

**UCCS** University of Colorado  
Colorado Springs


**CS4950/5950**  
**Homeland Security & Cybersecurity**

**No Going Back**

CS 4950/5950  
Homeland Security & Cybersecurity

**Lesson 32**  
**No Going Back**

Rick White, Ph.D.  
University of Colorado, Colorado Springs



1 Esc

1

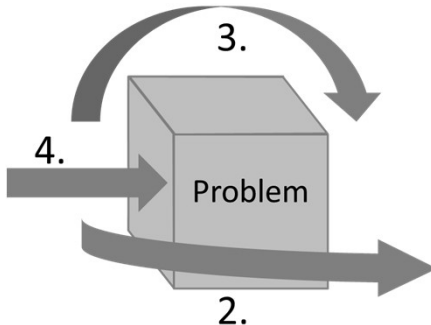
**UCCS** University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

**No Going Back**


When faced with any problem, you have at least four general options:

- 1) ignore it,
- 2) go around,
- 3) go over, or
- 4) go through it.



2 Esc

2



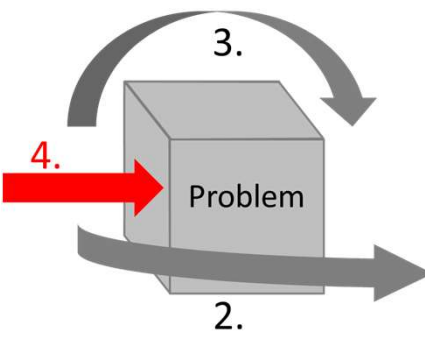
University of Colorado  
Colorado Springs


**CS4950/5950**  
**Homeland Security & Cybersecurity**

---


**No Going Back**

- The current approach to cybersecurity may be likened to option number four, “go through it”, with all its attendant uncertainty and risk.
- I hope this course has made clear why option one, **“ignoring the problem” isn’t even a consideration.**



3  


3



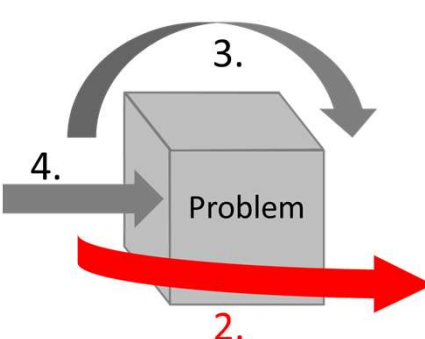
University of Colorado  
Colorado Springs


**CS4950/5950**  
**Homeland Security & Cybersecurity**

---


**No Going Back**

- But what option two?
- Can we go around?
- **Another way of putting this is to ask if we can go back?**



4  


4




University of Colorado  
Colorado Springs


**CS4950/5950**  
**Homeland Security & Cybersecurity**

---


**No Going Back**

Certainly there was **a time, before the Internet**, when cybersecurity wasn't a problem.



5  


5



University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

---


**No Going Back**

If we think about it, this option suggests two alternatives:


- 1. Disconnecting from the Internet**, and
- 2. Reverting to purely manual controls**, particularly with regard to cyber physical systems, i.e., industrial control systems.

**Going Back**

1. Disconnecting from the Internet.
2. Revert to manual controls.

6  


6



University of Colorado  
Colorado Springs


**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

### No Going Back


- Disconnecting from the Internet really isn't an option.
- For one thing, the Internet will reach out and get you.
- The 2010 Stuxnet attack is such an example.

### Going Back




1. Disconnecting from the Internet.

2. Revert to manual controls.

7  


7




University of Colorado  
Colorado Springs


**CS4950/5950**  
**Homeland Security & Cybersecurity**

---

### No Going Back

- Stuxnet was a **supply chain attack** perpetrated against Iranian nuclear research facilities in 2010.
- Stuxnet targeted Siemens centrifuges used to refine nuclear materials.
- The worm was likely **introduced by a thumb drive** sometime after manufacture and set to work after the devices were installed.



8  


8



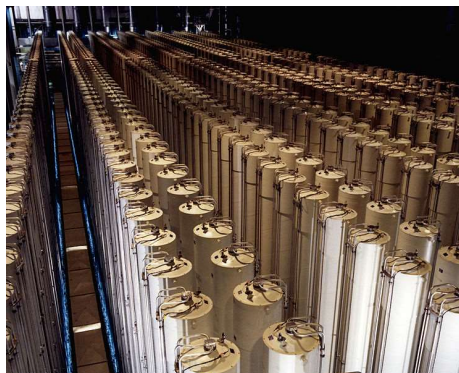
University of Colorado  
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

### No Going Back

- In other words, Stuxnet **jumped the air gap** and penetrated a highly secure facility without using the Internet.
- Certainly, screening methods can help avoid similar type problems in the supply chain.



9

Esc

9



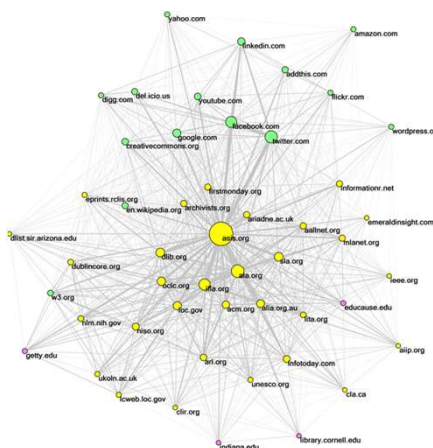
University of Colorado  
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

### No Going Back

But then, there are some sectors of critical infrastructure that quite literally can't afford to disconnect from the Internet.



10

Esc


10

UCCS University of Colorado  
Colorado Springs

CS4950/5950  
Homeland Security & Cybersecurity

**No Going Back**

**The electricity sector is one of them.**



11 Esc

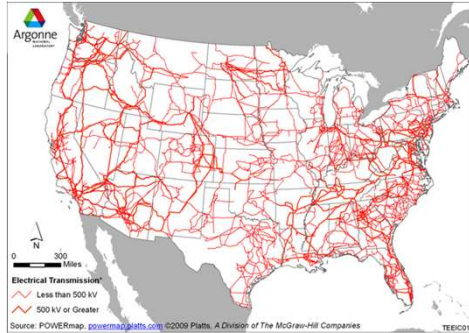
11

UCCS University of Colorado  
Colorado Springs

CS4950/5950  
Homeland Security & Cybersecurity

**No Going Back**

- The **Energy Policy Act of 2005** opened access to long-distance transmission lines allowing cheaper electricity from one region to be purchased by utilities in another region.
- **The monitoring and control required to facilitate such transmission cannot be accomplished without network access to controls.**



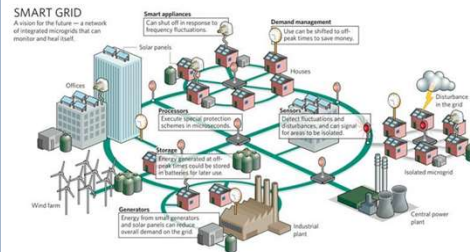
12 Esc

12



### No Going Back

- Similarly, the **Energy Independence and Security Act of 2007** promotes the implementation of Smart Grid technologies.
- Smart Grid is a general collection of capabilities designed to reduce electricity demand by monitoring and reporting usage.
- **Again, such capability cannot be achieved without network monitoring and control.**



13

Esc

13



### No Going Back

**So, can we revert to manual controls?**

### Going Back




1. Disconnecting from the Internet.

2. Revert to manual controls.

14

Esc

14




University of Colorado  
Colorado Springs


**CS4950/5950**  
**Homeland Security & Cybersecurity**

---


### No Going Back

- There's good reason why industry gravitated away from manual controls, chief among them was to **reduce labor costs**.
- But even if industry wanted to return to manual controls, **the previous cited examples work against this alternative.**



15  


15



University of Colorado  
Colorado Springs



**CS4950/5950**  
**Homeland Security & Cybersecurity**


---

### No Going Back

- Again, Stuxnet was able to **jump the air gap**, and the timing requirements and volume of traffic for managing the electric grid are **too fast and too much** for humans to intervene manually.
- The same goes for traffic management systems in the transportation sector and monetary transactions in the finance sector.

### Going Back

 Disconnecting from the Internet.  
 Revert to manual controls.

16  


16



**UCCS** University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

**No Going Back**

In short, there's no going back.  
We can't go around the  
cybersecurity problem.

17 Esc

17

**UCCS** University of Colorado  
Colorado Springs

**CS4950/5950**  
**Homeland Security & Cybersecurity**

**Conclusion**

Questions?

18 Esc

18