**Position:** Deputy Representative to the United Nations

**Institution:** Department of State

**Faction:** Diplomatic

**Historical Reference:** Rosemary DiCalro

Born in 1947, you have had a long and distinguished career in foreign affairs. You graduated from Brown University with a B.A., M.A., and PhD in comparative literature and Slavic languages. You have significant government policy experience and, also, a long career working for private foundations and non-governmental organizations, including UNESCO, Senior Fellow at Yale Jackson Institute, and President of the National Committee on American Foreign Policy. A primary focus of your professional career is dedicated to peacebuilding in order to help bring an end civil wars, gender-based violence, and genocide.

You are not a cyber-security expert. However, through your work on peacebuilding you understand better than most that even when groups have sharp differences, it is possible to find a common ground. This is the perspective you bring with you to these deliberations. As much as any member of the NSC, you are fully committed to the idea any long-term solution resolving political differences and disputes must be openly negotiated.

**Faction Advisory**

The US United Nations Delegation is part of the State Department. Your mission is to pursue US interests through the UN. As such, you share the core belief is that diplomatic action is always the first, best option to resolve tensions between countries. You oppose unilateral military action, except in extreme circumstances where the US, its allies, or the global community confronts an existential threat. While you work hand-in-glove with the State Department, you are more sensitive to the fact that rebuilding America’s global reputation, and its leadership role in the United Nations will require cooperation and, occasionally, compromise. For this reason, you oppose any unilateral action or policy will perceived by other governments as manipulative or secretive, as this would reinforce the believe that the US can no longer be trusted. Instead, you preferer a multilateral approach to problems, including cyber security. You understand that, while diplomacy may take some time, it is the only way to forge a real consensus between countries. You support economic sanctions if the purpose is to create political pressure and convince governments to negotiate in good faith. Sanctions designed solely for punishment do not advance diplomatic interests. Because the complexity of global cyber threats is increasing rapidly, you believe that unilateral action (including sanctions) will ultimately fail. other like-minded governments

**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:

* Establish new global no ‘first use’ of cyber norm.
* Establish new international institutions and cooperation that address cyber threats, under US leadership. Ideally, the goal is to design an institution that even US rivals - eg. China, Russia, etc. would accept.

You strongly oppose:

* Military or cyber-attacks as a policy in itself, or as a ‘first’ response to a crisis.
* Secrecy and hidden side-deals. Diplomacy happens in the open. The more information governments have, the better. The US and global community need to share information so that each government can clearly identify and articulate it interests.

**Strategy Advice**

In the NSC, your natural allies include other members of the diplomatic corps, including the UN delegation. You may want to coordinate with them first. You may also find common ground on specific issues with a number of 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 and that direct unilateral action is more effective.

Finally, you note that the Bush Administration’s cyber security plan emphasized domestic security over a global approach. But the world has changed, and you need to convince all factions that cyber security is no longer a national-level issue that countries can address on their own. For the US to be secure domestically, it must lead internationally.

**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.