრივ, სოციალური მედიის, ინტერნეტვაჭრობის და „ინტერნეტ ბანკინგის“ სწრაფი ზრდის შედეგია. მეორე მხრივ, განუწყვეტლივ ვითარდება ახალი ტექნოლოგიები, როგორებიცაა, მაგალითად, ელექტრონული მაცივრების გამოყენება („Internet of Things, IoT“) ან საწარმოში მიმდინარე პროცესების ინტერნეტზე დაფუძნებული მართვა (ე. წ. „ინდუსტრია 4.0“). ამით იზრდება ასევე მანიპულაციებისა და თავდასხმების შესაძლებლობები.[53] ამას ემატება, რომ დამნაშავეების პროფესიონალიზმი და ორგანიზებულობა არამხოლოდ იზრდება, არამედ კიბერდანაშაულების ჩადენა უფრო და უფრო მეტად შეუძლიათ იმ პირებსაც, რომელთაც არ აქვთ განსაკუთრებული კომპიუტერული ცოდნა.[54]

[49] შეად. http://www.wn.de/Freizeit/Ratgeber/Digitales/2941045-Digitaler-Hausfriedensbruch-soll-Straftatbestand-werden-Experten-zweifeln-an-Gesetzesentwurf.

[50] Gesetzesantrag vom 23.9.2016, Bundesrat – Drucksachen (BR-Drs.) 338/16 (B).

[51] Stellungnahme der Bundesregierung vom 2.11.2016, Bundestagsdrucksache (BT-Drs.) 18/10182.

[52] Vorschläge bei *Sieber, Ulrich,* in: 69. Deutscher Juristentag München 2012, Thesen der Gutachter und Referenten, 32 f. (ხელმისაწვდომია: http://www.djt.de/fileadmin/downloads/69/120809_djt_69_thesen_web.pdf).

[53] Bundeskriminalamt, Bundeslagebild Cybercrime 2016, 25, 26 (ხელმისაწვდომია: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html).

[54] Bundeskriminalamt, Bundeslagebild Cybercrime 2016, 27 (ხელმისაწვდომია: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html).

რადგან ე. წ. ელექტრონული „მიწისქვეშა ეკონომიკა“ **(„Underground Economy“)** დღეს მომსახურებისათვის საკმაოდ დიდ გამტარუნარიანობას ქმნის, ისეთს, როგორებიცაა ე. წ. სპეციალური ჯგუფური პროგრამები, ე. წ. Botnet-ები, ცალკეული კომპიუტერული პროგრამები, საკომუნიკაციო პლატფორმები, ანონიმურობის მიმნიჭებელი და ე. წ. სახოსტინგო მომსახურებები,[55] რომლებიც სისხლისსამართლებრივი დანაშაულების ჩადენის შესაძლებლობას იძლევიან ან მათ ჩადენას ამარტივებენ.

მომავალში ფოკუსირება უმეტესად ინფრასტრუქტურაზე მოხდება, როგორც ამას **საქართველოზე განხორციელებული კიბერთავდასხმები** ნათლად აჩვენებს. უსაფრთხოების სამსახურებს აქვთ შიში ელექტრონული 11 სექტემბრის განხორციელებისა. სწორედ ამიტომ, გერმანიაში ჯერ კიდევ 2011 წლის აპრილში შეიქმნა **კიბერთავდასხმების თავიდან აცილების ეროვნული ცენტრი** (NCAZ), რომელიც ფუნქციონირებს, როგორც უსაფრთხოების ორგანოების თანამშრომლობისათვის შექმნილი გაერთიანება საინფორმაციო და საკომუნიკაციო ტექნოლოგიების ინფრასტრუქტურებზე ელექტრონული თავდასხმების თავიდან ასაცილებლად. [56]

2017 წლის აპრილში ფედერაციის თავდაცვის სამინისტრომ **კიბერარმიასაც** ჩაუყარა საფუძველი, რათა ინფრასტრუქტურები მომავალში უკეთ იქნას დაცული უცხო ქვეყნების ჰაკერული თავდასხმებისაგან და ძალებისაგან.[57] არმიის, საზღვაო ფლოტის და საჰაერო ძალების გვერდით, კიბერარმია შექმნის ახალ შეიარაღებულ დანაყოფს, რომელიც თავდაპირველად 260 ჯარისკაცისაგან შედგება. 2021 წლისათვის საბრძოლო დანაყოფს 13.500 ჯარისკაცი და 1500 სამოქალაქო თანამშრომელი ეყოლება. ამით ასევე გათვალისწინებული იქნება ის ფაქტიც, რომ ნატომ კიბერსივრცე 2016 წლის ივნისში ოპერაციების დამოუკიდებელ სივრცედ გამოაცხადა.[58] მას შემდეგ შესაძლებელია ჰაკერულმა თავდასხმებმა ნატოს წევრ ქვეყანაზე ჩრდილოატლანტიკური ხელშეკრულების მე-5 მუხლის ამოქმედება გამოიწვიოს.

გარდა ამისა, ითვლება, რომ კიბერდანაშაულთან, როგორც ტრანსნაციონალური დანაშაულის ფორმასთან ბრძოლა უსაფრთხოების სამსახურებისა და ეკონომიკის სფეროში მოქმედი კომპანიების მჭიდრო და ნდობაზე დაფუძნებულ **კოოპერაციას** მოითხოვს, არამხოლოდ ეროვნულ, არამედ ევროკავშირის და საერთაშორისო დონეზე. მხოლოდ ინფორმაციის მუდმივი გაცვლით იქნება შესაძლებელი მომავალში ელექტრონულ დანაშაულთან ეფექტიანი და მდგრადი ბრძოლა.

და ბოლოს, ცენტრალური მნიშვნელობის მქონეა, რომ მთავრობებმა და უსაფრთხოების სამსახურებმა იზრუნონ **ეფექტიან პრევენციაზე,** განსაკუთრებით მოსახლეობისა და კომპანიებისათვის არსებულ საფრთხეების და მათი ახალი ფორმების შესახებ მუდმივ რეჟიმში ინფორმაციის მიწოდებით. ამიტომ გერმანიაში ინფორმაციული უსაფრთხოების შესახებ ფედერალური უწყება – **Bundesamt für Informationssicherheit (BSI)**[59] – ფლობს ყოვლისმომცველ ინფორმაციას კიბიერუსაფრთხოების თვალსაზრისით არსებულ მდგომარეობასთან დაკავშირებით და განუწყვეტლივ ავრცელებს ცნობებსა და გაფრთხილებებს აქტუალური კრიტიკული წერტილებისა და IT-უსაფრთხოების ინციდენტების შესახებ.

VI. დასკვნა

კიბერდანაშაული მნიშვნელოვან გამოწვევას წარმოადგენს. გერმანიაში მასზე რეაგირება ტრადიციული სისხლისსამართლებრივი დანაშაულების მოდიფიცირებით და შევსებით განხორციელდა, რომლებიც დანაშაულის სხვადასხვა სფეროს ფარავენ. საფრთხისა და ზიანის მიყენების ზრდის საფუძველზე აუცილებელია არამხოლოდ ეროვნული უსაფრთხოების ორგანოებსა და კომპანიებს შორის თანამშრომლობის შესაძლებლობების შექმნა და

[55] Bundeskriminalamt, Bundeslagebild Cybercrime 2016, 16 f. (ხელმისაწვდომია: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html).

[56] https://www.bka.de/DE/UnsereAufgaben/Kooperationen/NCAZ/ncaz_node.html; Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland, 2011, 8 f. (ხელმისაწვდომია: https://www.bmi.bund.de)

[57] შეად. http://www.zeit.de/digital/internet/2017-04/cyber-armee-bundeswehr-ursula-von-der-leyen; Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland, 2016, 38 f.

[58] შეად. http://www.zeit.de/politik/ausland/2016-06/cyberwar-nato-jens-stoltenberg-operationsgebiet.

[59] ვებ-გვერდი: https://www.bsi.bund.de.

გაფართოება, არამედ სახელმწიფოები ვალდებულნი არიან კონკრეტული ღონისძიებები განახორციელონ კიბერთავდასხმების თავიდან ასაცილებლად, მაგალითად, საბრძოლო დანაყოფის შექმნით. და ბოლოს, აუცილებელია მოსახლეობისა და კომპანიების მუდმივი ინფორმირება საფრთხის შესახებ, რადგან ეფექტიანი პრევენცია დანაშაულთან ბრძოლის პოლიტიკის საუკეთესო ფორმას წარმოადგენს.