**United States Cyber Deterrence, Stuxnet, and the 2016 Presidential Election[[1]](#footnote-1)**

Jeffrey Berejikian

*University of Georgia*

and

Andrew P. Owsiak

*University of Georgia*

Version 1.0, July 2020

Our game focuses on cybersecurity—a topic of growing interest among our students and those that employ them post-graduation—and the issues policy-makers grappled with in cyberspace during the Obama Administration (2009-2017). At the outset of the game, Obama (the Gamemaster) convenes his United States National Security Council (NSC) and asks it to write a National Security Strategy for Cyberspace (NSS)—a document that the United States (US) government historically creates and re-creates. Students first receive a character assignment; these characters perform primary and supporting roles on the NSC (e.g., Secretary of Energy). The students then organize into factions (i.e., those with a similar, but not identical perspective; e.g., those focused on ‘national intelligence’ or ‘military/defense’), research their organization (e.g., what does the Department of State *do*?), review a cache of instructor provided resources (e.g., historical information on cyberspace, as well as academic work on cyberspace concepts), and then build an individual/faction-based *general* policy position on cyberspace. The National Security Advisor convenes plenary sessions of the NSC to integrate the complementary policy recommendations, as well as to reconcile the contradictory policy recommendations, of the various factions. At the end of Phase I, students have their own NSS. That document outlines the government’s approach to addressing cyber conflicts that *might* arise; thus, students (unknowingly) define the parameters of their policy autonomy in the game *before* encountering the first crisis scenario (Phases II-III). They can later deviate from this policy, but not without a cost, since the American public and other stakeholders—who typically lack detailed information about cyber operations—will expect the NSC to do what they promised to the American people in the NCP.

After negotiating the NSS, a dilemma arises (Phase II). Iran continues to develop nuclear weapons, and the US has possession of a cyber weapon (Stuxnet) that might slow the Iranians down. The Bush Administration began development of the weapon, which Obama then inherited. His NSC, however, must decide whether to continue supporting Stuxnet and whether to deploy it (in history, this becomes the Stuxnet Operation). If students deploy this offensive cyber weapon against Iranian nuclear facilities, (i) it *may* delay Iranian acquisition of nuclear weapons, (ii) it does not promise to eradicate the Iranian nuclear program entirely, and (iii) it is challenging to deploy (i.e., the Iranian computers are not connected to the internet). The NSC must provide President Obama with a policy recommendation, in the form of a National Security Study Memorandum (NSSM). An NSSM defines a problem, lays out various solutions, adjudicates the solutions’ advantages and disadvantages, and then recommends (and justifies) a policy.

Once students submit the first NSSM, the game advances to Fall 2016 (Phase III). At that time, intelligence officials believe that Russia is actively intervening—through cyberspace—in the US Presidential Election. The US now becomes the target of a cyberattack, and Obama convenes the NSC to ask for an NSSM on this matter. Thus, students first encounter the opportunity to use a cyber weapon *offensively* and later, after submitting their recommendation to the President, play defense in cyberspace against a foreign adversary—that is, students confront both sides of the cybersecurity coin—offense (aggressor) and defense (target). Each side emphasizes distinct concepts and characteristics, and both sides will continue to define the cyber policy space moving forward. After both crisis scenarios finish, students then have the opportunity to revise their (general) NSS in light of the game’s activities (Phase IV).

**Instructor’s Guide (and Schedule)**

*General Narrative:*

See summary/abstract above.

*Rationale:*

Two inherent obstacles impede effective teaching in our discipline (International Affairs, or Political Science more broadly). The first is familiar to many programs. As they enter the major, few students have had exposure to the subject matter, except perhaps through current events. Issues of national security, cyber conflict, or military deterrence therefore feel remote and obscure, leaving students to struggle to understand the relationship between their coursework and their future careers. The second obstacle arises more specifically in our discipline. Undergraduate students typically cannot practice or obtain actual foreign policy experience while in residence on campus, and not all students have the financial resources to pursue highly competitive—often unpaid—internships.

In this environment, we work as instructors to design classroom experiences—through simulation (or role-playing exercises)—that encourage students to practice and hone the skills required of budding foreign policy professionals. In particular, we confront students with historically accurate foreign policy challenges and ask them to design solutions, thereby creating a simulated experiential learning cycle in the classroom. The setting, although historical, develops that skills needed of contemporary policy-makers as well.

We selected the Obama Administration as the context for this game because it grappled with two prominent policy decisions in cyberspace: Iranian nuclear proliferation and the 2016 US elections. The first concerned the offensive use of a cyber weapon against a foreign adversary, while the latter forced the United States to play defense against a foreign adversary. The game therefore requires students to confront both sides of the cybersecurity coin—offense (aggressor) and defense (target). Each side emphasizes distinct concepts and characteristics, and both sides will continue to define the cyber policy space moving forward.

*Major Issues for Debate:*

Individual interest v. parochial/group interest v. general interest.

Privacy v. security

Public notification of threats v. intelligence gathering

Coercive action v. non-coercive action

*Adaptations:*

Because cyberspace touches diverse disciplines, instructors can modify the game as they wish, infusing it with course-relevant content (e.g., on ethics, politics, economics, justice, history, gender, and so on).

*Release of information:*

This game relies on the strategic dissemination of information—i.e., releasing documents to students in stages, as opposed to all at once and up front. This prevents one stage of the game from affecting another. For example, if students know about the Iranian threat (Game Sessions 3-4) early, they design their National Security Strategy to confront this specific threat (Game Sessions 1-2). We wish to avoid such a scenario, since one of the game’s objectives is for students to accommodate an existing policy to a new situation. We therefore recommend that you release information according to the schedule below. If you modify the schedule, please read ahead to be certain that you do not inadvertently change the game in ways you do not desire.

*Decisions:*

The NSC makes decisions through voting. A majority of the Council participants present must approve the NSS and NSC Recommendation(s). These votes can happen either piecemeal as the NSC constructs a given document (e.g., a vote on option one, a vote on option two, and so on) or in aggregate once the NSC completes the entire document (e.g., the final product). We leave that decision to the NSC Acting Chair.

*Selecting an Acting NSC Chair:*

Before Game Session 1, the NSC will need an acting chairperson (i.e., someone to run the Council’s proceedings in the President’s absence). Two options exist. First, the instructor can appoint an acting chairperson from among the Council positions allocated. Were one to do this, we recommend selecting the National Security Advisor for this role. Not only do other Cabinet officials have narrower, agency specific policy portfolios, but they also often introduce unwanted political dynamics (e.g., others might defer to a Vice President or Secretary of State as acting chair, which could limit debate). As a second option, the Council can elect its own acting chair. This gives the chair greater legitimacy, but also takes additional time and may introduce the political dynamics just discussed.

*Game Schedule:*

The game schedule below proposes 4 pre-game sessions, 6-8 game sessions, and 1-2 debrief sessions—or 11-12 sessions total. Instructors who wish to shorten the game can either: (i) cut one of the scenarios—either on cyber offense (Sessions 3-4) or cyber defense (Sessions 5-6), or (ii) reduce the number of pre-game sessions (e.g., introduce fewer foundational concepts). Were one to do the latter, we recommend keeping the non-reading assignments intact. Students will need time to learn about the cyber domain, discuss policy ideas with a working group, and develop the working group White Papers that motivate the National Security Strategy discussion.

**Table 1. Instructor Roadmap to the Game.**

|  |  |  |  |
| --- | --- | --- | --- |
| *Game Session* | *Before the Session* | *During the Session* | *After the Session* |
| -4 | * Read: Allison, Graham T. (1969) “Conceptual Models and the Cuban Missile Crisis.” *American Political Science Review* 63(3):689-718. | * Discussion: bureaucratic politics model * Distribute “0 Prologue” and “1 Cyber Intro” (Assignments #0 and #1) * Assign roles (see Repository E) | * Open Repository A (as desired) * Assignment #0: The NSC * Assignment #1: Independent research on the cyber threat (as at 6/1/2009). *[NOTE: The instructor may skip this, but it encourages students to begin looking for their own material, rather than relying only on what the instructor provides.]* |
| -3 | * Read: Jervis, Robert. (1968) “Hypotheses on Misperception.” *World Politics* 20(3):454-479. | * Discussion: Misperception | * Continue Assignments #0 and #1 |
| -2 | * **Assignments #0 and 1 due before class starts** * Read:   + Morrow, James D. (1999) “The Strategic Setting of Choices: Signaling, Commitment and Negotiation in International Politics.” In *Strategic Choices and International Relations*, edited by David A. Lake and Robert Powell. Princeton: Princeton University Press, pp. 77-114.   + Geer, Kenneth. (2010) “The Challenge of Cyber Attack Deterrence.” *Computer Law and Security Review* 26:298-303.   + For more detail, see Nye, Joseph. (2017) “ Deterrence and Dissuasion in Cyberspace” *International Security* 41(3):44-71. | * Discussion:   + Costly signaling and deterrence * Have students meet in factions * Distribute “2 NSS Background” (Assignment #2) | * Open Repository B (as desired)\* * Assignment #2: Working group White Paper *[Note: The instructor may skip this, but students will find it helpful to negotiate in factions and develop a bargaining position* before *the NSC first meets. Otherwise, the class struggles to (i) develop well-researched positions, and (ii) find like-minded bargaining blocs.]* |
| -1 | * Read:   + Putnam, Robert D. “Diplomacy and Domestic Politics: The Logic of Two-Level Games.” *International Organization* 42(3):427-460. | * Discussion: Domestic politics * Distribute “3 NSS” (Assignment #3, Oral presentation of the White Paper) | * Continue Assignment #2 and 3 |
| 0  (Phase I) | Instructors can merge or expand the preparatory sessions as desired. Before the next session, however, students will definitely need:   * Some understanding of the NSC and how it works (see Repository A) * Some background in the major characteristics that define cyberspace (see Repository B) * A character/role assignment, ideally with time to think about their character’s interests in cyberspace policy * *Highly recommended:* Time to meet and negotiate as a faction. | | |
| 1 | * **Assignment #2 and 3 due before class starts** * Distribute:   + Symantec *Global Internet Security Threat Report, Trends for 2008* (in Repository A)   + *Technology, Policy, Law, and Ethics regarding US Acquisition and Use of Cyberattack Capabilities* (in Repository B) * Determine who will chair the NSC (see above) | * Distribute “4 Build the NSS” (Assignment #4) and “4b NSS Template” (as desired; see Assignment #4b). * Negotiating and drafting the NSS   + Factions presents their white papers to Council (as Assignment #3) | * Continue Assignment #4 |
| 2 |  | * Negotiating and drafting the NSS * Set due date for NSS (Assignment #4)   + **NOTE: NSS must be received before the information for the next game session can be released** | * Encourage continued discussion * If applicable, collect final NSS |
| 3  (Phase II) | * **After receiving the NSS (Assignment #4):**   + Distribute the President’s Request for Recommendations on the Iranian Nuclear Program (i.e., “5 Iran Crisis Response, Assignment #5)   + Distribute 2007 National Intelligence Estimate on Iran (in Repository C)   + Distribute Herman (2018) Tips for Writing Policy Papers (in Repository C) | * Negotiating and drafting the NSC Recommendation on Iran * **Thirty minutes before the end of this session, distribute Assignment #5b only to the National Security Advisor and the intelligence faction. Let the recipients know that they (i) may share the contents with the entire NSC (or not), but (ii) not before the last 10 minutes of this game session.** | * Open Repository C (as desired) * Continue Assignment #5 |
| 4 | * **If the Director of National Intelligence discusses the virus in Assignment #5b with the NSC during game session #3,** distribute the following reading to the class in time for them to read it prior to this session:   + Zettner, Kim. (2014) *Countdown to Zero Day*. New York: Broadway, pp. 59-68, (hold back pp 121-128). | * Negotiating and drafting the NSC Recommendation on Iran * **NOTE: NSC Recommendation on Iran due before the end of this session (or before the next session).** | * Continue Assignment #5 (if applicable) |
| 5  (Phase III) | * Distribute the Request for Recommendations on Potential Foreign Interference in the 2016 US Elections (“6 2016 Election Response”, Assignment #6) * Distribute Mueller Report, pp. 14-51. | * Negotiating and drafting the NSC Recommendation on US Elections | * Open Repository D (as desired), but not the sub-repository * NOTE: Additional documents in the unreleased repository may be added as the instructor sees fit. * Continue Assignment #6 |
| 6 | * At the outset of this session, release the media documents in the sub-repository (of Respository D) that deal with Clinton’s emails (October 2016). * If desired, release Comey’s October 2016 letter, or see if the FBI responds to the media release above instead. | * Negotiating and drafting the NSC Recommendation on US Elections * **NOTE: NSC Recommendation on the US Elections due before the end of this session.** * Distribute “7a Debrief Assignment” and/or “7b Debrief Assignment” | * Continue Assignment #7 * Release any post-game documents (as desired, in Repository F) |
| Optional  7-8  (Phase IV) |  | * *If the instructor assigns 7a Debrief Assignment, the class will need an additional session or two to meet as the NSC. If s/he selects only assignment (b), the class can proceed directly to the debriefing sessions.* | * Continue Assignment #7 |
| Debrief 1 | * **Assignment #7 (a/b) due** | * Debrief discussion |  |
| Debrief 2  (Optional) | * Read: Gibson, William. (1984) *Neuromancer*. New York: ACE.   Identifying information known to the Administration as the 2016 election unfolded can be challenging. Instructors may therefore choose to assign one or more of the following as additional post-game reading:   * Mueller, Robert S. (2019) *Report on the Investigation into Russian Interference in the 2016 Presidential Election.* * Miller, Greg. (2018) *The Apprentice: Trump, Russia, and the Subversion of American Democracy*. New York: Custom House. [journalist account] * Nance, Malcolm. (2018) *The Plot to Destroy Democracy: How Putin and His Spies Are Undermining America and Dismantling the West.* New York: Hachette Press. [intelligence community / media analyst] * Pegues, Jeff. (2018) *Kompromat: How Russia Undermined American Democracy*. New York: Prometheus. [journalist account] | * Book discussion   + This session could be skipped entirely.   + *Neuromancer* is a work of fiction that brings together pop culture, science, technology, ethics, and politics. It therefore offers a unique final session.   + Alternatively, students might read more game-content-relevant books, like those further down the list. |  |

*Notes:*

\* Repository B contains information the Obama Administration collected during its 2009 Cyber Policy Review process (February-May 2009). This review process mirrors the students’ NSS activity (in part), making the information in this collection valuable to the students’ work.

1. *Funding:* The University System of Georgia supported the creation of this game, through an Affordable Learning Georgia Pilot Grant for Developing an Open-Licensed Historical Game. The authors are grateful to the USG (and ALG) for its support. [↑](#footnote-ref-1)