Introduction
It took 20 years for the first three billion users to come online. It will not take 20 more years for the next three billion to join them. As the global population arrives at near complete access to the Internet, there are emerging opportunities to use the Internet to attack the human rights of the world’s most vulnerable. Furthermore, as people become more educated about human rights they will go from just being online consumers to online citizens who demand more from government. Any number of existing or emerging crises will eventually confront the global community related to the intersection of cyber threats and human rights. We cannot be sure how or when a cyber human rights crisis will come to an inflection point, but we can propose three areas of inquiry in this critical arena. Below outlines the areas of inquiry that could be expanded upon in the creation of a deeper analysis of cyber security and human rights concerns globally.

- Cyber Security Technology
  - Cyber policy is not divorced from cyber technology. Thus, protecting human rights online has both policy and technical components.
  - Cyber hygiene can be promoted across the world to help stop nefarious individuals and governments from using the Internet to abuse humans’ civil rights.
  - CCS will help the UN to promote the 20 Critical Security Controls, which have been validated by cyber experts around the world.
    - The Critical Controls are best practices that can be taken to defend against the most pervasive attacks. More information can be found here: [http://www.counciloncybersecurity.org/critical-controls/](http://www.counciloncybersecurity.org/critical-controls/)

- Protecting Citizens From Governments Online
  - As billions more come online and learn what they can expect from their governments, they will invariably demand more from those governments, which will trigger some governments to shut down their citizens right to communicate, protest, speak freely and affect change in their communities.
  - United Nations should seek to protect minority groups via the Internet by working to prevent intimidation and prosecution of the most vulnerable in our society.
    - In December 2012, U.S. Ambassador to Syria, Robert Ford claimed "The Syrian government has been monitoring (the Internet) for years. They have been using the Internet with Iranian assistance to track opposition activists, arrest and kill them.”

- Combating Cyber Criminal Predators
  - As the next three billion people come online, many individuals who do not have as much economic opportunity in the physical world will be tempted to revert to illegal commerce in the virtual world. The Internet is already used to kidnap, sexually abuse, traffic and exploit millions of individuals across the globe. We can only assume that activity will increase as more people come online.
    - Child pornography is one of the fastest growing businesses online, and the content is becoming much worse. In 2008, Internet Watch Foundation found 1,536 individual child abuse domains.
Course Description:
This course is designed to offer students an overview of the current cybersecurity landscape and the corresponding human rights implications. Students will hear first-hand insider perspectives from public and private sector cyber professionals and international experts across the cybersecurity and human rights fields. Divided into 3 parts, students will gain insight on Cyber Security Technology, Protecting Citizens From Governments Online, and Combating Cyber Predators.

Class Structure:
Each class will begin with a 20 – 30 minute presentation from expert guest speakers (Short bios for each speakers included in the ‘Resources’ section of the syllabus) followed by Q & A and class discussion. Additionally, students are expected to come to class prepared to discuss the week’s assigned readings.

Projects/Exams
- Response and Analysis Papers (3)
The class is divided into 3 parts (Cyber Security Technology, Protecting Citizens From Governments Online, and Combating Cyber Criminal Predators). Each student will submit a memo brief that provides a summary and analysis of the information gleaned from the speakers and assigned readings from each of the 3 sections. These papers will be submitted (hard copy) during the last week of each section.

- Final Project
The final project will be a comprehensive report drawing from knowledge gained from the prior 3 work sections. During the final class we will present the findings to a representative at the United Nations. Additionally, we will share the report with the Office of the United Nations High Commissioner for Human Rights (OHCHR), the Office of the Under Secretary for Civilian Security, Democracy, and Human Rights at the US State Department, and the Council on Cybersecurity.

Schedule

Part I: Cyber Security Technology

Week 1 (Sept. 28th, 2015) - Course Introduction and Overview
- Review syllabus
- Defining “cybersecurity” from the technical and policy perspective
- Introduction to the 20 Critical Controls

Reading:
- Read 1-10 of the 20 Critical Security Controls
  https://www.sans.org/critical-security-controls/controls
- The New Digital Age – Chapter 1, “Our Future Selves”

Week 2 (Oct. 5th, 2015) - “The Fog of More”: Deciphering the 20 Critical Controls
Speaker: Tony Sager, Senior Vice President & Chief Evangelist, Center for Internet Security. Former Chief Operating Officer of the National Security Agency Information Assurance Directorate

Reading:
- Read 10 – 20 of the 20 Critical Security Controls
  https://www.sans.org/critical-security-controls/controls
- The New Digital Age – Chapter 2, “The Future of Identity, Citizenship and Reporting”
Assignment:
- **Due Next Week:** Part I policy brief - 20 Critical Security Controls and potential implications for human rights policy. Use any outside materials necessary.

Part II: Protecting Citizens From Governments Online

**Week 3 (Oct. 12th, 2015) - “The Intersection b/w Cybersecurity and Human Rights”**
Speaker: Jane Holl Lute
CEO, Center for Internet Security, former Deputy Secretary, U.S. Department of Homeland Security and former Head of Peacekeeping Operations at the United Nations

**Due TODAY:** Part I policy brief

Reading:
- Watch Secretary Clinton’s speech on Internet Freedom at George Washington University
  [https://www.youtube.com/watch?v=acDcUQoeFxY](https://www.youtube.com/watch?v=acDcUQoeFxY)
- **The Rule of Law on the Internet and in the Wider Digital World**
  Professor Douwe Korff
  Yale University (Information Society Project), and Oxford Martin Associate, Oxford Martin School, University of Oxford, UK.
  December 2014
- The New Digital Age – Chapter 3, “The Future of States”
- (Place holder for speaker’s suggested reading)

Speaker: Mary Ellen Callahan
Chair of Jenner & Block’s Privacy and Information Governance Practice, former Chief Privacy Officer, U.S. Department of Homeland Security

Reading:
- **Public Privacy: Human Rights in Cyberspace**
  Anja Mihr, Associate Professor
  The Netherlands Institute of Human Rights – Utrecht University
  December 2013
  [http://www.anjamihr.com/resources/Public+Privacy-WP-AnjaMihr$5B1S5D.pdf](http://www.anjamihr.com/resources/Public+Privacy-WP-AnjaMihr$5B1S5D.pdf)
- **Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms**
  James Andrew Lewis
  February 2014
- The New Digital Age – Chapter 4, “The Future of Revolution”
- (Place holder for speaker’s suggested reading)
Assignment:

- **Due Next Week:** Part II policy brief

Speaker: Office of Civilian Security, Democracy, and Human Rights, US Department of State (TBD)

**Due TODAY:** Part II policy brief

Reading:

- **Democratic Governance Challenges of Cyber Security**
  Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler
  2015
- The New Digital Age – Chapter 5, “The Future of Terrorism”
- (Place holder for speaker’s suggested reading)

Part III: Combating Cyber Criminal Predators

Week 6 (Nov. 2nd, 2015) – “Law Enforcement and Transnational Threats”
Speaker: Thomas Winkowski
Former Director of Immigration and Customs Enforcement agency (ICE), as well as, the former Commissioner of Customs and Border Protection (CBP) at the Department of Homeland Security
*Only person in to serve as both ICE Director and CBP Commissioner

Reading:

- **Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms**
  James Andrew Lewis
  February 2014
- The New Digital Age – Chapter 6, “The Future of Conflict, Combat and Intervention”
- (Place holder for speaker’s suggested reading)

Week 7 (Nov. 9th, 2015) – “Cyber Crime: How to prevent it without violating human rights”
Speaker: Troels Oerting
Chief Information Security Officer, Barclay’s Bank. Former Director of European Cyber Crimes Center (EC3) and Europol's Counter Terrorism and Financial Intelligence Centre

Reading:

- **UNPACKING “CYBERSECURITY”: THREATS, RESPONSES, AND HUMAN RIGHTS CONSIDERATIONS**
  Center for Democracy and Technology
  June 26, 2013
- The New Digital Age – Chapter 7, “The Future of Reconstruction”
Assignment:
- Due Next Week: Part III policy brief

Week 8 (Nov 16th, 2015)
Speaker: Princess Funke Adedoyin, (To be confirmed)
Member, Nigerian House of Representatives, and former Minister of Youth Development and later Minister of State for Health.

Due TODAY: Part III policy brief

*Begin to discuss final project

Assignment
- Prepare questions regarding final project

Week 9 (Nov 23rd, 2015) – Review Final Project
We will use this class to structure the final report. Each team presents to the group and discuss how to tie it together. Executive committee works to tie each team’s product into one document
Students graded the aspect of the report they as

Week 10 (Nov 30th, 2015) – Final Presentations
The class/executive committee members will present the final report to Human Rights officials

Reading Materials


The Rule of Law on the Internet and in the Wider Digital World
Professor Douwe Korff
Yale University (Information Society Project), and Oxford Martin Associate, Oxford Martin School, University of Oxford, UK.
December 2014

Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms
James Andrew Lewis
February 2014

UNPACKING “CYBERSECURITY”: THREATS, RESPONSES, AND HUMAN RIGHTS CONSIDERATIONS
Center for Democracy and Technology
June 26, 2013

Democratic Governance Challenges of Cyber Security
Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler
2015
http://www.dcaf.ch/Publications/Democratic-Governance-Challenges-of-Cyber-Security

Public Privacy: Human Rights in Cyberspace
Anja Mihr, Associate Professor
The Netherlands Institute of Human Rights – Utrecht University
December 2013
http://www.anjamihr.com/resources/Public+Privacy-WP-AnjaMihr$5B1$5D.pdf

Speaker Bios

Tony Sager, SVP & Chief Evangelist, Center for Internet Security

Tony Sager is the chief technologist at the Center for Internet Security, which recently merged with the Council on Cyber Security to form a single nonprofit organization with the goal of providing national and international leadership in cybersecurity. In this position, he helps identify, validate, scale and share promising cybersecurity practices for widespread adoption. Previously, Sager spent more than 30 years at the National Security Agency (NSA) where he headed the Systems and Network Attack Center, established and led security product evaluation teams, helped guide the agency’s top talent development programs, served as the founding chief of the Vulnerability Analysis and Operations Group and was the chief operating officer for the Information Assurance Directorate. In addition, he led the release of NSA security guidance to the public and greatly expanded the agency’s role in the development of open standards for security. In 2012, Sager was named director of the SANS Institute, a private corporation specializing in computer and network security training and also assumed the lead role for the Consortium for Cybersecurity Action. Sager holds a B.A. in mathematics from Western Maryland College and an M.S. in computer science from The Johns Hopkins University.
Jane Holl Lute, Chief Executive Officer, Center for Internet Security

Jane Holl Lute serves as Chief Executive Officer (CEO) of the Center for Internet Security (CIS), an international nonprofit organization focused on enhancing cyber security readiness and response for the public and private sectors. Ms. Lute most recently served as the President and Chief Executive Officer of the Council on CyberSecurity, an independent, expert organization dedicated to the security of an open Internet. Prior to joining CIS, Ms. Lute served as Deputy Secretary for the Department of Homeland Security (DHS). As the DHS chief operating officer, Ms. Lute was responsible for the day-to-day management of the Department’s efforts to prevent terrorism and enhance security, secure and manage the nation’s borders, administer and enforce U.S. immigration laws, strengthen national resilience in the face of disasters, and ensure the nation’s cybersecurity.

From 2003-2009, Ms. Lute served as Assistant Secretary-General of the United Nations (UN) and established the Department of Field Support, responsible for comprehensive on-the-ground support to UN peace operations worldwide, including rapid-response efforts in support of development and humanitarian operations and crises. Ms. Lute also served as Assistant Secretary-General for Peacebuilding, responsible for coordinating efforts on behalf of the Secretary General to build sustainable peace in countries emerging from violent conflict.

Prior to joining the UN, Ms. Lute was Executive Vice-President and Chief Operating Officer of the United Nations Foundation and the Better World Fund. From 1994-2000, she worked with David A. Hamburg, former president of the Carnegie Corporation of New York, and Cyrus Vance, former U.S. Secretary of State, on the Carnegie Commission on Preventing Deadly Conflict, a global initiative that pioneered the cause of conflict prevention.

Ms. Lute served on the National Security Council staff under both President George H.W. Bush and President William Jefferson Clinton and had a distinguished career in the United States Army, including service in the Gulf during Operation Desert Storm. She has a Ph.D. in political science from Stanford University and a J.D. from Georgetown University.

Mary Ellen Callahan, Partner and Chair, Privacy and Information Governance Practice

Mary Ellen Callahan, Chair of Jenner & Block’s Privacy and Information Governance Practice, has unique and broad experience advising clients at the interface of privacy protection with cybersecurity and national security issues. A nationally recognized privacy attorney with a decade and a half of outside counsel experience, she served as Chief Privacy Officer of the U.S. Department of Homeland Security from 2009 until August 2012. She is a prolific writer and speaker on cutting-edge commercial privacy issues. She provides advice and counsel to an array of clients in industries that include media, public health and health care, manufacturing, online retail, government contracts, energy and other critical sectors.

Mary Ellen Callahan, Chair of Jenner & Block’s Privacy and Information Governance Practice, has unique and broad experience advising clients at the interface of privacy protection with cybersecurity and national security issues. A nationally recognized privacy attorney with a decade and a half of outside counsel experience, she served as Chief Privacy Officer of the U.S. Department of Homeland Security from 2009 until August 2012. She is a prolific writer and speaker on cutting-edge commercial privacy issues. She
provides advice and counsel to an array of clients in industries that include media, public health and health care, manufacturing, online retail, government contracts, energy and other critical infrastructure sectors.

Office of the Under Secretary for Civilian Security, Democracy, and Human Rights

The Office of the Under Secretary for Civilian Security, Democracy, and Human Rights leads State Department efforts to prevent and counter threats to civilian security and effective governance, such as terrorism, violent extremism, mass atrocities and transnational crime. The bureaus and offices reporting to the Under Secretary contribute to the security of the American people and nations around the world by assisting countries to build more democratic, secure, stable, and just societies.

To achieve our mission, we work together, along with other U.S. Government agencies and foreign partners, to prevent and respond to conflict, promote peace and genuine stability, strengthen and develop the rule of law, achieve accountability for atrocities, counter terrorism and violent extremism, build democratic institutions, deepen respect for universal human rights, strengthen civilian protection and security, and advance the United States' humanitarian policies, practices, and programs around the world.

Thomas Winkowski, Former ICE Director and CBP Commissioner

Thomas S. Winkowski was appointed the Principal Deputy Assistant Secretary for U.S. Immigration and Customs Enforcement on March 16, 2014. As ICE's Principal Deputy Assistant Secretary, Mr. Winkowski leads the largest investigative agency within the U.S. Department of Homeland Security. Created in 2003, ICE has a budget of $5.6 billion and has nearly 20,000 employees in offices in all 50 states and 48 foreign countries. In this role, Mr. Winkowski advances ICE's mission to promote homeland security and public safety through the criminal and civil enforcement of approximately 400 federal laws governing border control, customs, trade and immigration. Mr. Winkowski brings deep law enforcement and customs-related experience to the job, having filled various positions of leadership during his nearly 4 decades with U.S. Customs and Border Protection (CBP) and its predecessor agencies, including as Acting Commissioner. Mr. Winkowski has worked side-by-side with ICE personnel while managing CBP’s mission. As the Deputy Commissioner, Mr. Winkowski oversaw the daily operations of CBP's 60,000-employee workforce. Mr. Winkowski also served as Assistant Commissioner in CBP's Office of Field Operations where he managed the largest division within CBP. Prior to his service at CBP headquarters in Washington, D.C., Mr. Winkowski served as the Director of Field Operations in Miami from 2002 to 2007, as well as Port Director in Miami and the Los Angeles International Airport.

Mr. Winkowski joined the U.S. Customs Service in 1975 as a cooperative education student. Upon graduating from Boston's Northeastern University in 1978, he was assigned to Los Angeles where he became a customs inspector.
Mr. Winkowski’s service has been recognized by multiple presidents and administrations, including being awarded the Meritorious Presidential Rank Award by President Bush in 2004 and the Distinguished Executive Presidential Rank Award by President Obama in 2009.

Troels Oerting, Chief Information Security Officer, Barclay’s Bank

Troels Oerting is the former current Assistant Director of Europol, and the Head of European Cybercrime Centre and Europol's Counter Terrorism and Financial Intelligence Centre. Oerting has over 30 years’ experience in Law Enforcement - the last 15 holding senior management positions including: former Director of the Danish NCIS, National Crime Squad, SOCA and Director of Operations in Danish Security Intelligence Service; Assistant Director in Europol's IMT Department; and Assistant Director in Europol's Operational Department. Oerting is the Chair of EC3 Programme Board; Chair of European Financial Coalition against sexual exploitation of children; on the Board of Managers in the Virtual Global Task Force and EU cybercrime Task Force; and EC3 representative in ICANN and ITU strategic meetings.

Princess Funke Adedoyin, Member, Nigeria’s House of Representatives