Table of Contents

A Letter from Your Chair ........................................................................................................................................... 2
A Letter from Your Crisis Director ......................................................................................................................... 2
Committee Structure and Procedure .......................................................................................................................... 3
Topic ........................................................................................................................................................................ 3
  What is Cybersecurity? ....................................................................................................................................... 3
  History ............................................................................................................................................................... 4
Crisis ...................................................................................................................................................................... 4
Character Descriptions ........................................................................................................................................ 7
A Letter from Your Chair

Dear Delegates,

Welcome to the College of the Canyons Model United Nations (COCMUN) Conference. My name is Christine Colindres, and I am honored to serve as your Chair for this crisis committee. The topic, Cybersecurity, has been designed to put your critical thinking skills to the test.

I have been a member of the Model United Nations (MUN) for two years, of which I have competed primarily in crisis committees. This semester will be my last at College of the Canyons, as I plan on transferring to a four-year university as an Accounting and Business Administration major in the fall. I joined MUN to further develop my research and communication skills that I will need to run a professional business.

This topic was chosen because the expansion of the internet has changed the nature and frequency of human communication forever. In this committee, you will deal with a worst case scenario in the not-too-distant future. The online world is a beast that needs taming, and your leadership skills may be all that stands between a harmonious society and an anarchist wasteland.

To ensure that we have a memorable crisis committee, we have assembled a diverse crisis staff.

We are excited to act as your staff for this crisis committee, and we look forward to watching you draw out the skills that make you a great delegate.

Christine Colindres
Chair, Crisis Committee on Cybersecurity

A Letter From Your Crisis Director

Hello delegates!
The crisis staff and I hope to lead you all through a harrowing scenario designed to stretch your creativity. We are at a turning point in history, where the physical limitations of our human world grow increasingly secondary to our digital experience.

Today's reality — a determined individual with freely acquired online technical expertise has the ability to wreak untold havoc. This crisis will explore a grim but plausible future, in which the menaces of the web become menaces to society. How will we respond to this dystopian tragedy?

Ryan Arroyo,
Crisis Director, Crisis Committee on Cybersecurity

**Committee Structure**

This crisis committee will be comprised of 15 countries, and to add to the excitement, will also feature five heads of internationally known organizations. The committee will follow the National Model United Nations rules and procedures, and **will** include moderated caucusing. Delegates are expected to utilize communiques and personal, joint, and committee directives. Delegates **will not** be writing resolutions.

**Topic**

The topic for the committee will be Cybersecurity and the Extension of Government Power over the internet. Delegates are expected to enter the committee with a firm grasp of their position on the topic. Consistency and command of the material will help all parties in the solution of this crisis.

**What is Cybersecurity?**

Effective cybersecurity measures are needed to combat rising cybercrimes and cyberterrorism. According to the [International Telecommunication Union (ITU)](https://www.itu.int), cybersecurity is defined as, “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.”
History

Technology has rapidly transformed society over the past half-century. With the invention and expansion of the internet, we find ourselves at the forefront of a new reality — a world of computers in which law and order exist only in theory.

It's possible to look back on 1998 as a landmark year in the realm of cybersecurity.

That year cybercrime was brought up as a talking point for the first time by the First Committee of the United Nations General Assembly (DISEC). When the Russian Federation proposed the draft resolution “Developments in the Field of Information and Telecommunications in the Context of Security,” to the First Committee of the General Assembly, which was later adopted (A/RES/53/70), a modest but legitimate dialogue on the security of the internet first began at the UN.

The Convention on Cybercrime (also referred to as the Budapest Convention) was the first international treaty created to assist in combating cybercrime. It was created and adopted by the Council of Europe, and targeted cyber-forgery, fraud, copyright infringement and hate crimes.

In 2007, the Global Cybersecurity Agenda (GCA) was launched in 2007 by the ITU to increase “international cooperation aimed at enhancing confidence and security in the information society.”

Through its five-pronged approach to legal measures, technical and procedural measures, organizational structures, capacity building, and international cooperation, the GCA has established initiatives like the Child Online Protection and International Multilateral Partnership Against Cyber Threats (IMPACT) programs.

Launched in 2009 and overseen by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), the Talinn Manual was created to provide “a comprehensive research agenda and practitioner-oriented training opportunities.”

Although this manual is viewed as authoritative on international cybercrime prevention, it is not enforceable by law.
As the discussion for the prevention of cybercrime continues, international cooperation is vital for success.

Crisis

By the year 2016, the expansion of the internet has shrunk the enormity of the world to fit in an individual’s pocket. But as citizens of the world become increasingly connected, previously small anarchistic political movements have a foothold in the shadows of the web. A far-reaching shift in perspective has led many to view national and regional governments as unnecessary evils that abuse power and stifle creativity.

As this view gains traction online, the seeds of revolution, planted at the inception of the internet, are yielding fruit. Wikipedia junkies and Bitcoin enthusiasts point to the success of their information sharing and currency exchange programs as a referendum. A fascination with “Agorism” or “market anarchy” sweeps the globe, followed by small revolutions by cultural separatists in the Catalan region of Spain and throughout Greece.

After gaining traction in the late 1920’s and early 1930’s, the independence movement in Catalon lost steam during the Spanish Civil War. Now, the region is an economic powerhouse situated in the southern region of a country that’s largely struggling as a whole. Because of this, new life has stirred among Catalonians.

As recently as 2012, the Catalan National Assembly orchestrated the Catalan Independence Demonstration, where up to 600,000 protestors and regional enthusiasts gathered in Barcelona to promote Catalon’s individual statehood in the EU. Municipal police at the event feared that the massive turnout would “compromise cellular communication patterns” in the city.

By 2017, the Catalanian play for independence has caused significant unrest in Spain, culminating in an ambiguously motivated hacker’s systematic identity theft of 25,000 Barcelona residents.

Elsewhere in Europe, debtor Greece threatens to leave the EU entirely and start fresh. European leaders fear that Greece’s departure from the EU will spell the beginning of the unravelling of the Union. “If Greece is permitted to leave, then we allow other countries the same idea, and sew the seeds of our dissolution,” says a concerned Angela Merkel at a summit in Marseilles, France.
Despite help from many EU power players, Greece’s economy continues to plummet for over a decade. Unemployment is 17% nationwide, and historic overhauls by the Coalition of the Radical Left have left many disillusioned. A party rival assassinates Greek Prime Minister Alexis Tsipras in Athens on November 2, 2017.

Globally, a movement away from tangible military power has shifted the political landscape. Countries which used to derive their national prestige from outward displays of force must readjust their thinking in the 21st century. Domination no longer begins on the oil fields, but on the internet. Control of the digital world is the new signature of authority.

That’s a hard reality to face in countries like the United States, where on April 20, 2018, two passenger airplanes collide following a brief system disruption in the air traffic control room of John F. Kennedy International Airport in New York City.

The disaster claims 450 civilian lives and serves as the catalyst for massive internet reform in America. Fearing the airport’s system disruption was the result of cyber terrorists, President Hillary Clinton issues executive order *Internet Freedom*, which effectively shuts down the country’s internet for two days. The play is seen by the American public as an abuse of wartime powers.

*Internet Freedom* is immediately followed by federal legislation known as the Interstate Communication Safety Act (ICSA), which allows the federal government to control the internet in “times of national distress” and use information gathered by NSA data phishing in court. Additionally, the United States begins pressing aggressively in the UN and among her allies for expanded authority over the regulation of internet traffic, and an expansion of laws enabling governments to crack down on cyber-activities. As a longstanding defender of internet freedom, this marks a turning point in the American role in the global dialogue on cybersecurity.

Characterizing the government response to this incident as a massive encroachment on freedom, agorist ideologue and student Nathaniel Schwartz spearheads an antigovernment, student-led movement at the University of California-Berkeley named Liber8.

In February of 2018, Liber8 goes live online with a mission statement, mailing list and recruitment videos. Exhibitions begin with small protests, pickets of congressmen and chain emails.

To a large extent, Liber8 is ignored and dismissed as a trendy, radical group with little vision or staying power. However, their message resonates deeply with college students and young adults nationwide.
In December of 2018, an anonymous online “hacktivist” organization launches attacks against public utilities facilities in Missouri. Kansas City and Columbia spend Christmas without running water. Streetlights in St. Louis are blacked out, and traffic in the city grinds to a halt as a tumultuous holiday season gets worse for the midwestern state.

The incident in Missouri only reinforces the United States' push for a strongly regulated internet. Members of the UN quickly fall in behind this charge and begin reform in their nations to regulate and restrict internet access in fear of cyber attacks destabilizing the delicate balance of the global economy.

As the international crackdown on a free and open internet comes into full swing, the previously marginal Liber8 expands. Soon Liber8’s influence spreads around the globe creating unrest as the U.N. tightens its grasp on the restriction and regulation of the internet. As experienced delegates, you’re going to have to explain how the United Nations manages to tighten its grasp on the Internet. Growing unrest quickly escalates, with Liber8 radicals taking severe action against their respective governments.

On Feb. 12, 2019, cyberterrorists claiming to represent Liber8 crash the North Korean firewall.

The incident serves a blow to North Korean leader Kim Jong Un’s legitimacy, who is portrayed as a weak central authority figure following the snafu. After a group of military advisors overthrows Kim Jong Un, the North Korean hegemony tightens its noose around its people even further.

The year is now 2020 and the world is in shambles. Liber8, once a peaceful student-led movement, has grown untamable since outgrowing its humble beginnings in a California college town.

Distrustful of everyone but themselves, North Korea’s new braintrust threatens to target the American city of Los Angeles in an act of revenge for the cyberattacks. The United States government claims that it had nothing to do with the incident, and a game of nuclear cat and mouse begins.

Liber8 has inadvertently created a global crisis, and in the midst of a chaotic argument on the floor of the UN General Assembly on Jan. 28, 2020, word gets out that North Korea’s nuclear capabilities have been disarmed, and that over 150 million American and Canadian citizens have had their credit card information stolen.
iSummit

In March of 2020, the United Nations called for a summit consisting of heads of state and international experts to address the worsening crisis. This summit, held in Geneva, Switzerland, will set an international precedent for the regulation of the internet. There is expected to be tension at iSummit due to the conflicting views on how to handle the matter. The P5, along with Germany and South Korea, are in favor of stronger internet censorship laws. The remaining countries favor decentralizing regulations with the purpose of making it a free internet.

Character Description:

Leaders of Countries:

United States- Hillary Clinton
United Kingdom- David Cameron
China- Xi Jinping
Russia- Vladimir Putin
Germany- Angela Merkel
Greece- Prokopis Pavlopoulos
Spain- Pablo Iglesias Turrión
Japan- Shinzō Abe
South Korea- Moon Jae-in
Indonesia- Joko Widodo
Brazil- Dilma Rousseff

All leaders are:
- Head of state
- Head of government
- Commander of country’s armed forces

Head of Organizations:

World Bank- Jim Yong Kim
International Telecommunication Union (ITU)- Houlin Zhao
- Reelected in 2016
Google CEO- Larry Page
- Global proponent for free, uncensored internet.
- While they cannot draft laws in their own right, they still yield tremendous influence because of Google’s position in the global market.

Alibaba CEO- Jonathan Lu
- While they cannot draft laws in their own right, they still yield tremendous influence because of Alibaba’s position in the global market.
- Head of one of the largest telecommunication firms in the world with major influence over National People’s Congress of China.
- Currently abides by Chinese internet censorship laws but would take an opportunity to break free of these restrictions.
- Has suspected ties with hacker groups within China seeking to break down The Great Firewall but claims so far have been unsubstantiated.

Der Spiegel- Reporter Wolfgang Büchner
- Reinstated in 2018 as Editor-in-Chief

Welcome to Wikiworld, where all that stands between harmony and disorder is the click of a mouse.