**Position:** Secretary of Treasury

**Institution:** Department of Treasury

**Faction:** Domestic Economics

**Historical Reference:** Timothy Geithner

**Biography:**

At 47 years of age, you are taking over the leadership of the Treasury Department at a trying time. As the former director of policy development and review for the International Monetary Fund (IMF), and former President and CEO of the Federal Reserve Bank of New York, you have significant experience in economic policymaking. You have advocated for greater transparency in financial institutions. However, the national economy is now turmoil as one of the worst recessions since the Great Depression rages on.

As such, you understand how fragile the American economy is to external shocks. For this reason, you believe that the most significant future threat posed by cyber is a potential attack against US financial instructions. You support a policy “deterrence by denial” wherein financial institutions improve their security, and significant sectors of the economy should work with the US government in coordinating cyber defenses. However, if a cyber-attack cripples the financial institutions in the country, you believe that this could destroy the country. For this reason, you are also willing to support a policy that threatens US military response to deter such attacks.

**Faction Advisory**

You are one of several NSC members to advocate for the domestic economic interests of the United States. Your singular obligation is economic growth and stability. In the NSC, you are generally supportive of attempts to craft new global agreements on cybersecurity and may support factions focused on diplomatic efforts. However, international law is not enough, and you would support direct action (military or covert) to protect the economy and the American way of life. The health of the American economy is as important as national security. Indeed, you believe it to be the most critical issue in the cyber domain.

**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:

* Strengthen public-private partnerships to ensure a robust cyber defense.
* Include what an ‘act of war’ against the American economy looks like and define a response that would deter bad actors.

You strongly oppose:

* The ‘first use’ of cyber. It establishes an unwanted norm.
* Trade sanctions.

**Strategy Advice**

You may find common ground with those who advocate for a firm policy of retaliation for other reasons - including the department of defense - but only if you can convince them to attach such threats to potential attacks against American financial intuitions. 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 other components of the domestic economy, and representatives from trade delegations. You may also find that some factions approach the issue differently. For example, the diplomatic corps would strongly oppose the threat of unliteral action.

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 focused on the threats to domestic interests posed by cybersecurity.

**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*