

# **HOT TOPICS** & **HOT SPOTS**

EXPLORING GLOBAL CHALLENGES



**GLOBALSCOPE**

A GLOBAL CONNECT @ UC IRVINE PUBLICATION





*Volume V*

---

# HOT TOPICS & HOT SPOTS

---

**GLOBALSCOPE PUBLICATIONS**

University of California, Irvine • School of Social Sciences



# GLOBALSCOPE PUBLICATIONS

---

University of California, Irvine • School of Social Sciences

*GlobalScope is a series of innovative curriculum guides created by the University of California, Irvine's School of Social Sciences for secondary school educators and students on the 21st Century forces and issues of globalization. The curriculum is designed to introduce high school students to the formal academic disciplines of anthropology, economics, geography, international studies, political science, and sociology. The GlobalScope publications allow us to share original University research and teachings with students and teachers beyond our immediate reach.*

All rights reserved. Printed in the United States of America. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without permission in writing from the publisher.

Copyright © 2018 Global Connect @ UCI | University of California, Irvine.



## Introducing GLOBAL CONNECT @ UCI

---

Global Connect @ UCI is an original educational partnership developed by the University of California, Irvine's School of Social Sciences to enrich California's secondary school curriculum in international studies. This is accomplished by translating current university-level concepts and knowledge into a curriculum that is age appropriate for high school students.

The global studies knowledge gap in our public schools is a critical problem that needs a flexible and immediate response. Students need lessons they can relate to as global citizens that will affect how they see themselves in the world. They must be capable of thinking in terms of worldwide issues to succeed in their respective careers and lives so that they may contribute to the general welfare of society. This cannot be achieved through textbook curriculum that is outdated by the time it is received by students. Teachers cannot abandon their classroom responsibilities to acquire current knowledge of the quickly changing international environment. Global conflicts and issues need to be brought to the students as current events – not as history.

The study of worldwide issues through Global Connect establishes an environment that creates responsible global citizens and leads to access for students to higher education. Global Connect builds a bridge to the world for our nation's secondary students.

Global Connect dedicates its educational program and publications to addressing California's History Social Studies curriculum framework and the National Curriculum Standards for Social Studies. This is being accomplished through the creation of an original year long course, "Globalization and International Relations"; implementation of the syllabus at select schools in Orange County; sponsorship of countywide teacher seminars; and the development of new on-line curriculum options for secondary educators statewide and beyond. Classroom lessons are innovative in structure and not only teach students factual information but serve as an ideal platform for analytical and reflective thinking about global issues.

For additional information, please visit our website at: [www.globalconnect.socsci.uci.edu](http://www.globalconnect.socsci.uci.edu)

## Common Core Standards in the Social Sciences

---

The pursuit of Common Core Standards is redefining America's educational priorities. One of the most central and elusive problems in addressing these standards is developing academically challenging and classroom effective curriculum that addresses the needs of our students in different subject areas. Global Connect @ UCI, a unique educational initiative based in the School of Social Sciences at the University of California, Irvine, has developed original curriculum and teaching strategies to introduce secondary students to 21st Century global issues and events through an interdisciplinary lens. The lens integrates the various disciplines within social science: anthropology, economics, geography, international studies, political science, and sociology.

This integration occurs through concepts, readings, and "problem sets" found in contemporary university classrooms. Our academically centered course of study has been adapted into age appropriate thematic presentations, dynamic interactive, and literacy building workshops that realize the Common Core objectives.

**Global Connect specifically targets and meets the Common Core Standards by:**

- *Focusing on non-fiction, discipline based content through formal academic PowerPoint presentations, interactive workshops, and readings*
- *Emphasizing Evidence Based Writing Skills through the introduction of take-home assignments, and unit capstone projects, and formal academic forms of in-class writing*
- *Building a discipline-based vocabulary (a set of new terms are defined to complement each week's academic theme)*
- *Expanding the students' abilities to: Use quality academic sources, organize data, analyze, and cite & discuss*
- *Integrating contemporary use of technology for online research and general inquiry*

The Global Connect course on "*Globalization and International Relations*" is already serving as a Common Core option for secondary educators and students in California's Saddleback Valley Unified School District and Newport Mesa Unified School District. The partnership between UCI, SVUSD, and NMUSD is currently exploring new strategies for sharing and advancing this dynamic new course so that other districts can adopt this as a vehicle for acquiring college ready critical thinking abilities and organizational skills. These strategies include the creation of effective teacher training modules for each unit; an expanded online topic-specific video library of presentations by UCI faculty and graduate students; and the continued development of *GlobalScope Curriculum Guides*.



This year, as with prior years, the content has been revised and edited to address the most recent global occurrences/issues and to introduce new resources. For an in-depth overview of our Program, please visit our website at: [www.globalconnect.socsci.uci.edu](http://www.globalconnect.socsci.uci.edu)

*Ellen Schlosser*

*Ellen Schlosser  
Global Connect @ UCI  
Founding Director  
Curriculum Development Advisor*

**Note:**

In 2011, the University of California recognized Global Connect's course, "*Globalization and International Relations*," as an approved A-G academic elective course for California's secondary students. The California Council for the Social Sciences recognized the program as being a Common Core ready curriculum and featured the program in their journal, *Sunburst: A Publication of the California Council for the Social Studies*.

## GUIDELINE TO GLOBALSCOPE

---

GlobalScope is an expanding library of in-print and online guides that mirror UCI School of Social Sciences' contemporary research and teachings related to 21st Century issues and conditions of globalization. The primary motivation behind this publication is to provide secondary teachers with an accessible social science resource that will help create “global” windows in the classroom. Our guiding principle is that high school students need to understand the contemporary changes that are influencing their educational and personal opportunities, and ultimately, their lives and careers.

### Explanation of GlobalScope format:

**Unit Presentations** vary in format. Each presentation is centered on a specific topic and reflects the style of the individual faculty, graduate, or undergraduate student presenter. Several of the authors have created PowerPoint presentations that can be used by the classroom teacher.

An annotated version with additional information has been included in the *Teacher Edition*. Some presenters have also provided lesson outlines.

**Workshop Scripts** seek to recreate the lecture/discussion format used in college courses. We alternate the formal introduction of topics with special interactive workshops. These age-appropriate workshops have been designed and successfully presented in the classrooms (grades 8 – 12) by *Global Connect* undergraduate interns. These workshops have been designed in a script-like manner with sections assigned to the university undergraduate interns. The workshop material can easily be adapted for “single voice” use by the classroom teacher.

**Literacy Building Readings and Assignments** provide students with exercises that will require them to read non-fiction primary source documents. After reading and analyzing the materials, the students will be given written assignments to strengthen their expository writing abilities. Some current topical articles and charts have been reprinted and cited.

**Global Perspectives: International Relations & Globalization Course Workbook** is a two-part workbook to be used in conjunction with the thematic module presentations throughout the semester.

**Part I: “A Sense of Place: Identifying Nations by Name and Location”** includes weekly political map identification exercises that provide students with the ability to recognize the location of the globe’s nations. These weekly exercises will allow students to locate and name the nations of each continent and significant regions.

**Part II: “People of Purpose: 21st Century Global Citizens (‘Real Heroes’)”** will introduce students to real heroes whose actions have impacted the distinct geographic areas being studied. These introductions will be made through video interviews/feature stories and assigned readings. Students will be asked to analyze the problems, strategies, and solutions associated with each of the featured social entrepreneurs through writing exercises. Over the semester the assignments will transition students from completing simple fill-in review sheets to composing five paragraph expository essays. The writing assignments, depending on length, can be used as in-class worksheets or as take home assignments. Grading of these assignments is recommended.

### **Identification of Curriculum Standards:**

Each workshop and presentation addresses an objective identified in the *National Council for the Social Studies Curriculum Thematic Strands* and/or the objectives set forth by the *California State History/Social Science Standards & Framework*. For your personal reference, we have included a copy of the *National Council’s Thematic Strands* in the Appendix.

**Complimentary Disk:** All of the primary *GlobalScope* materials presented in this curriculum guide are provided on a disk so that classroom teachers can independently present the PowerPoint presentations and reproduce the worksheet assignments.

All the original materials are for individual classroom use only and not to be reprinted without express permission from the School of Social Sciences, University of California, Irvine.

**Website:** All materials contained in *GlobalScope* will be posted on the *Global Connect @ UCI* website: [www.globalconnect.socsci.uci.edu](http://www.globalconnect.socsci.uci.edu)


## HOT TOPICS & HOT SPOTS

---

*Hot Topics & Hot Spots: Exploring Global Challenges* provides students with the opportunity to apply their newly acquired knowledge of geopolitical terms and concepts (nation-states, foreign policy, infrastructure, human rights, fragile states, etc.) to some of the critical issues and events we are facing today.

The reinforcement of classroom knowledge is best served when the students gain valuable insights about the realities of their world. What events and issues during the first years of the century have cast a shadow over the world in 2018? With this goal in mind, this edition will center on the following inquiries:

- *Media Literacy: How is the creation and circulation of misleading and false information impacting the well being of our global society? What is meant by news consumption? Is false news a historic phenomenon? How do you identify misleading headlines, images, and content? What methods can you take to check the facts? Who and how can citizens be protected from the constant flow of misinformation? (See additional editorial remarks on page 17.)*
- *Cybersecurity: How is the individual being negatively impacted through cyberspace? What does the term “cyberwarfare” mean? What are some of the specific motivations behind cyber attacks? How can information be used as weapons? What methods or procedures can sovereign nations adopt in order to protect their citizens?*
- *Nuclear Proliferation: What dangers are associated with the increasing technologically-driven communications of global actors? Why are North Korea, Russia, and China expanding their nuclear weapon arsenals? How does this new proliferation of nuclear weapons impact political alliances and expansion of trade? What 2017-2018 threats between nuclear powers threaten world peace?*
- *Terrorism in the Era of Globalization: What is the primary motivation behind terroristic acts? How has 20<sup>th</sup> century state based terrorism transitioned to non-state actors? Which dominant terrorist groups have emerged? What has fueled the creation of Al Qaeda, ISIS, and Boko Haram? What strategies have the United Nations and independent nation-states adopted to combat terrorism?*
- *The Great Exodus: Refugee Crisis – What global crises have created a historic number of refugees? What nations are they fleeing? Which nations have kept their borders closed and which nations have opened their borders? What are the initial needs and long-term challenges of the refugees?*

- 
- *New Nationalism and Global Risks 2018: What nations are questioning the benefits of globalization? Why have nations elected to create new political alliances, renegotiate trade agreements, and redefine their post-World War II character? What global risks have increased wealth disparity, political tensions, environmental dangers, and cyber vulnerabilities for nations?*

On behalf of the Global Connect team and the editorial staff of GlobalScope, I hope that you find this publication a valuable educational resource. We would sincerely appreciate your insights regarding future themes and effective techniques that we can incorporate in our workshop materials. Please forward your suggestions to Ellen Schlosser at [edschlos@uci.edu](mailto:edschlos@uci.edu).

# GLOBAL CONNECT VISIONARIES

---

## UNIVERSITY OF CALIFORNIA, IRVINE

**Manuel Gomez**, *Former Vice Chancellor of Student Affairs*

## SCHOOL OF SOCIAL SCIENCES

**Bill Maurer**, *Dean of Social Sciences*

**Mark Petracca**, *Associate Dean of Undergraduate Studies*

**Dave Leinen**, *Assistant Dean, Administration, Planning, and Resources*

**Caesar D. Sereseres**, *Professor of Political Science*

## NEWPORT-MESA UNIFIED SCHOOL DISTRICT

### EARLY COLLEGE HIGH SCHOOL

**Principal David Martinez**

**Host Teachers: Sandy Kipfstuhl**

### NEWPORT HARBOR HIGH SCHOOL

**Principal Sean Boulton**

**Host Teacher: Jennifer Thompson**

### ENSIGN INTERMEDIATE SCHOOL

**Principal Mike Sciacca**

**Host Teachers: Sarah Tucker**

### TEWINKLE MIDDLE SCHOOL

**Principal Alex Morales**

**Host Teachers: Misty Smith**

## SADDLEBACK VALLEY UNIFIED SCHOOL DISTRICT

### LAGUNA HILLS HIGH SCHOOL

**Principal Bill Hinds**

**Host Teachers: Yoleisy Avila, Carri Geiger, Kirk Brown, Steven Schrenzel**



# PUBLICATION CREDITS

---

## EDITORS-IN-CHIEF

**Jessica Bit**

*Director, Global Connect @ UCI*

**Ellen Schlosser**

*Curriculum Development Advisor, GlobalScope Curriculum Guides*

## UNDERGRADUATE EDITORS

**Maria Luiza Rivera**

*Sociology and Education Science*

**Suryanshi Pandya**

*Education Science*

## UNDERGRADUATE & ALUMNI STUDENT CONTRIBUTORS

**Shannen Dilag**, *Political Science & History*

**Alexandra Russo**, *Psychology and Social Behavior & Criminology, Law and Society, 2017*

**Claudia Cheffs**, *Political Science, 2013*

**Hannah Chang**, *History & Education Sciences*

**Marisol Moreno**, *Political Science*

**Emily Lin**, *Business Administration & International Studies*

**Charlene Cisneros**, *Global Cultures*

**Brandyn Murillo**, *Sociology*

# GLOBALSCOPE

## HOT TOPICS & HOT SPOTS

### *Table of Contents*

<i>Unit</i>	<i>Topic &amp; Presenter</i>	<i>Workshop(s)</i>
<b>I.</b>	<b>Media Literacy</b>	Patterns of News Consumption 17
		False News: A Historical Perspective 28
		Identifying Misleading Headlines, Images, and Content 32
		News Literacy: How to Fact Check 38
		Targeting the Spread and Creation of Misinformation 53
<b>II.</b>	<b>Cybersecurity</b>	Cyber Town 84
		Cybersecurity Threats & Protections 100
<b>III.</b>	<b>Nuclear Proliferation</b>	U.N. Conference Debate on North Korea 113
<b>IV.</b>	<b>Terrorism</b>	152
<b>V.</b>	<b>Refugee Crisis</b>	161 I am a Refugee 168
<b>VI.</b>	<b>Global Risks</b>	197 Fraying Global Cooperation 204

## ONLINE RESOURCES

---

<i>Unit</i>	<i>Online Resource</i>
Unit I	<b>Lecture: False News: A Historical Perspective</b>
	How False News Can Spread – Noah Tavlin <a href="https://ed.ted.com/lessons/how-false-news-can-spread-noah-tavlin#review">https://ed.ted.com/lessons/how-false-news-can-spread-noah-tavlin#review</a>
	<b>Workshop: Identifying Misleading News and Headlines</b>
	Skechers Shape-Ups Instructional Video <a href="https://youtu.be/HZ6_PtpSW3U">https://youtu.be/HZ6_PtpSW3U</a>
	'Deceitful propaganda' - Emmanuel Macron on RT and Sputnik <a href="https://youtu.be/XVB2cVYSVdM">https://youtu.be/XVB2cVYSVdM</a>
Unit II	Macron scolds RT, Sputnik, for coverage of French election <a href="https://youtu.be/1BoAUP5Cwco">https://youtu.be/1BoAUP5Cwco</a>
	The Fake News Machine <a href="http://money.cnn.com/interactive/media/the-macedonia-story/">http://money.cnn.com/interactive/media/the-macedonia-story/</a>
	<b>Workshop: News Literacy: How to Fact Check</b>
	How to choose your news - Damon Brown <a href="https://youtu.be/q-Y-z6HmRgI">https://youtu.be/q-Y-z6HmRgI</a>
	<b>Lecture: Cybersecurity</b>
Unit II	Cybersecurity by Alexandra Russo <a href="https://youtu.be/83tFq3Ir1Uc">https://youtu.be/83tFq3Ir1Uc</a>
	Defining cyberwarfare...in hopes of preventing it - Daniel Garrie <a href="https://youtu.be/ZVoDwtjvDJc">https://youtu.be/ZVoDwtjvDJc</a>

---

### **Workshop: Cybersecurity Threats & Protections**

How to Create a Secure Password | Molly Wood | The New York Times  
<https://youtu.be/G9TDMvABQis>

Phishing Quiz  
<https://www.opendns.com/phishing-quiz/>

Is Public Wi-Fi Safe?  
<https://youtu.be/bdVkkRmJEeM>

---

### **Lecture: Nuclear Threat**

Nuclear-Bomb Explosions  
[https://youtu.be/5gD\\_TL1BqFg](https://youtu.be/5gD_TL1BqFg)

President Harry Truman announces the Bombing of Hiroshima  
[https://youtu.be/FN\\_UJJ9ObDs](https://youtu.be/FN_UJJ9ObDs)

## **Unit III**

The history of the Cuban Missile Crisis - Matthew A. Jordan  
<https://youtu.be/bwWW3sbk4EU>

---

### **Workshop: United Nations Conference Debate**

The growing North Korean nuclear threat, explained [Updated]  
<https://youtu.be/NwbYpdGpx8U>

---

### **Lecture: Refugee Crisis**

Austria's far right set to enter government  
<http://www.aljazeera.com/news/2017/12/austria-set-enter-government-171216054027062.html>

## **Unit V**

People of Nowhere  
<https://vimeo.com/144857118>

---

### **Workshop: I am a Refugee**

UNHCR's New Global Trends Report  
<https://youtu.be/hBFgI4D8eEM>



---

## Workshop: Fraying Global Cooperation

Full Video: Vladimir Putin's presidential inauguration ceremony in Kremlin  
<https://youtu.be/TNiWnSOsAnE?t=25m50s>

### Unit VI

Theresa May: 'no unnecessary delays in invoking Article 50'  
<https://www.youtube.com/watch?v=duqkhz29gIo>

Erdogan's UN Speech (English)  
<https://www.youtube.com/watch?v=AxUf6s54ZDc>

Moments from Pres. Trump's inaugural address  
<https://www.youtube.com/watch?v=1SsB4leNp54>

---

---

## HOT TOPICS & HOT SPOTS

---

### *Cybersecurity*



# Cybersecurity

The Progression of Information Warfare

What is Cybersecurity?

## Cybersecurity:

the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this

## Information in the 21<sup>st</sup> Century

- › So much of the information we use is now online or connected to a greater network
- › We can exchange information in seconds
  - » E-mails, texts, snapchats, Dropbox
- › The ability to connect all this information allows the opportunity for information to fall into the wrong hands

**Can you think of ways you could be victimized through cyberspace?**

## Cyber Victimization

- › You are affected by cybersecurity too! People can access your social media and other accounts.
- › Cyberbullying
- › Identity use on social media
- › Use of your parents credit card information

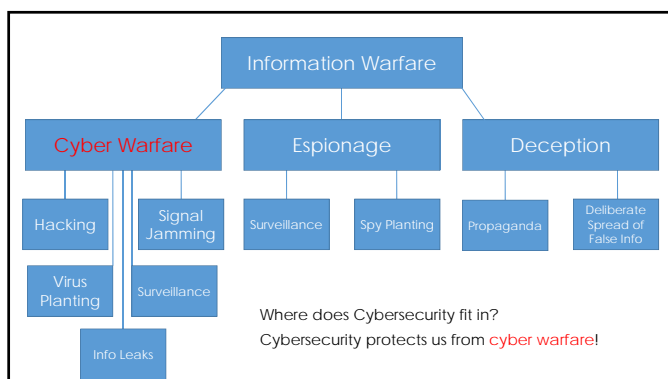
## Cyber Victimization

- › Identity theft
  - » The use of you or your parents social security number
- › Credit card information use
  - » Like the mass Target hack in 2013

**Do you think cyber information can be used to harm more than just individuals?**

## Cyber Warfare

- › **Information Warfare**: actions taken to achieve the upper hand by affecting or gathering an adversary's information; at the same time, making sure your information is secure
- › **Cyber Warfare**: the use of technology to disrupt the activities of a state or organization, especially attacking information systems used for strategic or military purposes
- › **Hacker Warfare**: the attack on computer systems



## Information Warfare

- › "All war is based on deception"
  - » Sun Tzu, 5<sup>th</sup> century B.C.
- › Information has always been a valuable tool in war
  - » Espionage
  - » Surveillance
  - » Propaganda
  - » Radio signal jamming

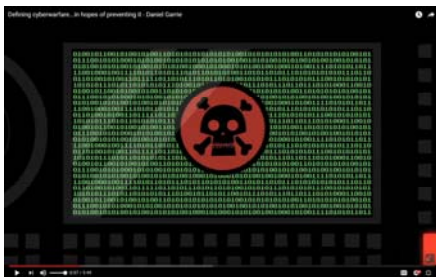


## Information Warfare

- › Espionage has always been a big business, but this required people physically entering an enemy's territory
- › Propaganda is used to spread deceptive information about enemies
- › Radar was first used in WWII and gave users the upper hand
  - › Imagine playing hide-and-seek and knowing where your opponent is
- › Jamming an opponent's radio signal keeps them from communicating with their allies and troops

**But cyber warfare can be  
so much more  
destructive...**

## Cyber Warfare



## Cyber Warfare

- › Today, individuals and governments can access classified information faster and easier than ever
- › Governments use information gained from cyber-methods to:
  - › Gain profit
  - › Sway politics
  - › Gain military advantages
  - › Deceive other nations
  - › Escalate conflict between other nations
  - › Etc.

## Cyber Warfare

- › This can directly affect you!
- › If another nation decided to hack into America's electric grid, they could shut down the entire nation
- › If America decided to hack into another nation's phone system, our government could face criminal charges
- › If an attack were to be carried out, **who would be responsible?**

## Sovereignty & Protection

- › Governments are responsible to protect their populations from all internal and external threats
- › Threats come in many forms and new threats arise with changing technology
- › **But who is to blame for non-physical cyber attacks?**
  - › An entire government?
  - › The government's leader?
  - › The hacker who created the program?
- › As of now, there is no protocol to address cyber warfare crimes

## Cyber Threats in the 21<sup>st</sup> Century

### Stuxnet

- › In 2009 the US and Israel launched a joint attack on Iran's nuclear facilities
- › The virus, called Stuxnet, targeted the facilities' centrifuges and caused them to spin out of control and break
- › Not only did this virus destroy the Iranian centrifuges, but it made the operators look incompetent
- › Sources later claimed that the attack "[changed global military strategy in the 21st century](#)"

### The Democratic National Committee

- › In 2016, reports confirmed that two Russian hacking groups accessed the DNC's e-mails
- › The hackers mimicked e-mail addresses in order to obtain classified information from party members and used existing information from the e-mails to leak restricted information
- › By installing malware onto representatives' computers, the hackers gained access to important files on both government and personal computers
- › As of now it is unclear whether the information was used to bias the election. [What would the impact be if this were true?](#)

### WikiLeaks

- › WikiLeaks is a multi-national media organization and associated library founded in 2006 by Julian Assange
- › The site publishes censored and restricted data on official materials involving war, espionage, and corruption
- › WikiLeaks protects people who send in censored information through its system of encryption

### WikiLeaks

- › One of the biggest controversies is the release of private emails from Clinton's campaign manager John Podesta
- › Another WikiLeaks controversy involves the NSA's alleged targeting of Assange
  - › Documents claim to show that as far back as 2010 the US NSA added Julian Assange to a "MANHUNTING" target list, together with suspected members of al-Qaeda
  - › The information revealed how the NSA collects information about American's phone calls, our email messages, our friends and contacts, how we spend our days and nights
  - › Assange currently lives in Ecuador, who is offering asylum against possible prosecution in the U.S.

### WikiLeaks

- › WikiLeaks allows for transparency on governmental actions to an international community and for this reason has received criticism
- › Some people view it as a legitimate source of information that ensures freedom of the speech, while others perceive it as unpatriotic and containing curtailed content
- › [Do you think classified information should be made public, as WikiLeaks promotes? What are the pros and cons?](#)

# Key Terms

 *Related Presentation:*  
*Cybersecurity*

1. **Cybersecurity:** The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.
2. **Cyber Victimization:** Falling victim to possible aggressive or illegal acts that can be committed through cyberspace.
3. **Cyberbullying:** The use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.
4. **Identity Theft:** The fraudulent acquisition and use of a person's private identifying information, usually for financial gain.
5. **Cyber Warfare:** The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes.
6. **Information Warfare:** Actions taken to achieve the upper hand by affecting or gathering an adversary's information; at the same time, making sure your information is secure.
7. **Hacker Warfare:** The attack on computer systems.
8. **Espionage:** The practice of spying or of using spies, typically by governments to obtain political and military information.
9. **Propaganda:** Information, especially of a biased or misleading nature, used to promote or publicize a particular political cause or point of view.



# **CYBER TOWN**

## **TOWN-HALL MEETING**

### **BE HEARD!**

Your fellow townspeople are being threatened by cyber-attacks. Our community needs your help to generate a list of steps that the citizens of Cyber Town should take to prevent cyber-attacks from occurring in the future. We ask you to attend our biweekly Cyber Town Town-Hall Meeting and hear from four expert panel groups.

Your mayor is depending on you.

## **Wednesday and Thursday**

Hosted by:

Your Local Global Connect Interns

Please be prepared to participate in crisis panels.

**Keep Cyber Town Safe from Cyber Threats!**

**Name:** \_\_\_\_\_

**Period:** \_\_\_\_\_

# Cyber Attack Review Questions

1. What organization was attacked?
2. What is the nature of the data breach? What was stolen? (Passwords, credit card numbers, personal information?)
3. What was the extent of the breach? How many people did it affect? How much money did the organization/corporation/government estimate it lost as a result of the data breach? What other information was compromised?

- For more information, visit:  
[https://learning.blogs.nytimes.com/2014/12/11/teaching-about-cybersecurity-taking-steps-to-improve-online-safety-and-prevent-data-breaches/?\\_r=0](https://learning.blogs.nytimes.com/2014/12/11/teaching-about-cybersecurity-taking-steps-to-improve-online-safety-and-prevent-data-breaches/?_r=0)

## Cyber Town Market Hacking

---



Recent data breaches have brought to mind last year's cyberattack on Cyber Town Market, when hackers stole 40 million credit and debit card numbers from its point-of-sale systems.

So what did hackers actually do with this information after they stole it?

The short answer is they sold it. Because the magnetic stripes (magstripes) on the back of customers' credit cards hold a person's account number, expiration date, and secret CVV code, they have value in the underground market. Hackers sell these magstripes to card counterfeiters who then easily paste them onto fake credit cards using their own magstripe encoding machines.

Between 1 and 3 million of the 40 million stolen cards were successfully sold on the black market for about \$27 each, reported Brian Krebs, a former Washington Post staffer who has written extensively on cybersecurity. According to Krebs, before credit card companies had the chance to

cancel the cards, hackers likely generated \$53.7 million in income.

According to a report released earlier this year by the RAND Corporation's National Security Research Division, the value of credit cards varies depending on how much of them are available on the hackers' black market. The table to the right, taken from RAND's report, shows how the average price of credit card data can change as demand fluctuates. After a large breach such as the Cyber Town Market breach, the market may be flooded with data, which causes prices to go down.

Card data can also be more or less valuable depending on the card's characteristics. According to RAND, no-limit cards such as the American Express black card or chip-and-PIN cards are typically worth more in the black market.

In the days after Cyber Town Market was breached, the stolen credit cards were unusually expensive— mostly because banks

did not cancel them quickly enough, according to Krebs. Some credit cards acquired in the Cyber Town Market breach were reportedly sold for as much as \$135, depending on the type of card, expiration date, and limit.

The good news is that consumers don't have to pay to get their credit cards replaced if their information is stolen. Instead, credit unions and community banks pick up the tab. Since Cyber Town Market was breached, these banks have spent a reported \$100 million reissuing 21.8 million cards— only about half of the amount stolen in the breach.



# Cyber High School Hacking

---



A tutor at the center of an alleged grade-changing scandal at Cyber High School was arrested Monday when police say he returned to Cyber State after fleeing the country.

Timothy Lance Lai, 29, was taken into custody by Cyber Town Police at Cyber International Airport and has been charged with a felony count of second-degree commercial burglary and four felony counts of computer access and fraud, police and prosecutors said Monday.

Prosecutors allege that Cyber Town resident Lai, who was working as a private tutor, broke into a campus building and placed a USB device capable of recording keystrokes on a teacher's computer. On June 14, they believe he was able to use the information gleaned from the recorded keystrokes to access the school's network and change the grades of three students.

A teacher noticed that grades had been changed and notified the campus administration. Police were called in and began

to investigate reports that a tutor had been involved.

In mid-December, a student told a vice principal and authorities that he had been asked by Lai to install a USB keylogger, according to a search warrant and affidavit.

The student met with investigators at the Cyber Town Police Department, where authorities say he called Lai. According to the affidavit, during a recorded phone conversation, Lai identified himself and admitted to his involvement in the hacking.

A search warrant was served at Lai's home and vehicle, but prosecutors say he fled the country before authorities could reach him.

Cyber Town police spokeswoman Jennifer Manzella did not comment on where he had been or what brought Lai back to Cyber Town but indicated that investigators surprised him at the airport.

The Cyber County District Attorney's Office indicated that it will be requesting Lai to be

held on \$200,000 bail. If convicted, he faces up to five years and eight months in jail. As of Monday night, the time of his arraignment had not been set.

“We are grateful for the ongoing support and diligence from the Cyber Town PD,” Cyber Unified School District spokeswoman Laura Boss wrote in a statement sent to blog Cyber Town Today. “The matter is now in their capable hands and the district will be referring all media inquiries to the Cyber County District Attorney’s Office. Cyber High School has moved beyond this incident. It no longer involves the campus or school district and is a matter for the legal system.”

Administrators ultimately punished 11 students believed to have been involved in the grade-changing scheme and were forced to investigate more than 52,000 grades.

Families and administrators described Lai as someone who profited from wealthy parents eager to send their children to the best colleges.

Despite teaching high-level math and science, Lai didn’t get his own bachelor’s degree in psychology from Cyber University until he was 26.

Administrators also say he ingratiated himself with students by hanging out with them, becoming not just a mentor but a friend. In the aftermath of the grade-changing scandal, some administrators admitted that the school’s hyper-driven tutoring culture had become unhealthy.

Some parents of the 11 students expelled from Cyber High questioned why their children were targeted for expulsion, arguing the cheating included a larger number of students.

Some parents alleged that as many as 150 students may have been involved.

# Cyber Town Electrical Grid Hacking

---



Cyber Town is investigating a suspected cyberattack on Cyber Town's power grid at the weekend, the latest in a series of strikes on its energy and financial infrastructure.

A power distribution station near Cyber Town unexpectedly switched off early on Sunday, leaving the northern part of the capital without electricity.

A Cyber Town security chief said last week that Cyber Town needed to beef up its cyber defenses, citing a spate of attacks on government websites that he said originated in Hacker Town.

The outage amounted to 200 megawatts of capacity, equivalent to about a fifth of the capital's energy consumption at night.

This kind of blackout is very rare. There are only two possible explanations for the accident: either a hardware failure or external interference.

The company's IT specialists had found transmission data that had not been included

in standard protocols, suggesting that external interference was the likeliest scenario.

Over the past month, Cyber Town's finance and defense ministries and the state treasury have said their websites had been temporarily downed by attacks aimed at disrupting their operations.

There are no final conclusions yet about what it was, but experts say that this was something new and they have not encountered this before.

Last December, another Cyber Town regional power company Cyber Power reported an outage, saying the area affected included the regional capital. Cyber Town's state security service blamed Hacker Town.

Experts widely described that incident as the first known power outage caused by a cyberattack. The Cyber firm iSight Partners identified the perpetrator as a Hacker Town hacking group known as "Sandworm."

"The purpose of this Cyber Town attack: Two options. Either it's a show of power. Prove to the people of Cyber Town that your government cannot protect you.

The other option is that there was something else happening at the same time and they needed this to be their cover or somehow to assist another operation to succeed as a result of the power outage.

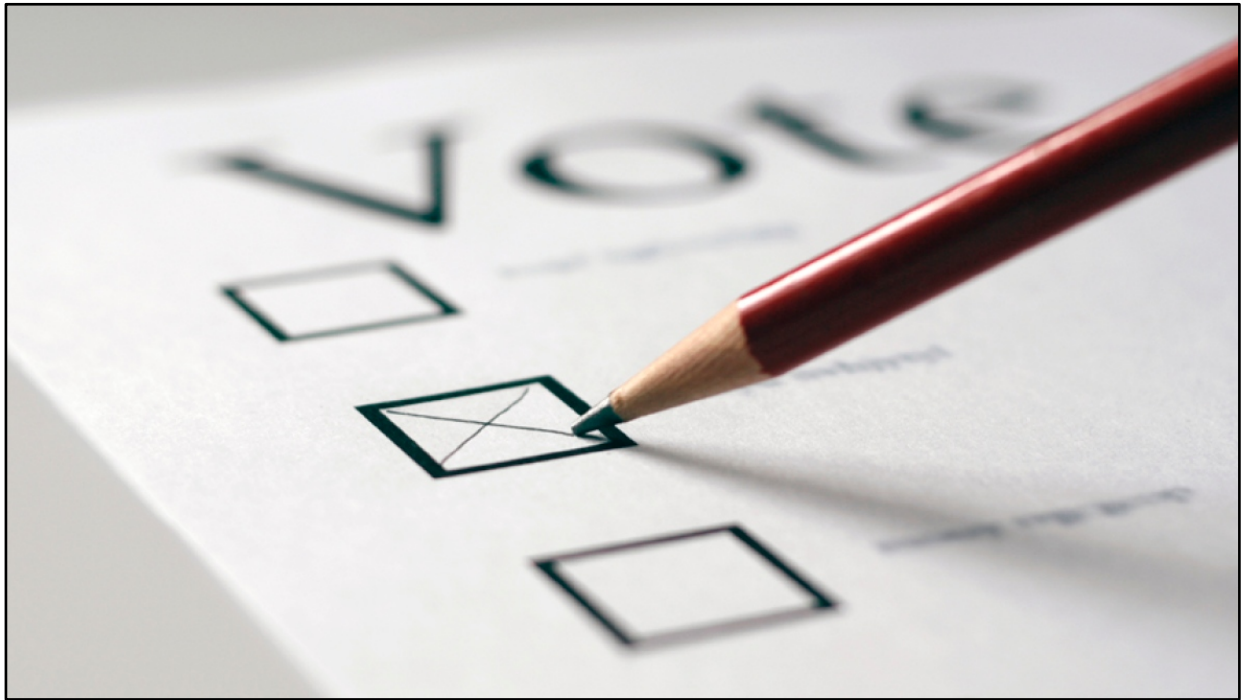
During this year the cyber capabilities of the Hacker Town government have done nothing but increase and we are seeing the beginnings of a new arms race, in both military and cyber activities.

We are tracking several different, separate attack campaigns which we link back to different Hacker Town intelligence agencies, and the targets are typically not just for sabotage, but for espionage.

The vast majority of government attacks that we attributed to the Hacker Town government are not about sabotage or disruption but about collecting intelligence and spying on foreign computer networks, and that has been increasing.

# Cyber Town Election Hacking

---



On the eve of the most consequential Cyber presidential election in decades, the staff of the centrist candidate John Johnson said late Friday that the campaign had been targeted by a “massive and coordinated” hacking operation, one with the potential to destabilize the nation’s democracy before voters go to the polls on Sunday.

The digital attack, which involved a dump of campaign documents including emails and accounting records, emerged hours before a legal prohibition on campaign communications went into effect. While the leak may be of little consequence, the timing makes it extremely difficult for Mr. Johnson to mitigate any damaging fallout before the runoff election, in which he faces the far-right candidate Will Williams.

In a statement, the Johnson campaign said the hackers had mixed fake documents along with

authentic ones, “to sow doubt and misinformation.”

“Intervening in the final hour of the official campaign, this operation is clearly a matter of democratic destabilization,” the statement said.

Earlier on Friday, Mr. William’s campaign staff said its website also had faced “regular and targeted” attacks during the campaign.

It also said that the Cyber Town authorities had investigated the attacks and, this week, arrested a suspect who was “close to extreme-left circles” and who had admitted to being responsible for several attacks on Mr. William’s campaign website. The arrest occurred on Cyber Town soil, the statement said.

Unlike Mr. Johnson, however, it did not appear that Mr. William’s campaign documents had been compromised. The authorities did not

immediately confirm the Williams camp's account.

The Johnson campaign said the documents leaked Friday were stolen several weeks ago after the personal and professional emails of staff members at his political movement, were hacked.

Trend Micro said the attack involved sending emails to campaign officials and others with links to fake websites designed to bait them into turning over passwords.

"The key goals and objectives of the campaign appear to be to undermine Johnson's presidential candidacy and cast doubt on the democratic electoral process in general," he said.

"If indeed driven by Hacker Town, this leak appears to be a significant escalation, expanding the approach and scope of effort from simple espionage efforts towards more direct attempts to sway the outcome," Mr. Kremez added.

Security researchers who have been tracking APT28, also known as Fancy Bear, say it has been moving aggressively using various hacking tools, including so-called spear-phishing attacks, but also through the exploitation of vulnerabilities in technologies that allow hackers to invade their targets undetected by security software.

The security researchers, who asked for anonymity to discuss an investigation, say they believe APT28 has previously passed stolen information taken from breached accounts to another Hacker Town group. It is that second group of Hacker Town cybercriminals that, in other instances, has published leaked information, security experts say, in large part to distance Hacker Town intelligence operatives from the hacks and maintain a measure of plausible deniability.

There was no firm evidence that APT28 was involved in the theft of the Johnson campaign documents.

"We call upon the news outlets that wish to report on this operation to shoulder their responsibilities, in all good conscience," the campaign said. "Indeed, this is not a simple hacking operation but well and truly an attempt to destabilize the Cyber Town presidential election. It is therefore important to consider the nature of the leaked documents, to be fully aware of the fact that a large part of them are purely and simply fake, and the appropriateness of giving an echo to this destabilization operation."



## CYBER THREATS

---

### 1. Ransomware Attack

Two days before Thanksgiving, Alina got hit by a ransomware attack.

5,726 files got locked by CryptoWall, an encryption malware so powerful it is almost impossible to recover the information.

Alina contacted the attacker through the ransomware's communication feature. As all ransomware creators, he told her she can either pay to get her files back or lose them forever. Despite backing up her files 6 months ago, she decided that losing half a year's worth of photos, documents and other files was too much, and so decided to pay the ransom.

The price to unlock her files was \$500 in the first week and \$1000 in the second one, after which the files would be deleted. Payment was to be done in Bitcoin, a complicated process which she had to learn on the fly.

Because of a major snowstorm that closed down the banks, Alina couldn't pay the ransom in the first week, and ended up having to plead with her attacker to not increase the price to \$1,000. Surprisingly, he accepted and gave her the key to unlock her files. However, no one should ever pay a ransom because the risks far outweigh the benefits.

### 2. Catfishing Hack

Cindy started using the online dating site Match.com, and eventually formed a connection with a soldier on active duty in Afghanistan. After a while, the soldier asked for a \$30,000 loan to help him clear a sizeable inheritance of gold and jewelry from US customs.

Cindy's brother intervened, suspecting the soldier was catfishing their sister. Catfishing means pretending to be someone else in order to extract financial gains. It can also be a twisted way to get attention and affection.

In the Match.com case, the victims confronted the man with their suspicions and other evidence they had accumulated over time. The supposed soldier revealed he was a man from Ghana trying to support his sisters, and scamming people online was the best way he knew how to do that.

### 3. Airline Scam

In 2017, Justin decided to move to Italy. Determined to find a cheap flight, he searched for sellers of frequent flyer miles. Eventually, he found two sellers, and talked to them over the phone, one of them even sent him a photo of his driver's license. Ultimately, both of them scammed him for a total sum of \$1350.

Justin tried to find a cheap shortcut and get that 'too good to be true' deal and became



blind to any potential scammers. In addition, the phone conversations and photos helped dispel any suspicions he might have had.

#### **4. Identity Theft**

One day, Laura received a call from her credit card company, saying someone else had tried to obtain a credit card using her name, address, and social security number.

Before telling the police, Laura decided to assess the damage and look over her credit card reports.

The impersonator had gotten so deep into the system, she managed to override Laura's answers to the security questions. Eventually, she guessed the answers and saw the extent of the damage.

The impersonator had created more than 50 accounts in Laura's name and got credit for utilities such as heat, cable, electricity and even a newspaper subscription. What's more, the companies went after Laura in order to get their money back.

After notifying the police and tracking down the impersonator, Laura got a court order and managed to fix a lot of the damage, but only after a lot of sweat and stress.

#### **5. Social Engineering Hack**

What happens when customer support gives away your information? This Amazon user's tale is an insightful one.

An impersonator once found out some of Eric's fake information he used to register a website by looking into a public registry for website owners.

The impersonator then used Eric's fake information in a conversation with an Amazon customer support representative and found out his real address and phone number. Using Eric's real information, the

impersonator got in touch with various services and even managed to issue a new credit card on Eric's name.

Eric got wind of his impersonator's efforts by reading the customer support transcripts, and also found out his real purpose: to get the last 4 digits of his credit card.

Amazon didn't do anything to protect Eric's account, even though he repeatedly signaled the problem, so he finally decided to switch from Amazon to Google. As a parting note, he received an email from Amazon implying they have provided the impersonator with the last 4 digits of his credit card.

This story about Eric's tumultuous experience with Amazon will make you think twice about storing confidential information in your online accounts. The fact that Amazon failed to protect his account and look into the matter shows how a lack of cyber security education can endanger users.

*For more information, visit:*

*<https://beimdalsecurity.com/blog/12-true-stories-that-will-make-you-care-about-cyber-security/>*



**Name:** \_\_\_\_\_

**Period:** \_\_\_\_\_

## Cyber Attack Review Questions

---

1. Who was the victim?
  
  
  
  
  
  
  
  
  
  
2. Who was the hacker?
  
  
  
  
  
  
  
  
  
  
3. How was the individual attacked?
  
  
  
  
  
  
  
  
  
  
4. What were the results of the attack?

## **PRACTICING CYBERSECURITY AWARENESS**

## **10 TIPS FOR CYBERSECURITY PROTECTION**

Source: OpenDNS

### **1. REALIZE THAT YOU ARE AN ATTRACTIVE TARGET TO HACKERS.**

*For more information visit <https://www.opendns.com/>*

### **2. PRACTICE GOOD PASSWORD MANAGEMENT.**

*For more information visit <https://www.opendns.com/>*



### **3. NEVER LEAVE YOUR DEVICES UNATTENDED.**

*For more information visit <https://www.opendns.com/>*

**4. ALWAYS BE CAREFUL WHEN CLICKING ON ATTACHMENTS OR LINKS IN EMAIL OR ATTENTION-GRABBING CLICKBAIT.**

For more information visit <https://www.opendns.com/>



Phishing Quiz: <https://www.opendns.com/phishing-quiz/>

**5. SENSITIVE BROWSING, SUCH AS BANKING OR SHOPPING, SHOULD ONLY BE DONE ON A DEVICE THAT BELONGS TO YOU, ON A NETWORK THAT YOU TRUST.**

For more information visit <https://www.opendns.com/>



**6. BACK UP YOUR DATA REGULARLY, AND MAKE SURE YOUR SOFTWARE IS ALWAYS UP TO DATE.**

For more information visit <https://www.opendns.com/>

**7. BE CONSCIENTIOUS OF WHAT YOU PLUG IN TO YOUR COMPUTER.**

For more information visit <https://www.opendns.com/>

**8. WATCH WHAT YOU'RE SHARING ON SOCIAL NETWORKS.**

*For more information visit <https://www.opendns.com/>*

**9. OFFLINE, BE WARY OF SOCIAL ENGINEERING, WHERE SOMEONE ATTEMPTS TO GAIN INFORMATION FROM YOU THROUGH MANIPULATION.**

*For more information visit <https://www.opendns.com/>*

**10. BE SURE TO MONITOR YOUR ACCOUNTS FOR ANY SUSPICIOUS ACTIVITY**

*For more information visit <https://www.opendns.com/>*

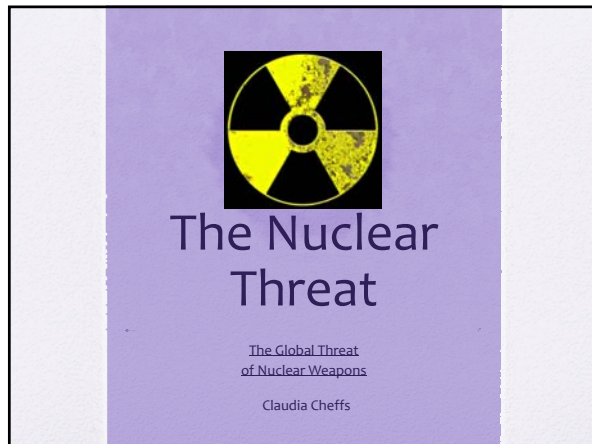
---

## HOT TOPICS & HOT SPOTS

---

### *Nuclear Proliferation*





## What is a Nuclear Weapon?

- Explosive weapon with destructive force from sudden release of energy
- Using “fission” and/or “fusion”
  - **Fission:** energy derived by SPLITTING atoms (1<sup>st</sup> gen bombs)
  - **Fusion:** energy derived by FUSING together atoms
- Today’s nukes have a combo of both fission and fusion
- Detonate chemical explosives around a sub-critical sphere/“pit”– usually Uranium or Plutonium

## Video of Nuclear Weapon

- [https://youtu.be/5gD\\_TL1BqFg?t=1m52s](https://youtu.be/5gD_TL1BqFg?t=1m52s)

## History of Nuclear Weapons

- United States was first country in the world to develop and use nukes
- **Manhattan Project** (Robert Oppenheimer, Father of Atomic Bomb)
  - Project sponsored by U.S. govt
  - U.K. and Canada supported it
  - Assigned to gather intelligence on German nuclear weapons project + create own nuke
- **Why was the U.S. govt interested?**
  - Pearl Harbor (Dec. 7, 1941)
  - “atmosphere of enthusiasm and urgency”
  - First atomic bomb detonated in New Mexico, July 1945 (Trinity Explosion)

## Use of Nuclear Weapons

**World War II (First and only time in history)**

- **Hiroshima:** August 6, 1945, “Little Boy” detonated
- **Nagasaki:** August 9, 1945, “Fat Man” detonated

- Killed an estimated of 226,000 people in Japan
- President Truman justified decision saying:
  - “We have used [the bomb] against those who attacked us without warning at Pearl Harbor...against those who have abandoned all pretense of obeying international laws of warfare”
  - Truman [Address](#) to the American public

## Did we win? Yes and No...

- Sept. 2, 1945, Japan surrenders after attack (V-J Day)
- But... two weeks after Hiroshima/Nagasaki, Stalin signed a decree to lay the basis for a Soviet nuclear program
- Four years later (1949) USSR conducted its first nuclear test explosion

*“The fact that the Americans used the bomb meant a lot. That meant they were ready to use it again, perhaps against another enemy, against another target.”– Vladislav Zubok, Russian Historian*

- U.K. (1952), France (1960) and China (1964) followed suit thereafter
- A nuclear arms race began this way...

## Arms Race (Cold War)

- Nuclear Arms Race took place during the Cold War (1947-1991)
- Mutual Assured Destruction (MAD)** was reached

MAD: military doctrine which full-scale use of nuclear weapons by two or more opposing sides would cause complete annihilation of BOTH the attacker and defender



- Both U.S. and Russia reached enough nuclear power to obliterate each other
- EX: Cuban Missile Crisis (next slide)

## Cuban Missile Crisis (Cold War)

- Cuban Missile Crisis** (October 1962): nuclear confrontation between U.S. and U.S.S.R. -- 90 miles away from Florida

- Closest the Cold War came to escalating a full scale nuclear war!!!**

- U.S. attempts to invade Cuba in Bay of Pigs Invasion (fails)
- US ballistic missiles deployed to Italy/Turkey (NATO allies); Soviet ballistic missiles deployed in Cuba (USSR ally)

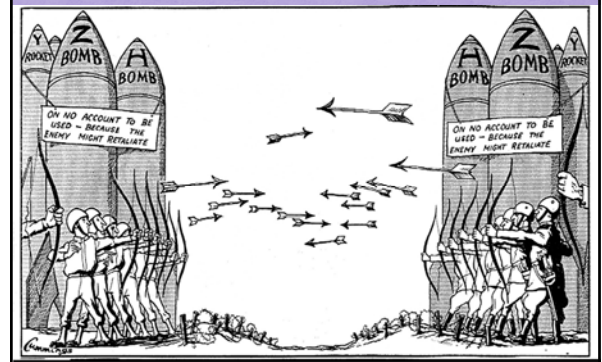


## Cuban Missile Crisis (Continued...)

- President Kennedy attempted a naval blockade to stop shipment of nukes to Cuba; Soviets continued to ship missiles
- Invasion and nuclear war ALMOST broke out!
  - Thankfully, due to **diplomacy efforts** by Kennedy/Khrushchev, a solution worked out, but close call (VIDEO)



## Arms Race (Cold War)



## Deterrence Theory

- Some argue that **nuclear weapons are necessary to avoid wars and conflicts**. AKA: Deterrence Theory
- Deterrence**: dissuading/deterring an adversary from using force by threatening with own force
- Could lead to a nuclear arms race
  - Belief that if one side had more weapons than enemy, they would be safer (enemy less likely to attack)

### Why is this problematic?

- Spend so much on weapons! \$\$\$
- Race seems to never end-- how many do we need to feel secure?
- Only works in **THEORY** with a stable leadership
  - What happens when you deal w/ unstable leaders? (Ex: North Korea, terrorists)

Kim Jong Un Would Have To Be Mad To Use His Nuclear Weapons -- But Nerve Agents Are Different

Kim Jong Un would have to be mad to use his nuclear weapons -- but nerve agents are different. Nerve agents are chemical weapons that can be used in a variety of ways, including as a weapon of mass destruction. They are highly toxic and can cause death within minutes of exposure. They are also highly unstable and can be easily dispersed in the air. This makes them a very dangerous weapon.

By Kim Jong Un



## Who are the nuclear powers today?

- 9 countries have nuclear weapons**

- U.S.: 7,200
- Russia: 7,500
- China: 260
- India: 90-110
- Pakistan: 100-120
- Israel: 80
- France: 300
- U.K.: 215
- North Korea: <10



See interactive map [here](#)

### How MANY total nukes?

There are more than 15,000 nuclear weapons on Earth







## Problem Cases: North Korea

### North Korean Nuclear Program

- Withdrew from NPT in 2003
- Bush attempted negotiations, but failed. Obama no attempt
- Developed first nuclear weapons in 2009



### Problem:

- NK nuclear weapons cannot reach U.S. yet, conflict with S. Korea or Japan affects U.S.
- Nuclear catastrophe = radiation spreading across the Pacific
- Anti-missile system deployed in S. Korea after latest NK nuclear test



### What can be done?

- Instead of worrying about Iran, let's focus on N. Korea
- Reopen dialogue, consider easing sanctions; Trump could have foreign policy legacy
- Rex Tillerson has rejected talks with North Korea on nuclear program

## Looking towards the future...

### Negatives:

- Trump pre-election: "proliferation will happen anyway"
- Denounced START Treaty, said was one sided w Russia
- U.S. recently deployed anti-missile system in S. Korea after N. Korea's latest test



- More nuclear spending- "U.S. must be on top of pack"
- 2018 budget= 11.3% increase in NNSA

Table 3. 2018 Discretionary Overview by Major Agency  
(The numbers are in billions of dollars)

	2017	2018	Change	% Change
<b>Base Discretionary Funding</b>				
Armed Forces	100.0	100.0	0.0	0.0%
Education	100.0	100.0	0.0	0.0%
Health	100.0	100.0	0.0	0.0%
Transportation	100.0	100.0	0.0	0.0%
Other	100.0	100.0	0.0	0.0%
<b>Total</b>	<b>500.0</b>	<b>500.0</b>	<b>0.0</b>	<b>0.0%</b>
<b>Supplemental Funding</b>				
Armed Forces	100.0	100.0	0.0	0.0%
Education	100.0	100.0	0.0	0.0%
Health	100.0	100.0	0.0	0.0%
Transportation	100.0	100.0	0.0	0.0%
Other	100.0	100.0	0.0	0.0%
<b>Total</b>	<b>500.0</b>	<b>500.0</b>	<b>0.0</b>	<b>0.0%</b>
<b>Grand Total</b>	<b>1,000.0</b>	<b>1,000.0</b>	<b>0.0</b>	<b>0.0%</b>

## Looking towards the future...

### Positives:

- Overall, we cut a large part of the world's nuclear arsenal
  - From 70,300 in 1986 to 14,900 in early 2017
- In the last 8 years, we have reduced U.S. and Russian arsenals; we can and should continue to do so!

### Perspective that nuclear proliferation is inevitable?



"Such fatalism is a deadly adversary. For if we believe that the spread of nuclear weapons is inevitable, then in some way we are admitting to ourselves that the use of nuclear weapons is inevitable." – Obama, 2009 Prague speech

## How can YOU make a difference?

### Educate yourself:

- Countdown to Zero movie
- Do your research



### Participate:

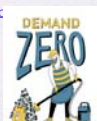
- Activism/Marches/Protest
- Contact your Representative, write to Trump, make your voice heard
- Join orgs that seek to eliminate nuclear weapons (GZ, ICAN)



## Resources



- List of anti-nuclear orgs: [https://en.wikipedia.org/wiki/Anti-nuclear\\_organizations](https://en.wikipedia.org/wiki/Anti-nuclear_organizations)
- Nuclear Blast site map: <https://nuclearsecrecy.com/nukemap/>
- Status of World Nukes: <https://fas.org/issues/nuclear-weapons/status-world-nuclear-forces/>
- Animation of how powerful nukes have become: <https://t.co/MKk2A3zrEY>
- UN Secretary General Ban Ki-Moon on nukes: <https://vimeo.com/26176369>
- How young people get involved: <https://vimeo.com/25716425>
- Global Nuclear Security: <http://www.nti.org/about/global-nuclear-policy/>
- Nuclear Terrorist Threat Bigger Than You Think (CNN): <http://www.cnn.com/2016/04/01/opinions/nuclear-terrorist-threat-cirincione/>
- U.S. deploys anti-missile system in South Korea: <http://www.reuters.com/northkorea-missiles-kcna-idUSKBN16D2MC>
- Hibakusha Short Film about Hiroshima Experience: <https://youtu.be/pYmW-6MV7GM>



## Whatever you do... DON'T LOSE HOPE!

- You are the future generation
- You have a voice; USE IT
- You can make a difference



Thank you!  
Claudia Cheffs  
ccheffs@gmail.com

A faint, light gray world map is visible in the background, showing the continents and a grid of latitude and longitude lines.

We hope you enjoyed this preview of

## **HOT TOPICS & HOT SPOTS**

For a complete edition, please contact:

**Stephanie Hertel**

---

Director, Global Connect @ UCI

Phone: (949) 824-9407

Email: [shertel@uci.edu](mailto:shertel@uci.edu)