**Position:** Attorney General

**Institution:** Department of Justice

**Faction:** Legal

**Historical Reference: Eric Holder**

**Biography:**

At 58 years old, you are the first African American to serve as United States Attorney General. In 1973, you graduated from Columbia with a bachelor's degree in American History. Two years later, you received your Juris Doctor degree from Columbia while you clerked for the NAACP and the Department of Justice during the summers. Following law school, you joined the United States Department of Justice to work in the Public Integrity Section. You worked there for 12 years.

During your Attorney General confirmation hearing, you expressed a desire to focus on issues regarding civil rights, immigration, and criminal justice reform. You also signaled your support to end the Bush administration policies of waterboarding, which you described as torture and endorsed the shutting down Guantánamo Bay. Importantly, you have also signaled that you would support President Obama's use of executive power concerning national security and the broader War on Terror. As such, you are committed to the principle that cybersecurity policy must be consistent with international and domestic law and that the rights of the American people are protected.

**Faction Advisory**

As the leader of the Department of Justice, your core obligation is to ensure that all public policy is consistent with the principles of the Constitution and US law. This includes the War Powers Act. In addition, as all formal international treaties have the legal standing of US domestic law, and your job is to enforce these as well. You are agnostic on the debate in the US over how to best respond to cyber threats. Instead, you view your role as guiding the Administration to assure that all policy sits upon a solid legal foundation.

**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:

* If military action is contemplated, you must assure it is consistent with the War Powers Act and US commitments to the United Nations Charter.
* If possible, the NSC should *justify* action in terms of these commitments. Indeed, any action should have an appropriate legal justification.

You strongly oppose:

* Anything that infringes on American citizens' right to privacy.
* Any policy that might imply personal liability for President Obama (e.g., war crimes).
* Any extra-legal activity

**Strategy Advice**

In the NSC, concerning the use of force, your natural allies include other members of the diplomatic corps, including the State Department and UN delegation. You may want to coordinate with them first. You may also find common ground on specific issues with several other factions. While no faction's interests will entirely overlap with your own, you should seek allies whenever possible. This may include department heads responsible for the domestic economy, and representatives from trade delegations. You may also find that some factions approach the issue differently. For example, the military and intelligence agencies may believe that transparency is a national security risk, that direct unilateral action is required, and that domestic threats are growing.

Finally, you note that the Bush Administration's cybersecurity plan emphasized domestic security over a global approach. But the world has changed, while many are now convinced all that cybersecurity is no longer a national-level issue, you must keep the NSC within the bounds of 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* position. You need to research with the game date(s) in mind. Any documents (or websites) after January 21, 2009, are not permissible.