**Position:** Chief of Staff

**Institution**: Executive Branch

**Faction:** Political

**Historical Reference:** Rahm Emanuel

**Biography:**

At 49 years old, President Obama asked you to serve as his Chief of Staff. As such, you have an broad political mandate. You have significant political experience, but minimal policy experience. Initially, you served as President Clinton’s presidential finance director. However, you quickly emerged a shrewd political operator, and Clinton tasked you to advance his political agenda while in office. This included the North American Free Trade Agreement and an assault weapons ban. As a member of the House of Representatives, you once again emerged as an effective political strategist and led the Democratic Congressional Campaign Committee during the 2006 midterms.

As Chief of Staff, you largely control the information flow to the President. You do not have any formal experience in cybersecurity; however, you understand that the issue is sensitive and that any significant attack against the United States would damage the President politically. However, you also view the process of NSC deliberation through a political lens. You are primarily focused on potential public reaction and, like with all policy issues, you primarily want an outcome that makes the President look strong, competent, and in command.

**Faction Advisory**

Your goal is simple, but achieving it is going to be quite complicated. First and foremost, you need a policy that will prevent a large-scale cyber-attack on the US, as this would be politically devastating. In addition, you want to avoid other outcomes that would damage the President politically. This includes ending up in a traditional military conflict that begins in cyber.

You are generally not supportive of secret or classified policies. This is a political document, and so whenever US policy is hidden from view, it does not benefit the Administration politically. You want a document that makes a strong public statement communicates two things. To the American people, it must signify strength and make them feel secure, but it cannot look as if the policy will lead to war. To potential rivals, the NSC policy must send a clear message that cyber-attacks against the US will not be tolerated.

**Assignment**

At an upcoming meeting, the President (instructor) will convene the National Security Council (NSC) and ask it to develop a National Security Strategy for Cyber Security. You need to ensure that the final document the NSC produces reflects your institution’s priorities (see objectives). Because the NSC contains representatives from institutions (or agencies) with vastly different perspectives, this will be no easy task. Government agencies fight hard for influence and resources (e.g., a budget). Not everyone can get what they want. Thus, your colleagues need to hear your ideas, but you also need to convince them that your priorities belong in a document that will not—indeed, *can not*—contain everything. Evidence-based arguments will serve you best here, and you can prepare in the following ways:

* Research your *institution*. What does your institution generally do day-to-day? What are its general interests? This puts you in the mindset of the institution.
* Research the current state of cyberspace (as of January 21, 2009; no later). What are its characteristics? What are its main opportunities and challenges? The instructor will provide you with access to a database of resources to get you started, but you should not confine yourself only to those resources. You may use any time appropriate research.
* Research your policy toward cyberspace. Given (i) and (ii) above, what do you think a national cyber policy needs to contain? What do you think it should avoid? What language should it use?

As the game unfolds, the instructor will distribute additional assignments. You will need to complete those assignments as they arise.

**Objectives**

Your mandate is broad, and there are many different ways that you can ensure that your goals are met. You will need to be both creative and direct in pursuing your agenda. At a minimum, you should seek to:

* A comprehensive policy that addresses all known threats, thereby making the American people feel safer and demonstrating that all aspects of the cybersecurity issue have been addressed.
* A document that makes the President “look good.” - i.e., demonstrates strength, American leadership in the world, and that the public is safe.
* Trade sanctions look good domestically. You prefer these. You oppose a policy where the most critical action is hidden from public view.

You strongly oppose:

* Entrapment. The President needs room to maneuver and to justify US actions. For example, he does not want to be “bogged down” in a war. So you oppose clear “if….then” statements the constrain what the President can do. Think here about creating a “political wiggle room” if the US is attacked.
* Policies where the US response to an attack must be kept secret.

**Strategy Advice**

You will want to encourage the NSC to think about different categories of cyber-attacks, and the different levels of US response that would be appropriate. So, for example, to prevent large-scale “Pearl Harbor” attacks, the US might have to threaten a wide-range of consequences (perhaps), including military action. However, in response to lower-level attacks - intellectual property theft, disinformation campaigns, etc., - may be best deterred with the threat of trade sanctions or “tit-for-tat” American cyber-attacks. Because most of the other factions have narrow interests in cyber, you will need to find a way to convince each side that they are getting some part of what they want. To demonstrate US leadership, a new global cyber-security agreement would be very beneficial politically.

Finally, you note that the Bush Administration’s cybersecurity plan emphasized domestic security over a global approach. But the world has changed. You must keep the NSC focused on developing a politically viable plan that you can “sell” to the American people. This will require compromise among all parties.

**A Cautionary Note**

The game begins on January 21, 2009. Many subsequent administrations, including the current one, likely have a cyberspace policy. Your institution may even currently have cyber-related policies. These, however, will not necessarily be the Administration’s or institution’s *historical*