**Position:** Director of National Intelligence

**Institution**: Homeland Security

**Faction:** Intelligence

**Historical Reference:** Dennis Blair

**Biography:**

Born on February 4, 1947, in Kittery, ME., you graduated from the United States Naval Academy then pursued a master’s degree in Russian Studies at Oxford University as a Rhodes scholar. You then returned to your roots, serving in the Navy for 34 years before becoming Director of National Intelligence. President Obama relies heavily upon you for accurate information to make the best decisions in the national interest. In particular, you spend a significant amount of time focusing on supporting the President's decision to wind down the wars in Iraq and Afghanistan.

While in the Navy, you served in critical intelligence positions. However, your role as a civilian intelligence officer is somewhat different. The focus of military intelligence primarily to understand an adversary’s military capabilities and intentions. This is also part of your new job. However, as the civilian head of all US intelligence, your mandate is now much broader, and the issues are complex. Perhaps the most critical and difficult challenge is that you oversea national security agencies that must collect and analyze information about foreign threats to US interests overseas and domestically.

**Faction Advisory**

Your role in the current NSC deliberations on cyber is to ensure that intelligence agencies have the resources and tools they need to protect America’s security and defend the national interest.

Concerning cyber operations, your interest is to have the NSC distinguish between the different ways the intelligence community engages with cyber. The first involves intelligence collection and timely threat identification. This is tricky as some agencies, like the CIA, cannot operate on American soil, so your intelligence collection about threats in the US must originate overseas. This requires new and increased capabilities. The second involves offensive cyber weapons that the US can deploy to attack its rivals overseas. There is a simple truth about offensive cyber capabilities. If you use it, then you lose it. Unlike traditional weapons that can be used over and over, cyber tools can only be used once. Once a cyber-attack is launched, even if successful, it is possible for the adversary to identify the code and protect against the next attack. This is a concern for the NSA, which is mainly responsible for developing offensive cyber capabilities.

**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:

* Robust, covert cyber intelligence collection of foreign actors.
* More funding, resources, etc. to develop offensive cyber capabilities.
* Increased use of cyber for intelligence gathering and threat analysis of threats against the US homeland directed from overseas.
* Offensive cyber only as a last resort.

You strongly oppose:

* A tit-for-tat policy of responding to cyber with cyber - minimize the "use it and lose it" risk.
* High publicity. The more the adversary knows about intentions and capabilities, the less effective intelligence collection will be.

**Strategy Advice**

You will want to encourage the NSC to think about different categories of cyber-attacks, and the different levels of US response that would be appropriate. So, for example, to prevent large-scale "Pearl Harbor" attacks, the US might have to threaten a wide-range of consequences (perhaps), including military action. However, in response to lower-level attacks - intellectual property theft, disinformation campaigns, etc., - may be best deterred with the threat of trade sanctions or "tit-for-tat" American cyber-attacks. Your allies are with the military in that they will only approve and overwhelming response in the fact of a significant attack. The diplomatic corps will support diplomacy, perhaps economic sanctions for lower-level offenses. However, most factions also believe that US cyber attacks can be used to deter cyberattacks from overseas. Also, the Attorney General and Presidential Legal council will be suspicious of increasing secret domestic surveillance.

Finally, you note that the Bush Administration's cybersecurity plan emphasized domestic security over a global approach and focused on public-private partnerships. But the world has changed. The US now needs a more focused and government-directed policy to confront new threats from abroad.

**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.*