What Students Need to Know:
How National Security and the Internet are Connected

WORLD AFFAIRS COUNCIL

CENTER FOR
global studies
UNIVERSITY OF WASHINGTON

IN·SER UNIVERSITY of WASHINGTON

Global Classroom Workshops made possible by:

BOEING

Microsoft

usbank

THE NORCLIFFE FOUNDATION

RAINIER INVESTMENT MANAGEMENT

And World Affairs Council Members
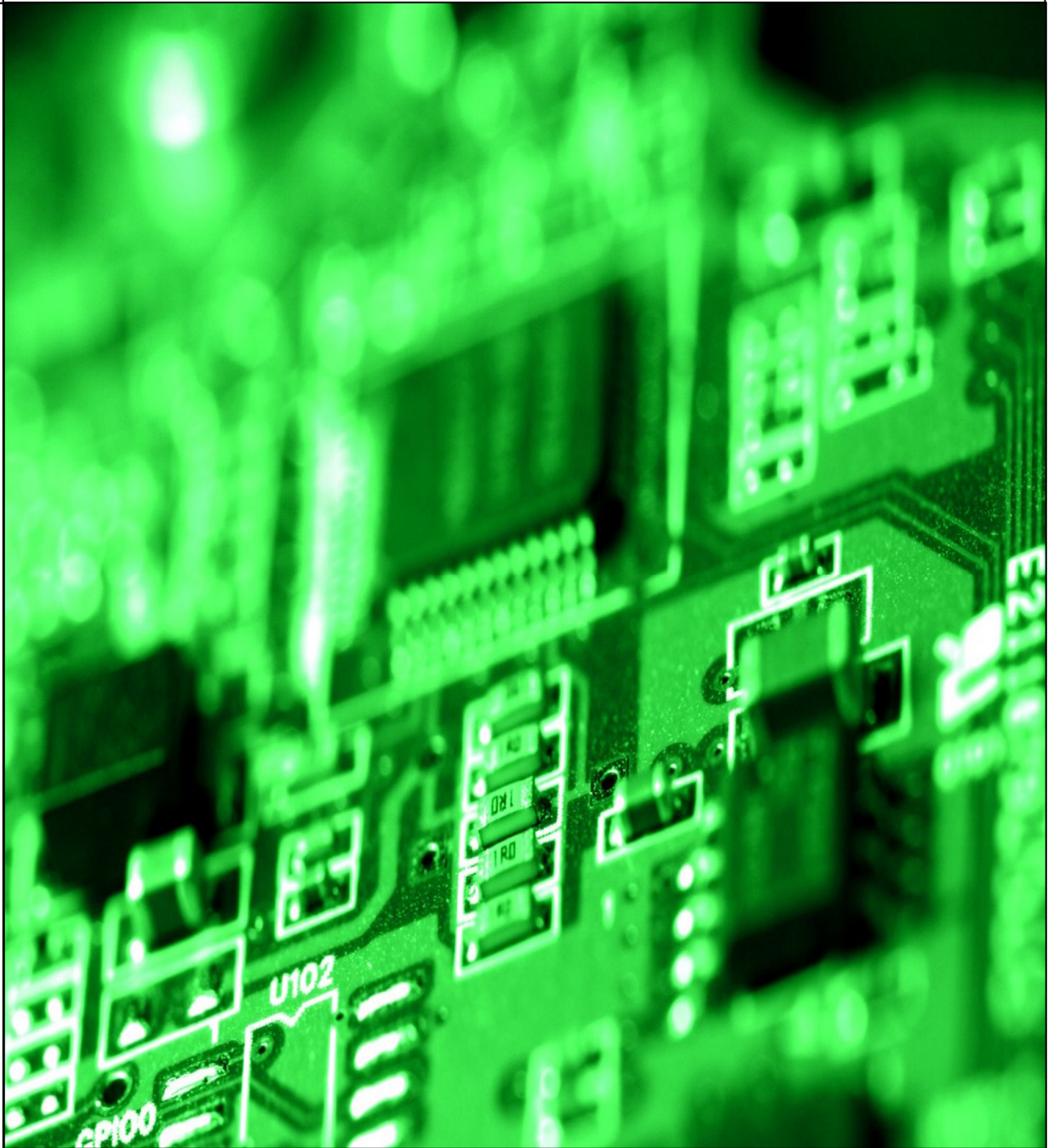
A Resource Packet for Educators
RESOURCES COMPILED BY:
Jacob Bolotin, Eileen Hynes,
Tese Wintz Neighbor
WORLD AFFAIRS COUNCIL
April 28, 2011

TABLE OF CONTENTS

USING THIS RESOURCE GUIDE
Packet published: 4/27/11; Websites checked: 4/26/11
Please note: many descriptions were excerpted directly from the websites.

Recommended Resources   Lesson Plans   Video

Maps and Charts   Audio   Books

Science, Technology, Engineering, and Math Lesson Plans

INTEGRATING STEM TOPICS INTO YOUR TEACHING

Global Classroom supports the Washington STEM Initiative which seeks to improve student achievement and opportunity in areas critical to our state's economic prosperity: Science, Technology, Engineering, and Mathematics (STEM). The Initiative aims to catalyze innovation in the state's K-12 education system, increase teacher effectiveness and student learning, and dramatically raise the number of Washington students graduating ready for college and work and succeeding in STEM degree programs. These efforts are intended to benefit every student in the state, with a particular emphasis on accelerating the achievement of low-income and minority students.

INTRODUCING GENERAL MICHAEL V. HAYDEN (RET.)

As Director of the CIA (2006-2009), General Michael V. Hayden was responsible for overseeing the collection of information concerning the plans, intentions, and capabilities of America's adversaries; producing timely analysis for decision makers; and conducting covert operations to thwart terrorists and other enemies of the US. Before becoming Director of the CIA, General Hayden served as the country's first Principal Deputy Director of National Intelligence (2005-2008) – and was the highest-ranking intelligence office in the armed forces. Earlier, he served as Commander of the Air Intelligence Agency, Director of the Joint Command and Control Warfare Center, Director of the National Security Agency (1999-2005) and Chief of the Central Security Service.

EDUCATION
1967 Bachelor of Arts degree in history, Duquesne University, Pittsburgh, Pa.
1969 Master's degree in modern American history, Duquesne University
1975 Academic Instructor School, Maxwell Air Force Base, Ala.
1976 Squadron Officer School, Maxwell AFB, Ala.
1978 Air Command and Staff College, Maxwell AFB, Ala.
1980 Defense Intelligence School (postgraduate curriculum), Defense Intelligence Agency, Bolling AFB, D.C.
1983 Armed Forces Staff College, Norfolk, Va.
1983 Air War College, Maxwell AFB, Ala.

MAJOR AWARDS AND DECORATIONS
Defense Distinguished Service Medal
Defense Superior Service Medal with oak leaf cluster
Legion of Merit
Bronze Star Medal
Meritorious Service Medal with two oak leaf clusters
Air Force Commendation Medal
Air Force Achievement Medal

EFFECTIVE DATES OF PROMOTION
Second Lieutenant   June 2, 1967
First Lieutenant   June 7, 1970
Captain   Dec. 7, 1971
Major   June 1, 1980
Lieutenant Colonel   Feb. 1, 1985
Colonel   Nov. 1, 1990
Brigadier General   Sept. 1, 1993
Major General   Oct. 1, 1996
Lieutenant General   May 1, 1999
General   April 21, 2005

Sources: http://www.af.mil/information/bios/bio.asp?bioID=5746

WHAT IS THE CIA?

WHAT DOES THE CENTRAL INTELLIGENCE AGENCY (CIA) DO?
The Central Intelligence Agency's primary mission is to collect, evaluate, and disseminate foreign intelligence to assist the president and senior U.S. government policymakers in making decisions relating to the national security. The CIA does not make policy; it is an independent source of foreign intelligence information for those who do. The CIA may also engage in covert action at the president's direction in accordance with applicable law.
More FAQs about the CIA: https://www.cia.gov/about-cia/faqs/index.html

The United States has carried out intelligence activities since the days of George Washington, but only since World War II have they been coordinated on a government-wide basis. President Franklin D. Roosevelt appointed New York lawyer and war hero, William J. Donovan, to become first the Coordinator of Information, and then, after the U.S. entered World War II, head of the Office of Strategic Services (OSS) in 1942. The OSS – the forerunner to the CIA – had a mandate to collect and analyze strategic information. After World War II, however, the OSS was abolished along with many other war agencies and its functions were transferred to the State and War Departments.

It did not take long before President Truman recognized the need for a postwar, centralized intelligence organization. To make a fully functional intelligence office, Truman signed the National Security Act of 1947 establishing the CIA. The National Security Act charged the CIA with coordinating the nation's intelligence activities and correlating, evaluating and disseminating intelligence affecting national security.

On December 17, 2004, President George W. Bush signed the Intelligence Reform and Terrorism Prevention Act which restructured the Intelligence Community by abolishing the position of Director of Central Intelligence (DCI) and Deputy Director of Central Intelligence (DDCI) and creating the position the Director of the Central Intelligence Agency (D/CIA). The Act also created the position of Director of National Intelligence (DNI), which oversees the Intelligence Community and the National Counterterrorism Center (NCTC).
https://www.cia.gov/about-cia/history-of-the-cia/index.html

How many people work for the CIA and what is its budget?
Neither the number of employees nor the size of the Agency's budget can, at present, be publicly disclosed.

Does the CIA spy on Americans? Does it keep a file on you?
By law, the CIA is specifically prohibited from collecting foreign intelligence concerning the domestic activities of US citizens. Its mission is to collect information related to foreign intelligence and foreign counterintelligence. Collection is allowed only for an authorized intelligence purpose; for example, if there is a reason to believe that an individual is involved in espionage or international terrorist activities.

Who decides when CIA should participate in covert actions, and why?
Only the president can direct the CIA to undertake a covert action.

Who is a spy? Are there secret agents like James Bond with secret gadgets?
A spy is someone who provides classified information about his country to another country. To clarify, CIA operations officers recruit foreign agents (you could also call them spies) who pass information to CIA. CIA operations officers do use some nifty "spy gadgets," and, while their jobs do occasionally present risks and challenges equal to the most exciting movies, for the most part, they are not nearly as glamorous or thrilling.

WHAT ROLE DID THE CIA PLAY IN FINDING BIN LADEN?

This section has been added on 5/3/11 for the web version of the resource packet, originally published 4/27/11. This section will specifically address what role the CIA played in finding Osama bin Laden.

THE GUARDIAN: OSAMA BIN LADEN: IT TOOK YEARS TO FIND HIM BUT JUST MINUTES TO KILL HIM (5/2/11)
http://www.guardian.co.uk/world/2011/may/02/how-osama-bin-laden-found

The trail that led the CIA to Osama bin Laden began with his most trusted courier. It had taken the CIA years to discover first his name and then the home where he was hiding the al-Qaida leader. But it took only 40 minutes on Sunday for U.S. special forces to kill both the courier and bin Laden. Contrary to repeated speculation over the past decade that bin Laden was living in one of the remote tribal areas of Pakistan or even across the border in Afghanistan, the al-Qaida leader was found in an affluent suburb of Pakistan's capital, Islamabad. Senior US administration officials, briefing journalists in a late-night teleconference, said that after 9/11 the CIA chased various leads about bin Laden's inner circle, in particular his couriers. One of these couriers came in for special attention, mentioned by detainees at Guantánamo Bay by his nom de guerre. He was said to be a protege of Khalid Sheikh Mohammed, the 9/11 mastermind, and one of the few couriers bin Laden trusted.

Two years ago, the CIA found the rough location where the courier and his brother lived in Pakistan, and on August last year they narrowed it down to a compound in Abbottabad, an affluent area about 35 miles north of Islamabad that had been founded as a British garrison town in the 1840s and named after its first deputy commissioner, Major James Abbott. They realized immediately this was no normal residence. The walls of the 3,000 sq ft compound were 12-18ft high, topped with barbed wire. There were two security gates, and access to the compound was severely restricted. The main part of the residence was three stories high but had few windows, and a third-floor terrace was shielded by a privacy wall. Built around five years ago, it was valued at about $1m but had no phone or internet connection.

The two brothers had no known source of income, adding to CIA suspicions. The CIA learned too that there was a family living with them, and that the composition of this family matched bin Laden's. Local suspicions were understood to have been aroused by the fact that the residents of the compound burned their rubbish rather than putting it out for collection. Salman Riaz, a film actor, said that five months ago he and a crew tried to do some filming next to the house, but were told to stop by two men who came out.

By September, the CIA had determined there was a "strong possibility" that the hideout was bin Laden's, and by February, they were confident they had the right location. In March Barack Obama began chairing a series of five national security meetings. At the last of these, on Friday 29 April, while the world's attention was on the royal wedding taking place in London, he gave the order to mount an operation.

At that meeting, at 8.20am in the diplomatic room at the White House, Obama met his national security adviser Thomas Donilon, counter-terrorism adviser John O Brennan, and other senior national security aides to go through the detailed plan to attack the compound and sign the formal orders authorizing it, the *New York Times* reported. "We shared our intelligence on this compound with no other country, including Pakistan," a senior administration official told the paper. Only a tiny handful of people within the administration were aware of the operation. Four U.S. military helicopters, carrying elite troops from Navy Seal Team Six, a top counter-terrorism unit, U.S. officials told the Associated Press, were under the direct command of the CIA director, Leon Panetta, whose analysts monitored the compound from his conference room, which was transformed into a command centre. The details of the operation, including

the number of US military personnel involved, remain unclear. Senior administration officials will only say that bin Laden "resisted" during a gun battle. He died from a bullet to the head, they said. bin Laden was identified by facial recognition, one official said, declining to say whether DNA analysis had also been used.

The al-Qaida courier, his brother and one of bin Laden's sons, whom officials did not name, were also killed. One of bin Laden's sons, Hamza, is a senior member of al-Qaida. The officials said one woman died when she was used as a shield by a male combatant, and two other women were injured. Other unidentified males were taken from the scene, a Pakistani official told the Associated Press, while four children and two women were arrested and left in an ambulance, the official said. The operation took 40 minutes in total, after which flames were visible on the roof of the building. Before withdrawing, U.S. forces blew up the helicopter wreckage. bin Laden's body was loaded on to one of the helicopters and taken from the scene. US officials later confirmed he had been buried at sea, mindful of the Islamic imperative for a speedy burial. The location was not revealed. "We don't want a bunch of people going to the shrine forever," an official told the *Washington Post*.

It was mid-afternoon at CIA headquarters when Panetta and his team received word that bin Laden was dead, the Associated Press reported, after which cheers and applause broke out across the conference room.

TIME: THE CIA GETS A RARE PUBLIC VICTORY (5/2/11)
http://news.yahoo.com/s/time/20110502/us_time/08599206899800
As the news of Osama bin Laden's death moves from exhilarating novelty to accepted reality, one group in the U.S. government will emerge as key to the win: the Central Intelligence Agency. From the earliest identification of a bin Laden courier, the pursuit of leads, the assessment of evidence and the execution of the raid in Abottabad, Pakistan, the CIA can rightly claim the most credit for finding and killing the world's most wanted terrorist. Taking credit for a win is not something the agency gets to do often. Though on high alert in the run-up to 9/11, the CIA was criticized afterward for failing to connect the dots of existing intelligence on the threat. Years of failed efforts to find and kill bin Laden thereafter embarrassed and frustrated the agency. But the picture already emerging from senior administration sources will begin to turn that opinion around. In a briefing for reporters last night, officials laid out in detail the intelligence work that went into finding bin Laden.

BIN LADEN KILL MAY REOPEN CIA INTERROGATION DEBATE (5/2/11)
http://www.reuters.com/article/2011/05/03/us-binladen-interrogations-idUSTRE7417SQ20110503
The possibility that U.S. spies located Osama bin Laden with help from detainees who'd been subjected to "enhanced interrogation" techniques seems certain to reopen the debate over practices that many have equated with torture, security experts said on Monday. One of the key sources for initial information about an al Qaeda "courier" who led U.S. authorities to bin Laden's Pakistani hide-out was Khalid Sheikh Mohammed, the al Qaeda operative said to have masterminded the September 11, 2001 attacks, a former U.S. national security official said. KSM was subjected to "waterboarding" 183 times, the U.S. government has acknowledged. But it was not until later, after waterboarding was suspended because it and other harsh techniques became heatedly debated, that Mohammed told interrogators about the existence of a courier particularly close to bin Laden, a fragmentary tip that touched off a years-long manhunt that ended in bin Laden's death at the hands of U.S. special forces on Sunday.

INTELLIGENCE GATHERING AND DEMOCRACY: HOW DO THEY COEXIST?

An intelligence gathering agency by its design must operate with a certain degree of secrecy in order to be effective. Yet, at the same time democracies must be transparent and civilian controlled. How can the CIA be an effective and secretive intelligence gathering agency while operating within the transparent, accountable, civilian controlled parameters of a democracy?   The following resources will examine the coexistence of the CIA within American democracy. Featured in this section are remarks by General Hayden and other resources that attempt to answer that question.

EXECUTIVE OVERSIGHT OF INTELLIGENCE
https://www.cia.gov/library/publications/additional-publications/the-work-of-a-nation/intelligence-oversight/index.html

NATIONAL SECURITY COUNCIL (NSC)
The NSC was established by the National Security Act of 1947 to advise the President with respect to the integration of domestic, foreign, and military policies relating to national security. The NSC is the President's principal forum and the highest Executive Branch entity for considering national security and foreign policy matters with his senior national security advisors and cabinet officials. The NSC is chaired by the President and its regular attendees (both statutory and non-statutory) are the Vice President, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense and the Assistant to the President for National Security Affairs (commonly referred to as the National Security Advisor). The Chairman of the Joint Chiefs of Staff is the statutory military advisor to the Council, and the DNI (Director of Nation Intelligence) is the intelligence advisor.

INTELLIGENCE OVERSIGHT BOARD (IOB)
The President's IOB was established by President Gerald Ford in 1976 as a White House entity within the Executive Office charged with oversight responsibility for the legality and propriety of intelligence activities. The Board, which reports to the President, is charged primarily with preparing reports "of intelligence activities that the IOB believes may be unlawful or contrary to Executive order or Presidential directive." The Board may also refer such reports to the Attorney General. This standard assists the President in ensuring that highly sensitive intelligence activities comply with law and Presidential directive. In 1993, the IOB was made a standing committee of the President's Intelligence Advisory Board (PIAB). The IOB is comprised of up to 5 PIAB members.

PRESIDENT'S INTELLIGENCE ADVISORY BOARD (PIAB)
The PIAB is maintained within the Executive Office of the President and acts as a nonpartisan body providing advice to the President concerning the quality and adequacy of intelligence collection, analysis and estimates, counterintelligence, and other intelligence activities. Its sixteen members serve without compensation at the pleasure of the President and are selected from individuals who are not employed by the Federal Government. The Board continually reviews the performance of all government agencies engaged in the collection, evaluation, or production of intelligence or in the execution of intelligence policy. It also assesses the adequacy of management personnel and organization in intelligence agencies and advises the President concerning the objectives, conduct, and coordination of the activities of these agencies. The Board is specifically charged to make appropriate recommendations for actions to improve and enhance the performance of the intelligence efforts of the United States.

INTELLIGENCE GATHERING AND DEMOCRACY: HOW DO THEY COEXIST?

LEGISLATIVE OVERSIGHT OF INTELLIGENCE
https://www.cia.gov/library/publications/additional-publications/the-work-of-a-nation/intelligence-oversight/legislative-oversight-of-intelligence.html

The U.S. Congress has had oversight responsibility over the CIA since the Agency was established in 1947. However, prior to the mid-1970s, oversight responsibilities resided in the Armed Services Committees of both chambers and were less formal than they are now. At the time, the DCI and his representatives interacted directly with the respective chairmen of the congressional committees, and formal hearings and testimony were rare.

Following allegations of wrongdoing by U.S. intelligence agencies, the Senate established the Senate Select Committee on Intelligence (SSCI) on 19 May 1976. The House of Representatives followed suit on 14 July 1977 by creating the House Permanent Select Committee on Intelligence (HPSCI). These committees, along with the Armed Services, Foreign Relations, and Foreign Affairs Committees, were charged with authorizing the programs of the intelligence agencies and overseeing their activities. The 1980 Intelligence Oversight Act established the current oversight structure by making the SSCI and the HPSCI the only two oversight committees for the CIA. However, the House and Senate Appropriations Subcommittees on Defense (HAC-D and SAC-D), given their constitutional role to appropriate funds for all U.S. Government activities, also exercise oversight functions. The Select Intelligence Oversight Panel (SIOP) is a joint House subcommittee created in the 110th Congress as a result of the 9/11 Commission recommendations. It is composed of members from the HAC (appropriators) and HPSCI (authorizers) to help coordinate intelligence budget issues to meet IC mission and capability requirements. There is no comparable joint SAC and SSCI subcommittee in the Senate.

The Office of Congressional Affairs (OCA) is the focal point for CIA activities with Congress—guiding and facilitating all CIA interaction with Congress, the development of clear strategies to promote and protect the Agency's Congressional equities, and CIA's legal responsibility to keep Congress fully and completely informed of our intelligence activities. In addition, OCA has the primary responsibility for ensuring the CIA workforce is fully prepared for all Congressional engagements.

OCA also leads the drafting, coordination, production, and advocacy for D/CIA proposals for the annual Intelligence Authorization bill packages, and works with other Intelligence Community agencies, ODNI, Office of Management and Budget, and the Congress to facilitate enactment of the D/CIA proposals. Likewise, OCA screens hundreds of bills at various stages of the legislative process, identifying those that might cause problems for CIA and pursuing coordinated efforts within CIA, ODNI, OMB, and Congress to prevent or fix the identified problems. In addition, OCA oversees and has primary responsibility for the provision of timely, coordinated D/CIA responses to about 500 Legislative Referral Memorandums a year from OMB that seek CIA concurrence and/or comments on various legislative proposals, draft testimony, or Administration signing statements. OCA keeps CIA leadership and other elements informed of major legislative developments.

Reminder: Please see the lesson plans section for additional resources for teaching about these topics.

INTELLIGENCE GATHERING AND DEMOCRACY: HOW DO THEY COEXIST?

CIA OPEN GOVERNMENT PLAN
https://www.cia.gov/open/cia-open-government-plan.html
The need for a secret intelligence service as a first line of defense to protect a free society is well understood, and has been a part of the fabric of our country since George Washington utilized a spy network to help win the Revolutionary War. Nevertheless, there always has been a concern about how a secret agency with special authorities fits within an open and democratic society. Endeavoring to resolve the tension between the need and the concern has been an important part of the Central Intelligence Agency (CIA) culture. The CIA is not an independent actor. It responds to the direction of the President under the oversight of the Congress, mindful of the need to ensure that all of its activities are in full compliance with U.S. law. The Agency strongly supports the President's Open Government Initiative because it also is mindful that continued public support for CIA is very much dependent upon public understanding of its mission and activities. This plan addresses the three core values or components of the open government initiative: Transparency, Participation, and Collaboration, and outlines the ways this agency will incorporate these core values into its programs. **See the link above for the full plan.**

DECLASSIFY CYBER VULNERABILITIES (3/14/11)
http://www.wired.com/threatlevel/2011/03/hayden-cyber/
The former head of America's most powerful and secretive intelligence agencies thinks the U.S. government classifies too much information on cybersecurity vulnerabilities.

INTELLIGENCE GATHERING AND DEMOCRACY: HOW DO THEY COEXIST?

 "Let me be clear: This stuff is overprotected," writes retired four-star Gen. Michael Hayden, in the new issue of the Air Force's *Strategic Studies Quarterly*. "It is far easier to learn about physical threats from U.S. government agencies than to learn about cyberthreats."
For a top spook, Hayden always had a unexpected soft spot for transparency. Until the Sept. 11 attacks turned government secrecy into a fetish, Hayden had been nudging NSA toward a bit of *glasnost*. And at his confirmation hearings for the CIA role, he admitted: "I do think we overclassify, and I think it's because we got bad habits."

CENTRAL INTELLIGENCE AGENCY: FREEDOM OF INFORMATION ACT (FOIA)
http://www.foia.cia.gov/
The FOIA Electronic Reading Room is provided as a public service by the CIA and its Office of Information Management. Here you can view previously released documents, released through the FOIA and other disclosure statutes. If you would like to view our previously released documents and collections, visit our Frequently Requested Records, our Special Collections, and our 25 Year Program Archive. Because of CIA's need to comply with U.S. national security laws, some documents—or parts of documents—cannot be released to the public. Specifically, the CIA has the responsibility to protect intelligence sources and methods from disclosure.

WASHINGTON POST: CIA LAUNCHES TASK FORCE TO ASSESS IMPACT OF U.S. CABLES' EXPOSURE BY WIKILEAKS (12/22/10)
http://www.washingtonpost.com/wp-dyn/content/article/2010/12/21/AR2010122104599.html?hpid=topnews
Only a handful of CIA files have surfaced on the WikiLeaks Web site, and records from other agencies posted online reveal remarkably little about CIA employees or operations.
CIA officials said the agency is conducting an extensive inventory of the classified information, which is routinely distributed on a dozen or more networks that connect agency employees around the world. And the task force is focused on the immediate impact of the most recently released files. One issue is whether the agency's ability to recruit informants could be damaged by declining confidence in the U.S. government's ability to keep secrets. "The director asked the task force to examine whether the latest release of WikiLeaks documents might affect the agency's foreign relationships or operations," CIA spokesman George Little said. The panel is being led by the CIA's Counterintelligence Center but has more than two dozen members from departments across the agency. To some agency veterans, WikiLeaks has vindicated the CIA's long-standing aversion to sharing secrets with other government agencies, a posture that came under sharp criticism after it was identified as a factor that contributed to the nation's failure to prevent the attacks of Sept. 11, 2001.

TIME: THE CIA GETS A RARE PUBLIC VICTORY (5/2/11)
http://news.yahoo.com/s/time/20110502/us_time/08599206899800
The article fits nicely in this section about intelligence gathering and democracy because in this secret operation the American public had no idea what the CIA was doing when it helped find and kill Osama bin Laden. However, now that it's been successful, the CIA is able to take credit for its part. As the news of Osama bin Laden's death moves from exhilarating novelty to accepted reality, one group in the U.S. government will emerge as key to the win: the Central Intelligence Agency. From the earliest identification of a Bin Laden courier, the pursuit of leads, the assessment of evidence and the execution of the raid in Abottabad, Pakistan, the CIA can rightly claim the most credit for finding and killing the world's most wanted terrorist. Taking

credit for a win is not something the agency gets to do often. Though on high alert in the run-up to 9/11, the CIA was criticized afterward for failing to connect the dots of existing intelligence on the threat. Years of failed efforts to find and kill bin Laden thereafter embarrassed and frustrated the agency. And reforms intended to fix the CIA's problems remained inconclusive in the public eye, without a win on the issue most important to Americans: bringing bin Laden to justice. But the picture already emerging from senior administration sources will begin to turn that opinion around. In a briefing for reporters last night, officials laid out in detail the intelligence work that went into finding bin Laden. The case started with human intelligence.

GO INSIDE THE $56 BILLION 'BLACK' BUDGET (2/18/11)
http://www.wired.com/dangerroom/2011/02/go-inside-the-56-billion-black-budget/
The Pentagon dropped its $533 billion budget this week. Some line items get a thorough public debate — like stealth jet engines and soldier health care. Others have opaque names like "RETRACT MAPLE," and are totally hush-hush. Welcome to the Defense Department's classified, or black, budget. It appears to be about $56 billion, the same as last year, less some inflation. The pencil pushers in Arlington play all kinds of tricks with the line items to keep outsiders from guessing where, exactly, the black budget actually gets spent. Some of the National Intelligence Program (NIP), a component of the country's intelligence budget, gets hidden away inside the Pentagon's ledger. For years, the Department stashed a chunk of the CIA's cash and its share of funds for the secret satellite makers at the National Reconnaissance Office in the blandly-named "Selected Activities in Other Procurement, Air Force" funding line. The NIP budget request was officially disclosed for the first time this year, and so you're likely looking at some of its $55 billion in these line items.

WHITE HOUSE, INTEL CHIEF CAN'T AGREE ON BUDGET SECRECY (2/15/11)
http://www.wired.com/dangerroom/2011/02/white-house-intel-chief-cant-agree-on-budget-secrecy/
For decades, U.S. spy chiefs kept their annual budget requests hidden from the public, saying national security would be damaged if the cash figure leaked out. But yesterday, the director of national intelligence released the request for the first time....

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
http://www.dni.gov/
The ODNI is headed by the Director of National Intelligence, or DNI, who is appointed by the President with the advice and consent of the Senate. The Director of National Intelligence (DNI) serves as the head of the Intelligence Community (IC), overseeing and directing the implementation of the National Intelligence Program (budget) and acting as the principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to the national security.

UNITED STATES INTELLIGENCE COMMUNITY
http://www.intelligence.gov/about-the-intelligence-community/
The Director of National Intelligence heads the intelligence community, which includes: Air Force Intelligence, Army Intelligence, Central Intelligence Agency Coast Guard Intelligence, Defense Intelligence Agency, Department of Energy, Department of Homeland Security, Department of State , Department of the Treasury, Drug Enforcement Administration, Federal Bureau of Investigation, Marine Corps Intelligence, National Geospatial-Intelligence Agency,

INTELLIGENCE GATHERING AND DEMOCRACY: HOW DO THEY COEXIST?

National Reconnaissance Office, National Security Agency, Navy Intelligence, and Office of the Director of National Intelligence.

TRANSPARENCY INTERNATIONAL
http://www.transparency.org/policy_research/surveys_indices/cpi/2010/results
How transparent, accountable, and free from corruption does the public believe their governments are? Corruptions Perceptions Index 2010. A ranking of "10" is the most clean (or most transparent, accountable, and corruption-free), while "0" is considered highly corrupt. Americans rank the United States a 7.1, while by comparison Danes rank Denmark 9.3, the French rank their country a 6.8, and Iraqis rank their country 1.5.

PRO-CON.ORG: USA PATRIOT ACT
http://aclu.procon.org/view.questions.php?issueID=000082&subissueID=000253
These teacher/student friendly resources include arguments in favor and against the Patriot Act. Full Text of the USA PATRIOT Act (PDF) Should the USA PATRIOT Act have been made law? Does the USA PATRIOT Act diminish civil liberties? Does the PATRIOT Act allow the government to conduct secret searches and access records of individuals held by third parties, without providing sufficient judicial overview? Does the PATRIOT Act provide the government with overreaching power to conduct searches, surveillances and wiretaps? Does the PATRIOT Act unfairly target minority and immigrant communities?

PRO-CON.ORG: DO NATIONAL SECURITY LETTERS GIVE EXCESSIVE SURVEILLANCE POWER TO THE GOVERNMENT?
http://aclu.procon.org/view.answers.php?questionID=000722
(This resource is not related to the CIA but does concern law enforcement activity of the FBI. Teachers may find this resource useful in the broader discussion of this section).
Yes: The American Civil Liberties Union (ACLU) stated in a July 2003 report titled "Unpatriotic Acts" that: "National Security Letters (NSLs) allow the FBI to obtain certain kinds of sensitive personal records without obtaining any kind of court order... The absence of judicial oversight means that, when it comes to the use of NSLs, the FBI has a free hand No: The Justice Department cannot secure our nation against terrorist attack unless investigators are equipped with tools that allow them to disrupt plots before they can be carried out. These same tools must protect civil liberties. National Security Letters (NSLs) satisfy both requirements.

NY TIMES: A CASE FOR ACCOUNTABILITY (1/26/11)
http://www.nytimes.com/2011/01/26/opinion/26wed3.html?_r=1&ref=centralintelligenceagency
A court hearing this month in Manhattan turned on a subject that has mostly been missing in the legal response to former President George W. Bush's abusive detention policies: some measure of accountability. The focus of the hearing before Judge Alvin Hellerstein of Federal District Court was not torture itself but the Central Intelligence Agency's deliberate destruction in 2005 of dozens of videotapes made three years earlier showing the brutal interrogation of high-level terrorism suspects, including the simulated drowning technique known as waterboarding. At the time, the agency had been ordered by Judge Hellerstein to preserve the tapes. They were part of the evidence being sought in a lawsuit brought by the American Civil Liberties Union under the Freedom of Information Act seeking details of prisoner mistreatment. Their destruction was seen as so egregious that the Bush administration felt compelled to order a special investigation when it was disclosed.

CYBER SECURITY

What do we mean by the term "cyber security?" What are America's cyber vulnerabilities? How do we protect ourselves against these threats? In order to be secure, should we regulate the internet? The resources below attempt to answer these questions and many others related to the United States' cyber security.

HACKERS FORCE INTERNET USERS TO LEARN SELF-DEFENSE (8/11/11)
http://www.pbs.org/newshour/bb/science/july-dec10/cyber_08-11.html

GEN. MICHAEL HAYDEN: *We have created this new domain, this new space called cyber, and, frankly, it's lawless. There are no natural technical barriers up there to protect information. That's why all of us are—kind of have to assume a personal responsibility for firewalls. I mean, when was the last time any of us have been asked to defend ourselves personally in any other space except the cyber-space?*

SPENCER MICHELS: But is there a serious threat? And what is it?

GEN. MICHAEL HAYDEN: *Because it is so anarchic, there are a variety of actors out there in this space that don't have your best interests at heart.*

There are state actors out there who are interested in stealing either state secrets or industrial secrets.

... who are interested in doing their espionage thing. And, frankly, in cyber-space, some stuff valuable to you may actually be of interest to them in ways that none of us could imagine five or 10 years ago.

You have got anarchists out there who just want to destroy things. You have potential terrorists out there who just want to do harm. And then, finally, you have got criminals. I mean, the modern-day bank robber isn't speeding up to a suburban bank with weapons drawn and notes passed to the teller. He's on the Web taking things of value from you and me. And they're all taking advantage of what is essentially anarchy out there in the global network....

SPENCER MICHELS: Is there a defense against a cyber-attack?

GEN. MICHAEL HAYDEN: *By the nature of the Internet, the advantage goes to the offense. We have built the Internet in such a way that it's very hard to defend it. It's built on openness. It's built on access. It's built on agility. None of those things help the defense.*

(Full transcript and video included at the above link.)

U.S. MILITARY CYBERWAR: WHAT'S OFF-LIMITS? (7/29/10)
http://news.cnet.com/8301-31921_3-20012121-281.html

Michael Hayden, who was the principal deputy director of national intelligence and retired last year, said the rules of engagement for electronic battlefields are still too murky, even after the Defense Department created the U.S. Cyber Command last spring. The new organization is charged with allowing the U.S. armed forces to conduct "full-spectrum military cyberspace operations in order to enable actions in all domains," which includes destroying electronic infrastructure as thoroughly as a B-2 bomber would level a power plant. Even a formal cyberwar may have rules different from those applying to traditional warfare, Hayden suggested. One option would be for the larger G8 or G20 nations to declare that "cyberpenetration of any (financial) grid is so harmful to the international financial system that this is like chemical weapons: none of us should use them," he said at the Black Hat computer security conference here. Another option would be for those nations to declare that "outside of actual physical attacks in declared conflicts, denial of service attacks are never allowed and are absolutely forbidden and never excused," and a consensus would "stigmatize their use," said Hayden, who's now a principal at the Chertoff Group. Nations "do not do it and they do not allow it to happen from their sovereign space." In 2008, for instance, Georgia accused Russia of

launching a coordinated denial-of-service attack against Georgian Web sites, which coincided with military operations in the breakaway region of South Ossetia.

JOURNAL OF HOMELAND SECURITY: UNDERSTANDING & DEFENDING AGAINST FOREIGN CYBER-THREATS (8/07)
http://www.homelandsecurity.org/journal/Default.aspx?oid=165&ocat=1
As the United States and its allies continue to wage the war on terror, the private sector is working in concert with branches of the federal government to develop new defenses against foreign-borne cyber-attacks designed to either cripple our mission-critical systems or steal from our private citizens. These threats may vary in their end goal, but whether financially or politically motivated, all cyber-crime requires a coordinated, vigilant, preventive effort by the private sector. However, to implement defenses against these types of attacks, we must understand the current landscape and the motivations of these cyber-terrorists and criminals. Check the website for additional scholarly articles related to cyber security.

MICHAEL HAYDEN ON INTERNATIONAL CHALLENGES OF CYBER-SECURITY (2009)
http://c-span.org/Events/Fmr-CIA-Dir-Michael-Hayden-on-International-Challenges-of-Cyber-Security/16003-1/
General Michael Hayden and others spoke about cyber-security threats to the nation's computer and telecommunications infrastructure. Among the topics addressed were advances in military technology, developing strategies for cyber-warfare, and constructing future protections from potential hackers. They also answered questions from the audience.

DECLASSIFY CYBER VULNERABILITIES (3/14/11)
http://www.wired.com/threatlevel/2011/03/hayden-cyber/
The former head of America's most powerful and secretive intelligence agencies thinks the U.S. government classifies too much information on cybersecurity vulnerabilities.
"Let me be clear: This stuff is overprotected," writes retired four-star Gen. Michael Hayden, in the new issue of the Air Force's *Strategic Studies Quarterly*. "It is far easier to learn about physical threats from U.S. government agencies than to learn about cyberthreats."
For a top spook, Hayden always had a unexpected soft spot for transparency. Until the Sept. 11 attacks turned government secrecy into a fetish, Hayden had been nudging NSA toward a bit of *glasnost*. And at his confirmation hearings for the CIA role, he admitted: "I do think we overclassify, and I think it's because we got bad habits.

SEATTLE TIMES: UW TEAM WINS CYBER DEFENSE COMPETITION (4/11/11)
http://seattletimes.nwsource.com/html/localnews/2014746226_uwcyberwin12m.html?syndication=rss
UW competed against eight other teams from around the country during the 17 hours of competition. Each group acted as a new IT department hired by a fake pharmaceutical company, Kwikepills, and attempted to fend off cyber attacks from professionals while maintaining company services. The UW team won the regional competition, the Pacific Rim Regional Collegiate Cyber Defense Competition, in March. It was the fourth year UW won regionals, and the third time the team battled for the national title.
More info (4/7/11 article): http://seattletimes.nwsource.com/html/localnews/2014715280_cybergame08m.html
"The bad guys that are attacking our systems, they don't really care whether the web address ends with .gov, .edu, .com; it's all the same to them," said Barbara Endicott-Popovsky, an associate research professor at UW who founded the regional competition. "We are in an interconnected world and what concerns me is that society doesn't get it." All nine teams aim to trounce cyber intruders, but, unlike many of their competitors, the UW team of computer-

World Affairs Council Resource Packet *What Students Need to Know: How National Security & the Internet are Connected*—April 28, 2011

13

science and engineering students does so without formal training in that area. Instead, its members rely on knowledge from years of learning cyber defense for fun.

UNITED STATES CYBER COMMAND (*USCYBERCOM)*
http://www.defense.gov/home/features/2010/0410_cybersec/

DEPARTMENT OF DEFENSE CYBER CRIME CENTER
http://www.dc3.mil/home.php

STRATEGIC STUDIES INSTITUTE: US ARMY WAR COLLEGE
Subscribe to free newsletter: http://www.strategicstudiesinstitute.army.mil/newsletter/

STRATEGIC STUDIES QUARTERLY: THE FUTURE OF THINGS "CYBER," MICHAEL V. HAYDEN (*SPRING* 2011) (PDF)
http://www.au.af.mil/au/ssq/2011/spring/hayden.pdf

Rarely has something been so important and so talked about with less clarity and less apparent understanding than this phenomenon. Do not get me wrong. There are genuine experts, and most of us know about patches, insider threats, worms, Trojans, WikiLeaks, and Stuxnet. But few of us (myself included) have created the broad structural framework within which to comfortably and confidently place these varied phenomena. And that matters. I have sat in very small group meetings in Washington, been briefed on an operational need and an operational solution, and been unable (along with my colleagues) to decide on a course of action because we lacked a clear picture of the long-term legal and policy implications of any decision we might make.

Privacy?
When we plan for operations in a domain where adversary and friendly data coexist, we should be asking: What constitutes a twenty-first-century definition of a reasonable expectation of privacy? Google and Facebook know a lot more about most of us than we are comfortable sharing with the government. In a private-sector web culture that seems to elevate transparency to unprecedented levels, what is the appropriate role of government and the DoD? If we agree to limit government access to the web out of concerns over privacy, what degree of risk to our own security and that of the network are we prepared to accept? How do we articulate that risk to a skeptical public, and who should do it?

Do we really know the threat?
Former Director of National Intelligence Mike McConnell frequently says we are already "at war" in cyberspace. Richard Clarke even titled his most recent cautionary book, Cyber War. Although I generally avoid the at war terminology, I often talk about the inherent insecurity of the web. How bad is it? And if it is really bad, with the cost of admission so low and networks so vulnerable, why have we not had a true cyber Pearl Harbor? Is this harder to do than we think? Or, are we just awaiting the inevitable? When speaking of the threat, citizens of a series of first-world nations were recently asked whom they feared most in cyberspace, and the most popular answer was not China or India or France or Israel. It was the United States. Why is that, and is it a good thing? People with money on the line in both the commercial and government sectors want clear, demonstrable answers.

Is there a role for international law?
Indeed, as a powerful cyberfaring nation, how comfortable are we with regulation at all? After all, this domain launched by the DoD has largely been nurtured free of government regulation. Its strengths are its spontaneity, its creativity, its boundlessness. The best speech given by an American official on macro net policy was given late last year by Secretary of State Clinton when she emphasized Internet freedom, not security or control or regulation. But there are moves afoot in international bodies like the International Telecommunications Union to regulate the Internet, to give states more control over their domains, to Balkanize what up until now has been a relatively seamless global enterprise. How and when do we play?

The Future of Things "Cyber" continued

Is cyber arms control possible ?
As a nation, we tend toward more freedom and less control but—given their destructiveness, their relative ease of use, and the precedent their use sets—are distributed denial-of-service attacks ever justified? Should we work to create a global attitude toward them comparable to the existing view toward chemical or biological weapons? Should we hold states responsible if an attack is mounted from their physical space even if there is no evidence of complicity? And, are there any legitimate uses for botnets? If not, under what authority would anyone preemptively take them down? These are questions for which no precedent in law or policy (domestic or international) currently exists. If we want to establish precedent, as opposed to likely unenforceable treaty obligations, do we emphasize dialogue with like-minded nations, international institutions . . . or multinational IT companies?

There are more questions that could be asked, many of them as fundamental as these. Most we have not yet answered or at least have not yet agreed on answers, and none of them are easy. How much do we really want to empower private enterprises to defend themselves? Do we want necessarily secretive organizations like NSA or CyberCom going to the mats publicly over privacy issues? At what point does arguing for Internet security begin to legitimate China's attempts at control over Internet speech? Do we really want to get into a public debate that attempts to distinguish cyber espionage (which all countries pursue) from cyber war (something more rare and sometimes more destructive)? Are there any cyber capabilities, real or potential, that we are willing to give up in return for similar commitments from others?

Tough questions all—tougher (perhaps) but not unlike those our airpower ancestors faced nearly a century ago. As pioneer air warriors grappled with the unfamiliar, so must we. Until these and other questions like them are answered, we could be forced to live in the worst of all possible cyber worlds— routinely vulnerable to attack and self-restrained from bringing our own power to bear.

WALLSTREET JOURNAL: **CYBER ATTACKS TEST U.S., ALLIES, AND FOES (9/25/10)**
http://online.wsj.com/article/SB10001424052748703793804575511961264943300.html
Cyber espionage has surged against governments and companies around the world in the past year, and cyber attacks have become a staple of conflict among states.
U.S. military and civilian networks are probed thousands of times a day, and the systems of the North Atlantic Treaty Organization headquarters are attacked at least 100 times a day, according to Anders Fogh Rasmussen, NATO's secretary-general. "It's no exaggeration to say that cyber attacks have become a new form of permanent, low-level warfare," he said.
More than 100 countries are currently trying to break into U.S. networks, defense officials say. China and Russia are home to the greatest concentration of attacks.
The Pentagon's Cyber Command is scheduled to be up and running next month, but much of the rest of the U.S. government is lagging behind, debating the responsibilities of different agencies, cyber-security experts say. The White House is considering whether the Pentagon needs more authority to help fend off cyber attacks within the U.S.
"The Obama administration is very focused on this. The president has designated [cyber security] as a critical national asset," said an Obama administration official, adding that agencies responsible for cyber security have been staffing up, including Homeland Security's development of SWAT teams to respond to cyber attacks on critical infrastructure. "Not only do we have a strategy, but we have moved beyond that to implementation."

CYBER SECURITY

FOREIGN POLICY: **THE TOP 10 CHINESE CYBER ATTACKS (THAT WE KNOW OF) (1/22/10)**
http://thecable.foreignpolicy.com/posts/2010/01/22/the_top_10_chinese_cyber_attacks_that_we_know_of

1) Titan Rain
In 2004, an analyst named Shawn Carpenter at Sandia National Laboratories traced the origins of a massive cyber espionage ring back to a team of government sponsored researchers in Guangdong Province in China. The hackers, code named by the FBI "Titan Rain," stole massive amounts of information from military labs, NASA, the World Bank, and others. Rather than being rewarded, Carpenter was fired and investigated after revealing his findings to the FBI, because hacking foreign computers is illegal under U.S. law. He later sued and was awarded more than $3 million. The FBI renamed Titan Rain and classified the new name. The group is still assumed to be operating.

2) State Department's East Asia Bureau
In July 2006, the State Department admitted it had become a victim of cyber hacking after an official in "East Asia" accidentally opened an email he shouldn't have. The attackers worked their way around the system, breaking into computers at U.S. embassies all over the region and then eventually penetrating systems in Washington as well.

3) Offices of Rep. Frank Wolf
Wolf has been one of the most outspoken lawmakers on Chinese human rights issues

4) Commerce Department
The Commerce Department's Bureau of Industry and Security had to throw away all of its computers in October 2006, paralyzing the bureau for more than a month due to targeted attacks originating from China. BIS is where export licenses for technology items to countries like China are issued.

5) Naval War College
In December 2006, the Naval War College in Rhode Island had to take all of its computer systems offline for weeks following a major cyber attack. One professor at the school told his students that the Chinese had brought down the system. The Naval War College is where much military strategy against China is developed.

6) Commerce Secretary Carlos Gutierrez

7) McCain and Obama presidential campaigns

8) Office of Sen. Bill Nelson, D-FL
At a March 2009 hearing, Nelson revealed that his office computers had been hacked three separate times and his aide confirmed that the attacks had been traced back to China.

9) Ghostnet
In March, 2009, researchers inToronto concluded a 10-month investigation that revealed a massive cyber espionage ring they called Ghostnet that had penetrated more than 1,200 systems in 103 countries. The victims were foreign embassies, NGOs, news media institutions, foreign affairs ministries, and international organizations.

10) Lockheed Martin's F-35 program
In April, 2009, the *Wall Street Journal* reported that China was suspected of being behind a major theft of data from Lockheed Martin's F-35 fighter program.

CYBER SECURITY

THE CHINESE RESPONSE: CHINA 'BIGGEST VICTIM' OF CYBER ATTACKS (1/25/10)
http://www.chinadaily.com.cn/china/2010-01/25/content_9368402.htm
A senior official in charge of Internet security has claimed that the country has become the world's biggest victim of cyber attacks. Last year, 262,000 IP addresses in China were hit by trojans planted by nearly 165,000 overseas IP addresses. In an interview with Xinhua over the weekend, Zhou Yonglin, deputy chief of the operations department of China National Computer Network Emergency Response Technical Team (CNCERT), also dismissed Google's allegation that hackers traced to China had attacked its servers."Those from the US ranked first, accounting for 16.61 percent," Zhou said.

IN CYBERSPY VS. CYBERSPY, CHINA HAS THE EDGE (4/14/11)
http://news.yahoo.com/s/nm/20110414/ts_nm/us_china_usa_cyberespionage
As America and China grow more economically and financially intertwined, the two nations have also stepped up spying on each other. Today, most of that is done electronically, with computers rather than listening devices in chandeliers or human moles in tuxedos.
And at the moment, many experts believe China may have gained the upper hand.
Though it is difficult to ascertain the true extent of America's own capabilities and activities in this arena, a series of secret diplomatic cables as well as interviews with experts suggest that when it comes to cyber-espionage, China has leaped ahead of the United States.
According to U.S. investigators, China has stolen terabytes of sensitive data—from usernames and passwords for State Department computers to designs for multi-billion dollar weapons systems. And Chinese hackers show no signs of letting up. "The attacks coming out of China are not only continuing, they are accelerating," says Alan Paller, director of research at information-security training group SANS Institute in Washington, DC.
Secret U.S. State Department cables, obtained by WikiLeaks and made available to Reuters by a third party, trace systems breaches—colorfully code-named "Byzantine Hades" by U.S. investigators—to the Chinese military. An April 2009 cable even pinpoints the attacks to a specific unit of China's People's Liberation Army.
Privately, U.S. officials have long suspected that the Chinese government and in particular the military was behind the cyber-attacks. What was never disclosed publicly, until now, was evidence.

***NY TIMES:* COMPUTER SECURITY (CYBER SECURITY)**
http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_security/index.html?scp=1-spot&sq=cyber%20security&st=cse
This NY Times page is the paper's central location for posting all articles related to cyber security. Bookmark it and check it regularly!

WATER BOARDING & MILITARY DETENTIONS: HISTORY & LEGAL STATUS

While the CIA has engaged in numerous programs outside of the public's eye and been the subject of numerous controversies, we have chosen to pay special attention to only one of those major recent controversies: water boarding. As part of this section, we have also included resources related to CIA and military detentions of "enemy combatants" in which water boarding or other enhanced interrogation techniques may or may not have been used. Please see the book section for other information about selected other CIA controversies and covert actions.

WHAT IS WATER BOARDING?
http://science.howstuffworks.com/water-boarding.htm

Water boarding has been around for centuries. It was a common interrogation technique during the Italian Inquisition of the 1500s and was used perhaps most famously in Cambodian prisons during the reign of the Khmer Rouge regime during the 1970s. As late as November 2005, water boarding was on the CIA's list of approved "enhanced interrogation techniques" intended for use against high-value terror suspects. And according to memos released by the U.S. Department of Justice in April 2009, water boarding was among 10 torture techniques authorized for the interrogation of an al-Qaida operative. In a nutshell, water boarding makes a person feel like he is drowning. Water boarding as it is currently described involves strapping a person to an inclined board, with his feet raised and his head lowered. The interrogators bind the person's arms and legs so he can't move at all, and they cover his face. In some descriptions, the person is gagged, and some sort of cloth covers his nose and mouth; in others, his face is wrapped in cellophane. The interrogator then repeatedly pours water onto the person's face. Depending on the exact setup, the water may or may not actually get into the person's mouth and nose; but the physical experience of being underneath a wave of water seems to be secondary to the psychological experience. The person's mind believes he is drowning, and his gag reflex kicks in as if he were choking on all that water falling on his face.

COMMON ARTICLE 3 OF THE GENEVA CONVENTIONS
http://www.nytimes.com/ref/us/AP-Guantanamo-Geneva-Conventions.html

(1) Persons taking no active part in the hostilities, including members of armed forces who have laid down their arms and those placed 'hors de combat' by sickness, wounds, detention, or any other cause, shall in all circumstances be treated humanely, without any adverse distinction founded on race, colour, religion or faith, sex, birth or wealth, or any other similar criteria.
To this end, the following acts are and shall remain prohibited at any time and in any place whatsoever with respect to the above-mentioned persons:
(a) violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture;
(b) taking of hostages;
(c) outrages upon personal dignity, in particular humiliating and degrading treatment;
(d) the passing of sentences and the carrying out of executions without previous judgment pronounced by a regularly constituted court affording all the judicial guarantees which are recognized as indispensable by civilized peoples.
(2) The wounded and sick shall be collected and cared for.
An impartial humanitarian body, such as the International Committee of the Red Cross, may offer its services to the Parties to the conflict.
The Parties to the conflict should further endeavour to bring into force, by means of special agreements, all or part of the other provisions of the present Convention.
The application of the preceding provisions shall not affect the legal status of the Parties to the conflict.

WATER BOARDING & MILITARY DETENTIONS: HISTORY & LEGAL STATUS

WATERBOARDING HISTORICALLY CONTROVERSIAL (10/5/06)
http://www.washingtonpost.com/wp-dyn/content/article/2006/10/04/AR2006100402005.html
...Inside the CIA, waterboarding is cited as the technique that got Khalid Sheik Mohammed, the prime plotter of the Sept. 11, 2001, terrorist attacks, to begin to talk and provide information—though "not all of it reliable," a former senior intelligence official said. ...
On Jan. 21, 1968, *The Washington Post* published a front-page photograph of a U.S. soldier supervising the questioning of a captured North Vietnamese soldier who is being held down as water was poured on his face while his nose and mouth were covered by a cloth. The picture, taken four days earlier near Da Nang, had a caption that said the technique induced "a flooding sense of suffocation and drowning, meant to make him talk."
The article said the practice was "fairly common" in part because "those who practice it say it combines the advantages of being unpleasant enough to make people talk while still not causing permanent injury."
The picture reportedly led to an Army investigation.
Twenty-one years earlier, in 1947, the United States charged a Japanese officer, Yukio Asano, with war crimes for carrying out another form of waterboarding on a U.S. civilian. The subject was strapped on a stretcher that was tilted so that his feet were in the air and head near the floor, and small amounts of water were poured over his face, leaving him gasping for air until he agreed to talk.

CIA BANS WATERBOARDING IN TERROR INTERROGATIONS (9/14/07)
http://blogs.abcnews.com/theblotter/2007/09/cia-bans-water-.html
The controversial interrogation technique known as waterboarding, in which a suspect has water poured over his mouth and nose to stimulate a drowning reflex, has been banned by CIA director Gen. Michael Hayden, current and former CIA officials tell ABCNews.com.
The officials say Hayden made the decision at the recommendation of his deputy, Steve Kappes, and received approval from the White House to remove waterboarding from the list of approved interrogation techniques first authorized by a presidential finding in 2002.

ONLY THREE HAVE BEEN WATERBOARDED BY CIA (11/2/07)
http://blogs.abcnews.com/theblotter/2007/11/exclusive-only-.html
For all the debate over waterboarding, it has been used on only three al Qaeda figures, according to current and former U.S. intelligence officials.
As ABC News first reported in September, waterboarding has not been used since 2003 and has been specifically prohibited since Gen. Michael Hayden took over as CIA director.

WATER BOARDING & MILITARY DETENTIONS: HISTORY & LEGAL STATUS

HAYDEN: WATERBOARDING MAY BE ILLEGAL (2/8/08)
http://www.military.com/NewsContent/0,13319,161672,00.html
Question: Some observers have been surprised at how ardently you defended—and continue to defend—*CIA*'s detention and interrogation program. Particularly, considering that the most aggressive and controversial enhanced interrogation technique—waterboarding—was last used more than three years before you became *CIA* director. Why did you take this approach, when you easily could have taken a different tack?

Answer: *A couple of thoughts. And clarity here is very important. I didn't quite defend all the [enhanced interrogation] techniques. I certainly didn't defend waterboarding. Remember, I said earlier that George Tenet made the tough decisions that I thank God I didn't have to make. People ask me, "Well, what would you have done?" and I say, "I thank God I didn't have to make that decision," and that's as far as I go. What I did was point out that whatever you may think of this, it worked and we did indeed get life-saving intelligence out of it.*
So the point I would make to folks who say, "I don't want you doing this, and it doesn't work anyway," I would point out, "Whoa. Stop. The front half of that sentence, you can say; that's yours, you own that, 'I don't want you doing it.' The back half of that sentence is not yours. That's mine. And the fact is it did *work. So here is the sentence you have to give. 'Even though it may have worked, I still don't want you doing it.' That requires courage. That requires you going out to the American people and saying, 'We're looking at a tradeoff here folks, and I want you to understand the tradeoff.'" I can live with that tradeoff. I can live with the person who makes that tradeoff. Either way. That's an honorable position. But I felt duty-bound to be true to the facts. There's a second element. I felt morally obligated to the people in the Agency not to allow them to feel as if they had been abandoned by the senior leadership. What they did was done out of duty, not enthusiasm. They weren't volunteers; they were thrown into the breach. The republic asked them to do things that were very difficult, and they did them. And they did them frankly knowing that there would be a day—after the republic felt safe again—that some people would begin to question their actions.*
I often say the reality of the intelligence world is an element of the political leadership that wants to be free to criticize us when they feel endangered, for not doing enough, and they want to be free to criticize us for doing too much when they no longer feel in danger. That's not just unfair and unjust, it's inefficient. It's no way to backstop an intelligence agency. So, you know, most of this didn't happen on my watch, and I've been somewhat identified with it because of the positions I've taken publicly. But I couldn't see myself doing it any other way.

HAYDEN OVERHAULS CIA DETENTION (10/24/07)
http://www.upi.com/Top_News/Special/2007/10/24/Analysis-Hayden-overhauls-CIA-detention/UPI-64681193234226/
In the year since it was publicly acknowledged by President Bush, the CIA's controversial program of detaining suspected terrorist leaders, and subjecting some of them to interrogation techniques critics say constitute torture, has been overhauled by the agency's new director.
In a wide-ranging TV interview Monday, Gen. Michael Hayden declined to give any details of the changes made to the program but said they had followed a "rich dialogue" with the agency's overseers on the congressional intelligence committees. "I can't describe that (new) program to you," he told PBS interviewer Charlie Rose, "but I would suggest to you that it would be wrong to assume that the program of the past is necessarily the program moving

forward into the future." Hayden insisted the CIA's detention and interrogation program, even as it was run under his predecessors, had been "appropriate, lawful and effective" but said the legal territory on which it was run had shifted over the years since it was set up in March 2002, when senior al-Qaida commander Abu Zubaydah became the first of what Hayden said were less than 100 prisoners who had passed through the system.

In the last 2 1/2 years alone, Hayden said, "We had the Detainee Treatment Act in December of 2005, we had the Hamdan decision (by the U.S. Supreme Court) in the summer of 2006, we had the Military Commissions Act in the fall of 2006. They have all changed the legal landscape under which the CIA's program is operated."

But beyond just ensuring the program was legal, Hayden said, he made changes because he wanted buy-in for what the agency was doing, above all from Congress.

"We made a conscious decision inside CIA ... that this program, if it were to go forward, had to go forward on something more than just a definition of its lawfulness."

CIA BACKS OFF DETENTION, INTERROGATION (4/11/11)

http://www.upi.com/Top_News/US/2011/04/11/CIA-backs-off-detention-interrogation/UPI-13021302524193/

The CIA has all-but ended its interrogation role abroad, except for those caught in Iraq and Afghanistan, causing concern among some U.S. congressional members. Criticism of President George W. Bush's administration interrogation and detention policies prompted President Obama to stop sending suspected terrorists to the U.S. naval base at Guantanamo Bay, Cuba, while publicity forced the CIA to shut down a network of secret prisons, leaving U.S. officials without an obvious place to hold new prisoners. In addition, a criminal investigation has been under way for a while into whether CIA officers broke the law by conducting extreme interrogations of suspected terrorists during the Bush administration.

"The CIA is out of the detention and interrogation business," a U.S. official familiar with intelligence operations told the *Los Angeles Times*.

BIN LADEN KILL MAY REOPEN CIA INTERROGATION DEBATE (5/2/11)

http://www.reuters.com/article/2011/05/03/us-binladen-interrogations-idUSTRE7417SQ20110503

The possibility that U.S. spies located Osama bin Laden with help from detainees who'd been subjected to "enhanced interrogation" techniques seems certain to reopen the debate over practices that many have equated with torture, security experts said on Monday.

One of the key sources for initial information about an al Qaeda "courier" who led U.S. authorities to bin Laden's Pakistani hide-out was Khalid Sheikh Mohammed, the al Qaeda operative said to have masterminded the September 11, 2001 attacks, a former U.S. national security official said. KSM, as he was known to U.S. officials, was subjected to "waterboarding" 183 times, the U.S. government has acknowledged. But it was not until later, after waterboarding was suspended because it and other harsh techniques became heatedly debated, that Mohammed told interrogators about the existence of a courier particularly close to bin Laden, a fragmentary tip that touched off a years-long manhunt that ended in bin Laden's death at the hands of U.S. special forces on Sunday.

WATER BOARDING & MILITARY DETENTIONS: HISTORY & LEGAL STATUS

GENERAL HAYDEN'S REMARKS AT THE COUNCIL ON FOREIGN RELATIONS (9/7/07)
https://www.cia.gov/news-information/speeches-testimony/2007/general-haydens-remarks-at-the-council-on-foreign-relations.html
A year and a day ago, the president publicly acknowledged the existence of CIA's detention and interrogation program. It began with the capture of Abu Zubaydah in the spring of 2002. Fewer than 100 people had been detained at CIA's facilities. And I mentioned renditions, the number of renditions—that's moving a terrorist from A to B—apart from that 100 that we've detained, the number of renditions is actually even a smaller number, mid-range two figures. These programs are targeted and they are selective. They were designed only for the most dangerous terrorists and those believed to have the most valuable information, such as knowledge of planned attacks, but they've also been the subject of wild speculation both here and overseas.

Additional resources related to the legality of water boarding and CIA/military detentions. This list is meant to serve as primer to these complicated issues and is not complete.

COMMON ARTICLE 3 OF THE GENEVA CONVENTIONS
http://www.nytimes.com/ref/us/AP-Guantanamo-Geneva-Conventions.html
Relates to the rights and treatment of combatants during war. (Please see earlier pages in this section for full text).

HABEAS CORPUS
http://topics.nytimes.com/topics/reference/timestopics/subjects/h/habeas_corpus/index.html
"Habeas corpus is the legal concept that a prisoner has a right to challenge the basis of confinement—to demand that the government produce a valid reason for detention."

***NEW YORK TIMES*: MILITARY COMMISSIONS**
http://topics.nytimes.com/top/reference/timestopics/subjects/d/detainees/military_commissions/index.html
(Excerpted and edited)
     The legal struggles around the commissions date back to a series of orders in 2001 and 2002 in which the Bush administration created a system of tribunals that specifically did not adhere to the standards set out in the Geneva Convention, arguing that as "non-state actors" the suspects were not entitled to that kind of protection; the system was also declared to be beyond review by federal courts.
     In 2004, the Supreme Court disagreed, in a case named Rasul v. Bush. A Supreme Court decision in June 2006, Hamdan v. Rumsfeld, struck down military tribunals that the Bush administration had established shortly after the Sept. 11 attacks. The court ruled that the tribunals violated the Constitution and the Geneva Conventions.
     In response, the Bush Administration and Congress effectively rewrote the law, by passing the Military Commissions Act of 2006. The measure broadened the definition of enemy combatants beyond the traditional definition used in wartime, to include noncitizens living legally in the United States as well as those in foreign countries and anyone determined to be an enemy combatant under criteria defined by the president or secretary of defense. In place of habeas proceedings, it said detainees could challenge their imprisonment only through hearings known as combatant status review trials.

WATER BOARDING & MILITARY DETENTIONS: HISTORY & LEGAL STATUS

In a 2008 decision in the case of Boumediene v. Bush, the Supreme Court overturned those portions of the law, finding that foreign terrorism suspects held at Guantánamo Bay have constitutional rights to challenge their detention in United States courts.

Among the first acts carried out by the administration of President Barack Obama in January 2009 was an executive order closing Guantánamo. It also issued an immediate halt to the military commission proceedings for prosecuting . Mr. Obama suggested during his 2008 presidential campaign that, in place of military commissions for the detainees, he would prefer prosecutions in federal courts or, perhaps, in the existing military justice system, which provides legal guarantees similar to those of American civilian courts. However, he never explicitly ruled out the use of military commissions, though possibly with different procedures than those used by the Bush administration. On May 15, 2009, Mr. Obama said the commissions would be used as one avenue for prosecution along with existing American courts. The new system would limit the use of hearsay evidence against detainees, ban evidence gained from cruel treatment, and give defendants more latitude to pick their own lawyers.

DETAINEE TREATMENT ACT OF 2005
http://www.cfr.org/terrorism-and-the-law/detainee-treatment-act-2005-hr-2863-title-x/p9865
Congressional act that prohibits inhumane treatment of prisoners (including those at Guantanamo Bay).

HAMDAN V. RUMSFELD (2006)
http://www.law.cornell.edu/supct/html/05-184.ZS.html
This ruling found military commissions lack the legal authority to try detainees at Guantanamo Bay.

MILITARY COMMISSIONS ACT OF 2006
http://www.cfr.org/human-rights/military-commissions-act-2006/p11754
This legislation gives the U.S. president authorization to set up military commissions to try enemy combatants, and sets some limits for their interrogation and prosecution based on Common Article 3 of the Geneva Conventions. Defendants may not invoke the Geneva Conventions during trials or file habeas corpus petitions in federal court, and cannot prevent hearsay evidence from entering the court.

BOUMEDIENE V. BUSH (2008)
http://www.law.cornell.edu/supct/html/06-1195.ZS.html
Ruling found prisoners (including those at Guantanamo Bay) have a right to habeas corpus.

MILITARY COMMISSIONS ACT OF 2009
http://www.defense.gov/news/2009%20MCA%20Pub%20%20Law%20111-84.pdf

A FIRST LOOK AT THE MILITARY COMMISSIONS ACT OF 2009
http://writ.news.findlaw.com/mariner/20091104.html?pagewanted=all
A lawyer for *Human Rights Watch* analyzes Obama-era changes and continuities with previous Bush-era laws related to military commissions.

LESSON PLANS ABOUT THE CIA/INTELLIGENCE GATHERING

LESSON PLANS FROM THE CIA
https://www.cia.gov/kids-page/parents-teachers/teacher-resources/index.html
Lesson Plan A: Examples of Problem Solving
Grade Level: Middle/High School
Subjects Involved: Social Studies, History, Science, English
Time: 30 minutes; or two 30 minute sessions if used as an in-class assignment
Objective: Students will learn how technology and problem solving have been used throughout CIA history by applying those tools in their own scenarios.
Materials: Access to the CIA Museum Web page or printouts of those pages.
https://www.cia.gov/about-cia/cia-museum/index.html
The teacher should have students select an item from the list of CIA Museum artifacts, read about it, and then write a short story about how it might be used today. Encourage students to use their imagination to create the story as a homework or in-class assignment.
In the next class, the teacher should ask volunteers to read their stories, and then encourage class discussion. Direct the discussion toward the use of today's advanced technology for practical uses in national security – e.g., micro-technology, satellite surveillance. Bring relevance to the discussion by introducing applications from everyday life, such as the micro-cameras available in cell phones.

LESSON PLAN B: GATHERING AND ANALYZING INFORMATION
Grade Level: Middle/High School
Subjects Involved: Social Studies, History, English
Time: two class periods, 30-45 minutes each
Objective: Students will learn how to plan, gather, and analyze data by providing a simulation of the **CIA's Intelligence Cycle** – the process used by CIA employees to collect and disseminate intelligence. https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html
Materials: "Intelligence Cycle" print outs, pen/pencil and paper
This lesson will take place over two class sessions and include a homework assignment.
To begin the lesson, the teacher will hand out the "Intelligence Cycle" print out and discuss its five steps: Planning & Direction, Collection, Processing, Analysis & Production, and Dissemination.
After the students understand the "Intelligence Cycle," the teacher should write the following on the blackboard: "Back in my day...." Begin a discussion by asking students how many of them have heard their parents or grandparents use that phrase in conversation and what they learned about their family's past from those reminiscences.
Next, the teacher should ask students to pick a parent or grandparent they can interview before the next class and write three paragraphs comparing the student's current day-to-day life to their subject's life at the same age. Discuss what kind of questions to ask to see the differences in the student's life compared to their subject's life at the same point.
The teacher should then break the class into smaller groups so students can make up a list of questions to ask to gather the best information. After a few minutes, each group should share their best questions with the class.

In addition to the questions that the students come up with, the teacher can provide students with some of the sample interview questions listed below:

1. Where did you live?
2. What did you do after school?
3. What did you do for fun?
4. Where did you go with your friends?
5. How did you communicate with your friends?
6. Family photos can also be sources of information –
   o Where did the family vacation when they were younger?
   o How does that compare to where the family vacations now?
   o What can we learn from this information?
7. How important is geography? Why do you live in this city or town? Is it driven by economics?
8. How has technology impacted lives of kids today versus when you were a kid?
9. How has the educational process changed? Or has it?

In the next class, the teacher should break the class into small groups and have students compare their findings with one another and then have the groups report to the class. Ask students to talk about the process of gathering information and analyzing the data. What would they have done differently? What additional questions should have been asked? What have they learned about their day-to-day lives versus their subject's?

Finally, the teacher should give students the assignment to add a paragraph about what they learned from final group discussion to their original homework.

LESSON PLAN C: MYTHS ABOUT CIA VS. REALITY

Grade Level: Middle/High School
Subjects Involved: Social Studies, History, Career Development
Time: 30 minutes
Objective: Students will gain a more realistic view of the CIA and intelligence work than available in popular culture and modern media.
Materials: Print outs of "**We'd Like to Dispel a Few Myths About the Central Intelligence Agency**" brochure, pen/pencil and paper. https://www.cia.gov/careers/cia-personality-quiz-text.html

The teacher should ask volunteers to read aloud some of the Myths pages to stimulate discussion. At the same time, the teacher should compile a list on the blackboard of the skills an intelligence officer needs to be successful – traits like courage, the ability to speak foreign languages, comfort using technology, and the ability to analyze information.

The teacher should then discuss the diversity of occupations within the CIA and the intelligence community, showing the range of careers beyond the "clandestine operative." Discuss and compile a list on the blackboard of other necessary CIA jobs – scientists, engineers, IT professionals, language teachers, analysts, lawyers, etc. Teachers can find a list of specific jobs for which the CIA is currently hiring on the CIA Careers page. https://www.cia.gov/careers/opportunities/index.html

Finally, discuss with the class how each of these CIA occupations plays a role in national security and the world of intelligence.

LESSON PLAN D: INTELLIGENCE'S ROLE IN WAR
 Grade Level: High School
 Subjects Involved: Social Studies, History
Time: several class periods, 60 minutes each
Objective: Students will learn the positive impact of gathering intelligence.
Materials: Pen/pencil and paper.
The teacher should write on the blackboard: "Ben Franklin," "Washington's Crossing of the Delaware," "Yorktown," and "D-Day."
Teacher and students should then discuss the role of intelligence and espionage in wartime. Discussion topics could include the main goals of intelligence during war, including tracking troop movements, enemy intentions, battle plans, and where arms are stored. Advancements in technology to enhance intelligence gathering could also be discussed, although the basic purpose of intelligence gathering has remained the same.
Below are four examples that highlight the use of intelligence from U.S. history and how the successful use of intelligence has shortened conflict or effectively ended wars. The teacher should divide the class into four groups and assign one of the following examples to each group. The students should research each example (by Internet or library research) and report back to the class:

- **Ben Franklin's Most Successful Intelligence Gambit**
  Knowing French spies followed him, Benjamin Franklin made sure he was observed meeting British government officials shortly after the American revolutionary victory at Saratoga. Worried that the Americans and British would reconcile their differences after that battle, the French rushed into an alliance – thanks to Franklin's ploy – with the Americans that helped lead to America's ultimate victory. Discuss Franklin's influence overseas as a diplomat and covert "spy," the political tenor in America before and after the Battle of Saratoga, and/or French and English relations in the era.

- **Washington's Surprise Attack**
  In 1776, American spy John Honeyman reported to Gen. George Washington how lazy and unprepared a garrison of Hessian troops in Trenton, New Jersey, had become. Honeyman was involved in persuading the Hessians that the Americans would not attack. Washington and his troops crossed the Delaware River at night and recorded a major victory on Dec. 26, 1777. Discuss American espionage in the Revolutionary War, Hessian troops in the Revolutionary War, Washington's army and their desperate situation at the time of the attack, and/or how the war turned with the American victory.

- **Code-Breaking Sets Stage for D-Day**
  During World War II, a Japanese ambassador in Berlin, who was a military man, studied German military deployments and reported them at length back to Tokyo via "Purple"-enciphered messages. He reported troop placements on the Atlantic wall fortifications along the coasts of France and Belgium. Allied forces used the intercepted transmissions to plan the D-Day invasion of Western Europe. Discuss American espionage and intelligence operations in WWII, the German Enigma machine and the use of code-breaking in WWII, and/or D-Day invasion planning.

- **Eisenhower's D-Day Deception**
  Allied force commander Gen. Dwight Eisenhower chose to land in Normandy, France, because he knew the German command expected the invasion to come in Calais, France. The Germans posted 19 divisions in Calais, France, as Eisenhower built an elaborate fake headquarters across the channel from Calais. Details of a Calais invasion were deliberately leaked to known German agents. For every aerial scouting mission flown over Normandy,

one was flown over Calais, as well, and the Calais area was bombed as heavily as Normandy. The deception worked so well that even after the Normandy invasion began, the German divisions stayed in Calais, sure Normandy was just a diversion. Discuss American espionage and intelligence and counterintelligence operations in WWII.

LESSON PLAN E: CODES AND CODE-BREAKING
Grade Level: Upper Elementary and Middle School
Subjects Involved: Social Studies, Math, and English
Time: 30-45 minutes
Objective: Students will learn different methods to breaking codes.
Materials Needed: Pen/pencil and paper
The teacher should begin by writing a statement on the blackboard using one of the four methods provided below. Students should then attempt to decipher the code. Show the students how the code works.

- Using numbers to represent letters of the 26-letter alphabet
- Reverse imaging (write words backward so they appear correct in a mirror)
- Scrambling the letters within the sentence
- Develop a secret pattern using the alphabet. For example, for each letter of the sentence, move up one letter on the alphabet to develop the code. (i.e., Csfbl uif dpef = Break the code)

Next, the teacher should divide the class into four groups and have each group create a coded message of their own using one of the four methods provided above. Teachers can use the suggested methods or develop new ones.
Finally, the teacher and students should discuss the importance of knowing how to write and break codes. One discussion might center on code breaking during WWII and planning the D-Day invasion. This information can be found in the **Operation History** section of the CIA Kids' Page.

LESSON PLAN F: THE IMPORTANCE OF ACCURATE COMMUNICATIONS
Grade Level: Upper Elementary, Middle/High School
Subjects Involved: Social Studies, History, English
Time: 15-30 minutes
Objective: Students will learn how messages can become jumbled in common communication.
The teacher should divide the class into multiple groups of four or more, and give each group a different worded message to relay. For example, "My dog was feeling blue about the book he read at the cafeteria." or "When I went to start the car, the bunny high-fived the squirrel." Random sentences such as these will work the best. Students will then whisper their "interpretation" of the message to the next student in the group, spreading the message around a small circle. The last student will write the message down and then share with the entire class. The teacher will then share what the message(s) should have been. The activity can be repeated several times, reversing directions and increasing in complexity. At the end of the activities, the teacher can talk about the importance of clear and accurate communications and how messages can get mixed up when more people get involved. In summary, the teacher should ask students to consider some incidents in history where accurate communications were vital, such as Paul Revere knowing that two lanterns in the Old North Church meant the British were advancing on the Charles River instead of over land.

CIA: GAMES
https://www.cia.gov/kids-page/games/index.html
These games can be adapted for classroom use/included with lesson plans listed above.

World Affairs Council Resource Packet *What Students Need to Know: How National Security & the Internet are Connected*—April 28, 2011

27

SECRET INK
http://www.kidzworld.com/article/3844-making-invisible-ink-appear
For this lesson, teachers can combine the above link on how to create different types of invisible ink with the recently declassified resources below about how secret ink was used in WWI to relay secret messages. *CIA Declassifies WWI-Era Secret Documents* (4/20/11)
http://news.yahoo.com/s/ap/20110419/ap_on_re_us/us_cia_secret_writing
The CIA lifted the lid on one corner of the cloak and dagger world of World War I, declassifying six of the oldest secret documents in the U.S. government archives, the agency announced Tuesday. The documents show top techniques used by spies, generals and diplomats to send secret messages in a diplomatic war that raged long after the guns stopped. The records reveal how invisible ink was used to send word between allies, and spies learned to open letters to read each others' secrets without leaving a trace. There's even a document written in French of the German's secret ink formula, showing the French had cracked the enemy's code. View this resource to examine some of the actual documents. *CIA Declassifies Oldest Documents in U.S. Government Collection* (4/19/11) https://www.cia.gov/news-information/press-releases-statements/press-release-2011/cia-declassifies-oldest-documents-in-u.s.-government-collection.html

LESSON PLANS ABOUT CIVIC ENGAGEMENT/CIVIL RIGHTS

THE CENTER FOR CIVIC EDUCATION
http://new.civiced.org/resources/curriculum
Every year, more than 4.5 million students around the world participate in the Center's education for democracy programs. Through its curriculum, the Center engages young people to become informed, responsible citizens. The Center's curricula include We the People: The Citizen and the Constitution; Project Citizen; the School Violence Prevention Demonstration Program; Representative Democracy in America; Citizens, Not Spectators; and Foundations of Democracy.

> The Center for Civic Education is a nonprofit, nonpartisan educational corporation dedicated to fostering the development of informed, responsible participation in civic life by citizens committed to the values and principles fundamental to American constitutional democracy. The Center offers a wide range of curricular materials, teacher trainings, community-based programs, and other free resources including the National Standards for Civics & Government.

WHAT ARE THE POSSIBLE CONSEQUENCES OF PRIVACY?
http://www.civiced.org/index.php?page=fod_ms_privo6_sb
This lesson examines some of the possible consequences of privacy. You will classify these consequences as benefits or costs. Later, you will be asked to evaluate positions on issues of privacy by thinking about the consequences of privacy. When you have completed this lesson you should be able to explain some common benefits and costs of privacy. Grades: 6-8

WHAT MIGHT BE SOME OF THE BENEFITS AND COSTS OF THE GOVERNMENT KEEPING A SECRET?
http://www.civiced.org/pdfs/yfj/YFJHighLesson.pdf
This lesson provides an opportunity to examine the benefits and costs of allowing the federal government to keep secrets. Specifically, the lesson concerns a report on the Vietnam War which was "leaked" without authorization to reporters for the *New York Times* and the

Washington Post. The lesson asks you to role-play a Supreme Court hearing in which the government seeks to prevent the newspapers from publishing the report.

A RESOURCE GUIDE FOR TEACHING THE BILL OF RIGHTS (ACLU OF MARYLAND)
http://www.aclu-md.org/aYourRights/MD_Guide.pdf
This Resource Guide is designed to assist teachers in introducing Bill of Rights' issues to students. Topics include the First Amendment issues of freedom of expression, speech, and religious freedom, as well as the Fourth Amendment issue of searches.
See also: http://www.aclu.org/

BILL OF RIGHTS INSTITUTE
http://www.billofrightsinstitute.org/teach/freeresources/lessons/
The Bill of Rights Institute delivers free materials to more than 2,000 teachers and 170,000 students in all 50 states every year. Supported by original intent, right-leaning individuals/ organizations such as the CATO Institute and Heritage Foundation.
Includes free resources, including lesson plans, weekly emailed lesson, teacher- and student-friendly summaries of Supreme Court decisions, and all sorts of other great information related to Constitutional issues (focusing especially on those dealing with the Bill of Rights).

PRO-CON.ORG: USA PATRIOT ACT
http://aclu.procon.org/view.questions.php?issueID=000082&subissueID=000253
These teacher/student friendly resources include arguments in favor and against the Patriot Act.
Full Text of the USA PATRIOT Act (PDF)
Should the USA PATRIOT Act have been made law?
 Does the USA PATRIOT Act diminish civil liberties?
 Does the PATRIOT Act allow the government to conduct secret searches and access records of individuals held by third parties, without providing sufficient judicial overview?
 Does the PATRIOT Act provide the government with overreaching power to conduct searches, surveillances and wiretaps?
 Does the PATRIOT Act unfairly target minority and immigrant communities?

PRO-CON.ORG: DO NATIONAL SECURITY LETTERS GIVE EXCESSIVE SURVEILLANCE POWER TO THE GOVERNMENT?
http://aclu.procon.org/view.answers.php?questionID=000722
(This resource is not related to the CIA but does concern law enforcement activity of the FBI. Teachers may find this resource useful in the broader discussion of this section).
Yes: The American Civil Liberties Union (ACLU) stated in a July 2003 report titled "Unpatriotic Acts" that:
"National Security Letters (NSLs) allow the FBI to obtain certain kinds of sensitive personal records without obtaining any kind of court order... The absence of judicial oversight means that, when it comes to the use of NSLs, the FBI has a free hand.
No: The Justice Department cannot secure our nation against terrorist attack unless investigators are equipped with tools that allow them to disrupt plots before they can be

carried out. These same tools must protect civil liberties. National Security Letters (NSLs) satisfy both requirements.

TRANSPARENCY AND ACCOUNTABILITY IN LEGISLATIVE AND GOVERNMENTAL INSTITUTIONS
http://www.wmd.org/resources/whats-being-done/transparency-accountability/transparency-and-accountability-legislative-a
These resources are not related to democracy in the United States but elsewhere around the world. Nonetheless, students can learn about the importance of transparency and accountability by examining case studies in emerging democracies around the world.

NATIONAL CONSTITUTION CENTER
http://www.constitutioncenter.org/ncc_edu_Lesson_Plans.aspx
The National Constitution Center offers a variety of methods and materials to aid teachers in their mission to inspire active citizenship in their students. The Center offers lessons for every grade level and each is aligned with national standards. Browse our selection to discover how you can engage your students and enhance classroom instruction. Be sure to check back for new additions and the Featured Lesson Plan of the Month.
http://www.constitutioncenter.org/ncc_edu_Students.aspx
This link provides activities and opportunities for students to learn about the Constitution.
http://www.constitutioncenter.org/ncc_edu_Educators.aspx
This link is to the central location of the website for teachers. Resources include information about professional development, online activities, and more.

SECRECY
http://www.choices.edu/resources/film_guides.php
The Choices Program has developed the Teacher's Guide for *Secrecy*, a documentary by Peter Galison and Robb Moss. The film explores the tensions between our safety as a nation and our ability to function as a democracy.
http://www.secrecyfilm.org/resources/Secrecy_Guide.pdf
http://www.secrecyfilm.com/

TORTURING DEMOCRACY
http://www.choices.edu/resources/film_guides.php
The Choices Program has developed a study guide for the film *Torturing Democracy*. This film, tells the inside story of how the U.S. government adopted the Survival, Evasion, Resistance and Escape (SERE) program techniques as official policy in the aftermath of 9/11.
http://www.choices.edu/resources/twtn_torturingdemocracy.php
http://www.torturingdemocracy.org/

World Affairs Council Resource Packet *What Students Need to Know: How National Security & the Internet are Connected*—April 28, 2011

30

GLOBAL SANDBOX: DEMOCRACY IN ACTION

Eileen Hynes http://globalsandbox.blogspot.com/

In March, just when we were getting to work on the resource packet for General Hayden's Global Classroom visit at the World Affairs Council, I had the opportunity to spend a couple of days at University Child Development School (UCDS) in Seattle's University District. If I hadn't been working on developing teacher resources I may not have noticed what a great job UCDS was doing to promote the important skills required for a healthy and vibrant democracy within the daily curriculum of a strong elementary school program.

The UCDS Program description includes this statement about responsibility:

> Civic responsibility is central to the ethos of our school. Each child is responsible for sharing his/her knowledge and talent in a way that enriches the rest of the community. We teach children to listen carefully to others, to help one another, to share what they have learned, to coach one another, to participate in group discussions, and to develop areas of expertise where a child can assume leadership. We believe that developing tolerance for different points of view and empathy for the needs of others is essential to the moral development of a child. In our school, curriculum is organized around big ideas, interesting problems, interests of the students, and issues in the community. Learning is connected to the real world and children are able to build on what they already know.

During the two days I spent at UCDS I saw this philosophy in action in the 2/3 classroom. Throughout the day the students worked in small groups, while the teacher moved throughout the room asking clarifying questions and extending the students thinking. The class was in the middle of a project creating a toy store from conception to production, including developing a mission, branding and advertising. They had visited toy stores, met with graphic designers, and consulted with a toy inventor. All of the students I observed were actively engaged in the work of creating a successful toy store and they were doing so through a process of group consensus.

These seven-, eight-, and nine-year-olds are asked to collaborate and contribute to the class projects on a daily basis. When I got there they had already decided on the mission of their toy store and had spent a week or so developing ideas for toys in small groups. I observed the voting process as they made the decision of which toys to develop. Every group had a chance to share their toy ideas. Then the class voted on which ones they thought were worth developing. Students had put a lot of work into their toy ideas. They then had a few minutes to share their ideas with the group. Voting followed. Three toy ideas made the cuts. Were they the best ideas? Did they represent the most articulate students? Did they vote based on popularity? I didn't know the students well enough after just two days to know what drove their votes. What I did observe were young students who had invested a lot of thought and energy in their ideas and only a few faces showed some disappointment when their ideas were not chosen. Everyone seemed to accept the votes and within moments they had organized themselves into new groups, this time to work on different types of advertising for the selected toys. Billboards, print ads, and commercials would be developed over the next week and I imagine the ads would also be shared and voted on, with only a few making the cut.

Meanwhile, these students are all practicing on a daily basis the skills they need to be active and responsible citizens in a democracy. They understand it is important to be engaged, to share their ideas, and to contribute to the group. When the vote comes, their choice may or may not be the winning vote but either way they will continue to participate and trust that each member of the community is voting based on the best information they have available at the time. For a democracy to work all participants must trust the process. When the vote does not go your way you still participate, you work, you give and then you vote again. Most importantly, you cooperate and contribute to the greater good. These students at UCDS are experiencing a functioning democracy on a daily basis. Watching them at work makes me hopeful for our future.

Send comments to: http://globalsandbox.blogspot.com/

BOOKS

LEGACY OF ASHES: THE HISTORY OF THE CIA, TIM WEINER (2008)
http://www.amazon.com/Legacy-Ashes-History-Tim-Weiner/dp/0307389006/ref=sr_1_1?s=books&ie=UTF8&qid=1301418500&sr=1-1
Is the Central Intelligence Agency a bulwark of freedom against dangerous foes, or a malevolent conspiracy to spread American imperialism? A little of both, according to this absorbing study, but, the author concludes, it is mainly a reservoir of incompetence and delusions that serves no one's interests well. Pulitzer Prize–winning *New York Times* correspondent Weiner musters extensive archival research and interviews with top-ranking insiders, including former CIA chiefs Richard Helms and Stansfield Turner, to present the agency's saga as an exercise in trying to change the world without bothering to understand it.

BLANK CHECK: THE PENTAGON'S BLACK BUDGET, **TIM WEINER (1990)**
http://www.amazon.com/Blank-Check-Pentagons-Black-Budget/dp/0446514527
In this book based on his Pulitzer Prize-winning series of articles for the *Philadelphia Inquirer*, journalist Weiner probes the way the Pentagon has used secret budgets to fund huge military programs.

OPEN GOVERNMENT: COLLABORATION, TRANSPARENCY, AND PARTICIPATION IN PRACTICE, **DANIEL LATHROP, LAUREL RUMA (2011)**
http://www.amazon.com/Open-Government-Collaboration-Transparency-Participation/dp/0596804350/ref=sr_1_1?ie=UTF8&qid=1303237030&sr=8-1
In a world where web services can make real-time data accessible to anyone, how can the government leverage this openness to improve its operations and increase citizen participation and awareness? Through a collection of essays and case studies, leading visionaries and practitioners both inside and outside of government share their ideas on how to achieve and direct this emerging world of online collaboration, transparency, and participation.

THE CIA AND AMERICAN DEMOCRACY, **RHODRI JEFFREYS-JONES (2003)**
http://yalepress.yale.edu/yupbooks/reviews.asp?isbn=9780300099485
"I have read many books on the CIA, but none more searching and still dispassionate. Nor would I have believed that a book of such towering scholarship could still be so lucid and exciting to read."—Daniel Schorr, Senior News Analyst, National Public Radio.

OVERTHROW: AMERICA'S CENTURY OF REGIME CHANGE FROM HAWAII TO IRAQ, **STEPHEN KINZER (2007)**
Kinzer shows that long before Iraq, regime change has always been a policy of the United States government. In many of those cases, covert activity by the CIA and its predecessors played major roles.
http://www.amazon.com/Overthrow-Americas-Century-Regime-Change/dp/0805082409/ref=sr_1_4?ie=UTF8&qid=1301420260&sr=8-4

BITTER FRUIT: THE STORY OF THE AMERICAN COUP IN GUATEMALA, **STEPHEN SCHLESINGER AND STEPHEN KINZER (1982, EXPANDED 2005)**
http://www.amazon.com/Bitter-Fruit-American-Guatemala-Rockefeller/dp/067401930X/ref=sr_1_10?ie=UTF8&qid=1301420260&sr=8-10
A comprehensive and insightful account of the CIA operation to overthrow the democratically elected government of Jacobo Arbenz of Guatemala in 1954. The authors make extensive use of U.S. government documents and interviews with former CIA and other officials. It is a warning of what happens when the United States abuses its power.

ALL THE SHAH'S MEN: AN AMERICAN COUP & THE ROOTS OF MIDDLE EAST TERROR, **STEPHEN KINZER (2003)**
http://www.amazon.com/All-Shahs-Men-American-Middle/dp/047018549X/ref=sr_1_1?s=books&ie=UTF8&qid=1302644300&sr=1-1
With breezy storytelling and diligent research, Kinzer has reconstructed the CIA's 1953 overthrow of the elected leader of Iran, Mohammad Mossadegh. The coup ushered in the long and brutal dictatorship of Mohammad Reza Shah, widely seen as a U.S. puppet and himself overthrown by the Islamic revolution of 1979

World Affairs Council Resource Packet *What Students Need to Know: How National Security & the Internet are Connected*—April 28, 2011

33

***THE CIA AND CONGRESS*, DAVID BARRETT (2005)**
https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol50no1/8_BK_CIA_Congress.htm
Not often does a book come along that alters our understanding of history, but David M. Barrett's *The CIA and Congress: The Untold Story from Truman to Kennedy* does just that. The period covered by the book—from the creation of the CIA in 1947 until the Bay of Pigs in 1960—has heretofore been thought of as the "dark ages" of congressional oversight, when control rested with a few powerful committee chairmen, who did little monitoring of the CIA themselves, but held other committees at bay and fended off all efforts at reform. Barrett shows the relationship between the Agency and Congress, from the very start, to have been considerably more complicated.

BOOKS ABOUT CYBER SECURITY

***CYBER SECURITY*, EDWARD AMOROSO (2006)**
http://www.amazon.com/Cyber-Security-Edward-Amoroso/dp/0929306384
Edward Amoroso has overseen Cyber Security for one of the largest telecommunications companies in the world AT&T. In his role as Chief Security Officer, hes helped to discover and counter virtually every conceivable type of malicious threat that has been targeted at computers and networks around the world.

***THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM*, EVGENY MOROZOV (2011)**
http://www.amazon.com/Net-Delusion-Dark-Internet-Freedom/dp/1586488740
In this spirited book, journalist and social commentator Evgeny Morozov shows that by falling for the supposedly democratizing nature of the Internet, Western do-gooders may have missed how it also entrenches dictators, threatens dissidents, and makes it harder—not easier—to promote democracy. Buzzwords like "21st-century statecraft" sound good in PowerPoint presentations, but the reality is that "digital diplomacy" requires just as much oversight and consideration as any other kind of diplomacy.

***CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT*, RICHARD CLARK AND ROBERT KNAKE (2010)**
http://www.amazon.com/Cyber-War-Threat-National-Security/dp/0061962236/ref=sr_1_1?s=books&ie=UTF8&qid=1303161260&sr=1-1
International security experts—Clarke from the nuclear generation and Knake from the cyber generation—ponder the irony that although the U.S. pioneered the technology behind cyber warfare, outdated thinking, policies, and strategies make us vulnerable to losing any cyber contest with a hostile nation.

***INSIDE CYBER WARFARE: MAPPING THE CYBER UNDERWORLD*, JEFFREY CARR (2009)**
http://www.amazon.com/Inside-Cyber-Warfare-Mapping-Underworld/dp/0596802153/ref=sr_1_2?s=books&ie=UTF8&qid=1303162275&sr=1-2
This book provides fascinating and disturbing details on how nations, groups, and individuals throughout the world are using the Internet as an attack platform to gain military, political, and economic advantages over their adversaries. You'll learn how sophisticated hackers working on behalf of states or organized crime patiently play a high-stakes game that could target anyone, regardless of affiliation or nationality.

World Affairs Council Resource Packet *What Students Need to Know: How National Security & the Internet are Connected*—April 28, 2011

34

BOOKS ABOUT THE CIA AND INTELLIGENCE GATHERING

The CIA provides pamphlets for students. They can be viewed online or ordered in hard copy for free. Below are a couple examples:
K-5 publications https://www.cia.gov/kids-page/k-5th-grade/index.html
6-12 publications: https://www.cia.gov/kids-page/6-12th-grade/index.html

DEVOTION TO DUTY
https://www.cia.gov/library/publications/additional-publications/devotion-to-duty/index.html
This is the story of how the men and women of CIA responded to the attacks of September 11th. To the extent it can be told in an unclassified account, it offers a sense of the teamwork, creativity, and commitment displayed by Agency officers in the days and weeks after the tragedy. Love of country and dedication to mission sustained them in their vital work. Gr. k-5

THE WORK OF A NATION
https://www.cia.gov/kids-page/6-12th-grade/index.html
This publication offers an overview of CIA and its pivotal role in the Intelligence Community. I hope it gives readers a better understanding of the Agency's work, its unique and powerful capabilities, and, especially, its diverse and talented workforce. In their values, courage, and dedication, the people of the CIA truly represent the best of our nation.

BOOKS ABOUT AMERICAN DEMOCRACY, CIVIL RIGHTS, LAW, ETC.

FIREBOAT: THE HEROIC ADVENTURES OF THE JOHN J. HARVEY, **MARIA KALMAN (2004)**
http://www.amazon.com/Fireboat-Heroic-Adventures-Harvey-Picture/dp/0142403628/ref=sr_1_1?s=books&ie=UTF8&qid=1301349882&sr=1-1
In relating the heroic role of the John J. Harvey on September 11, intelligently conveys those unfathomable events in a way that a picture book audience can comprehend.

AND THE PURSUIT OF HAPPINESS, **MAIRA KALMAN (2010)**
http://www.amazon.com/Pursuit-Happiness-Maira-Kalman/dp/1594202672/ref=pd_sim_b_6
And the Pursuit of Happiness is beloved artist and author Maira Kalman's yearlong investigation of democracy and how it works.

> At a time when everyone around me seems to hate how the United States has become the Not "it" country. I found the book that restores my love for it. Being a student that wants to change this country for the better, this book shows me what it was before this mess came around. This book has humor, art history all mixed with a feeling of warmness.

D IS FOR DEMOCRACY: A CITIZEN'S ALPHABET, **ELISSA GRODIN (2007)**
http://www.amazon.com/Democracy-Citizens-Alphabet-Books/dp/1585363286/ref=sr_1_1?ie=UTF8&qid=1301350665&sr=1-1-spell
The organizing device for this book on the U.S and its government is the alphabet, with each letter introducing a person, place, thing, or concept. From "Amendment" and "Bill of Rights" to "You and me"...

BOOKS FOR YOUNG READERS

WE THE KIDS: THE PREAMBLE TO THE CONSTITUTION OF THE UNITED STATES, DAVID CATROW (2005)
http://www.amazon.com/We-Kids-Preamble-Constitution-United/dp/0142402761/ref=pd_sim_b_3

THE U.S. CONSTITUTION AND YOU, **SYL SOBEL (2001)**
http://www.amazon.com/U-S-Constitution-You-Syl-Sobel/dp/0764117076/ref=pd_sim_b_1
All elementary school students learn about the history of the U.S. Constitution when they first begin social studies. This book is different. It tells boys and girls about the great American document itself--explaining exactly what the Constitution does, as well as how it affects and protects people today.

THE BILL OF RIGHTS: PROTECTING OUR FREEDOM THEN AND NOW, **SYL SOBEL (2008)**
http://www.amazon.com/Bill-Rights-Protecting-Freedom-Then/dp/0764140213/ref=pd_sim_b_3

THE SUPREME COURT ,**CHRISTINE TAYLOR-BUTLER (2008)**
http://www.amazon.com/Supreme-Court-True-Books/dp/053114786X/ref=pd_sim_b_17

KNOWING YOUR CIVIL RIGHTS, **CHRISTIN DITCHFIELD (2004)**
http://www.amazon.com/Knowing-Your-Civil-Rights-Books/dp/0516279106/ref=pd_sim_b_24
The history of civil rights in America has come a long way since men but not women, free men but not slaves, were granted certain rights by our Constitution. Walk in the footsteps of our nation's founding fathers. Learn about the civil rights all Americans share and the responsibilities that go along with them.

THE VOICE OF THE PEOPLE: AMERICAN DEMOCRACY IN ACTION, **BETSY MAESTRO (1998)**
http://www.amazon.com/Voice-People-American-Democracy-Action/dp/068816157X/ref=sr_1_2?s=books&ie=UTF8&qid=1301351871&sr=1-2
With election time drawing near, curious readers can turn to this handy primer for a better understanding of the electoral process, and of the origins and workings of American democracy.

HOW THE U.S. GOVERNMENT WORKS, **SYL SOBEL (1999)**
http://www.amazon.com/How-U-S-Government-Works-Sobel/dp/0764111116/ref=pd_rhf_shvl_1

A KIDS' GUIDE TO AMERICA'S BILL OF RIGHTS: CURFEWS, CENSORSHIP, AND THE 100-POUND GIANT, **KATHLEEN KRULL (1999)**
http://www.amazon.com/Kids-Guide-Americas-Bill-Rights/dp/0380974975/ref=pd_sim_b_40

> - *Why did early American founders (like James Madison, Congressman from Virginia) argue that individuals needed a Bill of Rights to protect them from government?*
> - *Why is freedom of speech so thrilling and so controversial?*
> - *What is religious intolerance, and when can it be fatal?*
> - *What does it really mean to take the Fifth?*
> - *And how does the Bill of Rights affect the rights of kids?*

MICHAEL HAYDEN ON INTERNATIONAL CHALLENGES OF CYBER-SECURITY (2009)
http://c-span.org/Events/Fmr-CIA-Dir-Michael-Hayden-on-International-Challenges-of-Cyber-Security/16003-1/
General Michael Hayden and others spoke about cyber-security threats to the nation's computer and telecommunications infrastructure. Among the topics addressed were advances in military technology, developing strategies for cyber-warfare, and constructing future protections from potential hackers. They also answered questions from the audience.

HACKERS FORCE INTERNET USERS TO LEARN SELF-DEFENSE (8/11/10)
http://www.pbs.org/newshour/bb/science/july-dec10/cyber_08-11.html
Correspondent Spencer Michels continues his series on cybersecurity with a conversation with former CIA and National Security Agency Director Michael Hayden who says the openness of the Internet's design puts hackers at an advantage over people who want to defend their data. (Audio clip also available)

A CONVERSATION WITH MICHAEL HAYDEN (9/7/07)
http://www.cfr.org/publication/14173/conversation_with_michael_v_hayden_video.html
Gen. Hayden discusses terrorism, national security, the CIA, transparency/free press/democracy, and other topics. This is the corresponding video for a transcript provided earlier in this packet.

WHAT IS WATER BOARDING?
http://science.howstuffworks.com/water-boarding.htm
Water boarding has been around for centuries. It was a common interrogation technique during the Italian Inquisition of the 1500s and was used perhaps most famously in Cambodian prisons during the reign of the Khmer Rouge regime during the 1970s. As late as November 2005, water boarding was on the CIA's list of approved "enhanced interrogation techniques" intended for use against high-value terror suspects.

SECRECY
http://www.choices.edu/resources/film_guides.php
The Choices Program has developed the Teacher's Guide for *Secrecy*, a documentary by Peter Galison and Robb Moss. The film explores the tensions between our safety as a nation and our ability to function as a democracy.
http://www.secrecyfilm.org/resources/Secrecy_Guide.pdf
http://www.secrecyfilm.com/

TORTURING DEMOCRACY
http://www.choices.edu/resources/film_guides.php
The Choices Program has developed a study guide for the film *Torturing Democracy*. This film, tells the inside story of how the U.S. government adopted the Survival, Evasion, Resistance and Escape (SERE) program techniques as official policy in the aftermath of 9/11.
http://www.choices.edu/resources/twtn_torturingdemocracy.php
http://www.torturingdemocracy.org/

World Affairs Council Resource Packet *What Students Need to Know: How National Security & the Internet are Connected*—April 28, 2011

37

WANT TO WORK FOR THE CIA? (AND OTHER LOCAL ORGANIZATIONS AND OPPORTUNITIES)

IS THE CIA THE RIGHT CAREER FOR YOU?
https://www.cia.gov/careers/student-opportunities/is-the-cia-the-right-career-for-you/high-school.html
Ever wonder if you have what it takes to work for the CIA? Truth is, we hire all kinds of people from different backgrounds and with varying skill sets and levels of education. However, there are a few common traits in those people we find best suited for our mission of protecting America. Take this brief quiz and see how you match up to just a few of the many qualifications we look for in new hires. And don't worry, there are really no wrong answers. In fact, this is just a fun, informative exercise, not a true career measurement tool.

CIA: KIDS' PAGE
https://www.cia.gov/kids-page/index.html
This resource was provided earlier, but encourage students to visit and explore the site if they are interested in learning more about the CIA.

STUDENT OPPORTUNITIES: CIA
https://www.cia.gov/careers/student-opportunities/index.html
(These student opportunities might be useful for graduating high school students)
Contribute to the work of the nation before you graduate. Apply to participate in one of the outstanding student work programs at the CIA, including undergraduate student internships or undergraduate co-ops, and graduate studies programs.
This is an opportunity to learn from highly skilled professionals who support US officials that make our country's foreign policy. You'll assist with substantive and meaningful work assignments, while earning a competitive income and gaining invaluable practical experience. There's no better place to learn than at the center of intelligence.

CAREER OPPORTUNITIES: CIA
https://www.cia.gov/careers/opportunities/index.html
The CIA is the premier agency responsible for providing global intelligence on the ever-changing political, social, economic, technological and military environment. Here, your paramount goal and mission will be to protect the national security of the United States. Virtually any job you can imagine is available at the CIA — plus, some you can't even imagine.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
http://www.dni.gov/
The ODNI is headed by the Director of National Intelligence, or DNI, who is appointed by the President with the advice and consent of the Senate. The Director of National Intelligence (DNI) serves as the head of the Intelligence Community (IC), overseeing and directing the implementation of the National Intelligence Program (budget) and acting as the principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to the national security. Working together with the Principal Deputy DNI (PDDNI), the Office of the DNI's goal is to effectively integrate foreign, military and domestic intelligence in defense of the homeland and of United States interests abroad.

WANT TO WORK FOR THE CIA? (AND OTHER LOCAL ORGANIZATIONS AND OPPORTUNITIES)

SOME LOCAL ENTITIES INVOLVED IN CYBER SECURITY

WATCHGUARD TECHNOLOGIES
http://www.watchguard.com/
Located in Seattle and employing more than 400 people, WatchGuard builds affordable, all-in-one network and content security solutions to provide defense in depth for corporate content, networks and the businesses they power. WatchGuard's award-winning extensible threat management (XTM) network security solutions combine firewall, VPN and security services to protect networks from spam, viruses, malware and intrusions.

F5
http://www.f5.com/
Headquartered in Seattle.
 Managing the delivery of applications across your entire IT infrastructure is a complex challenge. F5 tackles this challenge at its core, right where your network, storage, servers, and security come together, giving you strategic points of control throughout your IT infrastructure.

IOACTIV
http://www.ioactive.com/
North American headquarters is located in Seattle. IOActive is committed to helping our clients produce high quality software by adopting a holistic programming approach that keeps you secure while maximizing your competitive advantage. As one of three firms chosen by Microsoft to perform a source code security review on the Vista operating system, and a partner in the Microsoft SDL Pro Network, IOActive is a recognized leader in application security.

PACIFIC NORTHWEST NATIONAL LABORATORY (PNNL)
http://www.pnl.gov/about/
Located in Richland, in Eastern Washington, PNNL is one of the U.S. Department of Energy's (DOE's) ten national laboratories, managed by DOE's Office of Science. PNNL also performs research for other DOE offices as well as government agencies, universities, and industry to deliver breakthrough science and technology to meet today's key national needs. Our Laboratory
- provides the facilities, unique scientific equipment, and world-renowned scientists/engineers to strengthen U.S. scientific foundations for fundamental research and innovation
- prevents and counters acts of terrorism through applied research in information analysis, cyber security, and the non-proliferation of weapons of mass destruction
- increases U.S. energy capacity and reduces dependence on imported oil through research of hydrogen and biomass-based fuels

INSTITUTE FOR NATIONAL SECURITY EDUCATION AND RESEARCH (INSER) AT THE UNIVERSITY OF WASHINGTON
http://inser.ischool.uw.edu/

World Affairs Council Resource Packet *What Students Need to Know: How National Security & the Internet are Connected*—April 28, 2011

39

WANT TO WORK FOR THE CIA? (AND OTHER LOCAL ORGANIZATIONS AND OPPORTUNITIES)

(INSER) provides a forum for independent research and cutting-edge scholarship in areas with broad relevance to public safety and national security issues, including distributed collaboration in virtual organizations and knowledge management and decision-making.

WOMEN IN INTERNATIONAL SECURITY (WIIS) (LOCAL CHAPTER AT WESTERN WASHINGTON UNIVERSITY)
http://wiis.georgetown.edu/about/
Women In International Security (WIIS) is the only global network actively advancing women's leadership, at all stages of their careers, in the international peace and security field.
Seattle, WA Contact: Ms. Bidisha Biswas, Associate Professor, Department of Political Science at Western Washington University; E-Mail: Bidisha.Biswas@wwu.edu

CIVIC ENGAGEMENT RESOURCES FOR STUDENTS

GLOBAL YOUTH LEADERSHIP INSTITUTE
http://www.world-affairs.org/global-youth-leadership-institute
The Global Youth Leadership Institute (GYLI) is a five-day intensive summer program designed to encourage and assist high school students in learning about current global issues. Over the course of the program, students have the opportunity to hear from expert speakers, learn about career opportunities, explore an online international learning community, and develop leadership skills. Students also develop global awareness projects to educate their peers about world affairs over the forthcoming academic year. More info: Contact Laura Adriance here, at the World Affairs Council: ladriance@world-affairs.org

VOTE411
http://vote411.org/
Find where to register to vote, how to vote, about races in your areas, and about the issues and candidates from this nonpartisan source.

ASSOCIATION OF COLLEGE UNIONS INTERNATIONAL
http://acui.org/
Research opportunities for how you can impact local policies and development in your community. A list of national civic engagement organizations can be found here.

NATIONAL CENTER FOR THE PRESERVATION OF DEMOCRACY
http://www.ncdemocracy.org/
The National Center for the Preservation of Democracy is a non-profit, non-partisan educational institution that provides tools for living democratically in a diverse American society. Partnering with educators and community-based mentors, the National Center works to inspire youth to become active, informed participants in shaping democracy in America.

World Affairs Council Resource Packet *What Students Need to Know: How National Security & the Internet are Connected*—April 28, 2011

40

WANT TO WORK FOR THE CIA? (AND OTHER LOCAL ORGANIZATIONS AND OPPORTUNITIES)

KIDS VOTING USA
http://www.kidsvotingusa.org
A national leader in civic education, Kids Voting USA (KVUSA) gets students involved and ready to be educated, engaged citizens. Students learn about democracy through a combination of classroom activities, family dialogue and an authentic voting experience.
Our high-quality instructional materials provide K-12 teachers with valuable civic learning tools to be used throughout the year, every year. In addition to classroom activities about voting and elections, students also explore the right to vote and active citizenship.

NATIONAL ISSUES FORUMS
http://nifi.org/
Organize an issues forum to discuss contemporary social or policies with others in your community. Learn more about how to organize a forum at the website.

ICIVICS
 http://www.icivics.org/
iCivics is a web-based education project designed to teach students civics and inspire them to be active participants in our democracy. iCivics is the vision of Justice Sandra Day O'Connor, who is concerned that students are not getting the information and tools they need for civic participation, and that civics teachers need better materials and support. The website includes games, lessons, resources, and more.

NATIONAL SECURITY LANGUAGE INITIATIVE FOR YOUTH
http://exchanges.state.gov/youth/programs/nsli.html
The State Department's National Security Language Initiative for Youth (NSLI-Y) provides merit-based scholarships to U.S. high school students and recent graduates interested in learning less-commonly studied foreign languages. All applicants must be: A U.S. citizen who is currently enrolled in or just graduated from high school; 15-to-18.5 years old at the start of the program; have a minimum GPA of 2.5 There are seven languages: Arabic, Chinese (Mandarin), Hindi, Korean, Persian, Russian and Turkish.

World Affairs Council Resource Packet *What Students Need to Know: How National Security & the Internet are Connected*—April 28, 2011

41