# **National Security Strategy Overview**

The cyber domain continues to grow—as a source of information, as a venue for economic activity, as a means to connect us, and as a source of threat. This latter part concerns President Obama greatly. He has therefore asked you, the National Security Council (NSC), to provide a set of recommendations for the construction of a new National Security Strategy (NSS) for cyberspace. An NSS articulates a framework that broadly guides the conduct of policy. The NSS will therefore be both a policy *and a political* document.

The Executive Branch (EB) contains myriad offices working toward diverse—sometimes overlapping, sometimes contradictory—tasks. The NSS coordinates these offices. It constitutes a “whole of government” mechanism that helps all offices of the EB work toward a similar set of goals and objectives. It will be, in other words, a “conceptual roadmap” for how individual offices within the EB can integrate their efforts into a unified policy that serves the broader national interest.

At the same time, the NSS contains explicit political messages. For American citizens, it voices the country’s collective values and indicates what the government will do *for them*. To allies, it defines United States (US) priorities, how the US plans to cooperate with and support them, and what the US expects from them in return. To potential adversaries, it defines the consequences the US will mettle out to governments that challenge any “vital interests.” Those seeking a better relationship with the US have a path forward; after seeing US goals and how the US plans to punish actors that threaten these goals, these actors also know what opportunities exist for improving their relationship with the US (e.g., working toward similar, valued goals). Those not searching to better their relationship with the US likewise know where they stand—including potential “trip wires” that might escalate tension. In this way, the NSS helps avoid unnecessary conflicts.

Drafting an NSS will not be an easy process. In fact, an inherent tension underlies its writing. The NSS must provide guidelines for action that are specific enough to address what the NSC perceives to be current threats. Without this, EB offices will neither be sufficiently focused on the threats at hand nor able to coordinate their efforts effectively. They will be left asking *what should we do* and *how should we do that*. At the same time, the NSS cannot get too specific because it must adapt to address unexpected challenges that arise. Cyberspace changes constantly, and without flexibility, the NSS might—if too specific—be unhelpful tomorrow. To strike this balance, all NSSs focus on three components:

* Signal the country’s cultural and political values, its outlook on the world, and its role in the international system—both to the domestic audience and the international community.
* Identify a set of “vital” strategic interests, as well as any threats to those interests. Note that “interests” includes values (i.e., intangible) and material (i.e., tangible) things.
* Articulate any specific policies that the country will pursue, along with the goals the country intends to accomplish through those policies.

The best and most useful NSS documents integrate the three components above coherently and thoroughly. Because the NSC includes all major stakeholders within the EB, it is a natural place for the President to turn first for help.

## **Game Session 1:**

Contemporary cybersecurity threats touch every aspect of modern society. Banks connect with customers through online portals; energy companies use the internet to control and monitor the distribution of electricity across the country; the military relies on electronic networks to communicate with its assets and personnel; many polling stations use online rolls to verify voter identity[[1]](#footnote-1); and government officials, companies, and families communicate largely online (e.g., email or social media), often broadcasting sensitive information.

Given this diversity, the full NSC will participate in the NSS drafting. Each NSC member—like yourself—occupies a different role within the government and will interpret the values, threats, and policies that exist in cyberspace from their unique institutional perspective. To create a coherent and comprehensive NSS, the NSC will need to navigate these differences. In particular, it must: (i) identify areas of agreement and disagreement among NSC members, and (ii) where significant disagreement exists, find a path to compromise that serves the national interest. This does not mean the NSC should favor a “kitchen sink” NSS—or one that contains *everything* imaginable. An unwieldy document undercuts policy coordination and focus, so it might make sense for some people not to get what they want. You will want to be sure you are not one of those people.

How can you do that? And how can you forge consensus around what you want? A common “first step” involves an informal consultation with similar-minded individuals—that is, those likely to share your perspective (i.e., your faction). Such a “meeting of the minds” can take place before the full NSC meets to consider the issue; in fact, it will be *most* helpful to you if it does.

When the NSC initially meets to draft the NSS, its members will organize into working groups, or factions. Each working group will need to forge an initial consensus around three questions:

* What national interest(s) are at stake in the cyber domain—from *your* perspective?
* What is the most likely source of threat to the identified interest(s)?
* What policies will most likely protect and promote the interest(s) you identify?

As you answer these questions, keep several things in mind. First, change is the new “normal.” As the NSC begins its meeting in January 2009, technology continues to proliferate. The cyber environment has changed drastically since President Bush first articulated his National Strategy to Secure Cyberspace in 2003. Digital technologies evolve constantly—and fast! Each day, more Americans connect, and more activity moves into the cyber domain. Your NSS therefore needs not only to address current security needs but also to anticipate future threats to the country’s interests. You may find it useful to research how the world has changed over the last five years (2003-2008) so that you can project trends.

Second, the NSC holds great promise to set the rules in cyberspace. The international community is still creating international norms to govern behavior in cyberspace. Can states cross sovereign boundaries in cyberspace, and if so, what are the consequences? Are cyberattacks an “act of war,” an “act of aggression,” espionage, or something else entirely? What types of cyber intelligence gathering are acceptable? Is it legitimate to respond to cyberattacks with kinetic weapons? And so on. As a global power, the US sits in a position to shape future global norms and practices, depending on the policy it adopts. This means that the NSC must also think about how its recommendations might set important precedents that would affect—for good or ill—the long-term prospects of US security.

## **Assignment 2: Working-Group White Paper**

As a faction, draft a one-page White Paper proposal that clearly and directly communicates:

* The core values and interests at stake in the cyber domain—from your faction’s perspective;
* The specific policies that your faction would like the NSS to include; and
* The specific policies that your faction would oppose.

Your faction may reach consensus on all of the above, and it will probably help your cause if it does. Still, if consensus cannot be had, the faction can split into as many sub-factions as it likes, and sub-factions from different original factions may merge. Each sub-faction—regardless of how it forms and who belongs to it—will then submit its own White Paper.

Note: Each member of the NSC should be a(n) (co)author of a White Paper. A member can write her own, individual White Paper if she chooses; that might, however, complicate bargaining later.

*Some advice:*

Effective White Papers do not merely inform; they *persuade*, as the opening salvo in a political game. The White Paper must convince the full NSC, in other words, that your proposals should be included in the final document adopted. Do what it takes to make that happen, but note well: persuasion depends on information *and* rhetoric. NSC colleagues will quickly see through grandstanding and lofty, empty statements. Bring them objective data, analysis, research, and references.[[2]](#footnote-2)

Because White Papers persuade, you can organize the information within it as you like. Keep your eye on making a persuasive argument and including all the necessary components.

*Essential components*:

* A cover page, which contains a White Paper title and the names and institutional positions for each faction member that has signed onto the paper;
* A body—that is, the one page, single-spaced text that addresses the above points; and
* A references page (if applicable)

*Research:*

* The Gamemaster may offer you some research **to get you started**. A persuasive White Paper, however, will likely need information beyond these resources, especially to incorporate your personal, factional, or institutional perspective.

1. <https://www.npr.org/2019/05/28/727666387/security-experts-express-concern-over-electronic-system-to-check-in-at-polling-p>. [↑](#footnote-ref-1)
2. If you use references within the White Paper—an excellent idea—cite parenthetically and attach a separate reference page/bibliography. [↑](#footnote-ref-2)