**COMPLETE THE FORM BELOW**

**NUME ȘI PRENUME (CU INIȚIALA / INIȚIALELE TATĂLUI, AȘA CUM SE REGĂSESC ÎN CATALOG):**

|  |
| --- |
| Rusu M. Raul-Mihai |

**FACULTATEA DE:**

|  |
| --- |
| Matematică-Informatică |

**SPECIALIZAREA:**

|  |
| --- |
| Informatică |

**ANUL DE STUDIU: LINIA DE STUDIU: GRUPA:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **2** |  | **Engleza** |  | **926** |

\* \* \*

**TO BE COMPLETED BY THE EXAMINER**

|  |  |  |
| --- | --- | --- |
| **SCORE** |  | **CFR LEVEL OF PROFICIENCY** |
|  |  |  |

\* \* \*

**READING COMPREHENSION**

*Graduation Test of English*

*May - June 2020*

**INSTRUCTIONS:**

**1. Download the document onto your own PC. Do not change the format of the document.**

**2. Write your answers in the boxes provided.**

**3. Work individually. Use your own words to write your answers. Do not share your answers with any other student. Papers with identical or very similar answers will be invalidated regardless of who copied from whom. The same happens if you copy paste answers from the Internet.**

**4. Once you have completed all the tasks, name the document as follows:** Nume Prenume Grupa Reading (*for example* Suciu Valeriu 923 Reading) **and upload it to your Google Drive Folder** (**create a folder** entitled according to the following format: Grupa English Examination Nume Prenume *for example* 923 English Examination Suciu Valeriu and **share** **the folder via email using the following email address:** [english.exam.info@gmail.com](mailto:english.exam.info@gmail.com)).[[1]](#footnote-0)

**5. Upload your document before the deadline expires (May 31, 2020, 23.59) and do not modify your document after the deadline.**

**The test starts on the next page**

***Exercise 1***

**Read Text A and extract relevant words and phrases to create a concept map around the central concept of “open data”. You can use** [**coggle.it**](https://coggle.it/) **to help you create a map of your own. (2p)**

**Insert the link to your concept map in the box below.**

|  |
| --- |
|  |

\* \* \*

***Exercise 2***

**Read Text B and, in the space below, write in your own words 2 positive and 2 negative effects of “behavioural biometrics” in the boxes below. Do not copy and paste from the text. (3.5p)**

**Positive effects**

|  |
| --- |
| Behavioural biometrics can detect fraud. Every person has different behaviours and routines and it is very hard to copy them perfectly, thus a computer can detect when another person is using a device or when an account is accessed by another person. |
| Behavioural biometrics can uniquely identify a person and verify his identity. |

**Negative effects**

|  |
| --- |
| In a way the systems track every move you make and the way you behave in order to be sure that the user is really you. But if something is tracking you non stop it is like you have no privacy. |
| In bad hands behavioural biometrics can be used to spy on people. Letting the owners know every move you make . |

\* \* \*

***Exercise 3***

**Read Text C and, after carefully examining the author’s view on *superintelligent robots and artificial intelligence* write a reaction paper of no more than 300 words, using the given structure: (4.5p)**

**Suggested structure:**

Summary paragraph (overview of the main points from Text C)

Reaction paragraph 1

Topic sentence for first reaction paragraph

Argument for first reaction paragraph

Reaction paragraph 2

Topic sentence for second reaction paragraph

Argument for the second reaction paragraph

Concluding paragraph

**Write your article in the box below:**

|  |
| --- |
| In the given article written by Oren Etzioni he dives right in the fear of some people. The fear of an impending doom, the fear of super computers taking over the world and tries to show how far from an AI that can do everything better than us we really are. Exemplifying this through a few scenarios, or canaries.  Firstly, in my opinion the author is right about the statement that current AIs are idiot savants. Being a programmer myself i quickly understood that machines, laptops and other devices are not smart, or butter put are not smart by nature. We as programmers give a little bit of our intelligence to them. Programs are created every day that can solve problems much faster than we can, but those programs work in certain parameters and if the input is a little bit off the programs don’t know how to react. There is no program that can do every task.  Secondly, Oren says that the Turing Test is not a good canary and I do not agree with this one bit. If a computer convinces the participants to think that it is let's say an 6 year old child that means a lot. An eight year old understands a lot about the word, he can solve simple tasks with ease, he has his one thoughts and opinions about subjects, he can create bounds with others. In the first paragraph I was trying to illustrate the difference between real intelligence and the illusion of intelligence, a computer convincing people that it is a real person is a sign of real intelligence.  To summarize a computer that is really intelligent is nowhere close to the near future and we still don’t know what lies ahead for AI technology. |

**TEXTS**

\* \* \*

TEXT A

**A well-connected city**

Transparency and accountability initially fuelled the open data movement, but now public bodies, citizens and businesses are using open data as a way to provide practical information and services, from real-time car park space information to real-time information on river water levels. In the past two years alone, 90 percent of the world’s data was created, and by 2020, it’s estimated that 50 billion devices will be connected to the Internet. What’s even more surprising is that experts predict the number of devices connected, such as smart meters and intelligent lighting, will outnumber the people who are using them.

For cities like Cork, access to “official, open format non-personalised data” puts power in the hands of citizens, allowing them to take a more active role in the community in terms of decision-making. “Openness and transparency is a key government priority. Opening up government data will empower citizens, foster innovation and reform public services. This strategy aims at fostering an ecosystem that will enable Ireland to become a leader in Open data,” explained Patrick O’Donovan TD, Minister of State for Open Government and eGovernment, at the launch of the national Open Data Strategy for 2017-2020.

Citizens in Cork can already benefit from technology such as maps of real-time transportation information, which feature a number of available public bikes for hire, as well as train and bus times. While this technology provides a more connected and increased quality of life, these advancements may also come at a risk. As data is integrated into applications and services, smart cities need to be aware of the security risks open data could pose and put the right measures in place to protect the city - and the citizens - from potential cyberattacks.

*Adapted from* [*https://eu.smartcitiescouncil.com/article/cork-open-data-key-smart-region-success*](https://eu.smartcitiescouncil.com/article/cork-open-data-key-smart-region-success)

\* \* \*

**TEXT B**

**Online identification is getting more and more intrusive**

Most online fraud involves identity theft, which is why businesses that operate on the web have a keen interest in distinguishing impersonators from genuine customers. Passwords help. But many can be guessed or are jotted down imprudently. Newer phones, tablets, laptops and desktop computers often have beefed-up security with fingerprint and facial identification. But these can be spoofed. To overcome these shortcomings, the next level of security is likely to identify people using things which are harder to copy, such as the way they walk.

Many online security services already use a system called device fingerprinting. This employs software to note things like the model type of a gadget employed by a particular user; its hardware configuration; its operating system; the apps which have been downloaded onto it; and other features, including sometimes the Wi-Fi networks it regularly connects through and devices like headsets it plugs into.

The results are sufficient to build a profile of both the device and its user’s habits. If something unusual is then spotted - say, a bank detects access to an account from a phone with a different profile from that which a customer usually uses - it can take appropriate measures. For example, additional security questions can be posed.

LexisNexis Risk Solutions, an American analytics firm, has catalogued more than 4 billion phones, tablets and other computers in this way for banks and other clients. Roughly 7% of them have been used for shenanigans of some sort. But device fingerprinting is becoming less useful. Apple, Google and other makers of equipment and operating systems have been steadily restricting the range of attributes that can be observed remotely. The reason for doing this is to limit the amount of personal information that could fall into unauthorised hands. But such restrictions also make it harder to distinguish illegitimate from legitimate users.

That is why a new approach, behavioural biometrics, is gaining ground. It relies on the wealth of measurements made by today’s devices. These include data from accelerometers and gyroscopic sensors that reveal how people hold their phones when using them, how they carry them and even the way they walk. Touchscreens, keyboards and mice can be monitored to show the distinctive ways in which someone’s fingers and hands move. Sensors can detect whether a phone has been set down on a hard surface such as a table or dropped lightly on a soft one such as a bed. If the hour is appropriate, this action could be used to assume when a user has retired for the night. These traits can then be used to determine whether someone attempting to make a transaction is likely to be the device’s habitual user.

Behavioural biometrics makes it possible to identify an individual’s “unique motion fingerprint”, says John Whaley, head of Unifyid, a firm in Silicon Valley that is involved in the field. With the right software, data from a phone’s sensors can reveal details as personal as which part of someone’s foot strikes the pavement first, and how hard; the length of a walker’s stride; the number of strides per minute; and the swing and spring in the walker’s hips and step. It can also work out whether the phone in question is in a handbag, a pocket or held in hand.

Using these variables, Unifyid sorts gaits into about 50 000 distinct types. When coupled with information about a users’ finger pressure and speed on the touchscreen, as well as a device’s regular places of usage - as revealed by its GPS unit - that user’s identity can be pretty well determined, Mr Whaley claims. Unifyid began offering behavioural biometrics to its clients (which include retail banks, online retailers, delivery companies and ride-sharing firms) in 2017. In time, advertisers will pay for the scoop on individuals’ lifestyle-revealing moments, reckons Mr Whaley, though his firm has no plans yet to expand in that direction.

Behavioural biometrics can, moreover, go beyond verifying a user’s identity. It can also detect circumstances in which it is likely that a fraud is being committed. On a device with a keyboard, for instance, a warning sign is when the typing takes on a staccato style, with a longer-than-usual finger “flight time” between keystrokes. This, according to Aleksander Kijek, head of product at Nethone, a firm in Warsaw that works our behavioural biometrics for companies that sell things online, is an indication that the device has been hijacked and is under the remote control of a computer program rather than human typist.

On a device with a touchscreen, rather than a keyboard, however, the reverse is true. Most people type with their thumbs on touchscreens, so flight times between keystrokes are longer. In this case, therefore, it is short flight times between keystrokes which are a signal of something suspicious going on - for example, that a touchscreen device is actually being operated remotely, using the keyboard of a laptop.

Used wisely, behavioural biometrics can be a boom. As Neil Costigan, the boss of BehavioSec, a behavioural-biometrics firms in San Francisco, observes, the software can toil quietly in the background, continuously authenticating account-holders without badgering them for additional passwords, their mother’s maiden name “and all that nonsense.” Unifyid and an unnamed car company are even developing a system that unlocks the doors of a vehicle once the gait of the driver, as measured by his phone, is recognised.

Used unwisely, however, the system could become yet another electronic spy on people’s privacy, permitting complete strangers to monitor your every action, from the moment you reach for your phone in the morning, to when you fling it on the floor at night.

*Adapted from “The Economist”,*

[*https://www.economist.com/science-and-technology/2019/05/23/online-identification-is-getting-more-and-more-intrusive*](https://www.economist.com/science-and-technology/2019/05/23/online-identification-is-getting-more-and-more-intrusive)

**\* \* \***

**TEXT C**

**How to know if artificial intelligence is about to destroy civilisation**

*By Oren Etzioni*

Could we wake up one morning dumbstruck that a super-powerful AI has emerged, with disastrous consequences? Books like *Superintelligence* by Nick Bostrom and *Life 3.0* by Max Tegmark, as well as more recent articles, argue that malevolent superintelligence is an existential risk for humanity. But one can speculate endlessly. It’s better to ask a more concrete, empirical question: What would alert us that superintelligence is indeed around the corner?

We might call such harbingers canaries in the coal mines of AI. If an artificial-intelligence program develops a fundamental new capability, that’s the equivalent of a canary collapsing: an early warning of AI breakthroughs on the horizon.

Could the famous Turing test serve as a canary? The test, invented by Alan Turing in 1950, posits that human-level AI will be achieved when a person can’t distinguish conversing with a human from conversing with a computer. It’s an important test, but it’s not a canary; it is, rather, the sign that human-level AI has already arrived. Many computer scientists believe that if that moment does arrive, superintelligence will quickly follow. We need more intermediate milestones.

Is AI’s performance in games such as Go, poker or Quake 3, a canary? It is not. The bulk of so-called artificial intelligence in these games is actually *human* work to frame the problem and design solution. AlphaGo’s victory over human Go champions was a credit to the talented human team at DeepMind, not to the machine, which merely ran the algorithm the people had created. This explains why it takes years of hard work to translate AI success from one narrow challenge to the next. Even AlphaZero, which learned to play world-class Go in a few hours, hasn’t substantially broadened its scope since 2017. Methods such as deep learning are general, but their successful application to a particular task requires extensive human intervention.

More broadly, machine learning is at the core of AI’s success over the last decade or so. Yet the term “machine learning” is a misnomer. Machines possess only a narrow sliver of human’s rich and versatile learning abilities. To say that machines learn is like saying that baby penguins know how to fish. The reality is, adult penguins swim, capture *fish*, digest it, regurgitate into their beaks, and place morsels into their children’s mouths. AI is likewise, being spoon-fed by human scientists and engineers.

In contrast to machine learning, human learning maps a personal motivation (“I want to drive to be independent of my parents”) to a strategic learning plan (“Take driver’s ed and practice on weekends”). A human formulates specific learning targets (“Get better at parallel parking”), collects and labels data (“The angle was wrong this time”), and incorporates external feedback and background knowledge (“The instructor explained how to use the side mirrors”). Humans identify, frame, and shape learning problems. None of these human abilities is even remotely replicated by machines. Machines can perform superhuman statistical calculations, but that is merely the last mile of learning. The automatic formulation of learning problems, then, is our first canary. It does not appear to be anywhere close to dying.

Self-driving cars are a second canary. They are further in the future than anticipated by boosters like Elon Musk. AI can fail catastrophically in atypical situations, like when a person in a wheelchair is crossing the street. Driving is far more challenging than previous AI tasks because it requires making life-critical, real-time decisions based on both the unpredictable physical world and interaction with human drivers, pedestrians, and others. Of course, we should deploy limited self-driving cars once they reduce accident rates, but only when human-level driving is achieved can this canary be said to have keeled over.

AI doctors are a third canary. AI can already analyse medical images with superhuman accuracy, but that is only a narrow slice of a human doctor’s job. An AI doctor would have to interview patients, consider complications, consult other doctors and more. These are challenging tasks that require understanding people, language and medicine. Such a doctor would not have to fool a patient into thinking it is human - that’s why this is different from the Turing test. But it would have to approximate the abilities of human doctors across a wide range of tasks and unanticipated circumstances.

And though the Turing test itself is not a good canary, limited versions of the test could serve as canaries. Existing AIs are unable to understand people and their motivations, or even basic physical questions like “Will a jumbo jet fit through a window?” We can administer a partial Turing test by conversing with an AI like Alexa or Google Home for a few minutes, which quickly exposes their limited understanding of language and the world. Consider a very simple example based on the Winograd schemas proposed by computer scientist Hector Levesque. I said to Alexa: “My trophy doesn’t fit into my carry-on because it is too large. What should I do?” Alexa’s answer was “I don’t know that one.” Since Alexa can’t reason about sizes of objects, it can’t decide whether “it” refers to the trophy or the carry-on. When AI can’t understand the meaning of “it”, it’s hard to believe it is poised to take over the world. If Alexa were able to have a substantive dialogue on a rich topic, that would be a fourth canary.

Current AIs are idiot savants: successful on narrow tasks, such as playing Go or categorising MRI images, but lacking the generality and versatility of humans. Each idiot savant is constructed manually and separately, and we are decades away from the versatile abilities of a five-year-old-child. The canaries I propose, in contrast, indicate inflection points for the field of AI.

Some theorists, like Bostrom, argue that we must nonetheless plan for very low-profitability but high-consequence events as though they were inevitable. The consequences, they say, are so profound that our estimates of their likelihood aren’t important. This is a silly argument: it can be used to justify about anything. It is a modern-day version of the argument by the 17th-century philosopher Blaise Pascal that it is worth acting as if a Christian God exists because otherwise you are at risk of an everlasting hell. He used the infinite cost of an error to argue that a particular course of action is “rational” even if it is based on a highly improbable premise. But arguments based on infinite costs can support contradictory beliefs. For instance, consider an anti-Christian God who promises everlasting hell for every Christian act. That’s highly improbable as well; from a logical point of view, though, it is just as reasonable a wager as believing in the god of the Bible. This contradiction shows a flaw in arguments based on infinite costs.

My catalogue of early warning signals, or canaries, is illustrative, rather than comprehensive, but it shows how far we are from human-level AI. If and when a canary “collapses,” we will have ample time before the emergence of human-level AI to design robust “off-switches” and to identify red lines we don’t want AI to cross. AI eschatology without empirical canaries is a distraction from addressing existing issues like how to regulate AI’s impact on employment or ensure that its use in criminal sentencing or credit scoring doesn’t discriminate against certain groups.

As Andrew Ng, one of the world’s most prominent AI experts has said, “Worrying about AI turning evil is a little bit like worrying about overpopulation on Mars.” Until the canaries start dying, he is entirely correct.

*Adapted from:* [*https://www.technologyreview.com/2020/02/25/906083/artificial-intelligence-destroy-civilization-canaries-robot-overlords-take-over-world-ai/*](https://www.technologyreview.com/2020/02/25/906083/artificial-intelligence-destroy-civilization-canaries-robot-overlords-take-over-world-ai/)

**Evaluation Grid and Scoring**

***Exercise 1***

Ability to scan factual information in order to perform specific tasks = 1p

Organisation of content, overall presentation = 1p

***Exercise 2***

Ability to locate main information in sections of text = 0.5p x 4 items = 2p

Ability to rephrase given structures = 1p

Grammatical accuracy = 0.5p

***Exercise 3***

Ability to infer opinion, attitude and underlying meaning = 1p

Ability to understand the text as a whole = 0.5p

Ability to select specific information from the text = 0.5p

Ability to identify and use relevant vocabulary = 1p

Grammatical accuracy = 1p

Organisation of content according to given structure = 0.5p

1. You can find a document containing step-by-step instructions on:

   * Creating the exam folder [here](https://www.canva.com/design/DAD8N7ff0vU/DPm3riqc46RAmJpaikzHeA/view?utm_content=DAD8N7ff0vU&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton).
   * Downloading and uploading the exam document [here](https://www.canva.com/design/DAD8QlTdQPI/MTWPPcvn6dFZv_prM81bFg/view?utm_content=DAD8QlTdQPI&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton).

   [↑](#footnote-ref-0)