



# **SMH-MUN III**

## **Saturday, March 21, 2015**

### **G-20 Background Guide**

#### **Revolution: Demanding Progress or Endorsing Chaos?**

Topic 1: Maintaining Cyber security in an increasingly technological world

#### **I. Introduction**

The Group of Twenty was established as primarily an economic organization in 1998 to build off of the previously established G7 organization. The increased globalization and complication of the world economy provided the impetus to create a summit that worked for, as the 2006 summit articulated, “Building and Sustaining Prosperity”. The global financial crisis of 2008-2009 increased the need for what has evolved into the world’s premier alliance of the world’s most influential economies. Since that crisis occurred, G-20 Summits have been held twice a year, with Heads of State and Government being congregated rather than simply Ministers of Finance.

Although this organization is primarily economic, the issue of cyber security threatens the very fabric of the world economy, as well as the national security of all G-20 member nations. Since the advent of the Internet and Computer Age, cyberterrorism has been a very real danger to nations around the world, with most serious attacks only occurring in the 21<sup>st</sup> century. Cyberterrorists use viruses and bugs to disable communications, damage infrastructure, and even obtain classified documents with sensitive national security information. With the Internet economy now making up over 5% of all G-20 GDP, the security of developed and developing nations technological infrastructure is more important than ever before.

#### **II. History of the Problem**

- In 1998, Spanish protesters bombarded the Institute for Global Communications (IGC) with thousands of bogus e-mail messages, protesting the hosting of an American journal supporting Basque independence. The IGC was eventually forced to shut down the website because of these “mail bombings”
- NATO computers were hacked with similar email tactics during the Kosovo conflict in 1999
- After Estonia removed a Russian World War II memorial, many online government services were disabled for days, causing a major infrastructure issue
- Computer networks in Georgia were attacked around the time the country was in conflict with Russia, putting pressure on the Georgian government to concede to Russian demands
- In October 2012, Kaspersky discovered a worldwide cyber-attack since named “Red October” that had been operating since 2007, a hack that obtained information from foreign embassies, military installations, and energy providers of mostly Eastern European nations

#### **III. Past UN and G-20 Action**

- The UN held a summit with ECOSOC officials, the Secretary-General of the International Telecommunication Union, and members of the private sector, in order to discuss maintaining a safe Internet in an increasingly technological world
- The G-20 has not taken any substantive action in establishing cyber security regulations, but the conversation has begun



# SMH-MUN III

## Saturday, March 21, 2015

### G-20 Background Guide

#### IV. Possible Solutions

- Awareness must be the first step; many nations are unaware of the various types of cyber attacks that can cripple their technological infrastructure
- International standards for openness and collaboration between developed nations' major internet providers
- Cooperation between IT providers to create software better equipped to battle cyber crime
- Geneva Convention-type agreement for the Internet mandating mutual respect and peace between member nations, as well as political punishment for nations harboring cyber crime
- International regulations that outline how nations ought to deal with complaints of cyber crime at all levels

#### V. Helpful Links

History and Major Details of G-20:

[http://en.wikipedia.org/wiki/G-20\\_major\\_economies#History](http://en.wikipedia.org/wiki/G-20_major_economies#History)

G-20 and Cyber Security:

<http://www.euractiv.com/infosociety/huawei-cyber-chief-use-g20-platf-interview-528069>

Cyber Security Background:

<http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html>

Timeline of Major Cyber Attacks:

<http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm>

Possible Solutions to Cyber Security Problems:

<http://www.global-economic-symposium.org/knowledgebase/the-global-polity/cybercrime-cybersecurity-and-the-future-of-the-internet/proposals/five-concerns-and-five-solutions-for-cybersecurity>