**Position:** Deputy National Security Advisor for International Economics

**Institution**: Office of the United States Trade Representative

**Faction:** Trade

**Historical Reference:** David Lipton

**Biography:**

You were born in 1953 and grew up in Wayland, Massachusetts in a wealthy, educated family. You received a B.A. at Wesleyan University in 1975 and continued your education to receive an M.A., 1979., and Ph.D., 1981, from Harvard. In your career in public office, you have largely avoided partisan fights, but have an unyielding faith in capitalism and democratic institutions. You support globalization and believe that international cooperation and technological progress is the best path to global prosperity - i.e. you are committed to the truism that “a rising tide lifts all boats.”

Most importantly, you have advocated for the position a growing and stable global economy supports democratization. Because democracies are natural allies of the US, supporting a free market trading system is not just an economic issue; democratization is in the US national security interests as well. This perspective shapes your understanding of cyber security. Cyberattacks represent a threat to trading networks, and this represent a threat to free markets and economic growth. An integrated global economy requires that every country’s financial and commercial institutions must be secure from attack. For this reason, you personally support new international agreement in which countries share information about commercial cyberattacks. Collecting such information will make it easier for responsible trading partners to with the goal of isolating hackers and rogue states.

**Faction Advisory:**

Your faction is in favor of any policies that lead to economic growth and you always advocate for free markets. As states in the global economic system become ever more interdependent, you are one of many experts who believe that cyber-attacks could potentially undermine global economic growth. It is therefore paramount that the NSC draft a policy that supports US interests, and that also protects trading partners However, you oppose any policy that would disrupt trade, including economic trade sanctions, and would strongly prefer that cyber threats be dealt with diplomatically (long term) or as a security issue (use American cyber weapons to retaliate). The health US exporting industries and a vibrant global economy is the most important issue in the cyber domain. Your natural allies are those factions that are tasked with growing the US economy, and with the diplomatic corps responsible for negotiating new international agreements. However, some factions prefer a policy of deterrence through trade sanctions because it is both politically popular and less costly than military conflict.

**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, *cannot*—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:

* New international institutions and cooperation that address cyber threats.
* Protection of American companies and their intellectual property, from foreign cyber-attacks, even at the expense of foreign companies if necessary.
* Fewer regulations on trade.

You strongly oppose:

* Trade sanctions as a policy
* Any policy of “tit for tat” that might lead to increasing trade tensions.

**Strategy Advice**

You share common ground with other agencies (e.g. Commerce, Treasury) that focus on economic growth and prosperity, because you see cyber security vulnerabilities as a potential disruptor that negatively affects stability and economic growth. While you agree that a broad scale attacks against US commercial interests and financial institutions would constitute an existential threat, you would like to convince the diplomatic corps to focus developing a new global cyber security agreement that promotes US interests. In addition, you would prefer that the national security agencies primarily responsible for cyber security (NSA, CIA) take the lead. If you can convince the NSC the best way to deter cyber-attacks is to threaten in the cyber domain (i.e., US cyber attacks) then the issue stays “contained” within the domain and does not affect trade politics or policies.

Finally, you note that the Bush Administration’s cyber security plan emphasized domestic security over a global approach. However, you are now convinced all that cyber security is no longer a national-level issue, you must keep the NSC focused on the threats to Americas foreign economic interests posed by cyber security.

**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*