ნიდერლანდების სამეფოს კიბერშესაძლებლობები

ნიდერლანდების სამეფომ კიბერუსაფრთხოების სტრატეგია მიიღო 2013 წელს[1] და სფეროს მთავარი მაკოორდინირებელი ორგანო არის კიბერუსაფრთხოების ეროვნული ცენტრი[2], რომელიც შედის ქვეყნის უსაფრთხოებისა და იუსტიციის სამინისტროში[3]. ცენტრის საქმიანობა ნახევრად გასაიდუმლოებულია, რაზეც პასუხისმგებელია დაზვერვისა და უსაფრთხოების გენერალური სამსახური[4]

ცენტრის სერვისებში შედის: - ექსპერტიზა და რეკომენდაციები[5]; - საფრთხეებსა და ინციდენტებზე რეაგირება[6] და - კრიზისების მართვის გაძლიერება[7].

საერთაშორისო დონეზე ცენტრი არის the Computer Security and Incident Response Teams (CSIRTs) – ის წევრი. ის ასევე აქტიურად თანამშრომლობს:

- FIRST (Forum of Incident Response and Security Teams)[8];
- EGC (European Government CERTs):
  - Germany - CERT-Bund[9];
  - Denmark - GovCertDK[10];
  - Finland - CERT-FI[11];
  - France - CERTA[12];
  - Great Britain- CPNI en GovCertUK[13];
  - Hungary - CERT-Hungary[14];
  - Norway - NorCERT[15];
  - Austria - GovCERT.AT[16];

---

[1] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf
[2] the National Cyber Security Centre https://www.ncsc.nl/english
[3] the Ministry of Security and Justice;
[4] the General Intelligence and Security Service (AIVD);
[5] https://www.ncsc.nl/english/services/expertise-advice
[6] https://www.ncsc.nl/english/services/incident-response.html
[7] https://www.ncsc.nl/english/services/crisis-management-reinforcement.html
[8] http://www.first.org/
[9] https://www.cert-bund.de/
[10] https://www.govcert.dk/
[11] http://www.cert.fi/
[12] http://www.certa.ssi.gouv.fr/
[13] http://www.govcertuk.gov.uk/
[14] http://www.cert-hungary.hu/
[15] http://www.cert.no/
[16] http://www.govcert.at/

  - Spain - CCN-CERT[17];
  - Sweden - CERT-SE[18];
  - Switzerland - GovCERT.ch[19];
- Terena (Trans-European Research and Education Networks Association)[20];
- ISF (Information Security Forum)[21];
- ENISA (European Network and Information Security Agency)[22];
- The following are other international CSIRTs with which we cooperate intensively:
  - Poland NASK[23] and CertPolska[24];
  - Australia AusCERT[25] and CERT.au[26];
  - United States of America CertCC[27] and US-CERT[28];
  - Japan JPCert[29];
- I4 (International Information Integrity Institute)[30].

ციფრული სისტემები სულ უფრო დიდ როლს თამაშობს ნიდერლანდების სამეფოს დაზვერვისა და უსაფრთხოების საკითხში. ამის გამო, ქვეყნის შეიარაღებული ძალების მიზანია დაძლიონ ყველა ის საფრთხე, რომელიც დაკავშირებულია ციფრულ სფეროსთან და ზოგადად კიბერსივრცესთან. ამიტომ ნიდერლანდების შეიარაღებული ძალების საზღვაო, სახმელეთო, საჰაერო და კოსმოსური შენაერთების გვერდით, შეიქმნა მეხუთე ოპერატიული დომეინი.

ნიდერლანდების თავდაცვის სამინისტრო თავის კიბერ თავდაცვის სტრატეგიაში, რომელიც 2012 წლის 27 ივნისს[31] იქნა მიღებული, პრიორიტეტს ანიჭებს შემდეგ ექვს მიმართულებას:

1) <u>ციფრული უსაფრთხოება უნდა იყოს მიმართული ყველა ფრონტზე</u>
   შეიარაღებული ძალები იყენებს ციფრულ სისტემებს პრაქტიკულად ყველა თავის ოპერაციაში. ისინი გამოიყენება ლოგისტიკაში, მართვასა

[17] https://www.ccn-cert.cni.es/
[18] http://www.cert.se/
[19] http://www.melani.admin.ch/
[20] http://www.terena.org/
[21] http://www.securityforum.org/
[22] http://www.enisa.europa.eu/
[23] http://www.nask.pl/nask_en/
[24] http://www.cert.pl/
[25] http://www.auscert.org.au/
[26] http://www.cert.gov.au/
[27] http://www.cert.org/
[28] http://www.us-cert.gov/
[29] http://www.jpcert.or.jp/english/
[30] https://i4online.com/
[31] https://ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf

და კონტროლში, დაზვერვაში, ჯარების დაცვაში, მანევრირებაში, ცეცხლის კორექტირებასა და წარმოებაში. თავდაცვის კიბერ სარდლობა[32] შედგება ყველა სამხედრო შენაერთის მოსამსახურისგან;

2) <u>თავდაცვის სამინისტროსი და შეიარაღებული ძალების ციფრული მდგრადობის გაძლიერება</u>
თავდაცვის ორგანიზაცია პასუხისმგებელია საკუთარი ქსელისა და სისტემების დაცვაზე. Joint Information Technology Command (JITC) უზრუნველყოფს ციფრული მდგრადობის გაძლიერებას.
JITC - ის დაქვემდებარებაშია თავდაცვის კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი[33], რომელიც უზრუნველყოფს თავდაცვის ციფრული ინფრასტრუქტურის დაცვას. 24/7 - ის რეჟიმში, ჯგუფი აფასებს რისკებს, თავდაცვის ქსელის სუსტ და მოწყვლად ადგილებს, იძლევა რჩევებს უსაფრთხოების ზომებზე;

3) <u>სამხედრო კიბერ ოპერაციების შესაძლებლობები</u>
ნიდერლანდების შეიარაღებული ძალები არ უნდა იყოს კიბერშეტევებისგან მხოლოდ თავდაცვის მდგომარეობაში, არამედ მას უნდა შეეძლოს განახორციელოს საპასუხო კიბერშეტევა, რათა დაიცვას მთლიანი თავდაცვითი ინფრასტრუქტურა. ამ კუთხით, აქტიურად თანამშრომლობს სამხედრო დაზვერვისა და უსაფრთხოების სამსახურთან[34];

4) <u>ციფრულ სამყაროში დაზვერვის პოზიციების გაძლიერება</u>
ნიდერლანდების შეიარაღებულ ძალებს უნდა ჰქონდეთ წარმოდგენა იმ საფრთხეების შესახებ, რომელიც არსებობს კიბერსივრცეში, რათა მიიღონ შესაბამისი ზომები. ეს არის პოტენციური ან რეალური მოწინააღმდეგეებისა და თავდამსხმელების ტექნოლოგიური შესაძლებლობები, საიდანაც მოდის საფრთხეები.
- მომავალ წლებში სამხედრო დაზვერვისა და უსაფრთხოების სამსახურს (DISS) მიეცემა მეტი უფლებები და ექნება უფრო მეტი შესაძლებლობები საიდუმლოდ შეაგროვოს ინფორმაციები კიბერუსაფრთხოებისა და კიბერსივრცის შესახებ. შედეგად, ინფორმაციის მიღების მიზნით, სამსახური შეძლებს რეგულარულად

[32] Defence Cyber Command (DCC).
[33] the Defence Computer Emergency Response Team (DefCERT);
[34] the Defence Intelligence and Security Service (DISS);

შეაღწიოს ქსელებსა და კომპიუტერულ სისტემებში. გარდა ამისა, სამსახური შეძლებს უკეთესად აკონტროლოს ქსელები და გამოიკვლიოს კიბერ შეტევების შესაძლებლობები;

- სამხედრო დაზვერვისა და უსაფრთხოების სამსახურსა (DISS) და მთავარ სადაზვერვო და უსაფრთხოების სამსახურს[35] ექნებათ საერთო ბლოკი, რომელიც აწარმოებს რადიო და კიბერ სადაზვერვო საქმიანობას - the SIGINT Cyber Unit (cyber and signals intelligence);
- DISS მჭიდროდ თანამშრომლობს გაერთიანებული მართვის საინფორმაციო ცენტრთან[36], ნიდერლანდების სასამართლო მედიცინის ინსტიტუტთან[37], პოლიციის მომსახურების ეროვნულ სააგენტოსთან[38] და ნიდერლანდების სამეფო ჟანდარმერიასთან[39];

5) <u>ცოდნის მყარი ბაზის მიღება და კიბერსივრცეში ინოვაციური შესაძლებლობების გაზრდა</u>

თავდაცვის სამინისტრო მუდმივად მუშაობს კიბერსივრცის შესახებ ცოდნის, ახალი ტექნოლოგიებისა და უნარების განახლებაზე.

- თავდაცვის კიბერსივრცის ცენტრის ექსპერტები[40] განავითარებენ ცოდნას კიბერ ოპერაციების შესახებ. ცენტრი მჭიდროდ თანამშრომლობს სამეცნიერო - კვლევით ცენტრებთან[41];
- თავდაცვაში შექმნილია ვირტუალური ლაბორატორია, სადაც ტესტურ გარემოში ტარდება სამეცნიერო კვლევები;
- თავდაცვის საკადრო პოლიტიკაა კიბერ სფეროს მაღალკვალიფიციური სპეციალისტების მოზიდვა და მათი შენარჩუნება;
- 2012 წელს ნიდერლანდების თავდაცვის აკადემიაში დაინიშნა კიბერ ოპერაციების უფროსი ლექტორი;

6) <u>თავდაცვის უწყება ეროვნულ და საერთაშორისო დონეებზე თანამშრომლობს სხვადასხვა მიმართულებით</u>

[35] the General Intelligence and Security Service (GISS);
[36] the Joint Information Management Command;
[37] the Netherlands Forensic Institute;
[38] the National Police Services Agency;
[39] the Royal Netherlands Marechaussee.
[40] the Defence Cyberspace Centre of Expertise (DCEC);
[41] ერთერთი ასეთი ინსტიტუტია the Netherlands Organisation for Applied Scientific Research https://www.tno.nl/en/

- თავდაცვის უწყება წარმოდგენილია კიბერუსაფრთხოების ეროვნულ ცენტრში[42];
- თავდაცვის სამინისტრო წარმოდგენილია კიბერუსაფრთხოების საბჭოში, სადაც ასევე შედიან წარმომადგენლები სახელმწიფო და კერძო სექტორიდან, და სამეცნიერო წრეებიდან;
- თავდაცვის უწყება მჭიდროდ თანამშრომლობს IT ინოვაციების პლატფორმასთან 'Veilig Verbonden' [Safe Connection];
- თავდაცვის სამინისტრო ატარებს ერთობლივ ოპერაციებსა და ღონისძიებებს ალიანსთან და მის წევრებთან.

ნიდერლანდების ციფრული გარემოს დაცვის გასაძლიერებლად შეიარაღებული ძალების შემადგენლობაში შეიქმნა კიბერ სარდლობა[43], რომელიც არის ნიდერლანდების სამეფოს არმიის ნაწილი და პასუხისმგებელია კიბერუსაფრთხოების უზრუნველყოფაზე თავდაცვის უწყებასა და მის პარტნიორ ორგანიზაციებში.

კიბერ სარდლობა კონცენტრირდება კიბერუსაფრთხოების შემდეგ სამ მიმართულებაზე:

- *თავდაცვა* - ყველა ციფრული სისტემა უნდა იყოს დაცული კიბერ შეტევებისგან და ჯაშუშობისგან;
- *დაზვერვა* - შეიარაღებული ძალები უნდა იყვნენ წინასწარ ინფორმირებულნი ციფრულ სფეროში არსებული საფრთხეების შესახებ. ეს საფრთხეები შეიძლება მოდიოდეს როგორც გარედან, ისე საკუთარი სისტემებიდან;
- *შეტევა* - შეიარაღებულ ძალებს შეუძლია თავად განახორციელოს შეტევა, მოახდინოს მანიპულირება და მწყობრიდან გამოიყვანოს მოწინააღმდეგის სისტემები. პოტენციური მოწინააღმდეეგები არის სხვა სახელმწიფოები, ტერორისტული ორგანიზაციები და ჰაკერები.

ციფრული სისტემები ასრულებს დიდ და მნიშვნელოვან როლს ქვეყნის შეიარაღებულ ძალებში. საკომუნიკაციო, სანავიგაციო, სენსორული და სამხედრო ციფრული სისტემები მუდმივად არის კიბერ შეტევის რისკის ქვეშ. საფრთხეები შეიძლება მოდიოდეს სხვა სახელმწიფოებიდან, ასევე ტერორისტული, რელიგიური თუ კომერციული სუბიექტებისგან. საფრთხეებს შეიძლება მოჰყვეს:

- სისტემებზე ლოკალური და მასირებული შეტევა;
- ჯაშუშობა.

[42] the National Cyber Security Centre (NCSC) https://www.ncsc.nl/english
[43] the Dfence Cyber Command (DCC).

ამა წლის 2 თებერვალს შეიარაღებული ძალების კიბერ ოპერაციების ხელმძღვანელად დაინიშნა პოლკოვნიკი, დოქტორი Paul Ducheine, რომელიც აწარმოებს კვლევებს კიბერუსაფრთხოების სამხედრო და სამართლებრივი ასპექტების შესახებ. ახალი ხელმძღვანელი არის უფროსი ლექტორი ნიდერლანდების თავდაცვის აკადემიის სამხედრო მეცნიერების ფაკულტეტზე, სადაც კითხულობს კიბერ ოპერაციებსა და კიბერუსაფრთხოებას. შეიძლება ის მალე გახდეს ბრიგადის გენერალი.