**Position:** Council to the President

**Institution**: Executive Branch

**Faction:** Political

**Historical Reference:** Gregory B. Craig

**Biography:**

Born on March 4, 1945, you have spent the majority of your professional career as a lawyer in private practice. Your first relevant governmental experience was in the Clinton Administration as Director of Policy and Planning at the State Department. Then, during the impeachment trial, you joined President Clinton’s legal defense team. During the Democratic primary in 2007, announced that your support for Barak Obama over Hillary Clinton developed after you read his book *Dreams of My* Father. You found yourself moved to support Obama’s candidacy.

As you enter your new position in the Obama Administration, the primary focus of your work is to find a legal justification for closing Guantanamo Bay. You have a somewhat similar role on the NSC with respect to cybersecurity policy. Your obligation is to protect the president politically, and so you must assure that any policies and actions adopted by the NSC have a sound legal rationale. The president cannot be perceived as having broken the law. In this way, you serve as a kind of legal guardrail for the President, and you are obligated to inform the Administration whenever you believe that a proposal or action not be justified as lawful.

**Faction Advisory**

While your position is as legal counsel, your role is also significantly political. You support a policy that will, in your opinion, prevent a large-scale cyber-attack on the US as this would be politically devastating. However, you must prevent the adoption of policies and actions that could, in hindsight, be viewed as extra-legal as that would also damage the President politically. This requires aligning NSC recommendations with guiding legal authority, including the War Powers Act and United Nations commitments respecting the sovereignty of other nations. You strongly oppose policies that might place the President in legal jeopardy or open a avenue for political attack by his rivals.

**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, so whenever possible, this is preferable to military conflict.

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.
* Any policies that the President’s political opponents could subsequently claim as violations of law.

**Strategy Advice**

You will want to encourage the NSC to think about identifying clear categories of cyber-attacks because each will have distinct legal consequences. So, for example, to prevent large-scale “Pearl Harbor” attacks, the US might legitimately threaten a wide-range of consequences (perhaps), including military action. However, 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. You may find that the Attorney General is an ally, as that role is also to assure compliance with the law. However, the intelligence agencies, to the extent that they mostly operate outside of public view, may want to define the President’s legal authority more broadly than the Attorney General. In part, your job is to find the middle ground between these two factions.

Finally, note that the Bush Administration’s cybersecurity plan emphasized domestic security over a global approach. You must keep the NSC focused on developing a politically viable plan that you can “sell” to the American people as consistent with the US **and** international law.

**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*