www.iup.edu/iupgencyber

IUP's 2018 Combination GenCyber Camp

JUNE 18 TO JUNE 22, 2018

IUP GENCYBER: CYBERSECURITY CAMP FOR MIDDLE AND HIGH SCHOOL STUDENTS

- Learn detailed information about cybersecurity basics
- Learn hacking defense techniques
- Acquire skills to land your dream job
- Do any of the topics interest you? Apply today at www.iup.edu/iupgencyber

Through this opportunity, you will learn safe online behavior, increase knowledge of cyberspace, and explore cybersecurity careers.

Advantages*

Offered at no cost!

Sphero Ollie Robot for each participant!

FREE lunch and afternoon snack!

Instruction and mentorship from IUP faculty and other experts!

Skills and knowledge for a growing career field!

Apply NOW space is limited!

Questions?

gen-cyber@iup.edu

Location:

IUP main Campus

Project PI and Co-PI

Waleed Farag, PhD
PI - Computer Science

Soundararajan Ezekiel, PhD
Co-PI - Computer Science

*program is contingent on funding released by NSA

www.iup.edu/iupgencyber

IUP's 2018 Combination GenCyber Camp

JUNE 18 TO JUNE 22, 2018

IUP GENCYBER: CYBERSECURITY CAMP FOR MIDDLE AND HIGH SCHOOL TEACHERS

- Learn detailed information about cybersecurity
- Learn about promising careers for students
- Acquire skills to change the future of your students
- Do any of the topics interest you? Apply today by visiting www.iup.edu/iupgencyber

Through this opportunity, you will learn safe online behavior, become part of the solution to the nation's shortage of skilled cybersecurity professionals, and help inspire young people to join the field

Advantages*

Offered at no cost!

$500 stipend for each participant!

Act 48 Credits

FREE lunch and afternoon snack!

Mileage reimbursement for those who qualify

Multidisciplinary cybersecurity teaching skills, and modules to be used in the classroom!

Apply NOW space is limited!

Questions?

gen-cyber@iup.edu

Location:

IUP main Campus

Project PI and Co-PI

Waleed Farag, PhD
PI - Computer Science

Soundararajan Ezekiel, PhD
Co-PI - Computer Science

*program is contingent on funding released by NSA

ADVANTAGES FOR STUDENTS

- Offered at no cost!
- Sphero Ollie Robot for each participant!
- FREE lunch and afternoon snack!
- Instruction and mentorship from IUP faculty and other experts!
- Skills and knowledge for a growing career field!

ADVANTAGES FOR TEACHERS

- Offered at no cost!
- $500 Stipend for each participant!
- FREE lunch and afternoon snack!
- ACT 48 Credits!
- Mileage reimbursement for those who qualify!
- Multidisciplinary cybersecurity teaching, skills, and modules to be used in class!

HOW TO APPLY

Applications are accepted online only. To apply or view other important information, please visist:

www.iup.edu/iupgencyber

CAMP DATES

Combination Camp
(Middle and High School Students and Teachers)
June 18 to June 22, 2018

CONTACT INFORMATION

Dr. Waleed Farag
Professor of Computer Science
E-mail: farag@iup.edu

Dr. Soundararajan Ezekiel
Professor of Computer Science
E-mail: sezekiel@iup.edu

Proudly affilliated with

IUP NSF NSA GenCyber

Summer 2018 GenCyber Camp

PRESENTED BY IUP AND NSA

IUP GENCYBER

SUMMER 2018 PROGRAM

Gen Cyber is a new national initiative that is supported by the National Science Foundation and the National Security Foundation. This program has the following objectives:

- Increase interest in cybersecurity careers and diversity in the cybersecurity workforce of the nation.
- Help all students understand correct and safe on-line behavior.
- Improve teaching methods for delivering cybersecurity content for K-12 curricula.

THE FUNDED GRANT

Under the leadership of Dr. Waleed Farag, grant PI, IUP, along with a selected group of national universities, has been awarded funding to hold a combination summer camp for middle and high school students and teachers.

For the third year in a row, the funded project titled "Cultivating a Strong Cybersecurity Culture in Western PA through a Holistic Multidisciplinary Approach" proposes an interesting, novel, and multidisciplinary approach to foster interest in cybersecurity among middle and high school students and teachers in western Pennsylvania.

CAMP PROGRAM SUMMARY

This project will host a FREE (no cost to participants), five-weekday day-camp held June 18-22, 2018. Instruction will be delivered by a team of professors and high/middle school teachers with numerous backgrounds but established expertise in cybersecurity teaching, research, and K-12 education.
Camp will include:

- An engaging content delivery approach that includes direct instruction, group activites, structured discovery, and hands-on laboratory.
- 90 teaching hours proposed (30 for each group at a rate of six hours per day).
- 55 projected participants. 20 middle school students, 20 high school students, and 15 teachers.
- Upon completion of camp, participants will have a strong understanding of cybersecurity in addition to mastering basic skills that help them be safer online.

CYBERSECURITY CAMP DAILY SCHEDULE — DAY 1 - JUNE 18, 2018

	Middle School Students	High School Students	Teachers
9:00 a.m. to 9:50 a.m.	Welcome, Introduction to team members, orientation and logistics Cybersecurity First Priniciples - Dr. Farag - HSS 126		
9:50 a.m. to 10:00 a.m.	BREAK		
10:00 a.m. to 10:50 a.m.	Welcome, Introduction to team members, orientation and logistics Cybersecurity First Priniciples - Dr. Farag - HSS 126		
10:50 a.m. to 11:00 a.m.	BREAK		
11:00 a.m. to 11:50 a.m.	Tynker Coding Mr. Stewart -- 107A Stright Hall	Robot Programming I Using KOOV Dr. Rodger -- 112A Stright Hall	Engaging Non-Tech Ways to teach Cyber Security Priniciples Mrs. Gentile -- 331/320 Stright Hall
11:50 a.m. to 1:00 p.m.	LUNCH - Stright 112B		
1:00 p.m. to 1:50 p.m.	Tynker Coding Mr. Stewart -- 107A Stright Hall	Robot Programming I Using KOOV Dr. Rodger -- 112A Stright Hall	Engaging Non-Tech Ways to teach Cyber Security Priniciples Mrs. Gentile -- 331/320 Stright Hall
1:50 p.m. to 2:00 p.m.	BREAK		
2:00 p.m. to 2:50 p.m.	Robot Programming I Using KOOV Dr. Rodger -- 112A Stright Hall	Networking Security and Password Cracking - Dr. Ezekiel -- 107A Stright Hall	Tynker Coding Mr. Stewart -- 320 Stright Hall
2:50 p.m. to 3:10 p.m.	SNACK BREAK - Stright 112B		
3:10 p.m. to 4:00 p.m.	Robot Programming I Using KOOV Dr. Rodger -- 112A Stright Hall	Networking Security and Password Cracking - Dr. Ezekiel -- 107A Stright Hall	Tynker Coding Mr. Stewart -- 320 Stright Hall

CYBERSECURITY CAMP DAILY SCHEDULE — DAY 2 - JUNE 19, 2018

	Middle School Students	High School Students	Teachers
9:00 a.m. to 9:50 a.m.	Digital Forensics Investigation Dr. Ezekiel - 107A Stright Hall	Intro to Programming and Cybersecurity Dr. Farag - 320 Stright Hall	Strategies to Decrease Cyberbullying Dr. Phillips-Shyrock - 112A Stright Hall
9:50 a.m. to 10:00 a.m.	BREAK		
10:00 a.m. to 10:50 a.m.	Digital Forensics Investigation Dr. Ezekiel - 107A Stright Hall	Intro to Programming and Cybersecurity Dr. Farag - 320 Stright Hall	Strategies to Decrease Cyberbullying Dr. Phillips-Shyrock - 112A Stright Hall
10:50 a.m. to 11:00 a.m.	BREAK		
11:00 a.m. to 11:50 a.m.	Robot Programming II Using KOOV Dr. Rodger -- 112A Stright Hall/ Outdoor	Blockchain Technology Mr. Stewart - 107A Stright Hall	Exploring Online Cybersecurity Resources Mrs. Gentile -- 320 Stright Hall
11:50 a.m. to 1:00 p.m.	WORKING LUNCH - HSS 126 with Guest Speaker Rear Admiral Norman Hayes		
1:00 p.m. to 1:50 p.m.	Robot Programming II Using KOOV Dr. Rodger -- 112A Stright Hall/ Outdoor	Blockchain Technology Mr. Stewart - 107A Stright Hall	Exploring Online Cybersecurity Resources Mrs. Gentile -- 320 Stright Hall
1:50 p.m. to 2:00 p.m.	BREAK		
2:00 p.m. to 2:50 p.m.	Applications of Ollie Robots Dr. Farag - 320 Stright Hall/ Outdoor	Robot Programming II Using KOOV Dr. Rodger - 112A Stright Hall/ Outdoors	Blockchain Technology Mr. Stewart - 107A Stright Hall
2:50 p.m. to 3:10 p.m.	SNACK BREAK - Stright 112B		
3:10 p.m. to 4:00 p.m.	Applications of Ollie Robots Dr. Farag - 320 Stright Hall/ Outdoor	Robot Programming II Using KOOV Dr. Rodger - 112A Stright Hall/ Outdoors	Blockchain Technology Mr. Stewart - 107A Stright Hall

CYBERSECURITY CAMP DAILY SCHEDULE — DAY 3 - JUNE 20, 2018

	Middle School Students	High School Students	Teachers
9:00 a.m. to 9:50 a.m.	Putting GenCyber Priniciples into Practice in All Subjects and All Grades Mrs. Gentile / Mr. Stewart - 112A/B Stright Hall		
9:50 a.m. to 10:00 a.m.	BREAK		
10:00 a.m. to 10:50 a.m.	Putting GenCyber Priniciples into Practive in All Subjects and All Grades Mrs. Gentile / Mr. Stewart - 112A/B Stright Hall		
10:50 a.m. to 11:00 a.m.	BREAK		
11:00 a.m. to 11:50 a.m.	Network Security and Password Cracking - Dr. Ezekiel - 107A Stright Hall	Applications of Ollie Robots Dr. Farag - HSS 126 / Outdoor	Perfecting the Plan (Lesson plans development session I) Mrs. Gentile - 320 Stright Hall
11:50 a.m. to 1:00 p.m.	WORKING LUNCH - HSS 126 with Guest Speaker Ms. Lisa Schlosser		
1:00 p.m. to 1:50 p.m.	Network Security and Password Cracking - Dr. Ezekiel - 107A Stright Hall	Applications of Ollie Robots Dr. Farag - HSS 126/ Outdoor	Perfecting the Plan (Lesson plans development session I) Mrs. Gentile - 320 Stright Hall
1:50 p.m. to 2:00 p.m.	BREAK		
2:00 p.m. to 2:50 p.m.	Intro to Programming and Cybersecurity Dr. Farag -- 320 Stright Hall	Digital Forensics Investigation Dr. Ezekiel - 107A Stright Hall	Robot Programming I Using KOOV Dr. Rodger - 320 Stright Hall
2:50 p.m. to 3:10 p.m.	BREAK - Stright 112B		
3:10 p.m. to 4:00 p.m.	Intro to Programming and Cybersecurity Dr. Farag -- 320 Stright Hall	Digital Forensics Investigation Dr. Ezekiel - 107A Stright Hall	Robot Programming I Using KOOV Dr. Rodger - 320 Stright Hall

CYBERSECURITY CAMP DAILY SCHEDULE — DAY 4 - JUNE 21, 2018

	Middle School Students	High School Students	Teachers
9:00 a.m. to 9:50 a.m.	Intro to Cryptography Dr. Ali - 107A Stright Hall	Intro to SQL and College Trends in Data-Based Majors Gentile - 320 Stright Hall	Education Use of Raspberry Pi Dr. Farag - 112A Stright Hall
9:50 a.m. to 10:00 a.m.	BREAK		
10:00 a.m. to 10:50 a.m.	Intro to Cryptography Dr. Ali - 107A Stright Hall	Intro to SQL and College Trends in Data-Based Majors Gentile - 320 Stright Hall	Education Use of Raspberry Pi Dr. Farag - 112A Stright Hall
10:50 a.m. to 11:00 a.m.	BREAK		
11:00 a.m. to 11:50 a.m.	Networking / Nodes Mr. Stewart -- 112A Stright Hall	Intro to Computer Graphics Dr. Ezekiel - 320 Stright Hall	Intro to Cryptography Dr. Ali - 107A Stright Hall
11:50 a.m. to 1:00 p.m.	LUNCH - Folgers Dining Hall		
1:00 p.m. to 1:50 p.m.	Networking / Nodes Mr. Stewart -- 112A Stright Hall	Intro to Computer Graphics Dr. Ezekiel - 320 Stright Hall	Intro to Cryptography Dr. Ali - 107A Stright Hall
1:50 p.m. to 2:00 p.m.	BREAK		
2:00 p.m. to 2:50 p.m.	Intro to Computer Graphics Dr. Ezekiel - 320 Stright Hall	Intro to Cryptography Dr. Ali - 107A Stright Hall	Perfecting the Plan (Lesson plans development session II) Mr. Stewart -- 112A Stright Hall
2:50 p.m. to 3:10 p.m.	BREAK - Stright 112B		
3:10 p.m. to 4:00 p.m.	Intro to Computer Graphics Dr. Ezekiel - 320 Stright Hall	Intro to Cryptography Dr. Ali - 107A Stright Hall	Perfecting the Plan (Lesson plans development session II) Mr. Stewart -- 112A Stright Hall

CYBERSECURITY CAMP DAILY SCHEDULE

DAY 5 - JUNE 22, 2018

	Middle School Students	High School Students	Teachers
9:00 a.m. to 9:50 a.m.	Cyber Knowledge Fair Mrs. Gentile / Mr. Stewart - 112A/B Stright Hall		
9:50 a.m. to 10:00 a.m.	BREAK		
10:00 a.m. to 10:50 a.m.	Cyber Knowledge Fair Mrs. Gentile / Mr. Stewart - 112A/B Stright Hall		
10:50 a.m. to 11:00 a.m.	BREAK		
11:00 a.m. to 11:50 a.m.	Competition/ Scavenger Hunt Dr. Fiddner - HSS 126/Outdoor		
11:50 a.m. to 1:00 p.m.	LUNCH - Folgers Dining Hall		
1:00 p.m. to 1:50 p.m.	Competition/ Scavenger Hunt Dr. Fiddner - HSS 126/Outdoor		
1:50 p.m. to 2:00 p.m.	BREAK		
2:00 p.m. to 2:50 p.m.	Competition/ Scavenger Hunt Dr. Fiddner - HSS 126/Outdoor		
2:50 p.m. to 3:10 p.m.	BREAK - Stright 112B		
3:10 p.m. to 4:00 p.m.	Post camp surveys/ certificates award Stright Hall 112A/B		

Lesson Plan*

LESSON TITLE: Blockchain Technology

SUMMARY:

Students will learn the basic concepts of blockchain technology and the impact on cybersecurity through an inquiry based approach to learning. Even though this technology is almost 10 years old, blockchain is still relatively new with many not fully utilizing or understanding how it works and how it could potentially be disruptive. In this lesson, students will be assigned to a group to explore one of the five largest cryptocurrencies and create a presentation that provides general information about its purpose and what users need to know to protect their accounts.

GRADE BAND:

- ☐ K-2
- ☐ 3-5
- ☐ 6-8
- ☑ High School

TIME REQUIRED:

80 minutes

LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:

Outcome Examples

Design/Build Test/Defend Compare/Contrast Apply/Use Explain/Discuss Identify/Describe	Students will research one form of blockchain technology and how it relates to cryptocurrency. Students will design a presentation that share key information about the assigned blockchain technology and share it with their peers.

Materials List (i.e., string, digital diary, raspberry pi, web link, drone):

Computer Lab

Describe any Previous Knowledge that may be Required:

While blockchain technology is a relatively new concept for many, this lesson is designed to give students a general overview. This lesson is designed for novice blockchain learners so previous experience is not necessary.

How will you facilitate the learning?

- Describe the Warm-up Activity:

Students will complete a simple accounting word problem and share their answers with a partner. A class discussion will occur to ensure that each student has the correct answer.

- Describe the Focused Activity:

This lesson will be designed around the pedagogical strategy of Self Organized Learning Environments (SOLE), where the teacher will begin the lesson with a set of questions. Students will then be assigned to groups and be expected to design a presentation and share it with their class. In this lesson, the teacher will post questions about Blockchain/Cryptocurrencies. Students will be assigned to groups of 3 and will collaborate to answer the questions through online research. Each group will be assigned 1 of the 6 largest cryptocurrencies. After obtaining the answers they will design a presentation that will be shared with the class. Approximately 35 minutes will be given for students to conduct their research and create the presentation. Following this time, students will then share their presentations with the class.

- Describe the Teacher Instruction:

The lesson will begin with a brief overview of Blockchain technology and how it relates to accounting. The teacher will then introduce the concept of Self Organized Learning Environment to the students and explain that today they will be utilizing this method to learn about blockchain technology and how it relates to the cybersecurity principles.
Students will work in groups to design a presentation on an assigned cryptocurrency that will be shared with the class. Their presentation will be completed using a presentation software of their choice. Google Slides or Powerpoint is preferred. Within the presentation, students will share its origin, purpose, value, how it is obtained and traded, and what users can store and protect their information. The teacher will facililtate student groups through their research and presentation design.

Mapping to Cyber Security First Principles:

- ☑ **Domain Separation**
- ☑ **Process Isolation**
- ☑ **Resource Encapsulation**
- ☑ **Modularity**
- ☑ **Least Privilege**
- ☑ **Abstraction**
- ☑ **Data Hiding**
- ☑ **Layering**
- ☑ **Simplicity**
- ☑ **Minimization**

Assessment of Learning:

TYPE (Examples listed below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	Students will design a presentation on blockchain technology and share it with their peers. The presentation will feature one type of cryptocurrency.

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Students will receive differentiated instruction based on their overall level of experience.
Students will work in a group to assist in research and presentation design.

Describe any Extension Activities (i.e., ideas for further work):

Students will have the opportunity to extend their learning by including details about market conditions and predications about future impacts of the technology.

Acknowledgements:

Lesson Plan*

LESSON TITLE: Intro to Cybersecurity and Password Cracking

SUMMARY:

The students will have a brief lesson on what Cybersecurity is, the difference between a cybercriminal and a security researcher, and how to stay safe on the Internet. Then, they will have a lab teaching them some basic Linux terminal commands, as well as the basics of password cracking, demonstrating the importance of a strong passwords.

GRADE BAND:

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

TIME REQUIRED:

120 minutes

LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:

Outcome Examples

Design/Build Test/Defend Compare/Contrast Apply/Use Explain/Discuss Identify/Describe	understand Cybersecurity fundamentals Be familiar with basic Internet Safety approach. Use Linux terminal commands Experiment with Password cracking software. Comprehend the importance of a strong password

Materials List (i.e., string, digital diary, raspberry pi, web link, drone):

Computer, virtual machine with Kali Linux.

Describe any Previous Knowledge that may be Required:

No previous knowledge required, instructor will be walk them through the steps.

How will you facilitate the learning?

- Describe the Warm-up Activity:

The students will begin with a short introduction to the field of computer science, including computer hardware components, and operating systems. They will then be taught the basics of cybersecurity as a profession, the hacker mindset and necessity of consent to research vulnerabilities. The level presentation will go further in-depth into the criminology of cybercrime, the differences between cybercriminals and security researchers, and hacker culture.

- Describe the Focused Activity:

Students will be taught how to create a virtual machine and boot into a Linux environment. They will then be introduced to several key commands used to navigate the Linux terminal. They will create a dummy user with a weak password, such as "Password1", a single word, etc. Then they will be taught a brief introduction to cryptography and hashing, where passwords are stored in the Linux registry, how to extract the password hash, and how to use a password cracking tool to break the password.

Instructor will use a brief PowerPoint to explain some basic cybersecurity concepts. Then the absolute majority of this session time will be a lab in which the instructor will aid students in setting up and explaining what various terminal commands do and how password cracking software works.

- Describe the Teacher Instruction:

N/A

Mapping to Cyber Security First Principles:

- [ ] **Domain Separation**
- [ ] **Process Isolation**
- [ ] **Resource Encapsulation**
- [ ] **Modularity**
- [x] **Least Privilege**
- [ ] **Abstraction**
- [x] **Data Hiding**
- [x] **Layering**
- [x] **Simplicity**
- [ ] **Minimization**

Assessment of Learning:

TYPE (Examples listed below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	The assessment will be a short project for the students to complete. The instructor will also go around the room making sure the students understand what to do and give help if necessary.

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

The lecture and lines of code for the project will be projected on the board via a PowerPoint so students who are hearing impaired will be able to read. Important commands are added to a short list in the corner of the screen.

Describe any Extension Activities (i.e., ideas for further work):

Students will be encouraged to experiment with different length and complexity passwords, and may do so if there is time left.

Acknowledgements:

Lesson Plan*

LESSON TITLE: Digital Forensics

SUMMARY:

1. Understanding the basic concepts of Digital forensics
2. Understanding the advantages of Meta Data
3. Mini challenge on finding the evidence from the meta-data of images

GRADE BAND:

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

TIME REQUIRED:

120.000 minutes

LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:

Outcome Examples

Design/Build Test/Defend Compare/Contrast Apply/Use Explain/Discuss Identify/Describe	Understand what digital forensics is and what it is used for. Describe how digital evidence is acquired and analyzed. Explain/Discuss the advantages of meta-data. Apply/Use ExifTool tool to find evidence on images. Use data recovery tools to recover deleted data.

Materials List (i.e., string, digital diary, raspberry pi, web link, drone):

Web links
Digital Forensics - https://www.youtube.com/watch?v=Pf-JnQfAEew
Meta Data explained - https://www.youtube.com/watch?v=xP_e56DsymA
Exiftool - http://manpages.ubuntu.com/manpages/trusty/man1/exif.1.html

Describe any Previous Knowledge that may be Required:

Basic math and problem solving skills.

How will you facilitate the learning?

- Describe the Warm-up Activity:

Using discussion-based and hands-on leaning approaches to explain the below concepts. Moreover, we will show various examples to demonstrate how meta data is used in Facebook, Google photos and forensic analysis.
i) What is meta data.
ii) Its advantages
iii) How it is used.

- Describe the Focused Activity:

Data Recovery:
The students are asked to install the data recovery software (Recuva in the virtual machine).
A folder is created with various random images and files.
The students are asked to delete all the files present in the folder.
With the help of the software they are asked to recover the accidentally deleted files.

Challenge:
The students have to use ExifTool to find the location of the images provided. They also have to plot the coordinates in chronological order in Google map. This is a group activity consisting of 4 students per group. The students will be provided with around 18 images.

Explained how a chain of custody is used in an investigation.
Described how digital evidence is analyzed from the meta data in a way that is acceptable for legal proceedings.
Gave instructions on how to install Recuva in the virtual machine.
Demonstrated the data recovery process on the screen.
Demonstrated the ExifTool with an example.

- Describe the Teacher Instruction:

N/A

Mapping to Cyber Security First Principles:

- ☐ **Domain Separation**
- ☐ **Process Isolation**
- ☑ **Resource Encapsulation**
- ☐ **Modularity**
- ☐ **Least Privilege**
- ☐ **Abstraction**
- ☐ **Data Hiding**
- ☑ **Layering**
- ☑ **Simplicity**
- ☐ **Minimization**

Assessment of Learning:

TYPE (Examples listed below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	The instructor and TAs will observe all participants while the activity are being performed. The instructor and TAs will walk around to see how different group are doing. The instructor and TAs will ask oral questions when needed to ensure the students understand what they are doing and why there are doing it. The instructor and TAs will make sure all group members are engaged in the activity. The students will be asked to present their final results.

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

None of our campers need special accomodation

Describe any Extension Activities (i.e., ideas for further work):

The activity could be extended to include more images and different scenarios.

Acknowledgements:

Lesson Plan*

LESSON TITLE: Intro to Programming and Cybersecurity

SUMMARY:

This module introduces the basics of computer programming: variables and data types, expressions, decision making, loops, arrays, and protective programming approaches (input validations and boundary checking) with Java and Eclipse and MS .NET as the programming languages/IDEs. The module starts with problem solving and algorithm development addressing modularity and design simplicity as essential FP. The module builds on the basic mathematical knowledge that middle/high school students normally have and effectively links this knowledge to programming concepts such as expression evaluation, precedence, and use of comparative operators to form logical expressions

GRADE BAND:

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

TIME REQUIRED:

120 minutes

LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:

Outcome Examples

Design/Build Test/Defend Compare/Contrast Apply/Use Explain/Discuss Identify/Describe	1. Demonstrate in-depth understanding of the cybersecurity First Principles. 4. Have a better understanding of essential problem solving and programming concepts. 5. Apply programming knowledge and skills to design and implement reliable software systems that takes into account software assurance concepts.

Materials List (i.e., string, digital diary, raspberry pi, web link, drone):

Lab Computers
Eclipse IDE
.NET Visual Studio IDE
Lab Handouts

Describe any Previous Knowledge that may be Required:

Basic Math and problem solving skills.

How will you facilitate the learning?

- Describe the Warm-up Activity:

This module will be taught in a highly interactive environment in which all attendees will be active participants in the learning process. One approach to start up the module is to use a lab-based activities (editing, compiling, running and debugging a number of programs) that allow hands-on learning, and enhances each student's comprehension of taught contents, making them positive contributors to the learning process. Another effective approach is the use of competitive, interactive quizzes via online services such as Kahoot and Quizizz. Students are focused and engaged during lessons to ensure they

- Describe the Focused Activity:

-Discussion of programming basics basics (variables and data types, expressions, decision making, loops, arrays).
-Discussion of protective programming approaches (input validations and boundary checking)
-Students will be involved in editing and running a number of Java and C++ programs
-Kahoot Quiz on programming basics
-Delivering customized modules to each group (more challenging labs will be given to high school students).

- Describe the Teacher Instruction:

N/A

Mapping to Cyber Security First Principles:

- ☐ **Domain Separation**
- ☑ **Process Isolation**
- ☐ **Resource Encapsulation**
- ☑ **Modularity**
- ☐ **Least Privilege**
- ☑ **Abstraction**
- ☐ **Data Hiding**
- ☑ **Layering**
- ☑ **Simplicity**
- ☑ **Minimization**

Assessment of Learning:

TYPE (Examples listed below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	A number of assessment approaches will be adopted: 1- Regular observation of campers performance in the given tasks 2- Interactive competitive quizzes as discussed above. 3- Oral questions and walking around.

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

N/A

Describe any Extension Activities (i.e., ideas for further work):

N/A

Acknowledgements:

Lesson Plan*

LESSON TITLE: Applications of Ollie Robots

SUMMARY:

In this module students will use the Sphero Edu App with a coding block style program development to develop programs for the Sphero Ollie Robots. They can download this app for free and allows them to automatically set paths for their robot to follow, they can change the lights on the robot, and also gain information from the robots.

GRADE BAND:

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

TIME REQUIRED:

120 minutes

LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:

Outcome Examples

Design/Build Test/Defend Compare/Contrast Apply/Use Explain/Discuss Identify/Describe	1. Demonstrate in-depth understanding of the cybersecurity First Principles. 4. Have a better understanding of essential problem solving and programming concepts. 5. Apply programming knowledge and skills to design and implement programs that can solve simple real world problems like controlling a Robot and navigating a maze.

Materials List (i.e., string, digital diary, raspberry pi, web link, drone):

Describe any Previous Knowledge that may be Required:

A background with programming or block coding development (Such as Scratch)

How will you facilitate the learning?

- Describe the Warm-up Activity:

Students will learn the basics of programming using the Sphero Edu app. They will develop sample programs that move the robot forward and backward. They will develop another program that moves the robot in a square. This section teaches them the basics in order to prepare them for the second project.

- Describe the Focused Activity:

This activity is all about programming the Ollie robot to navigate a maze. In these section the students will break up into groups in order to think through the programming logic. As they develop their programs they will get active feedback from other students, and the teachers there.

The role of the teacher is to explain what the Sphero Ollie is and how to download and install the Sphero Edu app. This will allow the students to develop programs to control the robots. The teachers will also show and demonstrate some sample programs. This activity is hands-on and is designed for open discussion and the answering of students questions.

- Describe the Teacher Instruction:

N/A

Mapping to Cyber Security First Principles:

- ☐ **Domain Separation**
- ☐ **Process Isolation**
- ☐ **Resource Encapsulation**
- ☑ **Modularity**
- ☐ **Least Privilege**
- ☑ **Abstraction**
- ☐ **Data Hiding**
- ☑ **Layering**
- ☑ **Simplicity**
- ☑ **Minimization**

Assessment of Learning:

TYPE (Examples listed below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	Students will complete a project to navigate a robot automatically through a maze. They will be observed through the instructor and assistants. This allows for discussion and instant feedback to each of the groups.

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Accommodations will be made on a case by case basis.

Describe any Extension Activities (i.e., ideas for further work):

The development of more programs to control the Ollie robots.

Acknowledgements:

Lesson Plan*

LESSON TITLE: Tynker

SUMMARY:

Students will learn how to create an interactive program using block based coding within the Tynker software program. Block based coding requires students to use logic and sequencing to create a workable and meaningful program. Although block based coding is not a formal coding practice, it is a perfect and age appropriate method for novice programmers. In this lesson, students will design a program that requires the user to answer a question. To accomplish this task, students will need to use a variety of coding concepts and skills to successfully build the project. At the conclusion, they should have a workable program that will provide users the ability to answer a question pertaining to the topic.

GRADE BAND:

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☐ High School

TIME REQUIRED:

80 minutes

LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:

Outcome Examples

Design/Build Test/Defend Compare/Contrast Apply/Use Explain/Discuss Identify/Describe	Students will be able to design an interactive program involving the cybersecurity principles, using the block based language Tynker. Their program will involve multiple blocks including loops, conditions, and events in order to design a robust program that meets the lesson objective. At the conclusion of the lesson, each student will have a greater understanding of the cybersecurity principles and computational thinking.

Materials List (i.e., string, digital diary, raspberry pi, web link, drone):

Describe any Previous Knowledge that may be Required:

This lesson is designed for novice learners so an advanced background is unnecessary. It would beneficial for students to have some experience with logic puzzles through programs like the Hour of Code, however it is not required. The teacher will differentiate the instruction by offering more guidance and assistance to students who have limited experience.

How will you facilitate the learning?

- Describe the Warm-up Activity:

Students will begin the lesson by completing a Quizlet match activity that features the cybersecurity principles. Students will be encouraged to play the match activity multiple times to help review the key cybersecurity principles.

- Describe the Focused Activity:

Students will be assigned to create an interactive program that asks a multiple choice question pertaining to the cybersecurity principles. The program should be constructed with conditions, loops, and events that ensure that the user will need to answer correctly to move to the next question. Students will have flexibility within the assignment to use characters and settings of their choice to the meet the objective. The teacher will assign each student a specific cybersecurity principle to feature within their designed program. After the program is created, students have the opportunity to test their peer's projects and attempt to answer the cybersecurity question correctly.

- Describe the Teacher Instruction:

To begin students will be required to create a Tynker account. The teacher will guide them through this process to ensure that all students are on the Tynker site and have an account built. The teacher will then provide a basic demonstration and overview of Tynker by explaining the stage, blocks, and workspace. The teacher will then display an example program that asks the students a multiple choice question pertaining to the cybersecurity principles. A student will be called on to answer the question by typing it into the Tynker program. After students produce and input the correct answer, the teacher will show the students the code used to create the program. At this time, students will learn that they will be designing an interactive program that is similar to the example. Students will have flexibility in the design and creation, but they must meet the project guidelines. The teacher will then distribute a different cybersecurity question to each student. Time will be given for students to design and create their projects. The teacher will serve as a facilitator to assist and guide students' projects. Approximately 30 minutes will be given for student work. Once students have created workable programs, they will be given a handout that lists the cybersecurity principles that will serve as a word bank. Students will then move to each of their peer's programs and attempt to answer the question correctly.

Mapping to Cyber Security First Principles:

- ☑ **Domain Separation**
- ☑ **Process Isolation**
- ☑ **Resource Encapsulation**
- ☑ **Modularity**
- ☑ **Least Privilege**
- ☑ **Abstraction**
- ☑ **Data Hiding**
- ☑ **Layering**
- ☑ **Simplicity**
- ☑ **Minimization**

Assessment of Learning:

TYPE (Examples listed below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	Students will be assessed on their program creation. Each student will have a workable interactive program that reviews a cybersecurity principle. Students will have an opportunity to connect and interact with their peer's programs. This will provide each student with a valuable insight into how their peer's tackled the set objective and may drive their creativity and future problem solving. Although the design is initially independent, students will have the opportunity to learn from their peers.

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Students will receive differentiated instruction based on their overall level of programming experience. If needed, students will have the opportunity to work with a partner.

Describe any Extension Activities (i.e., ideas for further work):

To extend the project students will have the opportunity to create a second interaction in their program that reviews a second cybersecurity principle. After a correct response is given, the program should change the background and character and ask a new cybersecurity question.

Acknowledgements:

Lesson Plan*

LESSON TITLE: Introduction to Cryptography

SUMMARY:

1. Learning a brief history of cryptography (encryption/decryption)
2. Understanding the basic concepts of cryptography
3. Learning several basic cryptographic techniques
4. Hand-on practice on encryption/decryption using online tools

GRADE BAND:

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

TIME REQUIRED: 120 minutes

LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:

Outcome Examples

Design/Build Test/Defend Compare/Contrast Apply/Use Explain/Discuss Identify/Describe	Understand of the basics of cryptography Learn why cryptography has been used from ancient to modern time Learn various methods of encryption and decryption Learn the significance of encryption and decryption

Materials List (i.e., string, digital diary, raspberry pi, web link, drone):

Web Links:
Navajo Code Talker Died, June 13, 2018:
https://nowthisnews.com/videos/news/one-of-the-last-living-navajo-code-talkers-from-wwii-passed-away
Cryptography in 60 Seconds: https://www.youtube.com/watch?v=j5fOynJrNOk
Simple Cryptography: https://www.youtube.com/watch?v=sz0AQYLi4k

Describe any Previous Knowledge that may be Required:

Knowledge of Mathematics, Pre-Algebra, and Algebra

How will you facilitate the learning?

- Describe the Warm-up Activity:

1. Explaining and discussing the basics of cryptography
2. Brief discussion on the history of cryptography from Egypt to modern time
3. What are encryption and decryption and how they are performed
4. Difference between private and public key cryptography
4. Hand-on practices on various cryptographic techniques using online tools

- Describe the Focused Activity:

Hand-on Practices:
The students are asked to practice on various cryptographic techniques, such as Caesar Cipher, DES, AES, Private-key cryptography, Public-key cryptography using tools available online. They will encrypt a message (a plain text) into cipher text and again decrypt the cipher text back to the plain text.

Challenge:
The students are provided with a cipher text and are asked to decrypt it (if they can) to the plain text using brute force technique.

- Describe the Teacher Instruction:

N/A

Mapping to Cyber Security First Principles:

- ☐ **Domain Separation**
- ☐ **Process Isolation**
- ☐ **Resource Encapsulation**
- ☐ **Modularity**
- ☑ **Least Privilege**
- ☑ **Abstraction**
- ☑ **Data Hiding**
- ☑ **Layering**
- ☐ **Simplicity**
- ☐ **Minimization**

Assessment of Learning:

TYPE (Examples listed below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	The instructor and TAs made observation while the activity was being performed. The instructor and TAs walked around to observe how different group are performing. The instructor and TAs asked oral questions when needed to ensure the students understood what they were doing and why. The instructor and TAs made sure all group members were engaged in the activities. The students were asked to present their final results.

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

N/A

Describe any Extension Activities (i.e., ideas for further work):

Activities could be extended to include more examples on decryption if students became more curious.

Acknowledgements:

N/A

Mrs. Gentile's and Mr. Stewart's Lesson Plan
I.U.P. GenCyber Combination Camp Merged Session
Friday, June 22, 2018 9:00 - Noon

Lesson Title: Cyber Knowledge Fair

Summary: Students will prepare an 8-minute presentation with teacher assistance to explain technology skills gained during the week in all of the camp's various topics and will explain how to incorporate cyber security principles into their respective topics to other camp participants.

Grade Band:
PK – 12 Teachers, 6-12th graders

Time Required:
Three hours with breaks

Lesson Learning Objectives/Outcomes:
Upon completion of this lesson, students and teachers will be able to:

- Describe technological concepts and devices explored during the week
- Align Cyber Security First Principles to technology topics from the week.

Materials List:
Computers

One set of materials/devices for each group

How will you facilitate the Learning?

9:00 - 9:05 Divide middle and high school students.. Ask all students to select a topic from the week's 8 topics out of a MS hat or HS hat. Students with the same topics will gather together to brainstorm how best to teach that topic to others. (about 2 students/topic) They will be informed that they will present their topics 8 times as we all rotate through the fair.	9:00 - 9:30 Teachers will work together to identify which Cyber-Security Principles match most closely to topics they have learned about during the week (robot programming, raspberry pi, cryptography, block chain technology, cyberbullying, Tynker, networking/nodes, password cracking, digital forensics, computer graphics) Teachers will decide among themselves which student topic they will help to advise
9:05 - 9:45 Students will be given a set of expectations to guide development of their 8-minute presentation for the fair. They must:	9:30 - 9:45 Each teacher will help to advise a group to be sure that they are following the expectations given to them.

1. Intro general uses of the topic 2. Demonstrate the most interesting aspect of the topic! 3. ****Discuss which cyber-security principle(s) is/are addressed in the topic**** 4. Ask questions from audience	Teachers can help to brainstorm how best to present the topics, if students need such support. ****Teachers should verify correct usage of the cyber-security principles.****
9:50 - 10:55 HS groups present topics, while MS groups, teachers, profs rotate among stations (8 min/ station)	
10:55 - 12:00 MS groups present topics, while HS groups, teachers, profs rotate among stations (8 min/ station)	

Mapping to ALL Cyber Security First Principles (ideally):

Domain Separation	**Abstraction**
Process Isolation	**Data Hiding**
Resource Encapsulation	**Layering**
Modularity	**Simplicity**
Least Privilege	**Minimization**

Assessment of Learning:

TYPE:	Name/Description:
Observations	As students share, demonstrate and collaborate
Oral Questioning	As teachers/students ask for clarification on principles
	As observers ask questions of each presentation

Accommodations:

Assistance may be needed for groups without a strong leader, which teachers can provide.

Description of Extension Activities:

Teachers and students in this Gen-Cyber Combination Camp are expected to share knowledge and skills gained this week in their school environments, and hopefully to maintain an interest in Cyber Security- related careers.

Acknowledgements:

Gen-Cyber.com

Mrs. Gentile's Lesson Plan
I.U.P. GenCyber Combination Camp
Thursday, June 21, 2018 9:00-10:50

Lesson Title: Introduction to SQL and College Trends in Data-Based Majors

Summary: Students will explore SQL with a tutorial on Khanacademy. Algorithmic and computational thinking drive their exporation as they complete customizable assessments within Khanacademy. Basic examples of Cyber-Security First Principles will be applied throughout their learning. Discussion of 21st Century skills, digital literacy skills and data literacy skills will lead to discussion of workplace skills and thus trends in college majors.

Grade Band:
9-12th Grade Students

Time Required:
Two 50-minute sessions

Lesson Learning Objectives/Outcomes:

Upon completion of this lesson, students will be able to:

- Apply Cyber-Security Principles to the topics of data management and data analysis in SQL.
- Create simple tables and queries using SQL.
- Understand the importance of certain operators and statements in SQL.
- Identify related careers and college majors to data management and cyber security.

Materials List:

Computers w/Internet
Projection Screen

How will you facilitate the Learning?

Session 1:

1) Using Google Slides, students will be given motivation for learning SQL and other digital literacy skills as an introduction.
2) Students will be asked log into www.khanacademy.org to independent study SQL and progress as far as possible until breaktime. All the while, I will assist them as they work on each challenge.

Session 2:

1) Before students resume their independent study, we will discuss the purposes of using data management systems from their experiences –

whether they realize them or not. (In gaming, for log-in validation, website use, business intelligence, testing computer function).

2) Ask for and/or provide clear examples to the Cyber Security Principles of domain separation, abstraction, data hiding, layering, simplicity and least privilege.
3) Allow students to get as far as they can in their studies with the goal of at least learning how to use CASE statements, if possible.
4) Return to the Google Slide to summarize how SQL fits into software engineering and many related careers.
5) Conclude the lesson with trends in college courses related to cyber-security and data management

Mapping to bold-faced Cyber Security First Principles:

Domain Separation	**Abstraction**
Process Isolation	**Data Hiding**
Resource Encapsulation	**Layering**
Modularity	**Simplicity**
Least Privilege	Minimization

Assessment of Learning:

TYPE:	**Name/Description:**
Observations	On-task completion of SQL challenges
Oral Questioning	Answers to my prompts

Accommodations: Differentiated complexity in khanacademy challenges for more able students, and the use of provided clues or my assistance for students with less experience in coding

Description of Extension Activities: Students will be encouraged to explore further topics in the Khanacademy SQL list specifically, or even in the wealth of computer science and computer programming topics available on Khanacademy.

Acknowledgements:
www.khanacademy.org

Lesson Plan*

LESSON TITLE: Intro to Computer Graphics

SUMMARY:

Demonstrate the basic principles of Computer Science and Computer Graphics. Students will be creating a simple OpenGL program to demonstrate some of the discussed principles.

GRADE BAND:

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

TIME REQUIRED:

120 minutes

LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:

Outcome Examples

Design/Build Test/Defend Compare/Contrast Apply/Use Explain/Discuss Identify/Describe	1. Understand the principles of Computer Science as well as Computer Graphics. 2. Create a simple graphical program in OpenGL. 3. Design and implement a simple Graphical application.

Materials List (i.e., string, digital diary, raspberry pi, web link, drone):

Students will need a cell phone or tablet

Describe any Previous Knowledge that may be Required:

No knowledge is needed, but an understanding of computer architecture and programming is recommended

How will you facilitate the learning?

- Describe the Warm-up Activity:

We plan to have several small activities, including a physical phishing example and a physical look at the inside of computers for students. This will let them learn through activity instead of someone just lecturing them

- Describe the Focused Activity:

We will be having the students create a simple program in OpenGL. We describe it as "simple" because we will have two options for the students to pick. One is a series of lines connected and the other a part of the Sine Function.

Also, we will be using a hands-on approach for the students learning. We plan to have them constantly engaged and moving if possible so I can have their interest.

- Describe the Teacher Instruction:

N/A

Mapping to Cyber Security First Principles:

- [ ] **Domain Separation**
- [ ] **Process Isolation**
- [ ] **Resource Encapsulation**
- [x] **Modularity**
- [ ] **Least Privilege**
- [x] **Abstraction**
- [ ] **Data Hiding**
- [x] **Layering**
- [x] **Simplicity**
- [ ] **Minimization**

Assessment of Learning:

TYPE (Examples listed below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	Walk around. Oral Questioning. Project.

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

N/A

Describe any Extension Activities (i.e., ideas for further work):

Creating models and have a computer render these models. All sources will be cited in the presentation

Acknowledgements:

Lesson Plan*

LESSON TITLE: Robot Programming II Security Module Using KOOV

SUMMARY:

This module presents an easy-to-understand introduction to fundamentals of robotic programming and security. The participants will be introduced to learn to code with KOOV! KOOV is a new and exciting way to introduce robotics and coding to students with a hands on experience. It is also an excellent application for illustrating cybersecurity collaboration and problem solving skills to students. The larger classrooms of 35 students can be put into teams of three to five students with assignments of specific roles for each student on the team.

GRADE BAND:

- ☐ K-2
- ☐ 6-8
- ☐ 3-5
- ☑ High School

TIME REQUIRED: 240 minutes

LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:

Outcome Examples

Design/Build Test/Defend Compare/Contrast Apply/Use Explain/Discuss Identify/Describe	1. Demonstrate substantial understanding of the cybersecurity First Principles. Numbers one, six, seven and eight 2. Explore the use of basic operating systems commands on different platforms. All robot OS can be compromised to alter what they were originally intended for in KOOV.

Materials List (i.e., string, digital diary, raspberry pi, web link, drone):

KOOV Starter kit
Bluetooth enabled computer
Windows environment
IOS Computer
iPad application

Describe any Previous Knowledge that may be Required:

None

How will you facilitate the learning?

- Describe the Warm-up Activity:

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection - Decribe the Teacher Instruction

- Describe the Focused Activity:

1. Make Observations: Show students images of several different types of animals, such as an alligator, a shark, a crab, and a bat. For each animal, ask students to describe the animal's features and their function. How do these features help the animal survive? Prompt students to consider how the animal moves, how it eats, features that keep it warm, etc. (For example, an alligator has four legs to walk on land and a tail that moves to help it swim and balance on land; a crab has 10 legs, eight that help keep it stable on the seafloor in moving water and two that are used to grasp things; a shark has sleek skin, strong jaws, and fins that help it move through the water; a bat has wings to fly; etc.)
2. Link Observations to Engineering: Show students a photo of an airplane. Ask students how they think scientists came up with the idea for the design of an airplane. (It has wings like a bird.) Explain to students that engineers are scientists who design new devices or objects in order to solve problems. Explain that engineers often look to organisms in nature for ideas

- Describe the Teacher Instruction:

OBJECTIVE: Students will gain an understanding of what algorithms are, and how they are translated into coding to drive the actions of computers and computer-controlled objects.
TIME: 30 minutes (60 minutes with lesson extension)
MATERIALS: Pencils or pens, "Step-by-Step" student worksheet
LESSON PLAN
1. Pre-Activity Discussion: What Is Coding?
Ask students to describe some of the actions that we use computers to do. (For example, send emails, play video games, perform calculations, etc.) Ask students how they think the computer performs these complicated tasks. (Students may say that there are computer programs that give computers instructions about what actions to take.) Explain to students that computer programmers rely on algorithms to direct the actions of a computer or a computer-controlled device like a robot. An algorithm is a set of steps that can be followed from start to finish to complete a task. In an algorithm, a complicated action is broken into many small steps. Explain that computer programmers write algorithms for each task a computer needs to do. Then they translate the algorithms into a language that a computer can read and follow. This language is called computer code.
2. Conduct the Activity: Hand out the "Step-by-Step" student worksheet. In the exercise, students will

Mapping to Cyber Security First Principles:

- [x] **Domain Separation**
- [ ] **Process Isolation**
- [x] **Resource Encapsulation**
- [x] **Modularity**
- [ ] **Least Privilege**
- [x] **Abstraction**
- [x] **Data Hiding**
- [ ] **Layering**
- [ ] **Simplicity**
- [ ] **Minimization**

Assessment of Learning:

TYPE (Examples listed below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	Four questions to be used in the Pre/Post assessment survey. 1. The artificial intelligence of the robot has gone “out of control” and the Bluetooth “brain” is not controlling the KOOV. The robot needs to be reprogrammed and it is experiencing which cybersecurity first principle? (A) Domain separation, (B) Process isolation, (C) Resource encapsulation, (D) Abstraction

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

The contents the module will be adapted to better fit the level of each of the proposed three groups. For the teachers group, topics covered will stress how the AI security concepts and techniques can be integrated into the K-12 curriculum in addition to covering advanced concepts such as robotic co-existence with the human world. The contents will also advance in the level of detail when being presented to the Middle school group compared to when being presented to the High school students.

Describe any Extension Activities (i.e., ideas for further work):

This component of the module is designed to use a variety of formative assessment strategies in order to ensure that the students has acceptably achieved the Intended Learning Outcomes (ILOs) of the module. Examples of the proposed techniques are use of discussion, questioning, peer-assessment, and constructive quizzes. For example, a carefully chosen set of questions on the covered topics can form a quiz given at the end of this module. After the students finish the quiz, all quiz questions will be reviewed and proper answers will be identified. This positively contribute to productive discussions in the classroom and increase the chances of students achieving higher degrees of learning.

Acknowledgements:

Four questions to be used in the Pre/Post assessment survey.

1. The artificial intelligence of the robot has gone “out of control” and the Bluetooth “brain” is not controlling the KOOV. The robot needs to be reprogrammed and it is experiencing which cybersecurity first principle?

(A) Domain separation,

Lesson Plan*

LESSON TITLE: Robot Programming I_MS_HS Security Module Using KOOV

SUMMARY:

This module presents an easy-to-understand introduction to fundamentals of robotic programming and security. The participants will be introduced to learn to code with KOOV! KOOV is a new and exciting way to introduce robotics and coding to students with a hands on experience. It is also an excellent application for illustrating cybersecurity collaboration and problem solving skills to students. The larger classrooms of 35 students can be put into teams of three to five students with assignments of specific roles for each student on the team.

GRADE BAND:

- ☐ K-2
- ☐ 6-8
- ☐ 3-5
- ☑ High School

TIME REQUIRED:

240 minutes

LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:

Outcome Examples

Design/Build Test/Defend Compare/Contrast Apply/Use Explain/Discuss Identify/Describe	1. Demonstrate substantial understanding of the cybersecurity First Principles. Numbers one, six, seven and eight 2. Explore the use of basic operating systems commands on different platforms. All robot OS can be compromised to alter what they were originally intended for in KOOV.

Materials List (i.e., string, digital diary, raspberry pi, web link, drone):

KOOV Starter kit
Bluetooth enabled computer
Windows environment
IOS Computer
iPad application

Describe any Previous Knowledge that may be Required:

None

How will you facilitate the learning?

- Describe the Warm-up Activity:

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection - Decribe the Teacher Instruction

- Describe the Focused Activity:

1. Evaluate a Set of Instructions: Tell students that you are going to give them instructions to bake a batch of cookies. Then write the following steps on the classroom board.
• Gather eggs, butter, sugar, flour, baking soda, and chocolate chips.
• Mix ingredients in large bowl.
• Place cookie dough on a pan.
• Bake until done.
Guide students to evaluate your instructions. Ask the class: Do they think a person could successfully bake cookies by following these steps? If 10 people followed these steps, would they all make the exact same cookies? Why or why not? Prompt students to be specific when they describe the limitations of the instructions. (For example: The instructions don't say how much of each ingredient is needed. They don't explain the order in which the ingredients should be added. They don't specify how the dough should be placed on the pan—in balls or as one large layer. The temperature that the cookies should be baked

- Describe the Teacher Instruction:

OBJECTIVE: Students will gain an understanding of what algorithms are, and how they are translated into coding to drive the actions of computers and computer-controlled objects.
TIME: 30 minutes (60 minutes with lesson extension)
MATERIALS: Pencils or pens, "Step-by-Step" student worksheet
LESSON PLAN
1. Pre-Activity Discussion: What Is Coding?
Ask students to describe some of the actions that we use computers to do. (For example, send emails, play video games, perform calculations, etc.) Ask students how they think the computer performs these complicated tasks. (Students may say that there are computer programs that give computers instructions about what actions to take.) Explain to students that computer programmers rely on algorithms to direct the actions of a computer or a computer-controlled device like a robot. An algorithm is a set of steps that can be followed from start to finish to complete a task. In an algorithm, a complicated action is broken into many small steps. Explain that computer programmers write algorithms for each task a computer needs to do. Then they translate the algorithms into a language that a computer can read and follow. This language is called computer code.
2. Conduct the Activity: Hand out the "Step-by-Step" student worksheet. In the exercise, students will

Mapping to Cyber Security First Principles:

- [x] **Domain Separation**
- [ ] **Process Isolation**
- [ ] **Resource Encapsulation**
- [x] **Modularity**
- [ ] **Least Privilege**
- [ ] **Abstraction**
- [x] **Data Hiding**
- [ ] **Layering**
- [ ] **Simplicity**
- [ ] **Minimization**

Assessment of Learning:

TYPE (Examples listed below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	Four questions to be used in the Pre/Post assessment survey. 1. The artificial intelligence of the robot has gone “out of control” and the Bluetooth “brain” is not controlling the KOOV. The robot needs to be reprogrammed and it is experiencing which cybersecurity first principle? (A) Domain separation, (B) Process isolation, (C) Resource encapsulation, (D) Abstraction

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

The contents the module will be adapted to better fit the level of each of the proposed three groups. For the teachers group, topics covered will stress how the AI security concepts and techniques can be integrated into the K-12 curriculum in addition to covering advanced concepts such as robotic co-existence with the human world. The contents will also advance in the level of detail when being presented to the Middle school group compared to when being presented to the High school students.

Describe any Extension Activities (i.e., ideas for further work):

This component of the module is designed to use a variety of formative assessment strategies in order to ensure that the students has acceptably achieved the Intended Learning Outcomes (ILOs) of the module. Examples of the proposed techniques are use of discussion, questioning, peer-assessment, and constructive quizzes. For example, a carefully chosen set of questions on the covered topics can form a quiz given at the end of this module. After the students finish the quiz, all quiz questions will be reviewed and proper answers will be identified. This positively contribute to productive discussions in the classroom and increase the chances of students achieving higher degrees of learning.

Acknowledgements:

Four questions to be used in the Pre/Post assessment survey.

1. The artificial intelligence of the robot has gone “out of control” and the Bluetooth “brain” is not controlling the KOOV. The robot needs to be reprogrammed and it is experiencing which cybersecurity first principle?

(A) Domain separation,

Lesson Plan*

LESSON TITLE: Educational Use of Raspberry Pi

SUMMARY:

The main goal of this module is to understand importance of computer programming and how it relates to Cybersecurity education. The module will presents to teacher participants interesting hands-on exercises in which participants will setup, run and use a Raspberry Pi. Then participant will explore various application with the Pi that they can later teach to their own students.

GRADE BAND:

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

TIME REQUIRED:

120 minutes

LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:

Outcome Examples

Design/Build Test/Defend Compare/Contrast Apply/Use Explain/Discuss Identify/Describe	1. Demonstrate substantial understanding of the Cybersecurity FP. 2. Explore the use of basic operating systems commands on different platforms. 6. Understand the basics of computer programming and experiment with simple programs.

Materials List (i.e., string, digital diary, raspberry pi, web link, drone):

Computer lab with I/O devices.
Several Raspberry Pis.

Describe any Previous Knowledge that may be Required:

Basic Math and problem solving skills

How will you facilitate the learning?

- Describe the Warm-up Activity:

We will first understand that a Raspberry Pi is a small computer that runs an operating system installer called NOOBS (New Out Of Box Software). Each camper will be instructed on what the Pi is, the parts of it, and the first time setup. During this time, the chosen operating system will be completing the first boot up. Since this takes some minutes, each camper will be instructed on the basics of computer science. This will include an explanation as to what hardware and software is, what a computer needs to run, and basic types of operating systems.

- Describe the Focused Activity:

-Once the installation is completed, each camper will be given a tour of his/her Raspberry Pi. This will include navigating the main menu of the device, creating a text file on the main screen, and learning basic Linux commands in the terminal and syntax.
-Then, the campers will be instructed to launch “Minecraft”; they will be shown where it is in the menu and will be given a small explanation as to what Minecraft is and what we will be doing with the program.
- Next, they will be taught how to execute the “Python 3 (IDLE)” program which they will use this to modify and augment the current game of Minecraft they are in.
-Also, each camper will be instructed as to what Python is and what scripts will be used to modify Minecraft in real time.

- Describe the Teacher Instruction:

This module is primarily designed for teacher participants to show them (via the activities discussed above) some applications of the Pi that they can later teach to their respective students.

Mapping to Cyber Security First Principles:

- ☐ **Domain Separation**
- ☑ **Process Isolation**
- ☐ **Resource Encapsulation**
- ☑ **Modularity**
- ☐ **Least Privilege**
- ☑ **Abstraction**
- ☐ **Data Hiding**
- ☐ **Layering**
- ☑ **Simplicity**
- ☑ **Minimization**

Assessment of Learning:

TYPE (Examples listed below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	A number of assessment approaches will be adopted: 1- Regular observation of campers performance in the given tasks 2- Oral questions and walking around. 3- Presentation of how the Pi can be used for Cybersecurity related applications.

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

N/A

Describe any Extension Activities (i.e., ideas for further work):

N/A

Acknowledgements:

Lesson Plan*

LESSON TITLE: Tynker

SUMMARY:

Students will learn how to create an interactive program using block based coding within the Tynker software program. Block based coding requires students to use logic and sequencing to create a workable and meaningful program. Although block based coding is not a formal coding practice, it is a perfect and age appropriate method for novice programmers. In this lesson, students will design a program that requires the user to answer a question. To accomplish this task, students will need to use a variety of coding concepts and skills to successfully build the project. At the conclusion, they should have a workable program that will provide users the ability to answer a question pertaining to the topic.

GRADE BAND:

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☐ High School

TIME REQUIRED:

80 minutes

LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:

Outcome Examples

Design/Build Test/Defend Compare/Contrast Apply/Use Explain/Discuss Identify/Describe	Students will be able to design an interactive program involving the cybersecurity principles, using the block based language Tynker. Their program will involve multiple blocks including loops, conditions, and events in order to design a robust program that meets the lesson objective. At the conclusion of the lesson, each student will have a greater understanding of the cybersecurity principles and computational thinking.

Materials List (i.e., string, digital diary, raspberry pi, web link, drone):

Describe any Previous Knowledge that may be Required:

This lesson is designed for novice learners so an advanced background is unnecessary. It would beneficial for students to have some experience with logic puzzles through programs like the Hour of Code, however it is not required. The teacher will differentiate the instruction by offering more guidance and assistance to students who have limited experience.

How will you facilitate the learning?

- Describe the Warm-up Activity:

Students will begin the lesson by completing a Quizlet match activity that features the cybersecurity principles. Students will be encouraged to play the match activity multiple times to help review the key cybersecurity principles.

- Describe the Focused Activity:

Students will be assigned to create an interactive program that asks a multiple choice question pertaining to the cybersecurity principles. The program should be constructed with conditions, loops, and events that ensure that the user will need to answer correctly to move to the next question. Students will have flexibility within the assignment to use characters and settings of their choice to the meet the objective. The teacher will assign each student a specific cybersecurity principle to feature within their designed program. After the program is created, students have the opportunity to test their peer's projects and attempt to answer the cybersecurity question correctly.

- Describe the Teacher Instruction:

To begin students will be required to create a Tynker account. The teacher will guide them through this process to ensure that all students are on the Tynker site and have an account built. The teacher will then provide a basic demonstration and overview of Tynker by explaining the stage, blocks, and workspace. The teacher will then display an example program that asks the students a multiple choice question pertaining to the cybersecurity principles. A student will be called on to answer the question by typing it into the Tynker program. After students produce and input the correct answer, the teacher will show the students the code used to create the program. At this time, students will learn that they will be designing an interactive program that is similar to the example. Students will have flexibility in the design and creation, but they must meet the project guidelines. The teacher will then distribute a different cybersecurity question to each student. Time will be given for students to design and create their projects. The teacher will serve as a facilitator to assist and guide students' projects. Approximately 30 minutes will be given for student work. Once students have created workable programs, they will be given a handout that lists the cybersecurity principles that will serve as a word bank. Students will then move to each of their peer's programs and attempt to answer the question correctly.

Mapping to Cyber Security First Principles:

- ☑ **Domain Separation**
- ☑ **Process Isolation**
- ☑ **Resource Encapsulation**
- ☑ **Modularity**
- ☑ **Least Privilege**
- ☑ **Abstraction**
- ☑ **Data Hiding**
- ☑ **Layering**
- ☑ **Simplicity**
- ☑ **Minimization**

Assessment of Learning:

TYPE (Examples listed below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	Students will be assessed on their program creation. Each student will have a workable interactive program that reviews a cybersecurity principle. Students will have an opportunity to connect and interact with their peer's programs. This will provide each student with a valuable insight into how their peer's tackled the set objective and may drive their creativity and future problem solving. Although the design is initially independent, students will have the opportunity to learn from their peers.

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Students will receive differentiated instruction based on their overall level of programming experience. If needed, students will have the opportunity to work with a partner.

Describe any Extension Activities (i.e., ideas for further work):

To extend the project students will have the opportunity to create a second interaction in their program that reviews a second cybersecurity principle. After a correct response is given, the program should change the background and character and ask a new cybersecurity question.

Acknowledgements:

Lesson Plan*

LESSON TITLE: Introduction to Cryptography

SUMMARY:

1. Learning a brief history of cryptography (encryption/decryption)
2. Understanding the basic concepts of cryptography
3. Learning several basic cryptographic techniques
4. Hand-on practice on encryption/decryption using computers

Note: This lesson plan is for K-12 school teachers.

GRADE BAND:

- ☐ K-2
- ☐ 6-8
- ☐ 3-5
- ☐ High School

TIME REQUIRED:

120 minutes

LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:

Outcome Examples

Design/Build Test/Defend Compare/Contrast Apply/Use Explain/Discuss Identify/Describe	Understand of the basics of cryptography Learn why cryptography has been used from ancient to modern time Learn various methods of encryption and decryption Learn the significance of encryption and decryption

Materials List (i.e., string, digital diary, raspberry pi, web link, drone):

Web Links:
Navajo Code Talker Died, June 13, 2018:
https://nowthisnews.com/videos/news/one-of-the-last-living-navajo-code-talkers-from-wwii-passed-away
Cryptography in 60 Seconds: https://www.youtube.com/watch?v=j5fOynJrNOk
Simple Cryptography: https://www.youtube.com/watch?v=sz0AQYLi4k

Describe any Previous Knowledge that may be Required:

Knowledge of Mathematics

How will you facilitate the learning?

- Describe the Warm-up Activity:

1. Explaining and discussing the basics of cryptography
2. Brief discussion on the history of cryptography from Egypt to modern time
3. What are encryption and decryption and how they are performed
4. Difference between private and public key cryptography
4. Hand-on practices on various cryptographic techniques using online tools

- Describe the Focused Activity:

Hand-on Practices:
The students will be asked to practice on various cryptographic techniques, such as Caesar Cipher, DES, AES, Private-key cryptography, Public-key cryptography using tools available online. They will encrypt a message (a plain text) into cipher text and again decrypt the cipher text back to the plain text.

Challenge:
The students will be given a cipher text and will be asked to decrypt it (if they can) to the plain text using brute force technique.

- Describe the Teacher Instruction:

More in-depth discussion and hand-on practices on various encryption and decryption techniques
More on systematic development of cryptography from ancient to modern age
More question and answers; and quizzes on various encryption and decryption techniques

Mapping to Cyber Security First Principles:

- [ ] **Domain Separation**
- [ ] **Process Isolation**
- [ ] **Resource Encapsulation**
- [ ] **Modularity**
- [x] **Least Privilege**
- [x] **Abstraction**
- [x] **Data Hiding**
- [x] **Layering**
- [ ] **Simplicity**
- [ ] **Minimization**

Assessment of Learning:

TYPE (Examples listed below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	The instructor and TAs made observation while the activity was being performed. The instructor and TAs walked around to observe how different group are performing. The instructor and TAs asked oral questions when needed to ensure the students understood what they were doing and why. The instructor and TAs made sure all group members were engaged in the activities. The students were asked to present their final results.

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

N/A

Describe any Extension Activities (i.e., ideas for further work):

Activities could be extended to include more examples on decryption if students became more curious.

Acknowledgements:

N/A

Mrs. Gentile's Lesson Plan
I.U.P. GenCyber Combination Camp
Tuesday, June 19, 2018 11:00 - 2:00

Lesson Title: Exploring On-Line Cyber Security First Principles Resources

Summary: Teachers will first discuss best practices in using Quizlet, Quizizz, Kahoot, FlipGrid and other common on-line learning tools. Then, time will be dedicated to discussion and development of engaging strategies for embedding Cyber Security First Principles through the use of Gen-Cyber.com, including the Day of Cyber experience.

Grade Band:
PK – 12 Teachers

Time Required:
Two 50-minute sessions

Lesson Learning Objectives/Outcomes:

Upon completion of this lesson, teachers will be able to:

- Develop at least one active, on-line game to practice the Cyber Security Principles
- Search and critique popular on-line learning games for resources already made
- Apply Webb's Depth of Knowledge levels and Marzano's 6-step Vocabulary Teaching to proposed activities and discussed strategies
- List ways they can model correct application of the Principles when using technology themselves, and how they can simplify the Principles with classroom design analogies.

Materials List:

Webb's DOK reference charts
Guided notes for on-line games
Google accounts

How will you facilitate the Learning?

Session 1:

1) Review Kahoot, Quizlet, Quizlet- Live, Quizizz and Flipgrid for variations and best practices. Especially demonstrate the use of Quizizz's individual assessment records.
2) Demonstrate Edpuzzle – discuss the benefits of assessment, retention-building, flipping the classroom.
3) Provide time for teachers to explore Gen-Cyber.com ready-made resources, keeping in mind that they could combine those with the assessment benefits of the on-line games previously viewed for their lesson they will attempt tomorrow with students.

Session 2:

1) Allow teachers time to explore the Day of Cyber experiences from the Gen-Cyber.com resources.

2) Discuss how some or all of this would be part of learning they can use in their classrooms, and if any part of it fits into what they will try tomorrow with students. Remind them that they can incorporate ideas presented yesterday, technology-based ideas presented today, and/or ideas students will offer to them in our merged session with students on Wednesday.

Mapping to ALL Cyber Security First Principles:

Domain Separation	**Abstraction**
Process Isolation	**Data Hiding**
Resource Encapsulation	**Layering**
Modularity	**Simplicity**
Least Privilege	**Minimization**

Assessment of Learning:

TYPE:	**Name/Description:**
Written Records	additions to guided notes as we discuss topics
Oral Questioning	Teachers offer additional examples, ask for clarification on difficult principles or workings of on-line tools
Lesson Plan	Tested out on students Day 3, Revised/submitted Day 5

Accommodations: N/A

Description of Extension Activities: It would be wonderful if we could also explore Hyperdocs, and if we could add our 2018 lesson plan ideas and resources to the shared Gen-Cyber teacher folder from 2017.

Acknowledgements:
Gen-Cyber.com

Mrs. Gentile's Lesson Plan
I.U.P. GenCyber Combination Camp
Monday, June 18, 2018 11:00 - 2:00

Lesson Title: Engaging, Non-Tech Ways to Teach Cyber Security First Principles

Summary: Teachers will be first discuss best practices in vocabulary development and the creation of differentiated activities as our combined experiences provide. Then, time will be dedicated to discussion and development of engaging strategies for embedding Cyber Security First Principles into all classrooms.

Grade Band:
PK – 12 Teachers

Time Required:
Two 50-minute sessions

Lesson Learning Objectives/Outcomes:
Upon completion of this lesson, teachers will be able to:

- Develop at least one GenCyber card game beyond the given suggestions
- Create an active game to practice the Cyber Security Principles
- Apply Webb's Depth of Knowledge levels and Marzano's 6-step Vocabulary Teaching to currently used activities and discussed strategies
- List ways they can model correct application of the Principles when using technology themselves, and how they can simplify the Principles with classroom design analogies.

Materials List:
GenCyber Cards
Webb's DOK reference charts
Guided Notes for class ideas
Pens
Marzano Six-Step Process for Vocabulary teaching
Word Wall Starters

How will you facilitate the Learning?
Session 1:
1) Begin with a Word Wall where key ideas/connections can be accumulated as our discussions progress, encouraging teachers to keep such an active reminder in their classrooms. Ask teachers to share other effective methods of **vocabulary teaching** (e.g. drawings/definitions on index cards, foldable notebooks, tech methods for 6/19/18).
2) Briefly discuss how the complex Cyber Security Principles terms can be made simpler for younger learners through the following **Physical Classroom Analogies:**
   Stations/Centers (Domain Isolation)
   Desks in rows, tables, formations (Modularity)
   Room Door/Cabinet/Storage Bin/Box of Crayons (Layering)
   Passwords/Student Id #s/User Id (Least Privilege, Info Hiding)

Helpers, Library and Guidance Office Aides (Least Privilege)
Behavior Rewards (Least Privilege)
Simple Signs or Symbol Use for Fire Escape Plans, Special Passes, Special Messages or Class Practices (Abstraction)
Lights vs. Screen vs. Computer (Process Isolation)

3) Play the originally suggested **GenCyber card game**.
Provide teachers answers for their decks.
Play other games/activities I created with the deck.
Then ask teachers to think of common card games that we could play with the deck (e.g. Rummy w/3 of a kind, GoFish with only 3 cards dealt at a time, Pokemon, Set, Concentration, I have…Who has, War? Poker? Crazy 8s? Solitaire?...)
4) Demonstrate one **active game** (Red Rover, Red Rover or Capture the Flag)
Then ask teachers to think of common active games that we could adapt to the practice the Principles (e.g. Duck, duck, goose; Mother May I; 7 UP; Chinese Freeze Tag, Scavenger Hunt, Trashketball, Breakout EDU, Charades, Dominos, Rube Goldberg devices …)

Session 2:

1) Briefly discuss Piaget's contribution to our understanding of differentiating for students and encouraging higher order thinking skills. Transition into the more currently used phrase "DOK levels," made by Dr. Norman Webb.
2) Provide handout with DOK prompts and make the following suggestions for classroom activities:

DOK 1 – play "Win, Lose, Draw" (Define, Label, Match) or play "Headbands"-type game
DOK 2 – Categorize Principles related to hardware, software, processes (Two Truths and a Lie)
DOK 3 – Critique the use of Principles in our school OR Investigate other Principles on Internet OR Revise the GenCyber Cards into a district-specific set of examples
DOK 4 – Apply Cyber Security principles to creation of an on-line game, phone app or skit; Create interview questions for district's computer gurus

3) Discuss how our own use of technology in the classroom can lead to impromptu modeling of Cyber Security Principles in our own Teaching, without having to make complete lessons about the topic:
Strong Password Usage, Not allowing passwords to be saved when prompted on screen, Not providing personal info, Not enabling unnecessary privileges on cell phones like allowing access to contact list or current location, Logging off sites/computers when done…
4) Briefly share that the teachers in this combination camp are expected to create a lesson plan by Friday to share with all GenCyber participants nationwide. They can incorporate ideas presented today, technology-based ideas presented tomorrow, and/or ideas students will offer to them in our merged session with students on Wednesday.

Mapping to ALL Cyber Security First Principles:

Domain Separation	**Abstraction**
Process Isolation	**Data Hiding**
Resource Encapsulation	**Layering**
Modularity	**Simplicity**
Least Privilege	**Minimization**

Assessment of Learning:

TYPE:	**Name/Description:**
Written Records	word wall contributions, additions to guided notes as we discuss topics
Oral Questioning	Teachers offer additional examples, ask for clarification on difficult principles
Lesson Plan	Tested out on students Day 3, Revised/submitted Day 5

Accommodations: **N/A**

Description of Extension Activities: **N/A**

Acknowledgements:

Dr. Norman Webb

Ms. Myra Collins

NSA GenCyber Cards

Mrs. Gentile's Lesson Plan
I.U.P. GenCyber Combination Camp
Wed., June 20, 2018 11:00-11:50, 1:00 to 1:50

Lesson Title: Perfect the Plan I

Summary: Camp teachers have tested out their draft lessons which incorporate cyber security principles in their respective classrooms on camp students. Students provided feedback each teacher and together they hunted for resources to create engaging lessons (videos, games, articles, examples, etc.). This session is for teachers to reflect upon all educational strategies and resources learned about to this point in the week, and to solidify their lesson plans for NSA submission. We will share our ideas aloud, brainstorm together how best to incorporate additional cyber-security principles, and submit our work to a shared Google folder for ongoing reference and revision.

Grade Band:
PK – 12 Teachers

Time Required:
Two 50-minute sessions

Lesson Learning Objectives/Outcomes:
Upon completion of this lesson, teachers will be able to:

- Finalize one engaging lesson to practice the Cyber Security Principles, which will be submitted to the NSA for its national database of GenCyber lesson plans
- Share respective lesson plans in a shared Google folder among participants

Materials List:
Teachers' draft plans
Computers
Notes from the morning's merged session

How will you facilitate the Learning?
Session 1:

1) Teachers will be given an opportunity to discuss the morning's merged session and its outcomes. I will encourage brainstorming and support of one another's lesson ideas.
2) Next, I will provide notes about what I noticed for each teacher, especially in regard to which cyber-security principles were addressed, and which remain to be covered.
3) Discussion can follow as we look to incorporate the non-tech games and activities discussed on Day 1, the on-line teaching strategies discussed on Day 2.
4) An example of a hyperdoc will be shared to provide inspiration to "tech-up" their lesson plans in a way that is differentiable for a variety of learners, possibly using Kidsdiscover.com or my own examples from algebra class.

Session 2:

This will be an opportunity to create a Hyperdoc for each teacher's plan, or simply to create a Google doc to be placed in our shared Team Drive. Hyperdocs can include teacher-made games, vocabulary building through Marzano's 6 step process, on-line explorations for acquiring new information or on-line games for building retention of concepts. Hyperdocs practice *minimization* where students are guided to explore only certain areas of the Internet.

Mapping to ALL Cyber Security First Principles (ideally):

Domain Separation	**Abstraction**
Process Isolation	**Data Hiding**
Resource Encapsulation	**Layering**
Modularity	**Simplicity**
Least Privilege	**Minimization**

Assessment of Learning:

TYPE:	**Name/Description:**
Observations	As teachers share and collaborate
Oral Questioning	Teachers ask for clarification on principles, and others offer good examples or clarification without me
Lesson Plan	Tested out on students today, revised now, submitted Day 5, possibly as a Hyperdoc

Accommodations:

Some teachers' districts do not have a contract for GAFE, but still have access to Google Docs. These teachers can just email attachments and make copies to share their knowledge gained from camp.

Description of Extension Activities: It would be wonderful if we would all continue to contribute to our team drive and add lesson plan ideas and resources

Acknowledgements:

Gen-Cyber.com

Hyperdoc Handbook – Lisa Highfill, Kelly Hitton, Sarah Landis

Mrs. Gentile's Lesson Plan
I.U.P. GenCyber Combination Camp
Tuesday, June 19, 2018 11:00 - 2:00

Lesson Title: Exploring On-Line Cyber Security First Principles Resources

Summary: Teachers will first discuss best practices in using Quizlet, Quizizz, Kahoot, FlipGrid and other common on-line learning tools. Then, time will be dedicated to discussion and development of engaging strategies for embedding Cyber Security First Principles through the use of Gen-Cyber.com, including the Day of Cyber experience.

Grade Band:
PK – 12 Teachers

Time Required:
Two 50-minute sessions

Lesson Learning Objectives/Outcomes:

Upon completion of this lesson, teachers will be able to:

- Develop at least one active, on-line game to practice the Cyber Security Principles
- Search and critique popular on-line learning games for resources already made
- Apply Webb's Depth of Knowledge levels and Marzano's 6-step Vocabulary Teaching to proposed activities and discussed strategies
- List ways they can model correct application of the Principles when using technology themselves, and how they can simplify the Principles with classroom design analogies.

Materials List:

Webb's DOK reference charts
Guided notes for on-line games
Google accounts

How will you facilitate the Learning?

Session 1:

1) Review Kahoot, Quizlet, Quizlet- Live, Quizizz and Flipgrid for variations and best practices. Especially demonstrate the use of Quizizz's individual assessment records.
2) Demonstrate Edpuzzle – discuss the benefits of assessment, retention-building, flipping the classroom.
3) Provide time for teachers to explore Gen-Cyber.com ready-made resources, keeping in mind that they could combine those with the assessment benefits of the on-line games previously viewed for their lesson they will attempt tomorrow with students.

Session 2:

1) Allow teachers time to explore the Day of Cyber experiences from the Gen-Cyber.com resources.

2) Discuss how some or all of this would be part of learning they can use in their classrooms, and if any part of it fits into what they will try tomorrow with students. Remind them that they can incorporate ideas presented yesterday, technology-based ideas presented today, and/or ideas students will offer to them in our merged session with students on Wednesday.

Mapping to ALL Cyber Security First Principles:

Domain Separation	**Abstraction**
Process Isolation	**Data Hiding**
Resource Encapsulation	**Layering**
Modularity	**Simplicity**
Least Privilege	**Minimization**

Assessment of Learning:

TYPE:	**Name/Description:**
Written Records	additions to guided notes as we discuss topics
Oral Questioning	Teachers offer additional examples, ask for clarification on difficult principles or workings of on-line tools
Lesson Plan	Tested out on students Day 3, Revised/submitted Day 5

Accommodations: N/A

Description of Extension Activities: It would be wonderful if we could also explore Hyperdocs, and if we could add our 2018 lesson plan ideas and resources to the shared Gen-Cyber teacher folder from 2017.

Acknowledgements:
Gen-Cyber.com

Mrs. Gentile's and Mr. Stewart's Lesson Plan
I.U.P. GenCyber Combination Camp Merged Session
Friday, June 22, 2018 9:00 - Noon

Lesson Title: Cyber Knowledge Fair

Summary: Students will prepare an 8-minute presentation with teacher assistance to explain technology skills gained during the week in all of the camp's various topics and will explain how to incorporate cyber security principles into their respective topics to other camp participants.

Grade Band:
PK – 12 Teachers, 6-12th graders

Time Required:
Three hours with breaks

Lesson Learning Objectives/Outcomes:
Upon completion of this lesson, students and teachers will be able to:

- Describe technological concepts and devices explored during the week
- Align Cyber Security First Principles to technology topics from the week.

Materials List:
Computers

One set of materials/devices for each group

How will you facilitate the Learning?

9:00 - 9:05 Divide middle and high school students.. Ask all students to select a topic from the week's 8 topics out of a MS hat or HS hat. Students with the same topics will gather together to brainstorm how best to teach that topic to others. (about 2 students/topic) They will be informed that they will present their topics 8 times as we all rotate through the fair.	9:00 - 9:30 Teachers will work together to identify which Cyber-Security Principles match most closely to topics they have learned about during the week (robot programming, raspberry pi, cryptography, block chain technology, cyberbullying, Tynker, networking/nodes, password cracking, digital forensics, computer graphics) Teachers will decide among themselves which student topic they will help to advise
9:05 - 9:45 Students will be given a set of expectations to guide development of their 8-minute presentation for the fair. They must:	9:30 - 9:45 Each teacher will help to advise a group to be sure that they are following the expectations given to them.

1. Intro general uses of the topic 2. Demonstrate the most interesting aspect of the topic! 3. ****Discuss which cyber-security principle(s) is/are addressed in the topic**** 4. Ask questions from audience	Teachers can help to brainstorm how best to present the topics, if students need such support. ****Teachers should verify correct usage of the cyber-security principles.****
9:50 - 10:55 HS groups present topics, while MS groups, teachers, profs rotate among stations (8 min/ station)	
10:55 - 12:00 MS groups present topics, while HS groups, teachers, profs rotate among stations (8 min/ station)	

Mapping to ALL Cyber Security First Principles (ideally):

Domain Separation	**Abstraction**
Process Isolation	**Data Hiding**
Resource Encapsulation	**Layering**
Modularity	**Simplicity**
Least Privilege	**Minimization**

Assessment of Learning:

TYPE:	Name/Description:
Observations	As students share, demonstrate and collaborate
Oral Questioning	As teachers/students ask for clarification on principles
	As observers ask questions of each presentation

Accommodations:

Assistance may be needed for groups without a strong leader, which teachers can provide.

Description of Extension Activities:

Teachers and students in this Gen-Cyber Combination Camp are expected to share knowledge and skills gained this week in their school environments, and hopefully to maintain an interest in Cyber Security- related careers.

Acknowledgements:

Gen-Cyber.com

Lesson Plan*

LESSON TITLE: Strategies to Decrease Cyberbullying

SUMMARY:

In this session I will focus on explaining what cyberbullying is and how it effects those involved, using research and case studies to explain the ramifications from cyberbullying. I will also discuss research based anticyberbullying programs being used in schools. I will show participants resources to use in their classroom anticyberbully lessons. Activities will be interspersed throughout this session starting with a think pair share activity to get participants thinking about what they know about cyberbullying and share this with the group. The final activity will consist of participants creating a rough draft of a lesson that they can use in their classrooms.

GRADE BAND:

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

TIME REQUIRED:

120 minutes

LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:

Outcome Examples

Design/Build Test/Defend Compare/Contrast Apply/Use Explain/Discuss Identify/Describe	Participants will; (1) understand what cyberbullying is, (2) learn effective strategies to decrease incidents of cyberbullying, and (3) resources to use when teaching their students about cyberbullying. As a final activity they will create a rough draft of a lesson that they can use in their own classrooms.

Materials List (i.e., string, digital diary, raspberry pi, web link, drone):

Web links, youtube videos, case studies, example lessons, websites and books that can be used as resources when teaching in their classrooms.

Describe any Previous Knowledge that may be Required:

None.

How will you facilitate the learning?

- Describe the Warm-up Activity:

I will start off this session with a think pair share activity to get participants thinking about what they already know about cyberbullying. I will ask them to think of cyberbullying incidents they have heard of. Then I will ask them to get into small groups and discuss these incidents, and strategies that could have been used/that were used during or after these incidents. Then the groups will report out to the larger group what they have discussed in their small groups.

- Describe the Focused Activity:

1. Overview of cyberbullying.
2. Strategies to decrease cyberbullying.
3. Resources and sample lessons

I will meet the lesson learning outcomes by the above three focused activities. I will start by explaining what cyberbullying is and how it differs from traditional at school bullying. I will use case studies of incidents that have occurred to explain the ramifications from cyberbullying. I will also discuss research based programs and education that are being used in schools to decrease cyberbullying incidents. I will ask participants for their input on cyberrbullying teaching they have used, if any, in their classrooms and what they feel are effective strategies to decrease incidents or intervene when incidents occur. I will show them resources to use in their classroom anticyberbully lessons. Activities will be interspersed throughout this session starting with a think pair share activity to get participants thinking about what they know about cyberbullying and share this with the group. The final activity will consist of participants creating a rough draft of a lesson that they can use in their classrooms.

- Describe the Teacher Instruction:

During the overview of cyberbullying I will discuss the differences between cyberbullying and traditional bullying. I will discuss evidence based cyberbullying strategies, and then I will give participants the opportunity to discuss how incidents are handled at their schools and education that is given to their students. We will then brainstorm what we feel would be the best strategies to be used in schools to decrease cyberbullying. As a final activity participants will use what they have learned during the session to make an outline/rough draft of a lesson they can use to teach their students about cyberbullying.

Mapping to Cyber Security First Principles:

- [ ] **Domain Separation**
- [ ] **Process Isolation**
- [ ] **Resource Encapsulation**
- [ ] **Modularity**
- [x] **Least Privilege**
- [ ] **Abstraction**
- [x] **Data Hiding**
- [ ] **Layering**
- [ ] **Simplicity**
- [ ] **Minimization**

Assessment of Learning:

TYPE (Examples listed below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	I will walk around during the group activities to ensure participants understand the material and do not need any assistance with the activity. When groups report out to the bigger group, it will be an opportunity for others to agree, disagree, or ask questions to clarify the information. Throughout the presentation I will ask if there are any questions and address questions as they arise. During the final activity, when teachers are creating their lesson rough drafts, this will enable them to evaluate their own learning, and will enable me to evaluate it also.

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

I will use a powerpoint that will allow hearing impaired students to see the information, and I will use youtube videos that will allow visually impaired students to hear the information. I can also make further accommodations as needed upon request.

Describe any Extension Activities (i.e., ideas for further work):

After we discuss strategies we have found successful or we think would be sucess for decreasing cyberbullying, and participants created their own lesson rough draft, then I will encourage teachers to implement what they have learned during the session in their classrooms. I will also offer to volunteer to teach cyberbullying/bullying lessons at their schools. I will encourage teachers to attend, and encourage their students to attend, other educational events that I organize at IUP dealing with bullying and related issues.

Acknowledgements:

I would like to acknowledge Waleed Farag for allowing me to teach this important topic!

Lesson Plan*

LESSON TITLE: Robot Programming I_MS_HS Security Module Using KOOV

SUMMARY:

This module presents an easy-to-understand introduction to fundamentals of robotic programming and security. The participants will be introduced to learn to code with KOOV! KOOV is a new and exciting way to introduce robotics and coding to students with a hands on experience. It is also an excellent application for illustrating cybersecurity collaboration and problem solving skills to students. The larger classrooms of 35 students can be put into teams of three to five students with assignments of specific roles for each student on the team.

GRADE BAND:

- ☐ K-2
- ☐ 6-8
- ☐ 3-5
- ☑ High School

TIME REQUIRED:

240 minutes

LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:

Outcome Examples

Design/Build Test/Defend Compare/Contrast Apply/Use Explain/Discuss Identify/Describe	1. Demonstrate substantial understanding of the cybersecurity First Principles. Numbers one, six, seven and eight 2. Explore the use of basic operating systems commands on different platforms. All robot OS can be compromised to alter what they were originally intended for in KOOV.

Materials List (i.e., string, digital diary, raspberry pi, web link, drone):

KOOV Starter kit
Bluetooth enabled computer
Windows environment
IOS Computer
iPad application

Describe any Previous Knowledge that may be Required:

None

How will you facilitate the learning?

- Describe the Warm-up Activity:

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection - Decribe the Teacher Instruction

- Describe the Focused Activity:

Discuss and Demonstrate a Case Study for KOOVBackground:
Bonita Vista Middle School
Chula Vista Middle School
Rancho del Rey Middle School
San Ysidro High School
Sweetwater Union High School
The Sweetwater Union High School District in Chula Vista, CA received four KOOV prototype kits from Oct 3, 2017 to December 1, 2017 in order to participate in the KOOV Pilot Program. Educators from five different schools within the school district used the kits for two weeks at a time. They introduced KOOV into their schools and provided students an opportunity to use KOOV for independent study or within a structured setting lead by an educator.
Educators were asked to observe the students' experiences with KOOV, and at the end of the program provide feedback via a survey and an exit interview.
Sony Electronics began the KOOV Pilot Program to gain insights and feedback from educators as they look to bring KOOV to the United States.
Pilot Program Participants:
The specific reasons for trying out KOOV varied from site to site but the overarching theme from the educators was that KOOV was a new and exciting way to introduce robotics and coding to students with a hands on experience.
"The hands on experience, and the kids get to put things they have learned in the classroom into practical use."

- Describe the Teacher Instruction:

OBJECTIVE: Students will gain an understanding
of what algorithms are, and how they are translated into coding to drive the actions of computers and computer-controlled objects.
TIME: 30 minutes (60 minutes with lesson extension)
MATERIALS: Pencils or pens, "Step-by-Step" student worksheet
LESSON PLAN
1. Pre-Activity Discussion: What Is Coding?
Ask students to describe some of the actions that we use computers to do. (For example, send emails, play video games, perform calculations, etc.) Ask students how they think the computer performs these complicated tasks. (Students may say that there are computer programs that give computers instructions about what actions to take.) Explain to students that computer programmers rely on algorithms to direct the actions of a computer or a computer-controlled device like a robot. An algorithm is a set of steps that can be followed from start to finish to complete a task. In an algorithm, a complicated action is broken into many small steps. Explain that computer programmers write algorithms for each task a computer needs to do. Then they translate the algorithms into a language that a computer can read and follow. This language is called computer code.
2. Conduct the Activity: Hand out the "Step-by-Step" student worksheet. In the exercise, students will

Mapping to Cyber Security First Principles:

- [x] **Domain Separation**
- [x] **Process Isolation**
- [x] **Resource Encapsulation**
- [x] **Modularity**
- [x] **Least Privilege**
- [x] **Abstraction**
- [x] **Data Hiding**
- [x] **Layering**
- [x] **Simplicity**
- [x] **Minimization**

Assessment of Learning:

TYPE (Examples listed below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	Four questions to be used in the Pre/Post assessment survey. 1. The artificial intelligence of the robot has gone “out of control” and the Bluetooth “brain” is not controlling the KOOV. The robot needs to be reprogrammed and it is experiencing which cybersecurity first principle? (A) Domain separation, (B) Process isolation, (C) Resource encapsulation, (D) Abstraction

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

The contents the module will be adapted to better fit the level of each of the proposed three groups. For the teachers group, topics covered will stress how the AI security concepts and techniques can be integrated into the K-12 curriculum in addition to covering advanced concepts such as robotic co-existence with the human world. The contents will also advance in the level of detail when being presented to the Middle school group compared to when being presented to the High school students.

Describe any Extension Activities (i.e., ideas for further work):

This component of the module is designed to use a variety of formative assessment strategies in order to ensure that the students has acceptably achieved the Intended Learning Outcomes (ILOs) of the module. Examples of the proposed techniques are use of discussion, questioning, peer-assessment, and constructive quizzes. For example, a carefully chosen set of questions on the covered topics can form a quiz given at the end of this module. After the students finish the quiz, all quiz questions will be reviewed and proper answers will be identified. This positively contribute to productive discussions in the classroom and increase the chances of students achieving higher degrees of learning.

Acknowledgements:

Four questions to be used in the Pre/Post assessment survey.

1. The artificial intelligence of the robot has gone “out of control” and the Bluetooth “brain” is not controlling the KOOV. The robot needs to be reprogrammed and it is experiencing which cybersecurity first principle?

(A) Domain separation,

Wednesday, June 20, 2018 Guest Speaker

Ms. Lisa Schlosser, City Commissioner and Technology/Cyber Security Executive

Talk Title:

The future of Cyber Security: The National Threats and Your Opportunity

Brief Bio:

Ms. Lisa Schlosser is a Technology and Cyber Security Executive who has served in the private sector; public sector; US military; and in academia.
She is now an elected Commissioner for the City of Rehoboth Beach, Delaware; serves on several boards; and is an instructor at Georgetown University. She also volunteers at local dog shelters.
Lisa worked in technology in Washington DC, at the Executive Office of the President and Environmental Protection Agency.
Before joining the Federal Government, Lisa worked in the private sector as a Senior Manager for Ernst & Young LLP; and as a Vice-President for Global Integrity.
Lisa served in the US Army, and retired as a Lieutenant Colonel from the US Army Reserves.
Lisa holds a B.A. degree in Political Science from Indiana University of Pennsylvania, and an M.S. degree in Administration from Central Michigan University.

Tuesday, June 18, 2018 Guest Speaker

NORMAN ROBERT HAYES
Rear Admiral, United States Navy (ret.)

Talk Title:

Cybersecurity Implications for the Worldwide Netted Environment.

Brief Bio:

Professor, Cybersecurity Studies program, College of Professional Studies, George Washington University and CEO, Deep Futures Consulting, LLC. Formerly Executive Vice President, Cybersecurity and Intelligence with responsibility for contract management, business development, development of IT security software and partnership growth strategies. Served with distinction for three years as President, Naval Intelligence Professionals Charitable Foundation. Prior to retiring in 2013, following a 31-year career in Naval Intelligence, culminating in achieving the rank of Rear Admiral, the first African-American Naval Intelligence Officer to do so, just one many firsts. He served as the first Naval Intelligence officer to be Director of Intelligence, United States European Command. His previous assignment was at the National Security Agency as Director, National Security Operations Center. Other highlights of his career include: Commanding Officer, Navy and Marine Corps Intelligence Training Center and Commanding Officer Center for Naval Intelligence, Director of Intelligence (CJ2), Combined Forces Command – Afghanistan, Executive Assistant to Director of Naval Intelligence, and Assistant Chief of Staff, Intelligence, Commander Seventh Fleet. He is blessed with four incredible children – Felicia Renee, Lofton Darnell, Inori Sala and Ai Thanda.

Cybersecurity Implications for the Worldwide Netted Environment

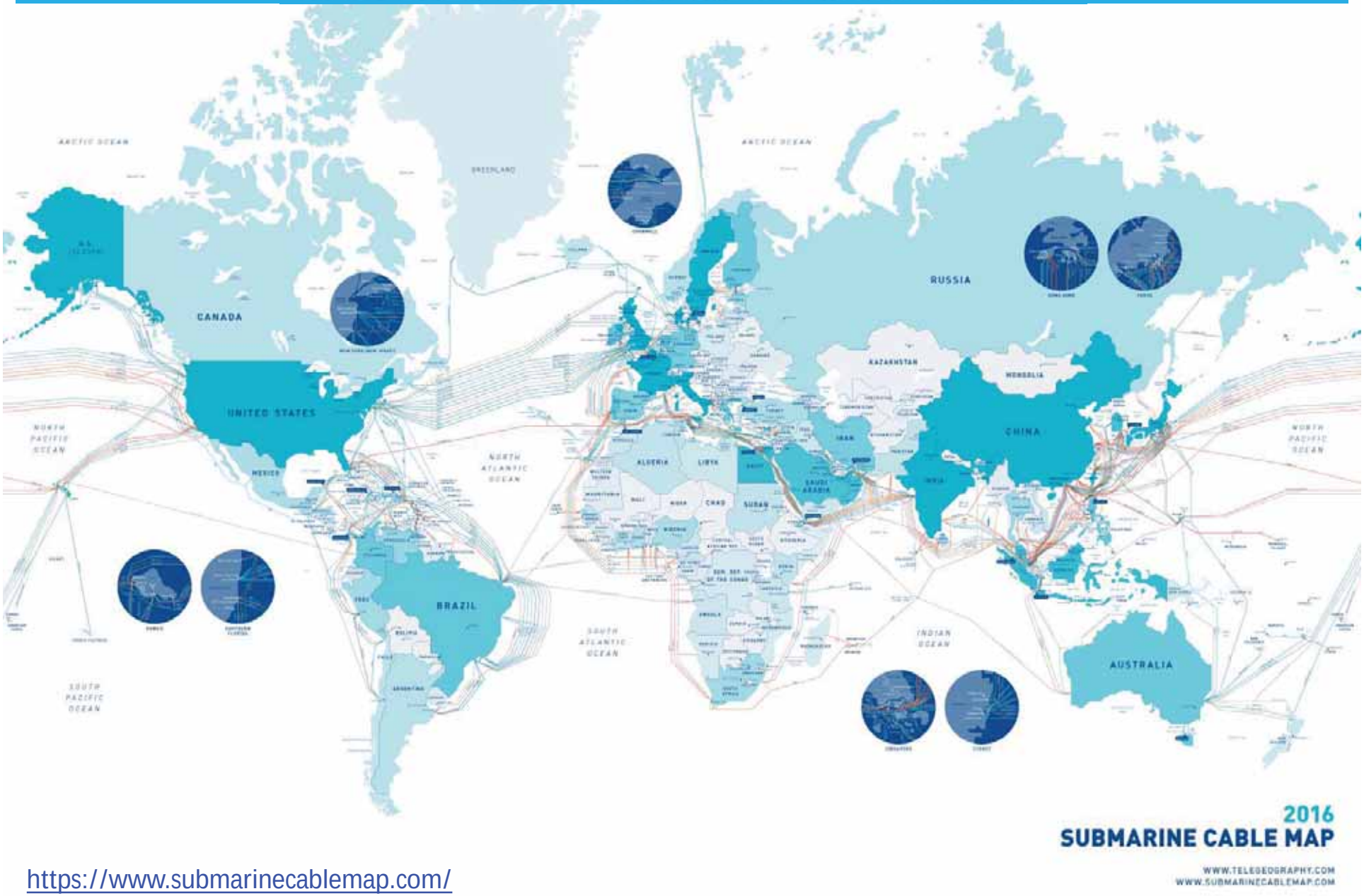
DEEP FUTURES, CONSULTING, LLC
CYBER LEADERSHIP

NORMAN R. HAYES
REAR ADMIRAL, USN
(RETIRED)

2018-2022:
The Interconnected World Environment

"Technology is fantastic and it influences outcomes. However we seem to forget that people solve the problems and technology only facilitates"

"We incorrectly distinguish a difference between the public and private cyber infrastructure. In the virtual environment they are one and the same"

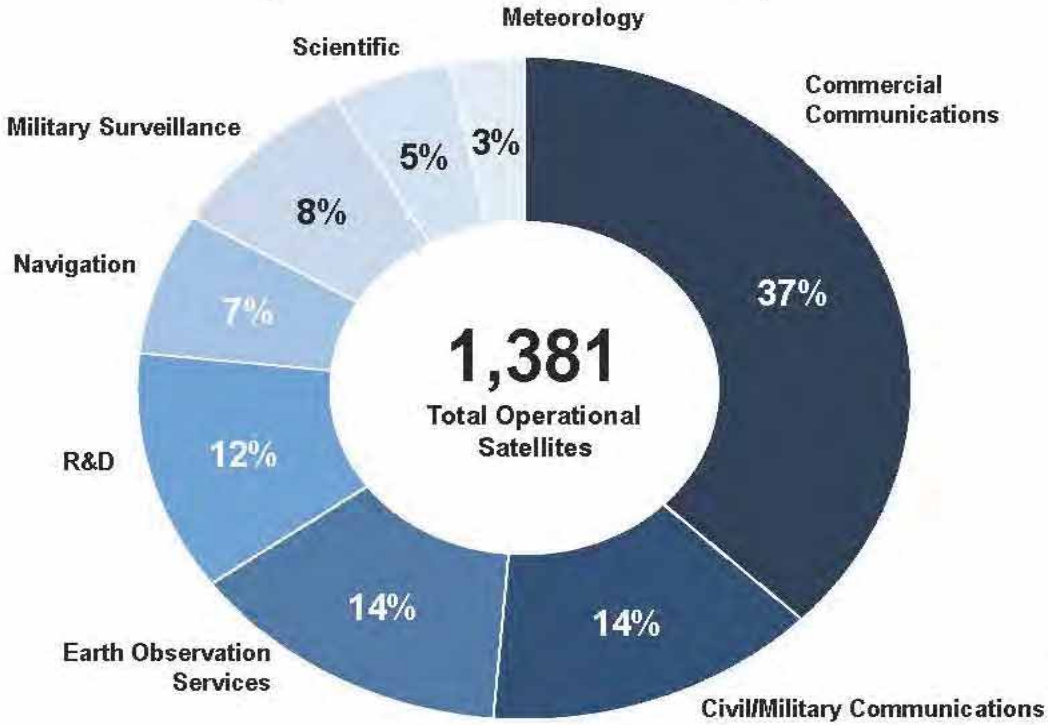


https://www.submarinecablemap.com/

Space – The Next Frontier

The Satellite Network in Context

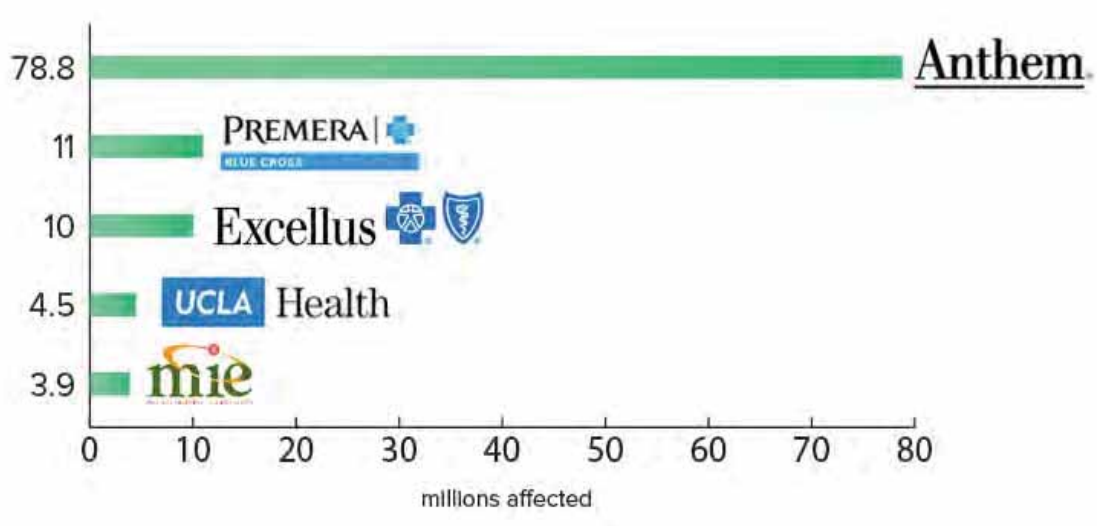
Operational Satellites by Function
(as of December 31, 2015)



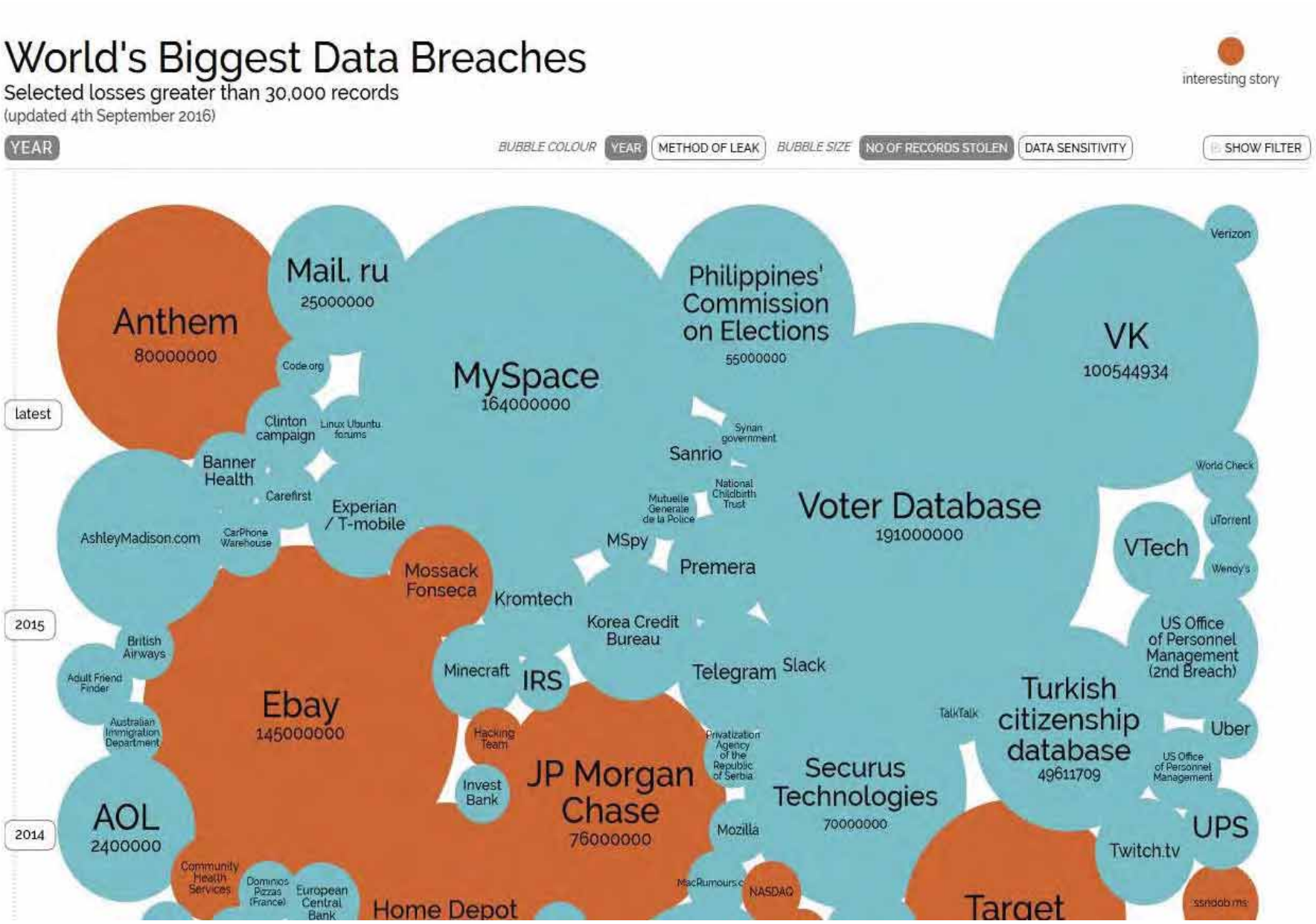
- Number of satellites increased 39% over 5 years, compared to 986 reported in 2011
  - » Average number of satellites launched per year in 2011-2015 increased 36% over previous 5 years
  - » Small and very small satellites deployed in LEO contribute to this growth
  - » Average operational lives of certain satellite types (such as GEO communications satellites) are becoming longer
- 59 countries with operators of at least one satellite (some as part of regional consortia)

https://www.statista.com/statistics/264472/number-of-satellites-in-orbit-by-operating-country/

Critical Data Breaches – 2015/16



Bigger is not Better



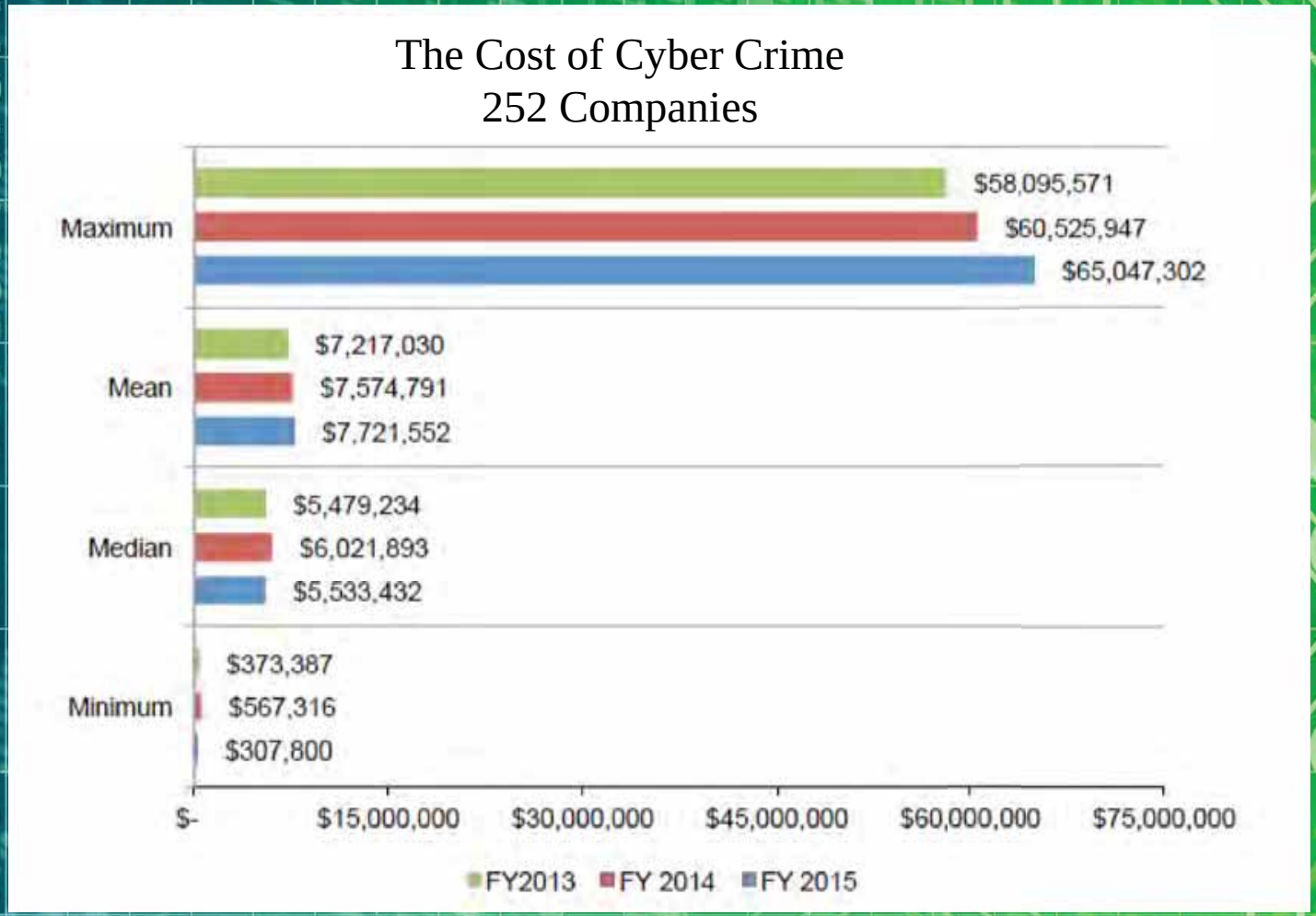
Wild Wild West

- **New Wave Crime**
  - Ransomware
  - Extortion
  - Intellectual Property
- **International Environment**
  - No Laws
  - No Universal Consensus
- **Information as currency**
  - Financial Gain

Cost to buy:
$0.55 video streaming credentials
$7.50 premium cable streaming
$5-8.00 credit card info
$20-100 bank account login

Digital inter-connectedness will make political, financial and social systems more vulnerable.

Staggering Costs



WORLDWIDE TOTAL SECURITY COSTS APPROACHING $200,000,000,000 ANNUALLY

Key Tenets of Cybersecurity

- Tenet 1: Security is a risk management issue, not a technological one
- Tenet 2: Know the metrics – make cybersecurity real to the Leadership
- Tenet 3: Understand the legal aspects of cybersecurity regulations
- Tenet 4: Identify acceptable cyber risk levels in business operations
- Tenet 5: Adopt a well-defined cyber risk management framework
- Tenet 6: Security is about people – they are your biggest risk and you have to take that risk. Focus on the people and you can have a marked reduction in RISK!

Personal Security Options

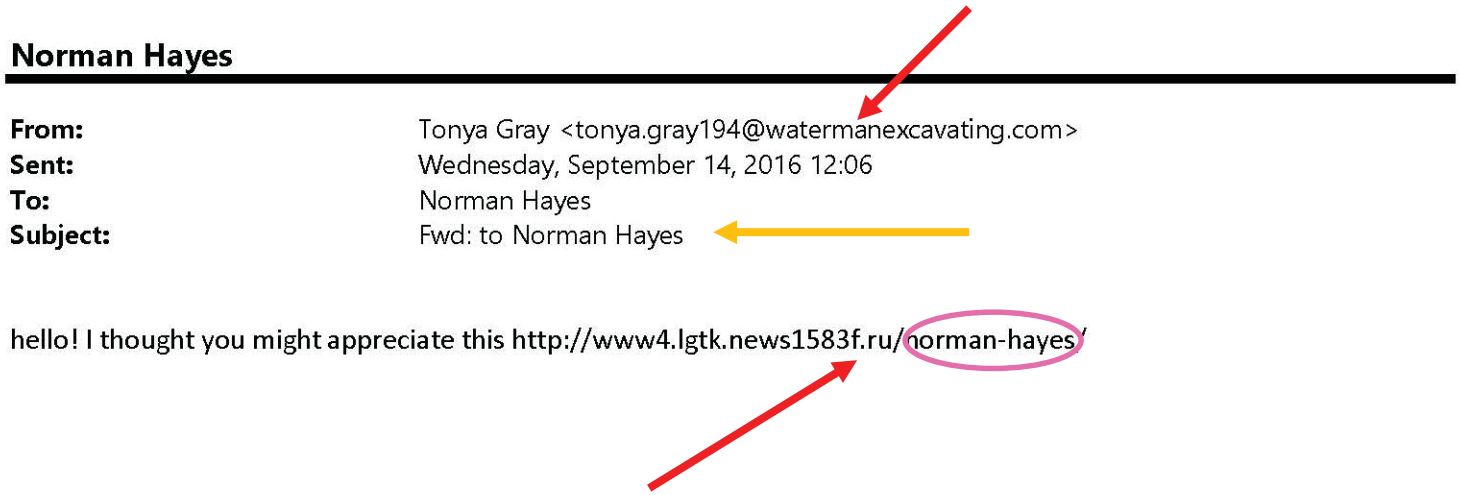
Smartphone Security

- Encrypt all data
- Android – buy security prog
- Use password/pin/biometric to lock-unlock cellphone
- Do not share you data
- Set OS security at highest comfortable settings
- Protect all passwords
- When available use two factor authentication

Password Security

- Stop using word or spreadsheet to keep PWs
- Use free program to guard PWs
- Use financial website two factor authentication
- Longer is better – why?
- Be creative

Social Media Attack

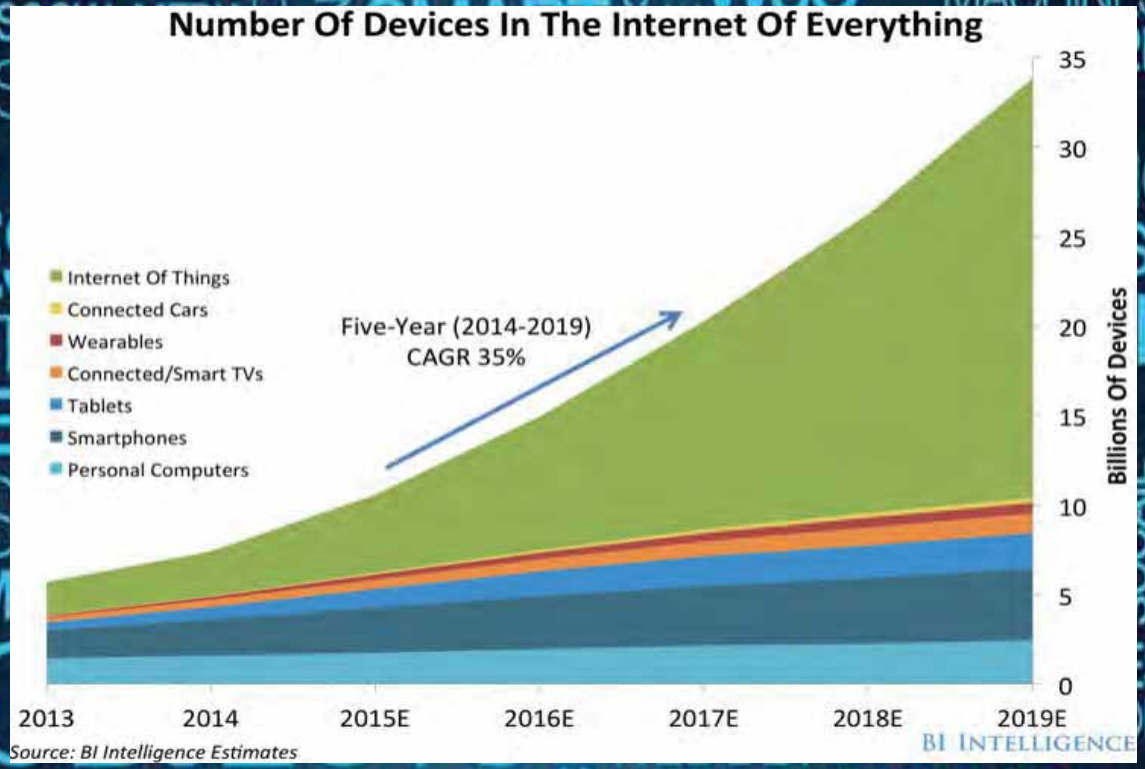


Norman Hayes

From: Tonya Gray <tonya.gray194@watermanexcavating.com>
Sent: Wednesday, September 14, 2016 12:06
To: Norman Hayes
Subject: Fwd: to Norman Hayes

hello! I thought you might appreciate this http://www4.lgtk.news1583f.ru/norman-hayes/

Internet of Things



*The **Internet of Things** is the network of physical objects or "things" embedded with network connectivity, enabling these devices to collect and exchange data. By 2020, IoT will connect 30+ billion devices. Security becomes ever more critical.*

Ultimate IoT Device

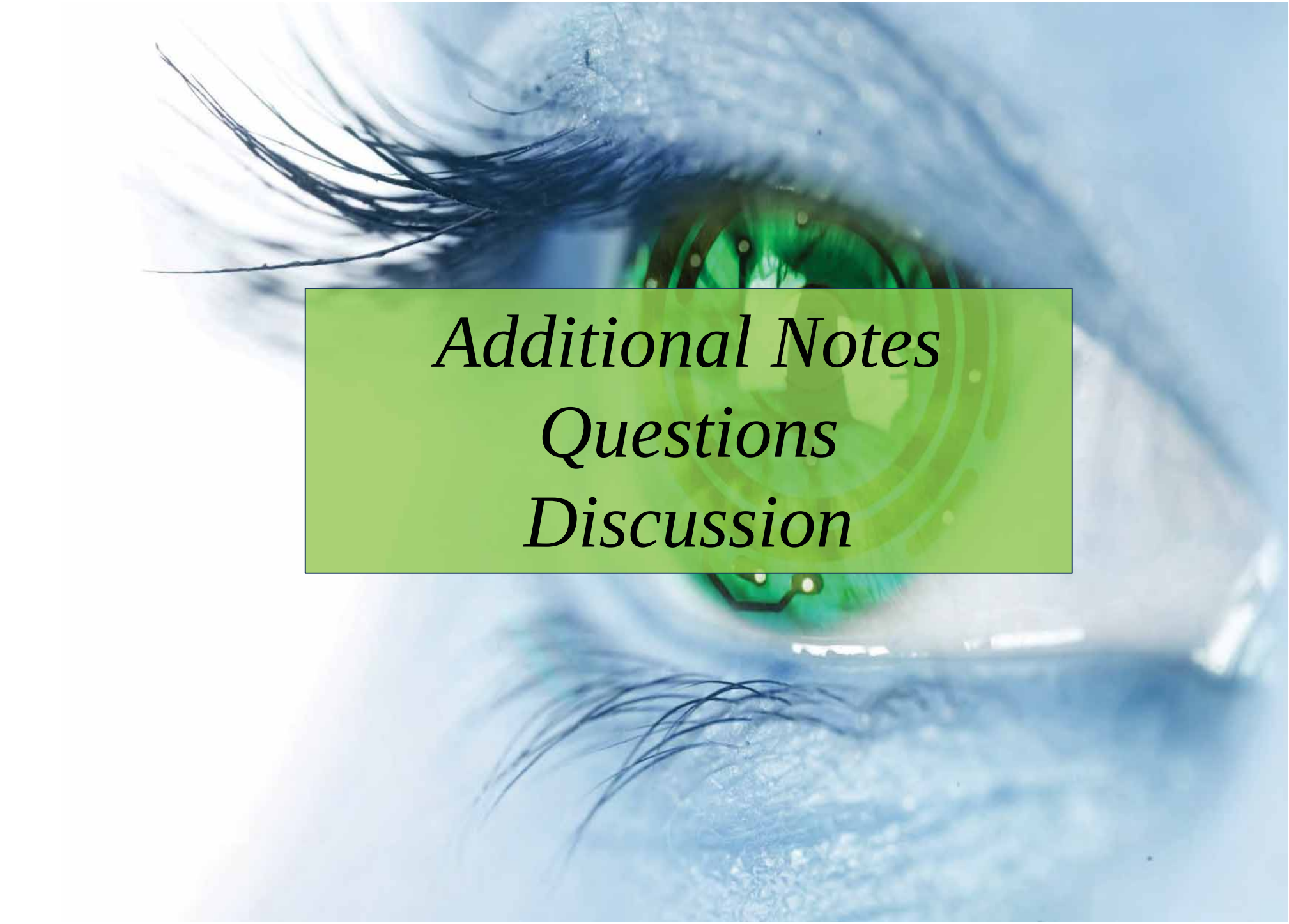
RUSSIA – Cold War II

The Putin Factor

- State Sponsored Criminal Element
- Difficulty with Attribution but…..
- Battles in the ether of Cyberspace

CHINA – Causes & Effects

- Sun Tzu – 600 B.C.E.
- Unrestricted theft – Ends Justifies the Means
- Intellectual property transfer at unprecedented scale
- Cost and Time barrier eliminated
- Economic Warfare by other means
- Changes the calculus


Additional Notes
Questions
Discussion

Locked and Loaded!

Shoot ’em at will:

The Response

- Federal annual cybersecurity spending - $13B & growing
- Presidential Executive orders
- National Institute Standards &Technology protocols
- Coordination across federal landscape
- Public – Private partnership
- Playing cybersecurity catch-up

"Our task in the Intel community . . . is to distinguish a terrorist sending directions on how to build a bomb or defeat TSA procedures from someone sending their granddaughter a recipe for apple pie. We're not just looking for a needle in a haystack. We are looking for thousands of needles in acres and acres of haystacks." Director National Intelligence

The Cyber Threat Offensive Attacks

Modes & Methods

Stuxnet & Flame
Buckshot Yankee
Georgia
Ukraine
Baltic States
Pakistan & India
Critical Infrastructure

	Cyber warfare Doctrine / Strategy		CW training/ Trained Units	CW exercises/ simulations	Collaboration w/ IT Industry and/or Technical Universities
Albania		X	X	X	
Argentina	X		X		
Australia		X	X		
Austria	X		X	X	
Belarus	X		X		
Brazil		X	X	X	
Bulgaria		X		X	
Canada				X	
China	X		X	X	X
Cyprus		X	X	X	X
Czech Republic		X	X	X	
Denmark		X		X	
Estonia		X	X	X	
Finland	X			X	
France	X		X	X	X
Germany	X		X	X	
Ghana		X			
Hungary		X	X	X	X
India	X		X	X	X
Iran			X		X
Israel	X		X	X	X
Italy			X	X	X
Japan			X		
Jordan		X	X		
Kenya			X		
Latvia		X	X	X	
Lithuania		X		X	
Malaysia		X	X		
Netherlands		X	X	X	
New Zealand		X	X		
North Korea			X		X
Norway		X		X	
Pakistan			X		
Philippines		X	X		X
Poland		X		X	
Russia	X		X		X
Slovak Republic		X		X	
South Korea		X			
Spain				X	
Sweden				X	
Switzerland		X		X	
Turkey		X	X	X	
United Kingdom		X	X	X	
USA		X	X	X	

2016 CYBERTHREAT DEFENSE REPORT

CYBEREDGE GROUP

NORTH AMERICA, EUROPE, ASIA PACIFIC, & LATIN AMERICA

SURVEY DEMOGRAPHICS

10 Countries represented around the world

20+ Industries represented

1,000 Qualified IT security decision makers & practitioners

RISING CYBERATTACKS

The percentage of respondents affected by successful attacks is rising each year.

SUSCEPTIBLE NATIONS

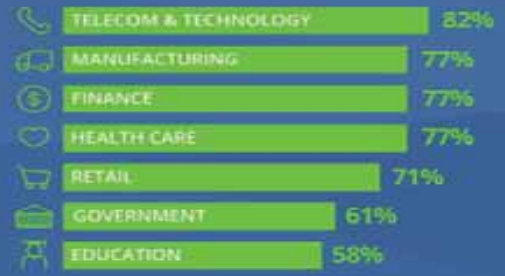
The percentage of respondents affected by successful attacks in 2015 varied by nation.

SINKING EXPECTATIONS

Respondents that believe a successful cyberattack is likely in the coming year is skyrocketing.

INCREASING SECURITY BUDGETS

Although three out of four IT security budgets are increasing in 2016, the percentage of growing IT security budgets varies by industry.



SECURITY'S WEAKEST LINKS

These areas are rated as most difficult to secure...

1. MOBILE DEVICES
2. SOCIAL MEDIA APPLICATIONS
3. LAPTOPS/NOTEBOOKS

CYBERTHREAT HEADACHES

Cyberthreats causing the greatest concern include...

1. MALWARE (VIRUSES, WORMS, TROJANS)
2. PHISHING/SPEAR PHISHING ATTACKS
3. SSL-ENCRYPTED THREATS

SECURITY'S BIGGEST OBSTACLES

These obstacles inhibit IT from defending cyberthreats...

1. LOW SECURITY AWARENESS AMONG EMPLOYEES
2. TOO MUCH DATA TO ANALYZE
3. LACK OF SKILLED PERSONNEL

NETWORK SECURITY ACQUISITIONS

The top four network security technologies targeted for acquisition in 2016 are...

1. NEXT-GENERATION FIREWALL (NGFW)
2. THREAT INTELLIGENCE SERVICE
3. USER BEHAVIOR ANALYTICS/ ACTIVITY MONITORING
4. SECURITY ANALYTICS/ FULL-PACKET CAPTURE & ANALYSIS

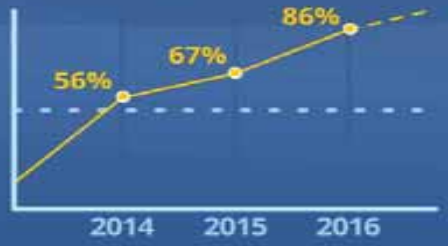
ENDPOINT SECURITY ACQUISITIONS

The top four endpoint security technologies targeted for acquisition in 2016 include...

1. CONTAINERIZATION/ MICRO-VIRTUALIZATION
2. SELF-REMEDIATION FOR INFECTED ENDPOINTS
3. DIGITAL FORENSICS/ INCIDENT RESOLUTION
4. DATA LOSS/LEAK PREVENTION (DLP)

ENDPOINT PROTECTION REVOLUTION

The percentage of organizations evaluating new endpoint protection solutions to augment or replace their existing investments is skyrocketing.



RESEARCH SPONSORS

PLATINUM: BLUE COAT, CITRIX, CODE42, IMPERVA

GOLD: FIDELIS CYBERSECURITY, invincea, MICRO FOCUS, NetIQ, LogRhythm, WEBROOT

SILVER: CloudLock, GURUCUL, IKANOW, SentinelOne, THREATQ

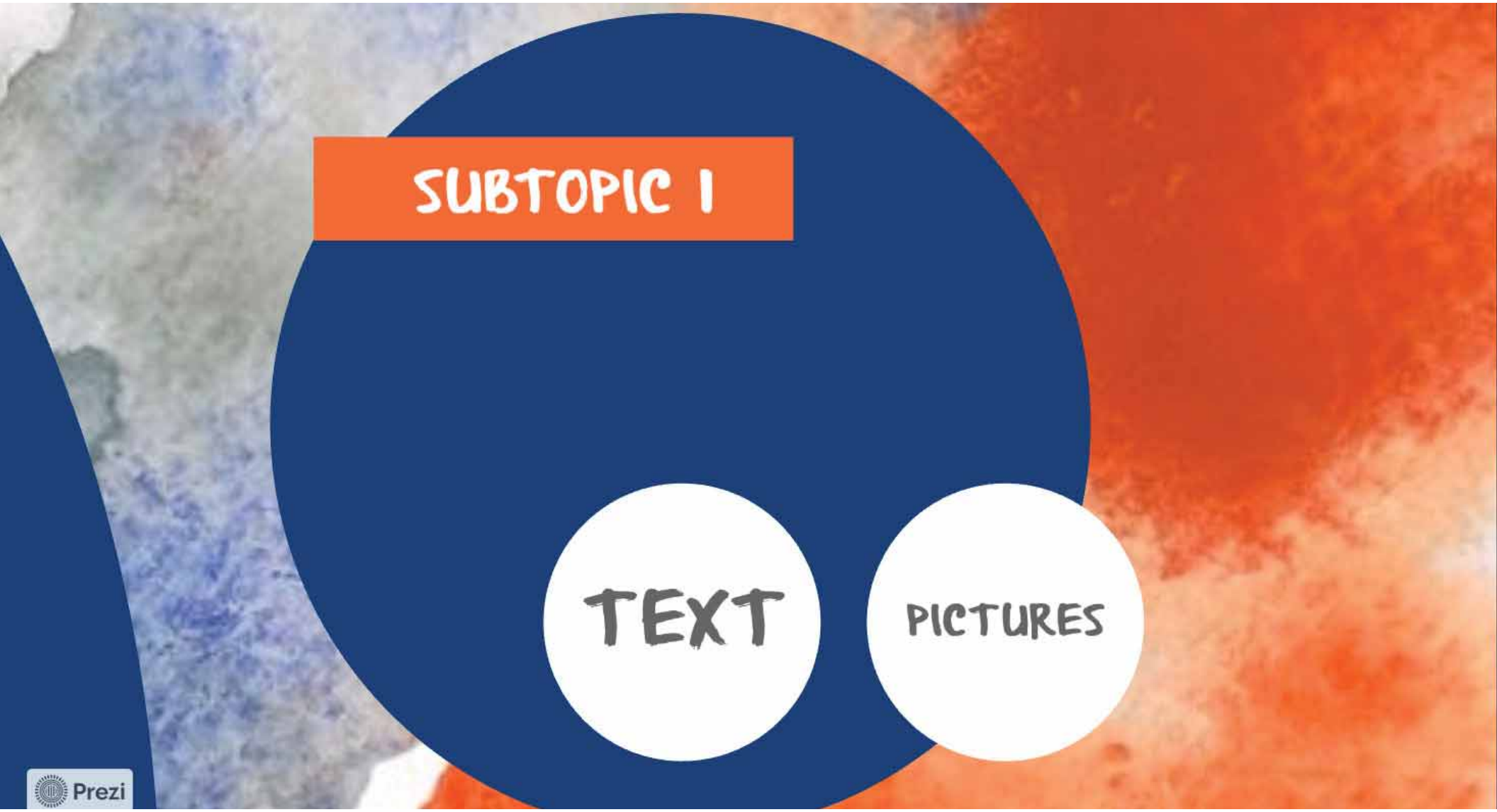

Cyber Security
Fun!
How
You!
Who Cares
Prevent
Presented by Lisa

and the Future

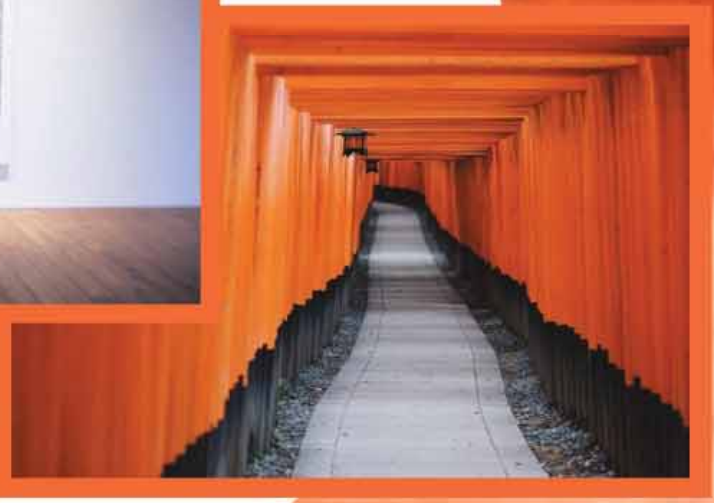
Problem

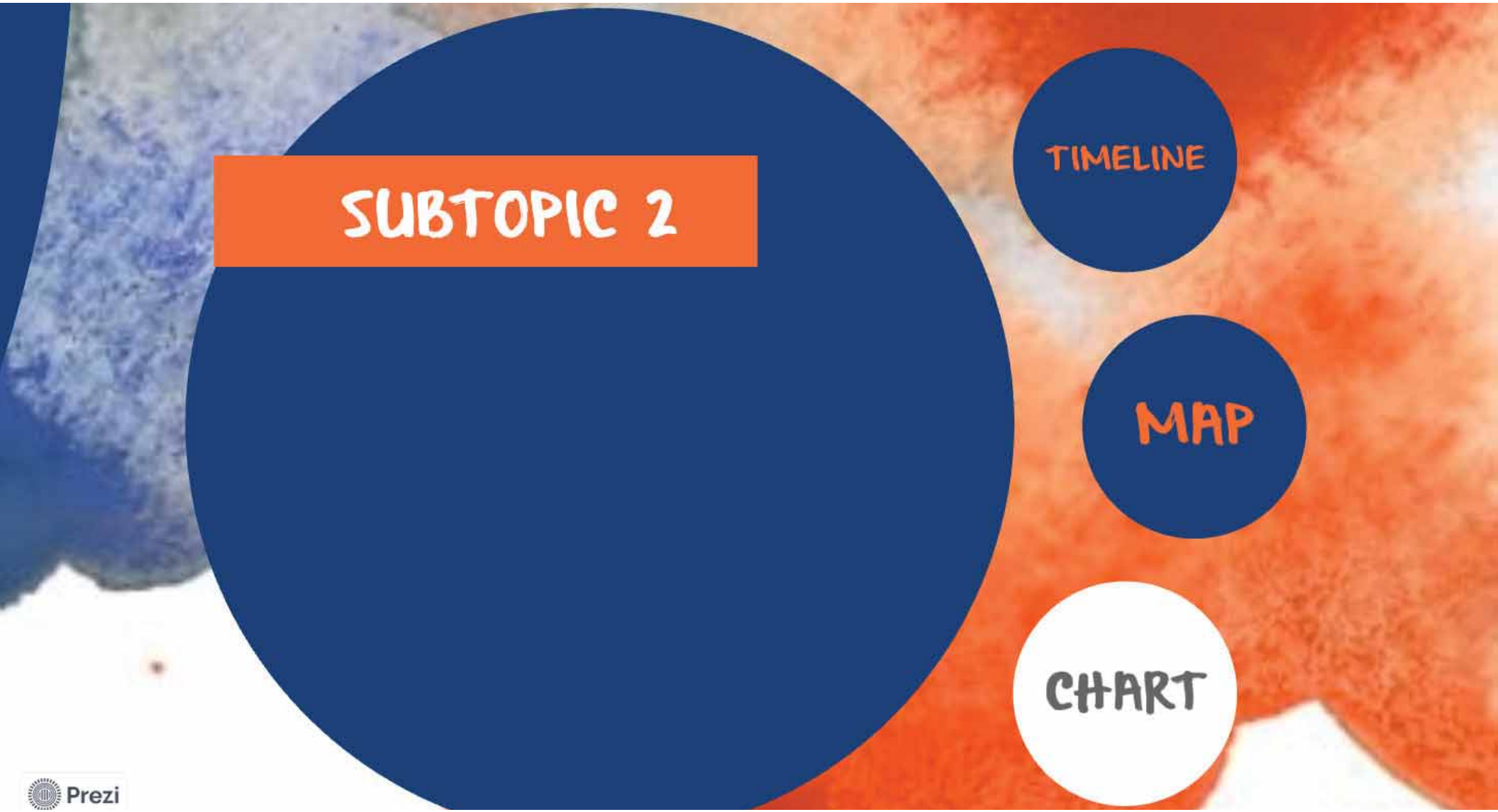
Loss of Privacy

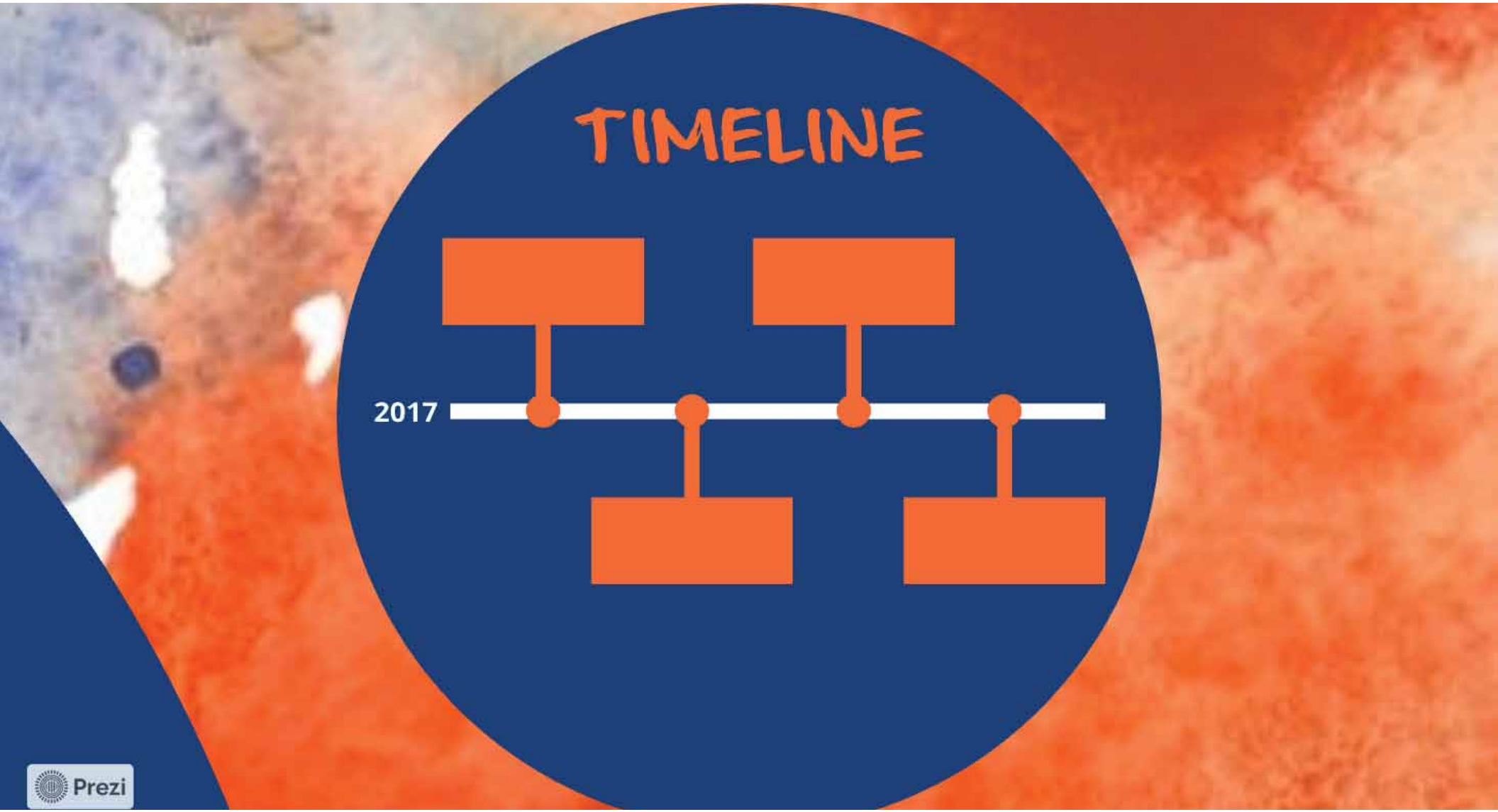
Loss of Electric


SUBTOPIC 1
TEXT
PICTURES

PICTURES



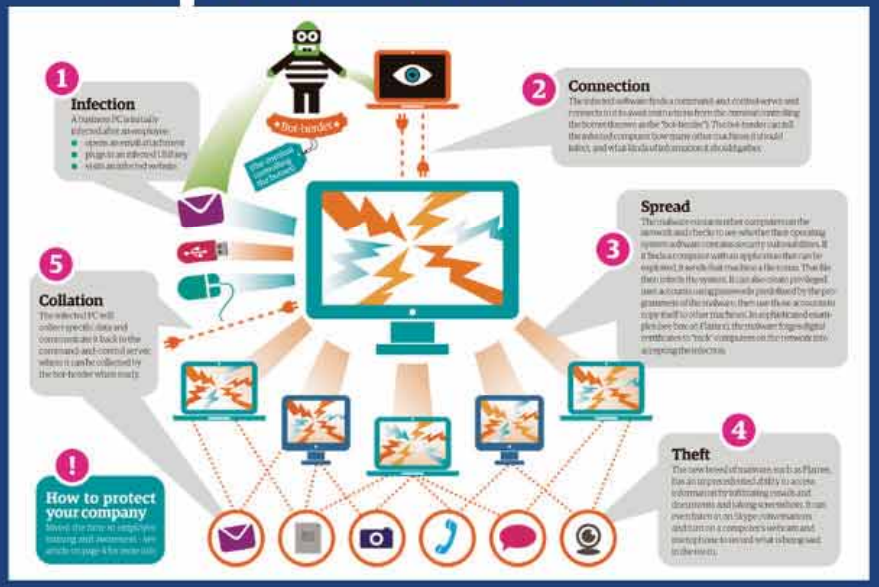



TIMELINE
2017

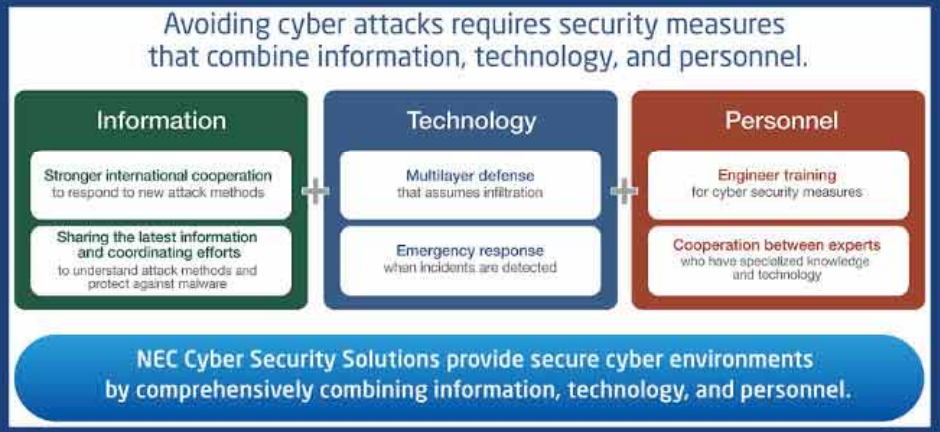

MAP

CHART

Cyber Attacks



What to Do



Careers

Average Salary:
$84000-$250000

Fun

Talk about why a computer would be attacked

Discuss what you can do to stop these attacks