ავტორი: დავით შაქარიშვილი

კორპორაციული შპიონაჟი

ეროვნული უსაფრთხოების განმარტება ყველა დისციპლინას სუბიექტურად ესმის. მაგალითად, ეკონომიკური სექტორი მიიჩნევს, რომ ეკონომიკური სიძლიერე ეროვნული უსაფრთხოების პირდაპირ პროპორციულია, სამოქალაქო სექტორი მას მოიზრებს საზოგადოებრივი ჩართულობის პოზიტიურ შედეგად, სამართლებრივი სექტორისთვის კი ეს კონსტრუქციულ ნორმათა სისტემაა. ნებისმიერ შემთხვევაში, ყველა ზემოთხსენებული და სხვა მიმართულება მართებულად ხსნის, რადგან ეროვნული უსაფრთხოება, სწორედ, სხვადასხვა დამოუკიდებელი ინტეგრალებით შედგება. კვეთის საერთო წერტილი შემდეგში მდგომარეობს, თუ ერთი სექტორი მაინც გამართულად ვერ წარმოებს სახელმწიფოში, ეროვნული უსაფრთხების სისტემაც ხელოვნური იქნება. სხვა სიტყვებით რომ ვთქვათ, ეროვნული უსაფრთხოება წარმოადგენს ბაზისს, რომელზედაც სხვა მიმართულებები სტრუქტურდება, შიდა და გარე სტაბილურობის დაცვა, რომლის წარმატებულად შესრულება ქვეყნის მნიშვნელობას განაპირობებს რეგიონსა და საერთაშორისო ასპარეზზე. ქვემოთ ჩვენ ვისაუბრებთ ეროვნული უსაფრთხოების ორ მამოძრავებელ

ღერძზე - დაზვერვაზე, როგორც ინფორმაციის მოპოვების მეთოდზე და კონტრდაზვერვაზე, უშიშროების სამსახურის სისტემურ დანაყოფზე, რომელიც სახელმწიფოს იცავს სხვა (მტრული, აგრესორი) ქვეყნის დაზვერვის სამსახურისგან.

თანამედროვე მსოფლიოში დაიწყო რეფორმისტული მიდგომები ინფორმაციის წვდომასთან დაკავშირებით - სახელმწიფო ინსტიტუტების ფორმირება, ეკონომიკური პოლიტიკის ცვლილება და ტექნოლოგიურ ინოვაციები. გამონაკლისი არც კერძო სექტორი გახლდათ და უკვე მე-20 საუკუნის მეორე ნახევრიდან ყალიბდება ახალი დისციპლინა, რომელსაც კორპორაციული დაზვერვა ეწოდება.

კორპორაციულ დაზვერვას (ან/და კორპორაციულ შპიონაჟს) სხვადასხვა ლიტერატურაში ვარიაციული დეფინიცია აქვს, თუმცა მსოფლიოს წამყვანმა კვლევითმა და საკონსულტაციო ცენტრმა, "გარტნერმა" (Gartner), შემდეგნაირი განმარტება გააკეთა - *კორპორაციული დაზვერვა არის პროცედურათა რთული სისტემა, რომელიც მოიაზრებს ინფრასტრუქტურის, ინსტრუმენტებისა და საუკეთესო პრაქტიკის გამოყენებით ინფორმაციაზე წვდომასა და მის ანალიზს.* როგორც განმარტებიდან ჩანს, კორპორაციული დაზვერვა წარმოადგენს კომპლექსური პროცესების ერთობლიობას, რაც მიმართულია სავაჭრო ბაზრის ორ ან მეტ სუბიექტებს შორის ფინანსური, მატერიალური ან ტექნიკური უპირატესობის მოსაპოვებლად. ბიზნეს დაზვერვის ორი მიდგომა არსებობს - კლასიკური და თანამედროვე. კლასიკური მოდელის თვალსაზრისით, ორგანიზაციის დაზვერვის ამოსავალი წერტილი გახლდათ ინფორმაციული ტექნოლოგიების განყოფილებები, ხოლო ინსტრუმენტს წარმოადგენდა სტატისტიკური მონაცემები. იმ შემთხვევაში თუ მენეჯერული რგოლების წარმომადგენლები ხარვეზს აღმოაჩენდნენ სადაზვერვო პროცესი თავიდან იწყებოდა.

ასეთი მიდგომა, თავის მხრივ, პროცესს დროში გაწელილსა და რთულს ხდიდა. თანამედროვე მოდელი ითვალისწინებს ციკლურ პროცედურას,

რომელშიც სამი შიდა საუწყებო სუბიექტი მონაწილეობს, კერძოდ პოზიციის მენეჯერი, ინტერაქციის, შეფასებისა და განხილვის საფუძველზე აგროვებს ინფორმაციას მომხმარებლის შესახებ, კონტენტის შემქმნელი (content creator) აანალიზებს მიღებულ ინფორმაციას და აწვდის ინფორმაციული ტექნოლოგიების მენეჯერს, რომელიც თავის მხრივ, მიღებულ ინფორმაციაზე დაყრდნობით იწყებს მოქმედებას.

დღესდღეობით, ბიზნეს დაზვერვის მოთხოვნა და გარანტიები იმდენად მაღალია, რომ იგი კოლოსალურ პოზიტიურ ან ნეგატიურ გავლენას ახდენს გლობალურ ეკონომიკაზე. უკანასკნელი სტატისტიკური მონაცემებით, 2016 წლიდან 2020 წლამდე კორპორაციების სადაზვერვო ხარჯები 15.24-დან 29.48 მილიარდ დოლარამდე გაიზრდება, 11 პროცენტიანი ნაერთი წლიური ზრდის ტემპით. მზარდი ტენდეციის სეგმენტად მოიაზრება „ქლაუდ“ სისტემებზე დაფუძნებული ბიზნესები, რომელთა ხარჯვითი წილი, 2013-2018 წლებში, გაიზარდა 750 მილიონი დოლარიდან 2.5 მილიარდ დოლარამდე, 31 პროცენტიანი ნაერთი წლიური ზრდის ტემპით. მცირე ბიზნესის 46 პროცენტი ბიზნეს დაზვერვის ინსტრუმენტებს, იყენებს როგორც ორგანიზაციის სტრატეგიის მთავარ ელემენტს. აგრეთვე, დასახელდა ბიზნეს დაზვერვის ოთხი ყველაზე მსხვილი და აგრეთვე, ყველაზე დაცული მეგა კორპორაციები: 1. Amazon Web Service; 2. Microsoft Azure; 3. Google Cloud; 4. IBM Bluemix.

ბიზნეს დაზვერვა იმდენად ეფექტიანი და დროში დინამიური გამოდგა, რომ ზოგიერთმა სახელმწიფომ დაიწყო ამ მიმართულებით თანმიმდევრული მუშაობა, რათა დაზვერვის ზოგიერთი ინსტრუმენტი დეცენტრალიზებული ყოფილიყო. ამ პროფილის შესაბამისად შეიქმნა დაზვერვის კერძო სააგენტოები (Private Intelligence Agencies). არ არის საფუძველს მოკლებული ის მოსაზრება, რომ სახელმწიფოები, სადაც ეს უკანასკნელი სააგენტოები ფუნქციონირებენ, ატარებენ დაზვერვის სამსახურის ბუნებას, მოქმედებენ საკუთრების უფლების იურისდიქციაში, რაც მათ

უფლებამოსილებებს უფრო ფართო არეალს უშლის, ვიდრე სახელმწიფოს. საკუთრების უფლების იურისდიქციაში მოიაზრება კერძო სექტორის ანუ ბიზნესის სტატუსი, შესაბამისად სახელმწიფო ნაკლებად ერევა და საერთაშორისო სამართალიც ნაკლებად ეხება კერძო სექტორს, საერთაშორისო სამართალს შეუძლია შეზღუდოს სახელმწიფოების სადაზვერვო ინსტრუმენტების მოქმედება, მაგრამ ურთულდება შეკვეცოს ბიზნესის უფლებები, რასაც თავის ინტერესებში კარგადაც იყენებენ კორპორაციულ შპიონაჟში. განვიხილოთ ზოგიერთი მათგანი:

1. „არქიმედეს ჯგუფი“ (Archimede Group) - შეიქმნა 2017 წელს და ოპერირების არეალს წარმოადგენს მედია საშუალებები. ყველაზე გახმაურებული შემთხვევა მოხდა 2019 წლის იანვარში, როცა ფეისბუქის ადმინისტრაციამ, გამოძიების მეშვეობით, დაადგინა, რომ „არქიმედეს“ ჯგუფმა ერთ მილიონ დოლარზე მეტი დახარჯა, რათა ფეისბუქზე გაევრცელებია პროპაგანდის შემცველი რეკლამები. როგორც ზემოთ აღვნიშნეთ, აქ წარმოიშვება დილემა - ერთი მხრივ ეს უკანასკნელი კერძო კომპანიაა და კომერციული კამპანიები მისი პრეროგატივაა, თუმცა წმინდა სამხედრო თვალსაზრისით, იგი შეიცავს ინფორმაციული და ფსიქოლოგიური ომის უამრავ ელემენტს;

2. „ეგისის თავდაცვის სამსახური“ (Aegis Defence Service) - ეგისის თავდაცვის სამსახური ფუნქციონირებს დიდ ბრიტანეთში და აქვს სამდივნოები ერაყში, საუდის არაბეთში, ლიბიაში, სომალსა და მოზამბიკაში. 2005 წლის 27 ოქტომბერს გავრცელდა ვიდეო, რომელშიც ასახულია სამხედრო პირების მიერ ცეცხლის გახსნის ფაქტი სამოქალაქო მანქანების მიმართულებით. ვიდეო რგოლები არაოფიციალურად უკავშირდებოდა ეგისის თავდაცვის სამსახურს. როგორც ამერიკულმა არმიამ, ისე ეგისმა ჩაატარეს გამოძიება ამ ვიდეოსთან დაკავშირებით; მიუხედავად იმისა, რომ ეგის ანგარიში დახურულია კლიენტის კონფიდენციალურობის მიზეზების გამო, აშშ-ს არმიის გამოკითხვამ დაასკვნა, რომ მონაწილე კონტრაქტორები მოქმედებდნენ ძალის გამოყენების ფარგლებში.

ამრიგად, ბიზნეს დაზვერვის სამსახურები დღითიდღე იძენენ პოლიტიკური მოთამაშეებისა და დიდი გავლენის მქონე სუბიექტების ბუნებას. მას შემდეგ რაც ამერიკის შეერთებულ შტატებში, ბოინგის ქარხნის თანამშრომელმა კომერციული საიდუმლო, სოლიდურ ფასად, მიყიდა ჩინეთს მიიღეს კანონი ეკონომიკური შპიონაჟის შესახებ, სადაც მინიმუმამდეა დაყვანილი ბიზნეს დაზვერვის მიერ პროვოცირებული პოტენციური სააფრთხეები, თუმცა ციფრულ სამყაროში მაინც დგას მთავარი პრობლემა - თუ ბიზნეს დაზვერვა გაიდაქცევა ინფორმაციული და ფსიქოლოგიური ომის ინსტრუმენტად, მაშინ საფრთხე შეექმნება, როგორც გლობალურ, აგრეთვე რეგიონალურ და ლოკალურ უსაფრთხოებას

გამოყენებული ლიტერატურა

- *B. S. Bhatia and G. S. Batra, "Management of Capital Markets, Financial Services and Institutions", New-Delhi, Deep & Deep Publication Pvt Ltd. Year 2001;*
- *Altfeld, Michael. "The Decision to Ally: A Theory and Test," The Western Political Quarterly, 37:4 (December 1984), pp. 523–544;*
- *Ayres, Robert U. "On Forecasting Discontinuities," Technological Forecasting and Social Change, 65:1 (September 2000), pp. 81–97;*
- *Adler, P.S., and Borys, B. 1996. "Two Types of Bureaucracy: Enabling and Coercive."Administrative Science Quarterly 41 (1): 61-87;*
- *Re-theorizing external learning: insights from economic and industrial espionage.*
- *Management Learning, 38(3), 297-317Fink, S. (1986). Crisis management: Planning for theinevitable: American Management Association. Herring, J. P. (1992).*
- *Business intelligence in Japan and Sweden: Lessons for the US. Journal of Business strategy,13(2), 44-49.] House, W. (1995). Annual Report to Congress on Foreign Economic Collection and Industrial Espionage. Washington, DC: Government Printing Office.*
- *Malone, N., Baluja, K. F., Costanzo, J. M., & Davis, C. J. (2000). The foreign-born*
- *population: 2000. US Census Bureau, US Department of Commerce, Census, 01-01. [8]*
- *Mendell, R. L. (2011).*
- *Brand Finance Institute (2017) Global Intangible Finance Tracker 2017 http://brandfinance.com/images/upload/gift_report_2017_bf_version_high_res_vers ion.pdf*

- *Button, M. (2008) Doing Security.Basingstoke: Palgrave. Cabinet Office/Detica (2011)The Cost of Cyber Crime. London: Cabinet Office;*
- *Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber*
- *security: a systematic literature review and meta-analysis. Big Data Analytics, 1(1), 6.*
- *Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human*
- *vulnerability. Journal of the Association for Information Systems, 18(1), 22.*
- *IP Commission (2017) The theft of American intellectual property: reassessments of the challenge and united states policy.*