**Position:** Director, Federal Bureau of Investigation

**Institution**: Homeland Security

**Faction:** Domestic Security

**Historical Reference:** Robert Mueller

**Biography:**

You are an experienced government official, having worked a variety of jobs before becoming Director of the Federal Bureau of Investigation. Before this, you were an officer in the marine corps, and this experience shaped your values and nurtured your patriotism. Across the political spectrum, you are viewed as tough, no-nonsense, and non-partisan. You were first appointed as FBI director in the Bush Administration, less than a week before the 911 attack against the twin towers in New York.

That attack cemented your view that preventing terrorist organizations from attacking the US is a core national security concern. This belief shapes your perspective on cybersecurity, as well. More than most, you are concerned about the possibility that non-state actors could deploy cyber-attacks against the United States. Because cyber-attacks require very few recourses - compared, for example, to nuclear terrorism - you believe that cybersecurity is a top domestic law enforcement priority.

**Faction Advisory**

Your role is domestic law enforcement. Since 911, this also extends to defending the homeland against foreign threats. For example, non-state actors can use cyber tools to reach American citizens directly. This provides a mechanism to “radicalize” US citizens to carry out attacks on American soil. So, while you share the concern with other agencies 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 can include political speech - in a democracy represents a delicate balance between protecting the homeland and laws protecting free speech.

**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 are willing to trade some individual privacy for greater security to prevent ‘self-radicalization.’
* Oversight of the tech industry, and regulation to protect American economic interests.

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. Other factions may oppose your desire to monitor electronic communications, including the Attorney General and agencies responsible for promoting economic interests. One way to convince the latter about the wisdom of monitoring would be to demonstrate that hostile governments and non-state actors also seek to steal intellectual property from US companies.

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 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* You were an officer in the marine corps.