

CYBER SECURITY

OVERVIEW

Students will investigate the technological application of quantum effects in cyber security. Students will research how quantum properties, such as superposition and entanglement enable quantum computers to create unbreakable codes. They will also research how quantum computers could render all current cyber security measures obsolete. Students will use their findings to engage in a debate about the promises and challenges of quantum computing for cyber security.

STEM LESSON FOCUS

<p>Engineering Design Cycle</p> <ul style="list-style-type: none"> Defining the Problem 	<p>21st Century Skills</p> <ul style="list-style-type: none"> Communication
---	--

OBJECTIVES

Students will be able to:

- distinguish between different types of cyber security approaches.
- summarize the advantages and disadvantages of different approaches to cyber security.

MATERIALS

- Computer with Internet access
- Quantum Computing Primer capture sheet (1 per student)
- Justification with Evidence capture sheet (1 per student)

HAVE YOU EVER WONDERED...

Why you need to complete those puzzles and tests to “Prove You’re Not a Robot”? These are one type of cyber security that prevents hackers taking control of websites.

CYBER SECURITY

What the future of computing looks like? In a few short decades, computers have shrunk from the size of a living room to everyday devices that fit in the palm of your hand. Computer scientists believe that advances in computing will continue the trend. They believe that the field of quantum computing will revolutionize the current state of technology.

MAKE CONNECTIONS!

How does this connect to students?	How does this connect to careers?	How does this connect to our world?
<p>Much of our daily lives revolve around digital resources such as the Internet, email, and personal communication devices. Cyber security ensures that these resources are not comprised by securing private data and network integrity.</p>	<p>A forensic computer analyst determines the causes and sources of network breaches or other cases when digital security is compromised. This role may involve detailed review of network systems, software vulnerability or insecure practices by employees. Forensic computer analysts typically work for digital security companies or as independent contractors.</p> <p>A security architect's role is to ensure an organization's digital security. The security architect may work to protect company data, network integrity and sensitive information. They may also work on mitigation and analysis when data is compromised. This career may be in any economic sector, whether for private companies, state entities or NGOs.</p>	<p>The worldwide web is a global information network. If you have an Internet connection, you can visit websites, email, chat with or text anyone in the world. This benefit also poses a risk. Anyone in the world with the right tools can access networks that control critical infrastructure. Unauthorized access could compromise financial markets, transport systems, power grids, and even military installations.</p>

CYBER SECURITY

	<p>Security consultants advise their clients on the best ways to protect digital resources such as private data, networks and intellectual property. Consultants typically work with small businesses that do not need full-time cyber security personnel. They may work with bigger companies to evaluate and assess existing the assets and vulnerabilities of existing systems.</p>	
--	---	--

Please allow for more classroom time if you want students to further explore careers.

BLUEPRINT FOR DISCOVERY

1. Ask students to individually create a list of everyday activities that involve secure computing (online banking, email, texting, social media activity, etc.). Invite students to share out their ideas. Ask students to put a 1 next to activities that seem safe and secure or a 2 next to activities that are more public. This is a subjective rating.
2. Provide the students with the following context:
Cyberspace is anything that has to do with the Internet. We use the Internet in many ways. We share media, post about our day, listen to music, watch videos, email, use it to help with classwork, play games, and connect with friends and family. There are many professionals that work to keep our computers and our country's networks safe. They are often engaged in protection of the future which could include quantum computing. This would enable us to use the power of atoms to perform memory and processing tasks instead of binary code.

What are some of the knowledge and skills needed to defend computers from cyber-attacks?

Invite students to first complete **Quantum Computing Primer** capture sheet to define important academic language used to explain this topic.

3. Clarify with students how quantum properties could enable quantum computers to create unbreakable codes.ⁱ
 - A key concept of quantum mechanics is the “measurement problem.” This principle states that measuring a system disrupts it.ⁱⁱ In other words, a message

CYBER SECURITY

that is encrypted at a quantum level cannot be intercepted without disrupting the message. A hacker will either make the message unreadable, or will be detected by the system. (Superposition and entanglement are the two quantum properties that enable quantum key distribution to ensure secure communications. ⁱⁱⁱ)

4. Direct students to form groups of 3-4. Each group will use these words to create a concept map to relate each of the terms. If needed, provide the Works Cited articles for a “big picture” view of the concepts behind quantum cryptography.
5. Divide the class into two groups. Each group develops a position for or against the motion: “Organizations and governments should invest in quantum computing research because the benefits of quantum based cyber security outweigh any risks.” Groups will use information from the visual organizers they created to support their arguments or as evidence against the opposing view. Students can record their thinking using Justification with Evidence capture sheet.

Take action!

There’s no doubt that combining quantum computing and cyber security will be vital to securing networks and digital infrastructure. The following resources will help students and educators to learn more about quantum computing and cyber security.

<https://arxiv.org/pdf/1307.0380v1.pdf>

http://drum.lib.umd.edu/bitstream/handle/1903/6459/TR_2004-47.pdf

<https://pdfs.semanticscholar.org/b4ac/17c649bc8dc4653ce6c114d4eeae3d6ed66f.pdf>

<http://physics.mq.edu.au/~jcresser/Phys301/Chapters/Chapter13.pdf>

<https://spectrum.ieee.org/tech-talk/computing/hardware/encryptionbusting-quantum-computer-practices-factoring-in-scalable-fiveatom-experiment>

<https://arstechnica.com/science/2010/09/quantum-key-distribution-in-superposition-of-insecure-and-unneeded/>

<https://phys.org/news/2008-08-siemens-quantum-cryptography.html>

NATIONAL STANDARDS

<p>Technology Education</p>	<p>Next Generation Science Standards and International Technology and Engineering Educators Association</p> <p>3.G Technology transfer occurs when a new user applies an existing innovation developed for one purpose in a different function.</p> <p>3.H Technological innovation often results when ideas, knowledge, or skills are shared within a technology, among technologies, or across other fields.</p>
-----------------------------	--

QUANTUM COMPUTING PRIMER

Cryptography: writing or solving codes.	Sketch:
Analogy:	
Use the word in a sentence:	

Cyber security: technologies, processes, and practices designed to protect networks from attacks or unauthorized access.	Sketch:
Analogy:	
Use the word in a sentence:	

Entanglement: an extensive barrier.	Sketch:
Analogy:	
Use the word in a sentence:	

Public-key encryption: a system that uses two keys. One is a public key and the other is private. This allows people to encrypt and decrypt messages.	Sketch:
Analogy:	
Use the word in a sentence:	

CYBER SECURITY

<p>Quantum key distribution: it enables two parties to make and share random secret keys only known to them. This allows people to encrypt and decrypt messages.</p>	<p>Sketch:</p>
<p>Analogy:</p>	
<p>Use the word in a sentence:</p>	

<p>Qubit: encoded information.</p>	<p>Sketch:</p>
<p>Analogy:</p>	
<p>Use the word in a sentence:</p>	

<p>RSA encryption: algorithm used by modern computers to encrypt and decrypt messages.</p>	<p>Sketch:</p>
<p>Analogy:</p>	
<p>Use the word in a sentence:</p>	

<p>Superposition: any two quantum states can be added together resulting in a new quantum state.</p>	<p>Sketch:</p>
<p>Analogy:</p>	
<p>Use the word in a sentence:</p>	

Claim:

Organizations and governments should invest in quantum computing research because the benefits of quantum based cyber security outweigh any risks

Evidence that strongly supports the claim:

Evidence that strongly supports the claim includes:

Reasoning:

This evidence supports the claim because . . .

Other evidence that supports the claim

Another line of evidence is . . .

Additional evidence states that . . .

Reasoning:

This evidence supports the claim because . . .

Counterclaim: Evidence that may refute the argument:

Evidence that may counter the argument is . . .

Reasoning

The counter-claim is weak because . . .

CYBER SECURITY

Cited Works

ⁱ Atherton, Kelsey D. To Make An Unbreakable Code, Use Quantum Physics. August 2, 2013
<http://www.popsoci.com/technology/article/2013-07/theoretical-quantum-encryption-machine-basically-unbreakable>

ⁱⁱ Yam, P. Bringing Schrödinger's Cat to Life October 9, 2102
<https://www.scientificamerican.com/article/bringing-schrodingers-quantum-cat-to-life/>

ⁱⁱⁱ Newman Lily Hay. Quantum Computers Versus Hackers, Round One. Fight! January 27, 2017
<https://www.wired.com/2017/01/quantum-computers-versus-hackers-round-one-fight/>