**Position:** Assistant to the President for Homeland Security and Counter-Terrorism

**Institution**: Homeland Security

**Faction:** Domestic Security

**Historical Reference:** John Brennan

**Biography:**

You began your career in CIA in 1980, after receiving a master’s degree from the University of Texas. You have a long career in counterterrorism, eventually becoming President Bill Clinton’s counterterrorism intelligence briefer in 1994. You returned to the CIA in the Bush administration, retiring in 2005. This professional experience has convinced you that non-state actors and their state sponsors constitute a direct threat to American national security. Your concern is that rapidly evolving cyber technologies now give these “bad actors” and opportunity to attack US interests from afar.

One of the essential lessons you have learned from your work on terrorism is that traditional deterrence, while it works against states, is difficult if not impossible against non-state actors. Instead, effective counterterrorism requires forward action - disruption terrorist networks, choking-off their financial resources, and, sometimes, covert military operations. So, while cyber technologies represent a new tool for terrorists, the traditional counterterrorism tools available to the US still work. Your view is that the US should fight terrorists overseas before they can reach the homeland.

**Faction Advisory**

Your responsibilities include domestic both domestic law enforcement and national security. Emerging cyber technologies complicates your mission. Terrorist groups can now use cyber tools to reach the US directly, and this means that a more significant number of (often smaller) groups are now a threat. Non-state actors can also deploy cyber as a tool to “radicalize” US citizens to carry out attacks on American soil. So, while you share the concern that cyber-attacks against physical assets - e.g., financial institutions, the power grid, air traffic control - could prove catastrophic, you are also focused on the need to manage the flow of information itself as this is the mechanism by which foreign actors can reach into the US. Managing such information - which includes political speech - in a democracy represents a delicate balance between protecting the homeland and laws protecting free speech. For all of these reasons, you prefer a firm policy of ‘preventive deterrence’ that will render adversaries unable to attack, rather than threatening to punish them after an attack occurs.

**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:

* Increased domestic surveillance. You will trade some level of individual privacy for greater security to combat ‘self-radicalization.’
* Robust foreign surveillance of governments that may be sponsors.
* Prevention rather than deterrence

You strongly oppose:

* Centralization of cyber under any one agency. No stovepipes.
* Restrictions on your ability to collect, use, and respond to information

**Strategy Advice**

You will want to encourage the NSC to address the threat of non-state actors as well as more conventional cyber threats. This requires a mechanism to monitor internet traffic to spot attempts to radicalize American citizens and prevent terrorists from coordinating attacks in the US. You could try to convince the NSC to go on the offensive in cyber; use US cyberweapons against non-state actors and the governments that support them before they can attack the US. You might also find common ground with the Department of Defense in shaping a deterrence policy by threatening military action in response to specific cyber-attacks. You will need to convince the NSC to act not just against terrorist groups, but also the states that sponsor them. This will often require preemptive and preventive action. The US cannot wait until an attack occurs to act. Prevention is more effective than mitigation.

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 government policy 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.