**Position:** Vice Chairman, Joint Chiefs

**Institution**: Department of Defense

**Faction:** Military

**Historical Reference:** James Cartwright

**Biography:**

You’ve spent over 38 years in the United States military - nearly two-thirds of your entire life. To put it simply, the military and its personnel it is the one thing you understand front and back. Your work history includes commander of the US Strategic Command, overseeing the American nuclear arsenal. However, you have limited Washington DC policymaking experience, and your politics are not prominent. You also have a good working relationship with the private defense industry, and one of your responsibilities in your new role is weapons system procurement.

Your time at the Strategic Command highlighted for you a unique aspect of cybersecurity. While many in the NSC are concerned about attacks against critical infrastructure in the US - e.g., power grid, financial institutions, stock markets - you are focused on attacks against US military assets, including the command and control systems for nuclear weapons. Your relationship with private industry gives you an appreciation of the role that domestic tech companies can play in hardening US cybersecurity defenses against attack.

**Faction Advisory**

While military force is not a solution to every problem, there are certain forms of potential large-scale cyber-attacks that represent an existential threat to the country, and here military action is appropriate. In addition, while the majority of cybersecurity issues are not equivalent to a traditional military attack against the US, the protection of military systems from cyber intrusion or attack is a critical concern. The primary function of the military in cybersecurity is to deter attacks against the US that would undermine the American way of life. For this reason, clearly defining the military’s role in cybersecurity is going to require that the NSC come to a clear consensus on when and where America will be willing to fight in response to a cyber-attack. A primary objective is to articulate a “red line” in cyber that defines the nature and magnitude of an attack that would require a military response.

The Department of Defense now believes that modern warfare will involve both traditional military action and cyber operations simultaneously. Therefore, you should attempt to have recourses to develop offensive cyber capabilities directed away from intelligence agencies to the Department of Defense so that they can be integrated into American warfighting plans.

**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:

* Ensure a clearly defined role for the military.
* More funding, resources, etc. to develop defensive cyber capabilities for the Department of Defense, so that these can be integrated into conventional warfighting.
* Tit for tat policy of escalation using cyber, not conventional military

You strongly oppose:

* Limited kinetic response to cyber-attacks (see Powell doctrine).
* Using the military before all other options have been exhausted.

**Strategy Advice**

You will want to encourage the NSC to carve-out cyber threats that do not require a military response. Your allies on the NSC may include the diplomatic corps because they believe that most cybersecurity issues are best dealt with diplomatically. You may be able to work with them on defining the red line. However, other factions may prefer an incremental “tit-for-tat” policy of gradual escalation from cyber to conventional military action. This approach may lead the US slowly, perhaps inadvertently, into a conflict that you believe to be unwise. Currently, intelligence agencies are primarily responsible for developing offensive cyber capabilities. You want to convince the NSC that some, if not all, of these resources should be redirected to the Department of Defense. You may be able to trade support for developing new diplomatic initiatives in exchange for this budget redirect.

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* position. You need to research with the game date(s) in mind. Any documents (or websites) after January 21, 2009, are not permissible.