REGULATION OF TECHNOLOGICAL HACKATHON CHALLENGE NAMED "CYBERSECURITY CHALLENGE"

I. Definition

1. The **Cybersecurity Hackathon Challenge** is an initiative developed by the Portuguese Blockchain Alliance in partnership with Instituto Superior de Coimbra (ISEC), duly framed in the defined goals of the Alliance, aiming to endorse the promotion of knowledge on Exponential Technologies and the development of innovative solutions based in cybersecurity.
2. ISEC will be the sponsor of this challenge, whose organization will be overseen by the Portuguese Blockchain Alliance.
3. The **Cybersecurity Hackathon Challenge** will focus on **developing a cybersecurity-based solution that can automatically classify and predict cybersecurity vulnerable entities (individuals, companies, agencies and countries) to support any entity to deal with its security vulnerability (low, medium, high, extreme, etc.)**. Through this challenge we have the mission of receiving proposed solutions that can leverage the provided data sets (ANNEX) to: identify "threats", build tools and services that alert entities of security vulnerabilities, create solutions that recommend any entity on protection from a cyber-attack and monetize the solution for distribution and management by any of the alerted entities.

II. Objective of the Challenge

1. In the context of the Portuguese Blockchain Alliance, the goal of the **Cybersecurity Hackathon Challenge** is:

    a) To promote innovation in the scope of exponential technologies in the Portuguese economic system;

III. Participants Categories

1. The **Cybersecurity Hackathon Challenge** addresses two categories of participants:

    a) Startups;
    b) Students.

The participants should always apply in groups of 2 to 8 people regardless of the category of the participant (startups or universities). Groups can be composed of a set of partner entities if they belong to the same macro category: Public or Private (example: either a group composed of students from several universities or a group composed of two companies with complementary skills).

IV. Application and Requirements

1. The participants of the **Cybersecurity Hackathon Challenge** must submit their application via the Hackathon site or the Alliance's website (in the form available at: https://all2bc.com/participar), completing all the mandatory fields below:

    a) Name of the group;
    b) Number of members of the group;
    c) Full name of the participants;
    d) Age of participants;
    e) Email of the participants;

f) Challenge selection;

2. For any question or additional information about the application process, contact info@all2bc.com.

V. Phases and Selection Process of the Challenge

1. The **Cybersecurity Hackathon Challenge** consists of three phases:

I. **Development** of the proposed solution. The first phase (**Development**) focuses on developing the concept of the presented solution. This development is done in group and is supported in a mentoring model by ISEC and the Alliance. A single document limited to 7 pages in the main body should be submitted. The content of the document should include at least the following mandatory topics:
- Solution's summary;
- Final Concept;
- Benefits;
- Attachments.

II. Solution **Mentoring**. After the development phase, the application is revised by the Challenge promoter, which includes a mentoring process. This phase focuses on improving the solution demonstration. In this phase, one document/mockup must be submitted:
- A **document / application mockup** with a maximum of 10 slides that should be the presentation to be used before the selection jury with at least the following mandatory topics:
  - Executive summary;
  - Approach to the chosen Challenge;
  - Final Solution;
  - Merit and Evolution of the Solution;
  - Applicability Potential;
  - Benefits;
  - Attachments;

III. **Presentation** of the final solution(s). Finally, the participants must make a presentation / solution demonstration before the selection jury. The presentation cannot exceed 15 minutes. After this period, the selection jury will have a maximum of 5 minutes to make questions to the competitors.

VI. Hackathon Deadlines and Selection Phases Formats

Phase I: Development

1. The Cybersecurity Hackathon Challenge starts on May 14th, 2019 and the idea submission ends at 15:59 pm on May 14th, 2019;
2. All documents must be sent in PDF format with a maximum of 5 Mb;
3. This phase will continue until the final presentation.
4. In partnership, ISEC and the Portuguese Blockchain Alliance will proceed with the evaluation of the initial ideas;

Phase II: Mentoring

1. From 16:00 of the 14th of May, ISEC and Portuguese Blockchain Alliance will evaluate the ideas ideias and will give feedback for improvement;
2. This phase will continue until the final presentation.

Phase III: Presentation

1. The presentations before the selection jury will take place on May 15 at the site of the hackathon and schedules to be designated after 5:00 p.m.;
2. The order of the presentations will be established randomly;
3. Following the presentations, the jury will evaluate the solutions presented and deliberate on which will be considered finalists to present at the conference the next day. By 23:59 on May 15, 2019, participants will be informed of the jury's decision. The next day (May 16) the finalists will present their solutions at the conference.

Videos or photographs are accepted only if contextualized in the submitted document(s). The videos must be on Youtube in Unlisted format and with a maximum duration of 2 minutes. Photographs must be in JPEG format and have no more than 1 Mb.

VII. Criteria of Analysis and Evaluation

The projects will be evaluated according to the following criteria:

- Innovation (25%)
- Impact on the public sector (20%)
- Applicability to the market (20%)
- Feasibility (15%)
- Scalability (10%)
- Presentation (10%)

VIII. Selection Jury

1. The evaluation of the concept and demonstration is up to the Selection Jury.
2. The Selection Jury will be composed of elements of the following entities: ISEC, Portuguese Blockchain Alliance, and other members to be designated.
3. The decision of the Selection Jury is final and cannot be appealed.

IX. Rewards

1. Some rewards might be delivered to the best projects by the entity that promotes the challenge.
2. The rewards may include the following possibilities:
   - Communication with the media and the Alliance partners;
   - Internships at the Alliance partners;
   - Mentoring hours with CEOs of the Alliance partners;
   - Non-cash rewards (e.g. Drones, Parrots).

X. Personal Data Protection

1. For the purposes of the legislation on Protection of Personal Data, it is advised that personal data provided by the participants of this Challenge will be processed by ISEC and the Portuguese Blockchain Alliance, as Managers for Treatment.
2. The treatment of personal data of the participants by ISEC and the Portuguese Blockchain Alliance aims to (i) manage their participation in the challenge, (ii) to reward the participants with the best projects and (iii) to be compliant with legal obligations.

The processing of personal data for purposes (i) and (ii) is carried out based on the need to perform this challenge, in which the competitors participate voluntarily, and the non-provision of personal data makes it impossible for the competitor to participate in the challenge.

The processing of the data for the purpose (iii) is a legal obligation and is carried out based on its necessity for the fulfilment of legal obligations to which ISEC and the Portuguese Blockchain Alliance are subject.

3. Personal data processed for purposes (i), (ii) and (iii) shall be retained for the duration of the challenge and, in addition, for the period of time strictly necessary for the fulfilment of legal obligations.

4. ISEC and the Portuguese Blockchain Alliance may contract third parties to provide logistical support or other administrative support (for example, parties that provide information technology). These parties may have access to personal data to the extent necessary to provide such services.

5. ISEC and the Portuguese Blockchain Alliance as responsible for the treatment ensure the strict compliance with the confidentiality rules regarding the data made available by the participants.

6. The foregoing does not prevent the data subject from exercising his rights of access, rectification, deletion, limitation and opposition to the data treatment by sending an email to info@all2bc.com, proving its identity through its identification document or other suitable means of proof.

XI. Rights of personality

1. The participants hereby authorize ISEC and the Portuguese Blockchain Alliance to use their name and image in the context of their participation in the Challenge, through any means of reproduction, both electronic (Internet and similar) and non-electronic (in paper, photographs and others) for the maximum duration allowed by law.

2. The participants authorize the organizing entity, the Portuguese Blockchain Alliance, and partners to develop audiovisual contents on the participants during the extent of the challenge and for the final conference. All audiovisual contents (photography and video) produced is owned by the Portuguese Blockchain Alliance, the organizing entity.

3. The use and publication of the images and data of the interested party as a winner as set forth in these Regulation, neither generates nor grants repayment, payment of compensation or economic rights of any kind to the winner.

XII. Intellectual property

The ownership of intellectual property rights will, if development and contributions to the proposed solution justify it, is going to be defined by an agreement to be celebrated by both parties concerning the sharing of ownership and the benefits of its commercial exploitation.

ANNEX

Context

Information on more than 180,000 Terrorist Attacks

The Global Terrorism Database (GTD) is an open-source database including information on terrorist attacks around the world from 1970 through 2017. The GTD includes systematic data on domestic as well as international terrorist incidents that have occurred during this time period and now includes more than 180,000 attacks. The database is maintained by researchers at the National Consortium for the Study of Terrorism and Responses to Terrorism (START), headquartered at the University of Maryland. More Information

Content

Geography: Worldwide
Time period: 1970-2017, *except 1993*
Unit of analysis: Attack
Variables: >100 variables on location, tactics, perpetrators, targets, and outcomes
Sources: Unclassified media articles (Note: Please interpret changes over time with caution.
Global patterns are driven by diverse trends in particular regions, and data collection is influenced by fluctuations in access to media coverage over both time and place.)
Definition of terrorism:
"The threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation."
See the GTD Codebook for important details on data collection methodology, definitions, and coding schema.

Acknowledgements

The Global Terrorism Database is funded through START, by the US Department of State (Contract Number: SAQMMA12M1292) and the US Department of Homeland Security Science and Technology Directorate's Office of University Programs (Award Number 2012-ST-061-CS0001, CSTAB 3.1). The coding decisions and classifications contained in the database are determined independently by START researchers and should not be interpreted as necessarily representing the official views or policies of the United States Government.
GTD Team

Publications

The GTD has been leveraged extensively in scholarly publications, reports, and media articles. *Putting Terrorism in Context: Lessons from the Global Terrorism Database*, by GTD principal investigators LaFree, Dugan, and Miller investigates patterns of terrorism and provides perspective on the challenges of data collection and analysis. The GTD's data collection manager, Michael Jensen, discusses important Benefits and Drawbacks of Methodological Advancements in Data Collection and Coding.

Source

Website: http://start.umd.edu/gtd

Terms of Use

Use of the data signifies your agreement to the following terms and conditions.
END USER LICENSE AGREEMENT WITH UNIVERSITY OF MARYLAND
IMPORTANT – THIS IS A LEGAL AGREEMENT BETWEEN YOU ("You") AND THE UNIVERSITY OF MARYLAND, a public agency and instrumentality of the State of Maryland, by and through the National Consortium for the Study of Terrorism and Responses to Terrorism ("START," "US," "WE" or "University"). PLEASE READ THIS END USER LICENSE AGREEMENT ("EULA") BEFORE ACCESSING THE Global Terrorism Database ("GTD"). THE TERMS OF THIS EULA GOVERN YOUR ACCESS TO AND USE OF THE GTD WEBSITE, THE DATA, THE CODEBOOK, AND ANY AUXILIARY MATERIALS. BY ACCESSING THE GTD, YOU SIGNIFY THAT YOU HAVE READ, UNDERSTAND, ACCEPT, AND AGREE TO ABIDE BY THESE TERMS AND CONDITIONS. IF YOU DO NOT ACCEPT THE TERMS OF THIS EULA, DO NOT ACCESS THE GTD.

TERMS AND CONDITIONS

1. **GTD means Global Terrorism Database** data and the online user interface **(www.start.umd.edu/gtd)** produced and maintained by the National Consortium for the Study of Terrorism and Responses to Terrorism (START). This includes the data and codebook, any auxiliary materials present, and the user interface by which the data are presented.

2. **LICENSE GRANT**. University hereby grants You a revocable, non-exclusive, non-transferable right and license to access the GTD and use the data, the codebook, and any auxiliary materials solely for non-commercial research and analysis.

3. **RESTRICTIONS.** You agree to NOT: a. publicly post or display the data, the codebook, or any auxiliary materials without express written permission by University of Maryland (this excludes publication of analysis or visualization of the data for non-commercial purposes); b. sell, license, sublicense, or otherwise distribute the data, the codebook, or any auxiliary materials to third parties for cash or other considerations; c. modify, hide, delete or interfere with any notices that are included on the GTD or the codebook, or any auxiliary materials; d. use the GTD to draw conclusions about the official legal status or criminal record of an individual, or the status of a criminal or civil investigation; e. interfere with or disrupt the GTD website or servers and networks connected to the GTD website; or f. use robots, spiders, crawlers, automated devices and similar technologies to screen-scrape the site or to engage in data aggregation or indexing of the data, the codebook, or any auxiliary materials other than in accordance with the site's robots.txt file.

4. **YOUR RESPONSIBILITIES:** a. All information sourced from the GTD should be acknowledged and cited as follows: "National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland. (2018). The Global Terrorism Database (GTD) [Data file]. Retrieved from https://www.start.umd.edu/gtd" b. You agree to acknowledge any copyrightable materials with a copyright notice "Copyright University of Maryland 2018." c. Any modifications You make to the GTD for published analysis must be clearly documented and must not misrepresent analytical decisions made by START. d. You agree to seek out an additional agreement in order to use the GTD, the data, the codebook or auxiliary materials for commercial purposes, or to create commercial product or services based on the GTD, the data, the codebook or auxiliary materials.

5. **INTELLECTUAL PROPERTY.** The University owns all rights, title, and interest in the GTD, the data and codebook, and all auxiliary materials. This EULA does not grant You any rights, title, or interests in the GTD or the data, the codebook, user interface, or any auxiliary materials other than those expressly granted to you under this EULA.

6. **DISCLAIMER AND LIMITATION ON LIABILITY.** a. THE GTD, THE CODEBOOK, USER INTERFACE, OR ANY AUXILIARY MATERIALS ARE MADE AVAILABLE ON AN "AS IS" BASIS. UNIVERSITY DISCLAIMS ANY AND ALL REPRESENTATIONS AND WARRANTIES – WHETHER EXPRESS OR IMPLIED, ORAL OR WRITTEN, IN FACT OR ARISING BY OPERATION OF LAW – WITH RESPECT TO THE GTD, THE CODEBOOK, AND ANY AUXILIARY MATERIALS INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF THE INTELLECTUAL PROPERTY OR PROPRIETARY RIGHTS OF ANY THIRD PARTY. UNIVERSITY MAKES NO REPRESENTATION OR WARRANTY THAT THE GTD, THE CODEBOOK, ANY AUXILIARY MATERIALS, OR USER INTERFACE WILL OPERATE ERROR FREE OR IN AN UNINTERRUPTED FASHION. b. In no event will the University be liable to You for any incidental, special, punitive, exemplary or consequential damages of any kind, including lost profits or business interruption, even if advised of the possibility of such claims or demands, whether in contract, tort, or otherwise, arising in connection with Your access to and use of the GTD, the codebook, user interface, or any auxiliary materials or other dealings. This limitation upon damages and claims is intended to apply without regard to whether other provisions of this EULA have been breached or proven ineffective. In no event will University's total liability for the breach or nonperformance of this EULA exceed the fees paid to University within the current billing cycle. c. Every reasonable effort has been made to check sources and verify facts in the GTD; however, START cannot guarantee that accounts reported in the open literature are complete and accurate. START shall not be held liable for any loss or damage caused by errors or omissions or resulting from any use, misuse, or alteration of

GTD data by the USER. The USER should not infer any additional actions or results beyond what is presented in a GTD entry and specifically, the USER should not infer an individual referenced in the GTD was charged, tried, or convicted of terrorism or any other criminal offense. If new documentation about an event becomes available, START may modify the data as necessary and appropriate. d. University is under no obligation to update the GTD, the codebook, user interface, or any auxiliary materials.

7. **INDEMNITY.** You hereby agree to defend, indemnify, and hold harmless the University and its employees, agents, directors, and officers from and against any and all claims, proceedings, damages, injuries, liabilities, losses, costs, and expenses (including reasonable attorneys' fees and litigation expenses) relating to or arising out of Your use of the GTD, the codebook, or any auxiliary materials or Your breach of any term in this EULA.

8. **TERM AND TERMINATION** a. This EULA and your right to access the GTD website and use the data, the codebook, and any auxiliary materials will take effect when you access the GTD. b. University reserves the right, at any time and without prior notice, to modify, discontinue or suspend, temporarily or permanently, Your access to the GTD website (or any part thereof) without liability to You.

9. **MISCELLANEOUS** a. The University may modify this EULA at any time. Check the GTD website for modifications. b. No term of this Agreement can be waived except by the written consent of the party waiving compliance. c. If any provision of this EULA is determined by a court of competent jurisdiction to be void, invalid, or otherwise unenforceable, such determination shall not affect the remaining provisions of this Agreement. d. This Agreement does not create a joint venture, partnership, employment, or agency relationship between the Parties. e. There are no third party beneficiaries to this agreement. You may not assign this agreement without the University's prior written approval. f. This EULA shall be governed by and interpreted in accordance with United States copyright law and the laws of the State of Maryland without reference to its conflicts of laws rules. Nothing in this EULA is or shall be deemed to be a waiver by the University of any of its rights or status as an agency and instrumentality of the State of Maryland. The parties mutually agree to opt out of application of the Maryland Uniform Computer Information Transactions Act (MUCITA), Maryland Code Annotated [Commercial Law] 21-101 through 21-816 to the greatest extent authorized under MUCITA.
   g. This EULA represents the entire agreement between You and the University regarding the subject matter of paragraphs 1-10. There are no other understandings, written or oral, that are not included in this Agreement.

10. **REPRESENTATION.** You represent that You are at least 18 years of age.

Training

START has released the first in a series of training modules designed to equip GTD users with the knowledge and tools to best leverage the database. This training module provides a general overview of the GTD, including the data collection process, uses of the GTD, and patterns of global terrorism. Participants will learn basic data handling and how to generate summary statistics from the GTD using PivotTables in Microsoft Excel.