University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cybersecurity Demise

CS 4950/5950
Homeland Security & Cybersecurity

Lesson 42
Cybersecurity Demise

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

1
Esc

1

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Infrastructure Solutions

In this lesson we ask the question "Does cybersecurity necessarily need to be a homeland security problem?"

2
Esc

2

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Infrastructure Solutions

The answer is "no".

3

Esc

3

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Infrastructure Solutions

Just as we cannot stop cyber attack, we cannot stop earthquakes.

4

Esc

4

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Infrastructure Solutions

- Until recently, a magnitude 6 earthquake was the source of major catastrophe.
- With the **implementation of stringent seismic standards in building codes**, magnitude 6 earthquakes are not nearly the problem they once were in California.

5
Esc

5

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Infrastructure Solutions

We cannot stop earthquakes, but we can mitigate their effects.

6
Esc

6

UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Infrastructure Solutions

Similarly, we may not be able to stop cyber attack, but we may be able to mitigate their effects when it comes to critical infrastructure.

7
Esc

7

UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Infrastructure Solutions

Let us see how we might mitigate the effects of cyber attack against the four lifeline infrastructure studied earlier.

8
Esc

8

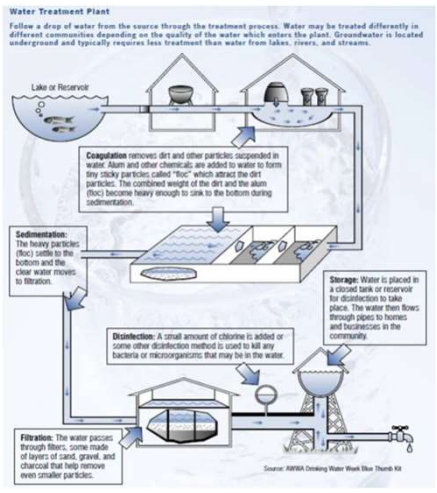
Infrastructure Solutions

Drinking Water

- The worst case scenario would be depriving a medium to large size city of any water.
- This would be worse than the situation in Flint Michigan which still has water, it's just not drinkable.
- Still, it is available for washing, sanitation, and most importantly firefighting.
- **In a worst case scenario, there would be no water for even these purposes.**

Infrastructure Solutions

- A cyber attack could conceivably bring about such conditions by causing strategic pumps and tanks to self-destruct.
- **Such mechanical failures, however, could be quickly repaired, probably in as little as 72-hours given requisite priority.**
- **So while the disruption would be significant, it could also be short lived and survivable.**



Infrastructure Solutions

Swift and effective response actions could mitigate the worst case consequences of a coordinated attack on the drinking water infrastructure.

11

Infrastructure Solutions

Aviation Infrastructure

- A worst case scenario in this respect would be the introduction of a **virus that disables the avionics suite of a number of aircraft or causes them to deliberately crash.**
- **The inherent problem with heavier-than-air aircraft is they tend to fall from the sky when things go wrong.**
- **Surface vehicles don't suffer from this vulnerability.**

12

UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Infrastructure Solutions

The obvious answer is not to take to the sky for travel.

13
Esc

13

UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Infrastructure Solutions

- For many reasons this is not practical today, but that does not mean it won't become so.
- **The expansion of high-speed rail service and the introduction of self-driving vehicles could significantly transform the future of mass transportation.**
- **Ironically, air travel today is significantly safer than ground travel;** the odds of dying in a plane crash are one in 11 million, whereas the odds of dying in a car crash are one in 5,000.

14
Esc

14

Infrastructure Solutions

Revolutionary changes in ground transportation could eliminate the fundamental risk of air travel.

15

Infrastructure Solutions

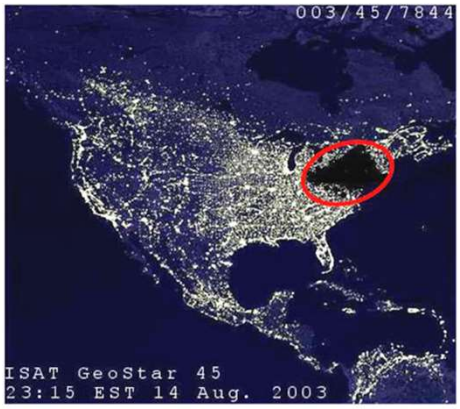
Electricity Infrastructure

- As was stated in Lesson 14, the worst case scenario is **shutting down a significant portion of the grid for an extended period of time, months if not years.**
- The reason the 2003 blackout didn't last longer was that no generators were destroyed.

16

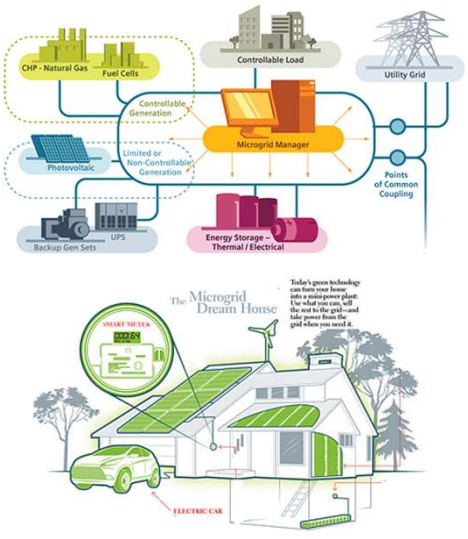
Infrastructure Solutions

- Again, **destroy the generators**, and we're talking a much longer recovery period because
  - **Few spares** are kept in stock, and
  - **They're no longer manufactured in the US.**
- Can this situation be fixed?



Infrastructure Solutions

- One answer is **segmentation**: subdivide the big grids into smaller ones.
- The idea is to stop little outages from becoming big outages, such as the 2003 northeast blackout, by halting their spread.
- **The concept is called "microgrids" and it's currently under development.**



Infrastructure Solutions

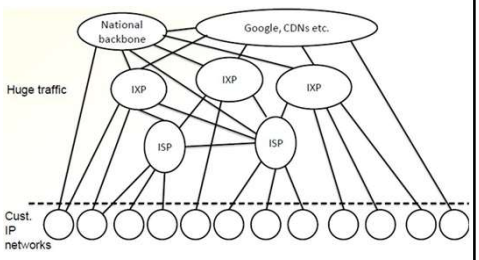
By changing the grid topology, it might be possible to localize outages, eliminating the threat from large-scale cyber attack.

19

Infrastructure Solutions

Internet Infrastructure

- Can the Internet be made immune to cyber attack?
- **Not much more than it is today.**



20

Infrastructure Solutions

- However, the beauty of the Internet is that it has **built-in redundancy** designed to withstand deliberate attack.
- So even if the worst case scenario could bring down all the root domain name servers, it would **probably be only a temporary disruption**, as the system is designed to self-repair and quickly restore normal services.

Infrastructure Solutions

Built-in redundancy and self-repair capabilities make it unlikely the Internet will experience regional outages for more than a short period.

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Infrastructure Solutions

While we cannot stop cyber attack, we can mitigate the effects to infrastructure such that they no longer pose a catastrophic threat.

23
Esc

23

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Infrastructure Solutions

Through the normal course of maintaining and upgrading the nation's critical infrastructure, and by whatever technological breakthroughs that may happen, it can gradually be made less vulnerable to cyber attack.

24
Esc

24

Infrastructure Solutions

And while cybersecurity will remain a problem for the foreseeable future, it need not remain a problem for homeland security.

25

Conclusion

Questions?

26