**Position:** Director, Office of Science and Technology

**Institution**: Executive Branch

**Faction:** Indeterminate

**Historical Reference:** John Holdren

**Biography:**

You were born in Sewickley, Pennsylvania, and earned a B.S. from the Massachusetts Institute of Technology (MIT) and your Ph.D. from Stanford University in aerospace engineering. You have broad policy experience, with a professional career that ranges topics as diverse as environmental change, population control, nuclear energy, and energy technology. You taught at Harvard for 13 years and the University of California, Berkeley, for more than two decades. You have many recognitions and awards for your credit, including delivering the Nobel Peace Prize acceptance lecture on behalf of the Pugwash Conferences in 1995. You continued your career by becoming the chair of the Committee on International Security and Arms Control of the National Academy of Sciences, and Co-Chairman of the bipartisan National Committee on Energy Policy.

Despite this broad and impressive record of scientific achievement, you have little experience or training in cybersecurity issues, and so on the NSC, you fall back to your core beliefs. Science is a skeptical enterprise. Any NSC policies or recommendations must be grounded in sound science. Your training has taught you that ideology and partisan beliefs are terrible foundations for public policy. Instead, the government must base its policies and data and evidence because this maximizes the change that they will be successful.

**Faction Advisory**

You are in the only faction that does not come to this to the NSC deliberations with a fixed set of pre-existing beliefs. In effect, you are the resident skeptics. You are open to supporting any approach, ***so long as they are evidence-based***. To get behind a proposal, you must be convinced. Because other factions have fixed interests, you are wary of their motives and are constantly pushing them to provide data in support of their arguments. To convince you, others need to provide evidence and data on the nature of the cybersecurity threat they intend to fix. Vague, hyperbolic claims of “national security threat” and “devastating consequences” might sound scary, but the nature of these concerns must be clearly defined and supported. The same is true for any policy proposals. To the extent possible, their likelihood of success must be supported with evidence. Only policies that have a high probability of succeeding should be adopted. Your core interest here is practical policy.

**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:

* Well-vetted policy. Each aspect supported by evidence and data.
* Thorough policy. The NSC must be comprehensive in its approach

You strongly oppose:

* The dominance of any one faction’s perspective or recommendations.

**Strategy Advice**

Your primary challenge will be to encourage other factions to improve their positions thought constructive criticism. In many ways, yours is a position of strength. Crafting recommendations in the NSC is a consensus-building exercise, and each faction will need allies. Make it clear that you are open to any proposals, so long as they are adequately supported with data and evidence. Most factions will be willing to accommodate your desires for a science-based approach to get you behind their initiatives.

Finally, you note that the Bush Administration’s cybersecurity plan emphasized government-industry partnerships as the best approach. However, the world has changed. A decentralized, loosely organized response to cyber is no longer viable. Only a coordinated, comprehensive, and science-based policy and approach can keep the country safe.

**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.