**Position:** Director, Central Intelligence Agency

**Institution**: Homeland Security

**Faction:** Intelligence

**Historical Reference:** Leon Panetta

**Biography:**

Born in 1938 to two Italian immigrant walnut farmers in Monterey California, you graduated magna cum laude from Santa Clara University in 1960 with a degree in political science. You graduated three years later from Santa Clara University Law School. In 1964, you joined the US Army and served as a First Lieutenant until 1966. You have a range of experience, including serving in the House of Representatives, Chairman of the Panetta Institute for Public Policy, and the Director of the Management and Budget Office in the Clinton Administration.

As Director of the Central Intelligence Agency, you report directly to the Director of National Intelligence. Your military and government service have led you to believe that upholding the rule of law and doing things "by the book" is absolutely essential. This means that all cybersecurity policies must be consistent with legal constraints, especially when done in secret. You also think that 'soft power' - diplomacy, law, and economic influence - are useful foreign policy tools. However, while new cyber technologies represent a potentially valuable tool for the US to understand and manage foreign affairs, in the hands of adversaries, they also represent a new threat that the country does not fully understand.

**Faction Advisory**

There are two dimensions of cybersecurity that are important to you. The first involves intelligence collection and timely threat identification. This is tricky as the CIA cannot operate on American soil, and so intelligence collection about threats in the US must originate from overseas. This requires new and increased capabilities. The second involves offensive cyber weapons that the US can deploy to confront its rivals abroad. 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.

Nonetheless, the CIA strongly prefers to confront threats overseas before they materialize on at home. Offensive cyber attacks, if they can be kept secret and not traced back to the US, are an excellent way to accomplish this. Also, to deter aggression, you prefer that the NSC recommend robust diplomacy, and/or the threat of economic sanctions and even limited military action over deploying your full cyber arsenal whenever possible.

**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 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.

You strongly oppose:

* A tit-for-tat policy of responding to cyber with cyber - avoid the "use it and lose" it dilemma.
* 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, 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 attacks. 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.*