



(51) International Patent Classification:

G06F 21/55 (2013.01) G01S 13/02 (2006.01)
G06F 21/57 (2013.01) G01S 13/06 (2006.01)
G05D 1/00 (2006.01)

(21) International Application Number:

PCT/IL2022/050768

(22) International Filing Date:

17 July 2022 (17.07.2022)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

285252 29 July 2021 (29.07.2021) IL

(71) Applicant: **ELTA SYSTEMS LTD.** [IL/IL]; 100 Yitzchak
Hanassi Blvd., P.O.B. 330, 7710201 Ashdod (IL).

(72) Inventor: **HAZAN, Alexander**; 22 Nimrov street,
7131925 Lod (IL).

(74) Agent: **LEVIN, Elena**; REINHOLD COHN AND PART-
NERS, P.O. Box 13239, 6113102 Tel Aviv (IL).

(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,

HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE,
KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU,
LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA,
NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO,
RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH,
TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS,
ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,
TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

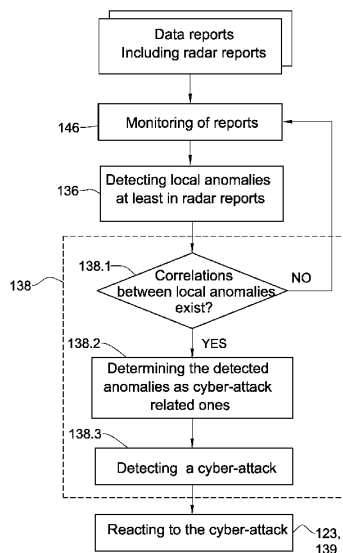
Declarations under Rule 4.17:

— of inventorship (Rule 4.17(iv))

Published:

— with international search report (Art. 21(3))

(54) Title: TECHNIQUE FOR DETECTING CYBER ATTACKS ON RADARS



(57) Abstract: A computer-implemented technique for detecting a cyber attack in a radar system which comprises a number of modules configured to produce data reports on their performance. The modules include one or more radars and perform the following actions: monitoring operation of the radar system by collecting and processing the data reports including the radar reports, detecting one or more local anomalies at least in the radar reports, analyzing the detected local anomalies for identifying one or more correlations there-between; if the correlations are identified, determining the detected anomalies as cyber anomalies (a cyber attack). Upon detecting the cyber attack, at least one predetermined action may be taken in response.

Fig. 5