Threat Artificial Intelligence and Cyber Security in Health Care Institutions

Ana Fernandes, Margarida Figueiredo, Filomena Carvalho, José Neves, and Henrique Vicente

Abstract In this work we go beyond what is called unsupervised learning, a decision-making method that results in large numbers of false positives and negatives. The study was carried out in cryopreservation laboratories and aims to gain access to the *General Data Protection Regulation* (*GDPR*) implementation. Indeed, on the one hand, using *Threat Artificial Intelligence, Chaos, Entropy and Security* (*TAICE&S*) based methodology for problem solving one may mimic behaviors that are similar to the best human analysts. With the entry into force of the *GDPR* in the health institutions of the *European Union* (*EU*), stronger rules (*TAICE based*) on data protection (*Security*) mean people have more control over their personal data and businesses benefit from a level playing field. To respond to this challenge, a workable tool had to be built exploring the dynamics between *TAICE&S* and *Logic Programming* for *Knowledge Representation and Reasoning*, leading to the implementation of an agency based on *TAICE/Cyber Security* based techniques for problem solving,

A. Fernandes · H. Vicente (✉)
Departamento de Química, Escola de Ciências e Tecnologia, REQUIMTE/LAQV, Universidade de Évora, Évora, Portugal
e-mail: hvicente@uevora.pt

A. Fernandes
e-mail: anavilafernandes@gmail.com

M. Figueiredo
Departamento de Química, Escola de Ciências e Tecnologia, Centro de Investigação em Educação e Psicologia, Universidade de Évora, Évora, Portugal
e-mail: mtf@uevora.pt

F. Carvalho
Departamento de Ciências Jurídicas, Escola Superior de Tecnologia e Gestão, Instituto Poltécnico de Leiria & Centro de Investigação IJP—Instituto Jurídico Portucalense, Leiria, Portugal
e-mail: filomena.carvalho@ipleiria.pt

J. Neves
Instituto Politécnico de Saúde do Norte, CESPU, Famalicão, Portugal
e-mail: jneves@di.uminho.pt

J. Neves · H. Vicente
Centro Algoritmi, Universidade do Minho, Braga, Portugal

S. Misra and A. Kumar Tyagi (eds.), *Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities*, Studies in Computational Intelligence 972, https://doi.org/10.1007/978-3-030-72236-4_13, 24 pp.

which is consistent with an *Artificial Neural Network* approach to problem definition. It is therefore possible to provide a full-bodied *TAICE* method to assist in threat identification and evaluation, activity prediction, mitigation, and response strategies. Using *TAI* procedures, one may identify patterns and matches in the activity of threat players, that combined with the issues of *Chaos* and *Entropy* gives us an opportunity to mimic how qualified specialists react in scenarios where models break off.

Keywords Threat artificial intelligence · Chaos · Entropy · Security · Logic programming · Knowledge representation and reasoning · Artificial neural networks