CYBER POLICY TRAINING AND COMPETITION CURRICULUM

1. INTRODUCTION

International Cyber Policy Training and Competition will provide a cyber policy competition and a training package composed of five modules. The target audience for the training will be freshmen in colleges and it can be expanded to high school students. This project will provide a framework which can be used by higher education institutions to organize cyber policy competition with accompanying training package for the intended audience. The project is aligned with COVA CCI strategic goals related to growing cybersecurity talent and building a collaborative network.

The project aims to improve collaboration between educational institutions by bringing students together in an interdisciplinary competition environment. Following an introductory module in cybersecurity, the students will be trained on topics like international law, foreign policy and decision making with their relevance to an international cyber crisis. This training will be finalized with a capstone competition where students can implement the knowledge and skills gained during the training.

This project provides an opportunity for students to appreciate the interdisciplinary nature of cybersecurity and has the potential to attract more students to the cybersecurity programs across the Commonwealth. There will be 5 modules and each module will have components of a lecture on the specific course content, discussion topics, group projects. A sample scenario, evaluation rubric for the scenario and a framework for the organization of a cyber policy competition will also be provided. The structure of the competition and the training package will be presented to the representatives from higher education via webinar sessions.

- Module 1: Introduction to Cybersecurity
- Module 2: Risk Management and Decision Making in Cybersecurity
- Module 3: International Relations and Cybersecurity
- Module 4: National and International Cyber Law
- Module 5: Effective Communication and Presentation Skills
- Capstone Competition: Scenario Based Cyber Policy Competition

2. MODULES

A. Module 1: Introduction to Cybersecurity

Module 1 provides students with an introduction to cybersecurity principles and is designed as the first step in preparation for a cyber policy competition. The module comprises three units that cover the following topics: cybersecurity principles, vulnerabilities and advanced persistent threats, and cybersecurity threat categories. In Unit 1, Cybersecurity Principles, the student will learn concepts and terminology that are essential to understanding how computing assets are secured against cybersecurity threats. The Confidentiality, Integrity & Availability (C-I-A) Triad security model is used to present these concepts. Each of the C-I-A triad pillars is defined, examples of attacks against each pillar are provided, and then security controls to prevent or limit the attack impacts is provided. Related security concepts of non-repudiation, identification, authentication, authorization, and auditing are also explained as methods to protect computing assets from cyber attacks.

In Unit 2, Vulnerabilities and the Advanced Persistent Threat, the student will learn about the various steps that attackers follow to execute successful cyber attacks against their targets. The Advanced Persistent Threat (APT) attack lifecycle stages are covered in depth from reconnaissance, tools development, exploit delivery, initial compromise, command and control, moving laterally through the network, completing the mission, and covering tracks. In Unit 3, Cybersecurity Threat Categories, students will learn the definitions, examples, goals, and actors involved in cyber crime, cyber espionage, cyber terrorism, and cyber warfare attacks.

-

B. Module 2: Risk Management and Decision Making in Cybersecurity

- Module 2 provides students with an introduction to cybersecurity risk management and decision making processes. The module comprises four units that cover the following topics: the cyber risk assessment process, cybersecurity risk management and governance, leadership styles and principles, and the decision-making process and biases.

- In Unit 1, Cyber Risk Assessments, the students will learn the definition of the terms "harm" and "risk" as they relate to the cyber risk assessment process. Next, several risk assessment approaches are discussed, followed by the steps of the risk assessment process . Finally, security controls to mitigate cyber risks are discussed, to include types of security controls, and how these security controls address harm.

- In Unit 2, Risk Management & Governance, the student will first learn about the definition and steps of the risk management process. Next, students will learn about risk governance as the term is defined, governance domains are explored and finally governance outcomes are discussed.

- In Unit 3, Cybersecurity Leadership, students will learn about various leadership styles, cybersecurity leadership principles, and organizational and global leadership concerns, to include Economic, Ethical, Legal, Political, Privacy, Social and Technical concerns. The students will also learn about stakeholders and their concerns within organizational and global constructs. In Unit 4, Decision Making Process and Biases, students will learn the steps for making effective decisions and the common biases that could impair their ability to make decisions.
    -

C. Module 3: International Relations and Cybersecurity

    - Module 3 is an examination of a large-scale cyber event through the application of US or international policies and strategies and the effects of the event in respect to socioeconomics, geopolitical, and national security. Topics will cover cyber deterrence and US federal agency roles, responsibilities, and responses to the cyber event. The learning objective is to understand the impact of a major cyber event and the United States' response. Although most cyber professionals will focus on events that directly affect their organization, module 3 illustrates the interconnections of cyber from the micro to macro level and the importance of events outside of their organization or originating from within has the potential of a larger impact.

D. Module 4: National and International Cyber Law

    - Module 4 is an examination of a large-scale cyber event in respect to both US and international laws that apply to cyber conflict or crisis. Topics will cover GDPR, Constitutional Rights, Computer Fraud and Abuse Act, Tallinn Manual, and Patriot Act. The learning objective is to be able to recognize infraction of laws that have occurred in the cyber event or the implications of an event. The module reinforces the application of the laws that govern cyber events or can limit the actions of a cyber-response.

E. Module 5: Effective Communication and Presentation Skills

    - Module 5 covers the topics of effective communication and presentation skills. This module has been designed as a final step in preparation for a cyber policy competition. A common problem in many policy topics (especially those related to complex issues) is the presentation of the overall problem to the executive leadership. Very often, the experts working on the problem tend to use a jargon that is not well received by people who are not familiar with the terminology. An important task of any advisor would be a clear communication with the leadership, so the problem and any course of action is well understood.

    - The time constraint for the leadership is another factor for a possible insufficient attention. This module teaches students basic approaches in making best use of a limited time and how to be prepared for time constrained briefs. While

it introduces several techniques for effective communication, it also provides practice of these skills in a group project. By the end of the module, the students are supposed to work on a group project drafting two one-page documents explaining an incident and making recommendations for response. The students are also expected to have an oral presentation of their recommendations.

3. COMPETITION OVERVIEW

The training is aimed at preparing the students for a capstone competition. The students are expected to assume the role of policy advisers and the scenario will address the students along the lines below:

You are a team of experienced policy advisers that is a part of a hypothetical Joint Cybersecurity Task Force (JCTF). As a JCTF, your mission is to process and evaluate the intelligence provided to you to develop a policy and written brief to mitigate the crisis and advise the National Security Council. The intelligence collected for you will provide insight at the micro and macro levels. In your brief, you need a full range of options and courses of action for the incidents that need to be resolved.

The JCTF's objectives are to:

- ***Analyze the issues:*** The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of potentially conflicting interests. Priority should be given to the analysis of the issues and not listing all possible issues or solutions.
- ***Engage the scenario*****:** Believe that the universe we have created is plausible and that the events that happen in it are real. Nevertheless, remember to think critically about the intelligence you have been provided and its provenance.
- ***Think multi-dimensionally*****:** When analyzing the scenario, remember to consider implications for other organizations and domains (e.g. private sector, military, law enforcement, different levels of government, diplomatic) and incorporate these insights along with cybersecurity.
- ***Consider who you are, and who you're briefing*****:** You are experienced cyber policy professionals briefing the National Security Council. As such, you should be ready to answer questions on agency responsibility, provide justifications for your recommendations, and have potential alternatives ready. A technical explanation should be understood by a non-technical audience.
- ***Be creative*****:** Cyber policy is an evolving discourse, and there is no single correct course of action to the scenario information provided. There are many ideas to experiment with in responding to the crisis.

- ***Don't fight the scenario:*** Unless stated otherwise, assume all inter-state relations, policies, and treaties have remained the same as they currently are. Explore the implications of that information, not plausibility.

From the intelligence reports, the JCTF will create a written policy brief and 10-minute oral presentation of the current situation and policy recommendation the NSC (Panel Judges) needs to consider. The written policy briefs will be scored before the presentations. The written policy briefs encourage preparation and an in-depth understanding of the situation to allow for the JCTF to field questions from the NSC. After the briefing, the judges will role play as the NSC and evaluate the recommendation of the JCTF in a 10-minute Q&A. The purpose of the role-play is to emphasize effective and concise communication for the NSC to make a decision. The NSC Q&A is for the panel to ask questions about the JCTF recommendation. Once the Q&A round is completed the JCTF will be excused and the NSC (judges) deliberate for 10 minutes and score the team. After the deliberation, the role-play ends to debrief the JCTF and the judge will provide an assessment for areas of improvement and strengths in the JCTF's policy recommendation and briefing skills.

The competition will have 3 rounds, the first round will have 3 weeks of preparation to create the written policy brief and first oral presentation. In Round 2 the JCTF present the next day to adjust their policy recommendation based on the new intelligence reports. In the final round, the top two teams will proceed to the final round and will be given 15 minutes to review the last intelligence brief and provide the recommendation to the NSC and to an audience. Depending on the size of the competition, elimination rounds may be needed to filter teams that make it into the final rounds.

The purpose of the multiple rounds for the JCTF to improve and adjust their strategy based on the intelligence reports. The additional rounds and shorter timetables are to simulate the pressures of an escalating situation.

4. APPENDICES

A. Appendix A: Course Syllabus

B. Appendix B: List of Case Studies for Training Modules

C. Appendix C: Lecture Presentations

D. Appendix D: Group Projects and Discussion Topics

E. Appendix E: Sample Scenario and Grading Rubric