SY403 Short Exercise –August 2019
This is the long form of the script… for the instructor
See *" SY403 – Short Exercise Fall 2018"* for the short form that's posted on the SY403

Forget what day it is. We're not in 2018 anymore. Instead... Today is March 15, 2021

l'm Emil J Paidar, the White House Chief of Staff and former Director of Cyber Policy.

This new Administration is just two months old, and we're facing our first crisis.

Most of the President's political appointees are still in the confirmation process, so we've asked you to come in and help us deal with this situation. The President very much appreciates your assistance in this matter of national urgency.

To be frank, it's also a matter of urgency for this Administration. As you all no doubt recall, failures of cybersecurity policy played a role in the last President 's failure to win re-election. We'll review a few of the issues that emerged over the past few years; the inability to coordinate a forceful Federal response became a costly political problem for that Administration. This
President does not intend to go down the same road.

Because we all come from different places and represent different points of view, it's important to start with a common context for understanding current events. So, please indulge me while I review a few salient points of recent history, and apologies if I'm telling you some things you may already know.

Our world has grown ever increasingly connected. Unless you've made a determined effort to go...
...totally "off the grid", you spend your days tied into an ever-growing global network...
...an "intemet of things". While we've long been accustomed to our computers, mobile telephones, tablets, and televisions communicating with one another, with streaming our music and movies from distant servers wherever they are to wherever we are, networked connectivity has penetrated our lives to a degree that most people don't recognize, and certainly don't think about.

By 2015, the number of networked devices exceeded the total population of the planet, and has only exploded since then. As the lPv6 Internet address protocol has been more widely adopted, the number of available Internet addresses has grown by a factor of... ...79 thousand million million million million. To put that number in perspective, that's roughly a billion billion IP addresses for every human on earth. And it sometimes seems that manufacturers and consumers are trying to use all of those up as fast as they can.

This geometrically expanding network can broadly speaking be thought of as existing on three levels.

On an industrial level there are the growing number of "smart" power grids around the world. These integrate tens of thousands of meters at homes, business, and factories to balance generation. Among other things, they can optimize the use of thousands of small-scale wind and solar electric production sites as load rises and falls.

Industrial farms increasingly rely on networked, wireless tractors and other machinery, increasing efficiency and greatly reducing the risk of injury to workers in the fields. Livestock can be tracked and

monitored with digital collars and implants, improving the health and quality of life of herds and flocks, and reducing the number of animals lost to accident or disease.

Industrial equipment, like these robots, can communicate with central controllers and each other. This streamlines production cycles, allowing more efficient use of materials, faster switchovers to new product lines, less waste and pollution.

The IoT is also all around you where you work, play, and shop. In restaurant and stores, inventory is managed automatically, helping rotate stocks and automatically re-ordering items when they're needed.

Doctors and nurses not only can monitor patients remotely, but adjust the administration of medications. Robotic pharmacies, like the one picture, instantly respond to changes in treatment plans.

Remote and robotic surgery has become commonplace, bringing advanced life-enhancing and life-saving techniques to more and more comers of the world.

As individuals, we're surrounded by the IoT. If you» buy a new car today, it will more than likely send you a text message when it's due for an oil change, and if on a cold Washington winter morning you want to start it from the comfort of your warm kitchen. . .well, there's an app for that.

The "black box" under the hood tracks speed, acceleration, and other variables. You can share that information with your insurance company to adjust your premiums, and law enforcement can use it to reconstruct events leading up to accidents.

Your "wired" home interacts with the "smart" grid to maximize efficiency and lower your bills. At times of peak demand, smart LED bulbs dim imperceptibly, and your air conditioner fan slows down.

You don't notice the changes, but the sum total of these tiny adjustments across thousands of homes, businesses, and factories mean fewer new power plants are needed.

During the winter, your furnace is notified when a cold front is approaching and reacts by pre-heating a stack of thermal bricks to make it easier—and cheaper—to keep your home toasty when the mercury plunges.

The same RF ID tags that help stores manage inventory can guide visually impaired shoppers to the items they need, increasing their independence.

There can be no doubt that this ever-increasing web of connectivity has had great benefits.
Our power grid is more efficient.

Our cars and homes use less energy and produce less pollution, and are more convenient to maintain.

Networked medical devices mean fewer treatment errors, saving millions of dollars and thousands of lives each year. Overall, the global economic value of the IoT are estimated to amount to nearly $2 trillion. But, as with every technology, the blessings don't come unalloyed.

Networked devices can be hacked, and networked devices manufactured by companies more accustomed to manufacturing light bulbs and hot-water heaters have proven to be especially

susceptible. Starting in the early twenty-teens, security experts demonstrated how various IoT devices could be compromised, including:

> … activity-tracking bands. . .
> … automobile computers. . .
> ...household appliances...
> ...cameras, microphones and other sensors in smart phones
> ...cardiac pacemakers, insulin pumps, and other medical implants
> ...even “smart” LED light bulbs

In many cases, exploits were demonstrated in industry and academic settings to motivate improvements in security. But, by 2018, hacks began to show up in the wild with sufficient frequency to spark public concern.

The three most notorious examples were. ..

First, the “ShagBit " hack. An attack by a sophisticated hacker group compromised millions of subscriber records on a popular fitness-tracking service.

> The group also hacked into several UK mobile phone providers, accessing the identity data on several million accounts along with the microphone and GPS hardware on their phones.
>
> Both the relative ineffectiveness of public agencies in handling the problem and revelations about the techniques investigators used to track the criminals—which themselves played fast and loose with net security and personal privacy——continue to reverberate.

Second came a rash of burglaries across the American Midwest tied to a vulnerability in a “smart” garage-door opener used by a major regional home developer. Because the crimes were local in nature, it took several months for the pattern to become evident and measures to be taken to correct the problem. Even today, three years after the exploit was first identified, unpatched units are still being victimized.

Finally, we had the largest automotive recall ever—over 50 million cars and light trucks sold by six U.S., German, Korean, and Japanese brands. All were assembled in North America and included an engine-control subsystem manufactured by a supplier in Illinois.

> In a dramatic “white hat” demonstration, a vehicle from each manufacturer was destroyed when it was remotely commanded to accelerate in an uncontrolled manner despite the brakes being fully applied and the ignition switch turned off once the acceleration began.

Less visible has been a recent trend of low-level crime directed against small enterprises. A sort of cyber “protection racket”, anonymous hackers threaten to sabotage basic business systems, like...

> ...refrigerators at restaurants and markets...
> ...security and alarm systems at shops...
> ...delivery and service vehicles...

...unless the owners make small, regular, online payments. Local law enforcement agencies have typically proven inadequate to the task of dealing with these cybercriminals, while state and federal authorities prove difficult to interest in a problem whose scale is hard to ascertain...

...though some estimates put the costs at more than a billion dollars annually.

Two weeks ago, however, these rackets broke into the headlines with the tragic deaths of two teenagers at a retail store in Tennessee.

A group of cyber-extortionists had been extracting payments from merchants in a small Tennessee town. When law enforcement was unable to offer much assistance, the owners banded together to stand up to the criminals.

Their refusal to pay was met by a series of escalating retaliations, starting with repeated triggering of burglar and fire alarms at various stores at all hours of the day and night.

One merchant, an ice-cream parlor, had its main freezer shut down overnight, resulting in the loss of several thousand dollars of inventory and a full day's business.

When the owners still refused to pay up, the perpetrators escalated to more drastic action. In an apparent effort to make an example of one business, they accessed its networked-enabled gas furnace in the basement after hours, creating a gas leak, and then igniting it by firing up the unit ’s pilot light. The subsequent explosion and blaze quickly consumed the building.

Unknown to them, or anyone else, two teenage employees of the store were still inside a second-floor stockroom, apparently for an after-hours tryst. Too far away, or too preoccupied, to notice the gas leak, they were killed in the conflagration.

Media coverage has been extensive, and grew increasingly angry as the storeowners recounted their frustrated attempts to get help from law enforcement.

The local sheriff turned out to be a down-home, charismatic figure, and his recounting of Federal officials indifference to his requests for assistance made him a media darling. His testimony before both House and Senate hearings called to investigate the tragedy made him a national celebrity, and the uproar forced the resignation of the director of the FBI ’s cybercrime division, and of not incidentally, one of my predecessors.

Three months ago, Paramount Pictures announced plans for a biopic on the life of [nb: real person] North Korean defector Song Ee Han——her heroic struggle to feed her family during the famine of the 1990s, her brutal treatment at the hands of the North Korean regime, and eventual escape to the United States. North Korean media reacted furiously, demanding cancellation of the “slanderous” project, and warning of “severe consequences” should it proceed.

Last week:

- the movie’s director’s car went out of control on a highway outside of San Francisco; from her hospital bed, she reported that the vehicle suddenly refused to respond to steering or brake inputs, and ran off the road into an embankment. Both she and her daughter, who was a passenger, were badly injured in the collision.

- Two days later, the producer's hospitalized mother nearly dies when her computerized IV machine inexplicably administers a 40-fold overdose of a powerful antibiotic.

Not surprisingly, these incidents have provoked a storm of attention in mainstream and social media. Paramount has announced that they're putting production on "hiatus", pending the director's recovery.

All of these events have led some to question whether the benefits of ever-increasing connectivity are worth the risk.

Questions of liability and regulatory responsibility are also coming to the fore, as insurers and government agencies struggle to cope with this brave new world.

So, these are the headline events that we've all been reading about. Some of them, frankly, contributed to this Administration's victory last November. We must address this criminal exploitation that threatens to undermine all of the benefits gained from the IoT but they're not principally why you're here.

You're here because of the part of the iceberg that's below the waterline. The problem goes beyond criminality, and is becoming a national security concern.

Hidden so far from public view but even more worrisome than these high-profile incidents are multiple reports we've received concerning cooperation between military intelligence and criminal hacking networks in Russia.

We've long been aware that, along with other potential adversaries, Russian intelligence has been scouring the Internet to collect personal information on U.S. military service personnel and government officials. While the focus has mainly been on more senior officers, recent reporting indicates that efforts have expanded and become much more wide reaching.

We have now received solid indications that Russia has developed multiple IoT exploits that they intend to deploy against the families of U.S service members in the event of a crisis with the West. Influential advisors to the Russian president are urging him to use them to blackmail our Administration into relaxing sanctions and backing away from defense commitments to certain Eastern European NATO members.

We have sufficient evidence to convince us that these threats are entirely credible and could put at risk the finances, reputations, and even the lives of thousands of U.S. citizens in a matter of hours to days if executed in full.

Ultimately, the consequences could be of the magnitude of another 9/11. Maybe larger.

The intelligence community has advised the President that Russia could maintain plausible deniability of responsibility unless the United States were willing to compromise vital intelligence sources and methods that would take years to reconstruct and likely cost the lives of many valuable assets, including those of friends and allies.

We've managed to keep this secret so far, but in combination with the public mishaps of recent days and weeks, it's clear that the "internet of things" is starting to show its dark side, and we have to figure out how to manage it. That's why you're here, and why the President needs your help.

Our internet of things—which has made our lives easier, our economy more productive, and our environment cleaner—is biting us back. The President wants to know what we're going to do about that.

Do you have any questions? If not, here's what we're going to do today….

- Break into small groups (5-7 students each)

- Consider the challenges and work up a recommended "Whole of Nation" plan to address them.

    - You will be given about 30-40 minutes to discuss this among the members of your workgroup … including the time needed to form your recommendations.

- Use the following two sheets to consider the issue, elements of solution, and to frame your recommendation

- Each group will nominate a spokesperson to make a 10 minute presentation back to the assembled class on your recommended solution

Student Workgroup – Guide for Reporting Back to the NSC

Problem definition – What's the cybersecurity Challenge here?

- Freeze adversaries in the short term, deter them in the long-term
- Protect our values (privacy, freedom of access, etc)
- Set future conditions

Who are the Stakeholders?

What Instruments of Power should be employed, when and by whom?

Recommendation(s) – *considering <u>more</u> than the use of cyber power*:

Student Workgroup – Worksheet

What is the fundamental Cyber Security Challenge here? Who are the stakeholders?

Remember the lens(es) through which to view the problem:

- Denial of Benefits
- Imposition of Cost
- Cultural Values
- User Benefits
- Technological Innovation
- Economic Vitality

What are [some] elements of a solution? Near-term? Long-term?

- Messaging
- Diplomatic
- Financial
- Criminal
- Military
- Intelligence
- Private sector
- International

What are the impediments?