**Position:** Director, National Security Agency

**Institution**: Executive Branch

**Faction:** Intelligence

**Historical Reference:** Keith Alexander

**Biography:**

You were appointed to the position of Director of the National Security Agency in 2005 by President Bush, and President Obama subsequently asked you to continue your service in his administration. You have over 30 years of experience in the Army and have held a string of intelligence-related positions. You have an in-depth understand of both the technical and operational aspects of cybersecurity. You are thus a voice of authority on the topic of cybersecurity, and you view your roles as non-political.

Historically, the US could confront its rivals overseas before they could reach US soil. However, this is no longer true. New cyber technologies allow America’s enemies to reach into US society from afar to organize terrorist attacks and/or radicalize disaffected Americans. In your view, confronting this challenge requires increased international and domestic surveillance so that the US has the information it needs to protect the homeland. Therefore, you believe that digital data and information are invaluable national assets, and they can be essential weapons in the American arsenal.

**Faction Advisory**

There are two dimensions of cybersecurity that are important to you. The first involves intelligence collection and timely threat identification. This requires new and increased surveillance of global and domestic risks using advanced digital technologies. The second involves offensive cyber weapons that the US can deploy to confront 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. For these reasons, you must try to convince the NSC to authorize increased intentional and domestic surveillance. Also, because your agency is responsible for developing and deploying offensive cyber weapons, your interest is in protecting this capability and using it only as a last resort. To deter attacks, 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:

* Ensure your faction maintains control over the development of new capabilities and the use of existing capabilities.
* More funding, resources, etc. to develop offensive cyber capabilities.
* Increased use of cyber for intelligence gathering and threat analysis

You strongly oppose:

* A tit-for-tat policy of responding to cyber with cyber - minimize "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 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.*